Citrix CWAAP GraphQL API Schema Reference

GraphQL is a query language for APIs and a runtime for fulfilling those queries with your existing data. GraphQL provides a complete and understandable description of the data in your API, gives clients the power to ask for exactly what they need and nothing more, makes it easier to evolve APIs over time, and enables powerful developer tools.

References

GraphQL

Apollo Federation

Version: 1.0.2

Authentication

Use the `Client ID` and `Client Secret` to request a token (JWT). This will be used as a Bearer token to make authenticated requests to the GraphQL API.

```
curl -L -X POST 'https:/auth.appsecportal.com/oauth/token' \
-H 'Content-Type: application/json' \
-d '{
    "client_id": "{*CLIENT_ID_VALUE*}",
    "client_secret": "{*CLIENT_SECRET_VALUE*}",
    "audience": "https://api.appsecportal.com/",
    "grant_type": "client_credentials"
}'
```

Formatting your API Request

The GraphQL API has a single endpoint.

Requires:

- Bearer Token *(see Authentication)*
- Query object

```
curl -L -X POST 'https://api.appsecportal.com/query' \
-H 'Authorization: Bearer <TOKEN>' \
-H 'Content-Type: application/json' \
--data-raw '<QUERY>'
```

Query Examples

Reseller's Data

Events

Mitigations

Mitigations Countermeasures

Violation Logs

Proxies

Policies

Audit Logs

Name	Request Example
Reseller's Data	Filter by Customer

```
{
 company(filter:{dName: "DNAME"}){
   dName
 }
}
```

Reseller's Data

```
{
  company {
    id
    dName
    allCustomers(perPage: 50) {
      results {
        dName
        enabled
        proxies {
          ip {
            string
          }
        }
        allCustomers {
          results {
            dName
            enabled
            proxies{
              ip {
                string
              }
            }
          }
```

Events

```
        }
      }
    }
  }
}
```

```
{
  company {
    dName
    events(from:"2020-09-30T00:58:57Z") {
      results {
        id
        start
        end
        destinationIPs
      }
    }
  }
}
```

Mitigations

```
{
  company {
    events(from: "2020-09-30T00:58:57Z") {
      results {
        id
        start
        end
        destinationIPs
        mitigations {
          results {
            id
            start
            end
            __typename
          }
        }
      }
    }
  }
}
```

Mitigation Countermeasures

```
{
  company {
    events(from: "2020-09-30T00:58:57Z") {
      results {
        id
        start
        end
        destinationIPs
        mitigations {
          results {
            id
```

```
            start
            end
          ... on DDOSMitigation {
            historicalDestinationIPs
            DDOSMitigation: countermeasures {
              name
              trafficData {
                field
                metric
                ... on TrafficData {
                  value
                }
              }
            }
          }
          ... on WAFMitigation {
            destinationIPs
            WAFMitigation: countermeasures {
              name
              violationsDetails {
                metric
                value
              }
            }
          }
          ... on BotMitigation {
            destinationIPs
            BotMitigation: countermeasures {
              name
              violationsDetails {
                metric
                value
              }
            }
          }
        }
      }
    }
  }
}
```

Violation Logs

```
{
  company {
    wafAnalytics(
      from: "2021-11-09T21:42:23Z"
      groupBy: {
          field: DOMAIN,
          direction: DESCENDING,
          timeInterval: {
```

```
              interval: 30,
              unit: DAY
              }
        }
      sortBy: {
          dimension: DOMAIN,
          direction: DESCENDING
          }
    ) {
      groups {
        key
        count
        __typename
      }
    }
  }
}
```

Proxies

```
{
  company {
    proxies {
      id
      name
      createdAt
      updatedAt
      deletedAt
      ip{
        string
      }
      ipVersion
      vServers{
        port
        protocol
        loadBalanceMethod
        certificateBindings{
          certificateID
          sni
        }
        applicationServices{
          port
          protocol
          origin
        }
      }
    }
  }
}
```

Polices

```
{
              company {
                id
```

```
                proxies {
                  id
                  name
                  ip {
                    string
                    __typename
                  }
                  policies {
                    id
                    __typename
                  }
                  vServers {
                    port
                    protocol
                    applicationServices {
                      ...ApplicationServicesFields
                      __typename
                    }
                    __typename
                  }
                  __typename
                }
                __typename
              }
            }
```

```
            fragment ApplicationServicesFields on
ApplicationService {
              port
              protocol
              origin
              __typename
            }
```

Audit Logs

```
{
  company {
    auditLogTransactions(
        from: "2021-01-01T00:00:00Z"
        to: "2021-11-20T00:00:00Z"
        sortBy: [{ dimension: TIMESTAMP, direction:
DESCENDING }]
        page: 1
        perPage: 20
    )
    {
        results
        {
          id
          description
          traceID
```

```
            timestamp
            userID
            applicationID
            apiClientID
            messages
            status
            operations
            {
              id timestamp action status
              callerID callerType serviceID resourceID
resourceType
              company {dName}
              image {oldObj newObj}
              transaction {id userID status }
            }
          }
          pageInfo {totalItems pageNumber itemsPerPage}
      }
    }
}
```

Queries

baseBotSignatures

A paginated list of available bot signatures
Returns a `BotSignaturesWithPagination`

Name	Description
`filter` - `BotSignatureFilterInput`	Reduce the returned list to specific items
`page` - `UnsignedInt32!`	The page number to fetch results for. Default = `1`
`perPage` - `UnsignedInt32!`	The maximum number of results to show per page. Default = `1000`
`sortBy` - `[BotSignatureSortBy!]`	Sort the results

Example

Query

```
query baseBotSignatures($filter: BotSignatureFilterInput, $page: UnsignedInt32!,
$perPage: UnsignedInt32!, $sortBy: [BotSignatureSortBy!]) {
  baseBotSignatures(filter: $filter, page: $page, perPage: $perPage, sortBy:
$sortBy) {
    pageInfo {
```

```
      ...PaginationFragment
    }
    results {
      ...BaseBotSignatureFragment
    }
    version {
      ...BotSignaturesVersionFragment
    }
  }
}
```

Variables

```
{
  "filter": BotSignatureFilterInput,
  "page": 1,
  "perPage": 1000,
  "sortBy": [BotSignatureSortBy]
}
```

Response

```
{
  "data": {
    "baseBotSignatures": {
      "pageInfo": Pagination,
      "results": [BaseBotSignature],
      "version": BotSignaturesVersion
    }
  }
}
```

Queries

`baseWAFSignatures`

A paginated list of available WAF signatures
Returns an `BaseWAFSignaturesResponse`

Name	Description
`filter` - `WAFSignatureFilterInput`	Reduce the returned list to specific items
`page` - `UnsignedInt32!`	The page number to fetch results for. Default = `1`

`perPage` - `UnsignedInt32!`	The maximum number of results to show per page. Default = `1000`
`sortBy` - `[BaseWAFSignatureSortBy!]`	Sort the results

Example

Query

```
query baseWAFSignatures($filter: WAFSignatureFilterInput, $page: UnsignedInt32!,
$perPage: UnsignedInt32!, $sortBy: [BaseWAFSignatureSortBy!]) {
  baseWAFSignatures(filter: $filter, page: $page, perPage: $perPage, sortBy:
$sortBy) {
    lastCheckedTime
    signatures {
      ...BaseWAFSignaturesWithPaginationFragment
    }
  }
}
```

Variables

```
{
  "filter": WAFSignatureFilterInput,
  "page": 1,
  "perPage": 1000,
  "sortBy": [BaseWAFSignatureSortBy]
}
```

Response

```
{
  "data": {
    "baseWAFSignatures": {
      "lastCheckedTime": Time,
      "signatures": BaseWAFSignaturesWithPagination
    }
  }
}
```

Queries

`company`

Query a company's information

Returns a `Company`

Name	Description
`filter` - `CompanyFilterInput`	

Example

Query

```
query company($filter: CompanyFilterInput) {
  company(filter: $filter) {
    accountID
    accountInfo {
      ...AccountInfoFragment
    }
    accountManagerEmail
    accountManagerName
    allCustomers {
      ...CompaniesWithPaginationFragment
    }
    apiPackage {
      ...APIAccessFragment
    }
    appDataAnalytics {
      ...AppDataAnalyticsResponseFragment
    }
    auditLogTransactions {
      ...AuditLogTransactionsWithPaginationFragment
    }
    bgpPackage {
      ...BGPPackageFragment
    }
    botAnalytics {
      ...BotAnalyticsResponseFragment
    }
    certificates {
      ...CertificateFragment
    }
    configurationChanges {
      ...ConfigurationChangeFragment
    }
    corporateDomain
    corporateName
    createdAt
    customers {
```

```
      ...CompanyFragment
    }
    dName
    deleted
    destinationIPs
    details {
      ...CompanyDetailsFragment
    }
    detectionAndAlertingPackage {
      ...DetectionAndAlertingPackageFragment
    }
    enabled
    event {
      ...EventFragment
    }
    events {
      ...EventsWithPaginationFragment
    }
    executiveReports {
      ...ExecutiveReportsWithPaginationFragment
    }
    formerlyKnownAs
    id
    isReseller
    legacyProxies {
      ...LegacyProxyFragment
    }
    managedObjects {
      ...ManagedObjectFragment
    }
    managementDomain
    mfaPackage {
      ...MFAPackageFragment
    }
    oneTimeExecutiveReportConfigurations {
      ...OneTimeExecutiveReportConfigurationsWithPaginationFragment
    }
    policies {
      ...PolicyFragment
    }
    proxies {
      ...ProxyFragment
    }
    proxyPackage {
      ...ProxyPackageFragment
    }
```

```
    recurringExecutiveReportConfigurations {
      ...RecurringExecutiveReportConfigurationsWithPaginationFragment
    }
    resellBGP
    resellBot
    resellDetectionAndAlerting
    resellProxy
    resellWAF
    reseller {
      ...CompanyFragment
    }
    responderAnalytics {
      ...ResponderAnalyticsResponseFragment
    }
    serviceProvider
    shortname
    technicalEmail
    technicalFirstName
    technicalJobTitle
    technicalLastName
    technicalMobile
    technicalPhone
    tunnels {
      ...TunnelFragment
    }
    updatedAt
    users {
      ...UsersWithPaginationFragment
    }
    wafAnalytics {
      ...WAFAnalyticsResponseFragment
    }
    whiteLabel {
      ...WhiteLabelFragment
    }
  }
}
```

Variables

```
{"filter": CompanyFilterInput}
```

Response

```
{
  "data": {
    "company": {
```

```
      "accountID": "xyz789",
      "accountInfo": AccountInfo,
      "accountManagerEmail": "xyz789",
      "accountManagerName": "xyz789",
      "allCustomers": CompaniesWithPagination,
      "apiPackage": APIAccess,
      "appDataAnalytics": [AppDataAnalyticsResponse],
      "auditLogTransactions": AuditLogTransactionsWithPagination,
      "bgpPackage": BGPPackage,
      "botAnalytics": BotAnalyticsResponse,
      "certificates": [Certificate],
      "configurationChanges": [ConfigurationChange],
      "corporateDomain": "abc123",
      "corporateName": "abc123",
      "createdAt": Time,
      "customers": [Company],
      "dName": "xyz789",
      "deleted": true,
      "destinationIPs": [CIDR],
      "details": CompanyDetails,
      "detectionAndAlertingPackage": DetectionAndAlertingPackage,
      "enabled": false,
      "event": Event,
      "events": EventsWithPagination,
      "executiveReports": ExecutiveReportsWithPagination,
      "formerlyKnownAs": "xyz789",
      "id": "xyz789",
      "isReseller": false,
      "legacyProxies": [LegacyProxy],
      "managedObjects": [ManagedObject],
      "managementDomain": "xyz789",
      "mfaPackage": MFAPackage,
      "oneTimeExecutiveReportConfigurations":
OneTimeExecutiveReportConfigurationsWithPagination,
      "policies": [Policy],
      "proxies": [Proxy],
      "proxyPackage": ProxyPackage,
      "recurringExecutiveReportConfigurations":
RecurringExecutiveReportConfigurationsWithPagination,
      "resellBGP": false,
      "resellBot": false,
      "resellDetectionAndAlerting": true,
      "resellProxy": true,
      "resellWAF": true,
      "reseller": Company,
      "responderAnalytics": ResponderAnalyticsResponse,
```

```
      "serviceProvider": "xyz789",
      "shortname": "xyz789",
      "technicalEmail": "abc123",
      "technicalFirstName": "xyz789",
      "technicalJobTitle": "xyz789",
      "technicalLastName": "abc123",
      "technicalMobile": "xyz789",
      "technicalPhone": "abc123",
      "tunnels": [Tunnel],
      "updatedAt": Time,
      "users": UsersWithPagination,
      "wafAnalytics": WAFAnalyticsResponse,
      "whiteLabel": WhiteLabel
    }
  }
}
```

Queries

`configurationChangesLock`

Get status of config changes lock

Returns a `ConfigurationChangesLockResponse`

Example

Query

```
query configurationChangesLock {
  configurationChangesLock {
    status
    timestamp
  }
}
```

Response

```
{
  "data": {
    "configurationChangesLock": {
      "status": ConfigurationChangesLockStatus,
      "timestamp": Time
    }
  }
}
```

Queries

`ipInfo`

Get IP reputation data for a given IP address
Returns an `IPInfo`

Name	Description
`address` - `IPAddressInput!`	

Example

Query

```
query ipInfo($address: IPAddressInput!) {
  ipInfo(address: $address) {
    address {
      ...IPAddressFragment
    }
    location {
      ...GeoLocationFragment
    }
    network {
      ...IPNetworkFragment
    }
    reputation {
      ...IPReputationFragment
    }
  }
}
```

Variables

```
{"address": IPAddressInput}
```

Response

```
{
  "data": {
    "ipInfo": {
      "address": IPAddress,
      "location": GeoLocation,
      "network": IPNetwork,
      "reputation": IPReputation
    }
  }
```

```
}
```

Queries

`isCustomer`

Query whether a specified company is a customer of the specified reseller
Returns a `Boolean!`

Name	Description
`customer` - `String!`	
`reseller` - `String!`	

Example

Query

```
query isCustomer($customer: String!, $reseller: String!) {
  isCustomer(customer: $customer, reseller: $reseller)
}
```

Variables

```
{"customer": "xyz789", "reseller": "abc123"}
```

Response

```
{"data": {"isCustomer": true}}
```

Queries

`networkNodes`

Returns `[NetworkNode!]`

Name	Description
`filter` - `NetworkNodeFilterInput`	

Example

Query

```
query networkNodes($filter: NetworkNodeFilterInput) {
  networkNodes(filter: $filter) {
    description
    iataCode
  }
}
```

Variables

```
{"filter": NetworkNodeFilterInput}
```

Response

```
{"data": {"networkNodes": [{"description": "xyz789", "iataCode": "xyz789"}]}}
```

Queries

`policyChanges`

A list of all policies bound to a proxy changed from UTC time (since) to UTC time (asOf)
Returns `[Company!]`

Name	Description
`asOf` - `Time`	
`since` - `Time!`	

Example

Query

```
query policyChanges($asOf: Time, $since: Time!) {
  policyChanges(asOf: $asOf, since: $since) {
    accountID
    accountInfo {
      ...AccountInfoFragment
    }
    accountManagerEmail
    accountManagerName
    allCustomers {
      ...CompaniesWithPaginationFragment
    }
    apiPackage {
      ...APIAccessFragment
    }
```

```
    appDataAnalytics {
      ...AppDataAnalyticsResponseFragment
    }
    auditLogTransactions {
      ...AuditLogTransactionsWithPaginationFragment
    }
    bgpPackage {
      ...BGPPackageFragment
    }
    botAnalytics {
      ...BotAnalyticsResponseFragment
    }
    certificates {
      ...CertificateFragment
    }
    configurationChanges {
      ...ConfigurationChangeFragment
    }
    corporateDomain
    corporateName
    createdAt
    customers {
      ...CompanyFragment
    }
    dName
    deleted
    destinationIPs
    details {
      ...CompanyDetailsFragment
    }
    detectionAndAlertingPackage {
      ...DetectionAndAlertingPackageFragment
    }
    enabled
    event {
      ...EventFragment
    }
    events {
      ...EventsWithPaginationFragment
    }
    executiveReports {
      ...ExecutiveReportsWithPaginationFragment
    }
    formerlyKnownAs
    id
    isReseller
```

```
    legacyProxies {
      ...LegacyProxyFragment
    }
    managedObjects {
      ...ManagedObjectFragment
    }
    managementDomain
    mfaPackage {
      ...MFAPackageFragment
    }
    oneTimeExecutiveReportConfigurations {
      ...OneTimeExecutiveReportConfigurationsWithPaginationFragment
    }
    policies {
      ...PolicyFragment
    }
    proxies {
      ...ProxyFragment
    }
    proxyPackage {
      ...ProxyPackageFragment
    }
    recurringExecutiveReportConfigurations {
      ...RecurringExecutiveReportConfigurationsWithPaginationFragment
    }
    resellBGP
    resellBot
    resellDetectionAndAlerting
    resellProxy
    resellWAF
    reseller {
      ...CompanyFragment
    }
    responderAnalytics {
      ...ResponderAnalyticsResponseFragment
    }
    serviceProvider
    shortname
    technicalEmail
    technicalFirstName
    technicalJobTitle
    technicalLastName
    technicalMobile
    technicalPhone
    tunnels {
      ...TunnelFragment
```

```
    }
    updatedAt
    users {
      ...UsersWithPaginationFragment
    }
    wafAnalytics {
      ...WAFAnalyticsResponseFragment
    }
    whiteLabel {
      ...WhiteLabelFragment
    }
  }
}
```

Variables

```
{"asOf": Time, "since": Time}
```

Response

```
{
  "data": {
    "policyChanges": [
      {
        "accountID": "abc123",
        "accountInfo": AccountInfo,
        "accountManagerEmail": "xyz789",
        "accountManagerName": "abc123",
        "allCustomers": CompaniesWithPagination,
        "apiPackage": APIAccess,
        "appDataAnalytics": [AppDataAnalyticsResponse],
        "auditLogTransactions": AuditLogTransactionsWithPagination,
        "bgpPackage": BGPPackage,
        "botAnalytics": BotAnalyticsResponse,
        "certificates": [Certificate],
        "configurationChanges": [ConfigurationChange],
        "corporateDomain": "xyz789",
        "corporateName": "xyz789",
        "createdAt": Time,
        "customers": [Company],
        "dName": "xyz789",
        "deleted": true,
        "destinationIPs": [CIDR],
        "details": CompanyDetails,
        "detectionAndAlertingPackage": DetectionAndAlertingPackage,
        "enabled": false,
        "event": Event,
```

```
        "events": EventsWithPagination,
        "executiveReports": ExecutiveReportsWithPagination,
        "formerlyKnownAs": "abc123",
        "id": "abc123",
        "isReseller": false,
        "legacyProxies": [LegacyProxy],
        "managedObjects": [ManagedObject],
        "managementDomain": "xyz789",
        "mfaPackage": MFAPackage,
        "oneTimeExecutiveReportConfigurations":
OneTimeExecutiveReportConfigurationsWithPagination,
        "policies": [Policy],
        "proxies": [Proxy],
        "proxyPackage": ProxyPackage,
        "recurringExecutiveReportConfigurations":
RecurringExecutiveReportConfigurationsWithPagination,
        "resellBGP": false,
        "resellBot": false,
        "resellDetectionAndAlerting": true,
        "resellProxy": false,
        "resellWAF": true,
        "reseller": Company,
        "responderAnalytics": ResponderAnalyticsResponse,
        "serviceProvider": "xyz789",
        "shortname": "xyz789",
        "technicalEmail": "xyz789",
        "technicalFirstName": "xyz789",
        "technicalJobTitle": "abc123",
        "technicalLastName": "abc123",
        "technicalMobile": "abc123",
        "technicalPhone": "xyz789",
        "tunnels": [Tunnel],
        "updatedAt": Time,
        "users": UsersWithPagination,
        "wafAnalytics": WAFAnalyticsResponse,
        "whiteLabel": WhiteLabel
      }
    ]
  }
}
```


Queries

---

proxyChanges

Get a list of all proxies changed from UTC time ($since) to UTC time ($asOf)

Returns `[Company!]`

Name	Description
`asOf` - `Time`	
`since` - `Time!`	

Example

Query

```
query proxyChanges($asOf: Time, $since: Time!) {
  proxyChanges(asOf: $asOf, since: $since) {
    accountID
    accountInfo {
      ...AccountInfoFragment
    }
    accountManagerEmail
    accountManagerName
    allCustomers {
      ...CompaniesWithPaginationFragment
    }
    apiPackage {
      ...APIAccessFragment
    }
    appDataAnalytics {
      ...AppDataAnalyticsResponseFragment
    }
    auditLogTransactions {
      ...AuditLogTransactionsWithPaginationFragment
    }
    bgpPackage {
      ...BGPPackageFragment
    }
    botAnalytics {
      ...BotAnalyticsResponseFragment
    }
    certificates {
      ...CertificateFragment
    }
    configurationChanges {
      ...ConfigurationChangeFragment
    }
    corporateDomain
    corporateName
    createdAt
```

```
    customers {
      ...CompanyFragment
    }
    dName
    deleted
    destinationIPs
    details {
      ...CompanyDetailsFragment
    }
    detectionAndAlertingPackage {
      ...DetectionAndAlertingPackageFragment
    }
    enabled
    event {
      ...EventFragment
    }
    events {
      ...EventsWithPaginationFragment
    }
    executiveReports {
      ...ExecutiveReportsWithPaginationFragment
    }
    formerlyKnownAs
    id
    isReseller
    legacyProxies {
      ...LegacyProxyFragment
    }
    managedObjects {
      ...ManagedObjectFragment
    }
    managementDomain
    mfaPackage {
      ...MFAPackageFragment
    }
    oneTimeExecutiveReportConfigurations {
      ...OneTimeExecutiveReportConfigurationsWithPaginationFragment
    }
    policies {
      ...PolicyFragment
    }
    proxies {
      ...ProxyFragment
    }
    proxyPackage {
      ...ProxyPackageFragment
```

```
    }
    recurringExecutiveReportConfigurations {
      ...RecurringExecutiveReportConfigurationsWithPaginationFragment
    }
    resellBGP
    resellBot
    resellDetectionAndAlerting
    resellProxy
    resellWAF
    reseller {
      ...CompanyFragment
    }
    responderAnalytics {
      ...ResponderAnalyticsResponseFragment
    }
    serviceProvider
    shortname
    technicalEmail
    technicalFirstName
    technicalJobTitle
    technicalLastName
    technicalMobile
    technicalPhone
    tunnels {
      ...TunnelFragment
    }
    updatedAt
    users {
      ...UsersWithPaginationFragment
    }
    wafAnalytics {
      ...WAFAnalyticsResponseFragment
    }
    whiteLabel {
      ...WhiteLabelFragment
    }
  }
}
```

Variables

```
{"asOf": Time, "since": Time}
```

Response

```
{
  "data": {
```

```
    "proxyChanges": [
      {
        "accountID": "abc123",
        "accountInfo": AccountInfo,
        "accountManagerEmail": "abc123",
        "accountManagerName": "abc123",
        "allCustomers": CompaniesWithPagination,
        "apiPackage": APIAccess,
        "appDataAnalytics": [AppDataAnalyticsResponse],
        "auditLogTransactions": AuditLogTransactionsWithPagination,
        "bgpPackage": BGPPackage,
        "botAnalytics": BotAnalyticsResponse,
        "certificates": [Certificate],
        "configurationChanges": [ConfigurationChange],
        "corporateDomain": "xyz789",
        "corporateName": "xyz789",
        "createdAt": Time,
        "customers": [Company],
        "dName": "abc123",
        "deleted": true,
        "destinationIPs": [CIDR],
        "details": CompanyDetails,
        "detectionAndAlertingPackage": DetectionAndAlertingPackage,
        "enabled": true,
        "event": Event,
        "events": EventsWithPagination,
        "executiveReports": ExecutiveReportsWithPagination,
        "formerlyKnownAs": "abc123",
        "id": "xyz789",
        "isReseller": false,
        "legacyProxies": [LegacyProxy],
        "managedObjects": [ManagedObject],
        "managementDomain": "abc123",
        "mfaPackage": MFAPackage,
        "oneTimeExecutiveReportConfigurations":
OneTimeExecutiveReportConfigurationsWithPagination,
        "policies": [Policy],
        "proxies": [Proxy],
        "proxyPackage": ProxyPackage,
        "recurringExecutiveReportConfigurations":
RecurringExecutiveReportConfigurationsWithPagination,
        "resellBGP": false,
        "resellBot": false,
        "resellDetectionAndAlerting": true,
        "resellProxy": true,
        "resellWAF": false,
```

```
        "reseller": Company,
        "responderAnalytics": ResponderAnalyticsResponse,
        "serviceProvider": "abc123",
        "shortname": "xyz789",
        "technicalEmail": "abc123",
        "technicalFirstName": "abc123",
        "technicalJobTitle": "xyz789",
        "technicalLastName": "abc123",
        "technicalMobile": "xyz789",
        "technicalPhone": "xyz789",
        "tunnels": [Tunnel],
        "updatedAt": Time,
        "users": UsersWithPagination,
        "wafAnalytics": WAFAnalyticsResponse,
        "whiteLabel": WhiteLabel
      }
    ]
  }
}
```

Queries

`user`

Query a user's information
Returns a `User`

Name	Description
`filter` - `UserFilterInput`	

Example

Query

```
query user($filter: UserFilterInput) {
  user(filter: $filter) {
    company {
      ...CompanyFragment
    }
    createdAt
    email
    enabled
    firstName
    id
```

```
    jobTitle
    lastLogin
    lastName
    mobile
    phone
    roles
    updatedAt
    userName
  }
}
```

Variables

```
{"filter": UserFilterInput}
```

Response

```
{
  "data": {
    "user": {
      "company": Company,
      "createdAt": Time,
      "email": "xyz789",
      "enabled": true,
      "firstName": "abc123",
      "id": "abc123",
      "jobTitle": "abc123",
      "lastLogin": Time,
      "lastName": "xyz789",
      "mobile": "abc123",
      "phone": "abc123",
      "roles": [UserRole],
      "updatedAt": Time,
      "userName": "xyz789"
    }
  }
}
```

Queries

`userLogs`

Query a user's Auth0 event logs
Returns `[UserLog!]`

Name	Description
`filter` - `UserLogsFilterInput!`	

Example

Query

```
query userLogs($filter: UserLogsFilterInput!) {
  userLogs(filter: $filter) {
    date
    description
    ip
    logID
    type
    userID
  }
}
```

Variables

```
{"filter": UserLogsFilterInput}
```

Response

```
{
  "data": {
    "userLogs": [
      {
        "date": Time,
        "description": "xyz789",
        "ip": "xyz789",
        "logID": "xyz789",
        "type": "abc123",
        "userID": "abc123"
      }
    ]
  }
}
```

Mutations

`createCertificate`

Returns a `CreateCertificateOutput!`

Name	Description
`input` - `CreateCertificateInput!`	

Example

Query

```
mutation createCertificate($input: CreateCertificateInput!) {
  createCertificate(input: $input) {
    certificate {
      ...CertificateFragment
    }
  }
}
```

Variables

```
{"input": CreateCertificateInput}
```

Response

```
{
  "data": {
    "createCertificate": {"certificate": Certificate}
  }
}
```

Mutations

`createOneTimeExecutiveReportConfiguration`

Creates a one time report generation configuration
Returns a `CreateOneTimeExecutiveReportConfigurationOutput!`

Name	Description
`input` - `CreateOneTimeExecutiveReportConfigurationInput`	

Example

Query

```
mutation createOneTimeExecutiveReportConfiguration($input:
CreateOneTimeExecutiveReportConfigurationInput) {
  createOneTimeExecutiveReportConfiguration(input: $input) {
```

```
    configuration {
      ...OneTimeExecutiveReportConfigurationFragment
    }
  }
}
```

Variables

```
{"input": CreateOneTimeExecutiveReportConfigurationInput}
```

Response

```
{
  "data": {
    "createOneTimeExecutiveReportConfiguration": {
      "configuration": OneTimeExecutiveReportConfiguration
    }
  }
}
```

Mutations

`createPolicy`

Create a policy
Returns a `CreatePolicyOutput`

Name	Description
`input` - `CreatePolicyInput!`	

Example

Query

```
mutation createPolicy($input: CreatePolicyInput!) {
  createPolicy(input: $input) {
    policy {
      ...PolicyFragment
    }
  }
}
```

Variables

```
{"input": CreatePolicyInput}
```

Response

```
{"data": {"createPolicy": {"policy": Policy}}}
```

Mutations

`createProxy`

Create a proxy
Returns a `CreateProxyOutput`

Name	Description
`input` - `CreateProxyInput!`	

Example

Query

```
mutation createProxy($input: CreateProxyInput!) {
  createProxy(input: $input) {
    proxy {
      ...ProxyFragment
    }
  }
}
```

Variables

```
{"input": CreateProxyInput}
```

Response

```
{"data": {"createProxy": {"proxy": Proxy}}}
```

Mutations

`createRecurringExecutiveReportConfiguration`

Creates a recurring report generation configuration
Returns a `CreateRecurringExecutiveReportConfigurationOutput!`

Name	Description
`input` - `CreateRecurringExecutiveReportConfigurationInput`	

Example

Query

```
mutation createRecurringExecutiveReportConfiguration($input:
CreateRecurringExecutiveReportConfigurationInput) {
  createRecurringExecutiveReportConfiguration(input: $input) {
    configuration {
      ...RecurringExecutiveReportConfigurationFragment
    }
  }
}
```

Variables

```
{
  "input": CreateRecurringExecutiveReportConfigurationInput
}
```

Response

```
{
  "data": {
    "createRecurringExecutiveReportConfiguration": {
      "configuration": RecurringExecutiveReportConfiguration
    }
  }
}
```

Mutations

`createUser`

Create a user

Returns a `CreateUserOutput`

Name	Description
`input` - `CreateUserInput!`	

Example

Query

```
mutation createUser($input: CreateUserInput!) {
  createUser(input: $input) {
```

```
    user {
      ...UserFragment
    }
  }
}
```

Variables

```
{"input": CreateUserInput}
```

Response

```
{"data": {"createUser": {"user": User}}}
```

Mutations

`deleteCertificate`

Returns a `DeleteCertificateOutput!`

Name	Description
`input` - `DeleteCertificateInput!`	

Example

Query

```
mutation deleteCertificate($input: DeleteCertificateInput!) {
  deleteCertificate(input: $input) {
    deletedCertificateID
  }
}
```

Variables

```
{"input": DeleteCertificateInput}
```

Response

```
{"data": {"deleteCertificate": {"deletedCertificateID": "abc123"}}}
```

Mutations

`deleteExecutiveReport`

Deletes a report based on name or ID. - check other delete mutations and follow pattern.
Add a date range for delete, so create new filter type with these params
Returns a `DeleteExecutiveReportOutput!`

Name	Description
`input` - `DeleteExecutiveReportInput`	

Example

Query

```
mutation deleteExecutiveReport($input: DeleteExecutiveReportInput) {
  deleteExecutiveReport(input: $input) {
    deletedExecutiveReportID
  }
}
```

Variables

```
{"input": DeleteExecutiveReportInput}
```

Response

```
{"data": {"deleteExecutiveReport": {"deletedExecutiveReportID": "xyz789"}}}
```

Mutations

`deleteOneTimeExecutiveReportConfiguration`

Deletes a one time executive report configuration
Returns a `DeleteOneTimeExecutiveReportConfigurationOutput!`

Name	Description
`input` - `DeleteOneTimeExecutiveReportConfigurationInput`	

Example

Query

```
mutation deleteOneTimeExecutiveReportConfiguration($input:
DeleteOneTimeExecutiveReportConfigurationInput) {
```

```
  deleteOneTimeExecutiveReportConfiguration(input: $input) {
    deletedOneTimeExecutiveReportConfigurationID
  }
}
```

Variables

```
{"input": DeleteOneTimeExecutiveReportConfigurationInput}
```

Response

```
{
  "data": {
    "deleteOneTimeExecutiveReportConfiguration": {
      "deletedOneTimeExecutiveReportConfigurationID": "abc123"
    }
  }
}
```

Mutations

`deletePolicy`

Delete a policy

Returns a `DeletePolicyOutput`

Name	Description
`input` - `DeletePolicyInput!`	

Example

Query

```
mutation deletePolicy($input: DeletePolicyInput!) {
  deletePolicy(input: $input) {
    deletedPolicyID
  }
}
```

Variables

```
{"input": DeletePolicyInput}
```

Response

```
{"data": {"deletePolicy": {"deletedPolicyID": "xyz789"}}}
```

Mutations

`deleteProxy`

Delete a proxy

Returns a `DeleteProxyOutput`

Name	Description
`input` - `DeleteProxyInput!`	

Example

Query

```
mutation deleteProxy($input: DeleteProxyInput!) {
  deleteProxy(input: $input) {
    deletedProxyID
    permanentlyDeleted
  }
}
```

Variables

```
{"input": DeleteProxyInput}
```

Response

```
{
  "data": {
    "deleteProxy": {"deletedProxyID": "xyz789", "permanentlyDeleted": true}
  }
}
```

Mutations

`deleteRecurringExecutiveReportConfiguration`

Deletes a recurring executive report configuration

Returns a `DeleteRecurringExecutiveReportConfigurationOutput!`

Name	Description

`input` - `DeleteRecurringExecutiveReportConfigurationInput`

Example

Query

```
mutation deleteRecurringExecutiveReportConfiguration($input:
DeleteRecurringExecutiveReportConfigurationInput) {
  deleteRecurringExecutiveReportConfiguration(input: $input) {
    deletedRecurringExecutiveReportConfigurationID
  }
}
```

Variables

```
{
  "input": DeleteRecurringExecutiveReportConfigurationInput
}
```

Response

```
{
  "data": {
    "deleteRecurringExecutiveReportConfiguration": {
      "deletedRecurringExecutiveReportConfigurationID": "xyz789"
    }
  }
}
```

Mutations

`deleteUser`

Delete a user

Returns a `DeleteUserOutput`

Name	Description
`input` - `DeleteUserInput!`	

Example

Query

```
mutation deleteUser($input: DeleteUserInput!) {
```

```
  deleteUser(input: $input) {
    deletedUserID
  }
}
```

Variables

```
{"input": DeleteUserInput}
```

Response

```
{"data": {"deleteUser": {"deletedUserID": "abc123"}}}
```

Mutations

`lockConfigurationChanges`

Returns a `ConfigurationChangesLock`

Example

Query

```
mutation lockConfigurationChanges {
  lockConfigurationChanges {
    createdAt
    ended
    id
    lockedBy
    started
    unlockedBy
    updatedAt
  }
}
```

Response

```
{
  "data": {
    "lockConfigurationChanges": {
      "createdAt": Time,
      "ended": Time,
      "id": "xyz789",
      "lockedBy": "abc123",
      "started": Time,
      "unlockedBy": "abc123",
```

```
      "updatedAt": Time
    }
  }
}
```

Mutations

sendUserActivationEmail

Send user activation email
Returns a `SendUserActivationEmailOutput`

Name	Description
`input` - `SendUserActivationEmailInput!`	

Example

Query

```
mutation sendUserActivationEmail($input: SendUserActivationEmailInput!) {
  sendUserActivationEmail(input: $input) {
    email
    id
  }
}
```

Variables

```
{"input": SendUserActivationEmailInput}
```

Response

```
{"data": {"sendUserActivationEmail": {"email": "abc123", "id": "abc123"}}}
```

Mutations

sendUserPasswordResetEmail

Send user reset password email
Returns a `SendUserPasswordResetEmailOutput`

Name	Description
`input` - `SendUserPasswordResetEmailInput!`	

Example

Query

```
mutation sendUserPasswordResetEmail($input: SendUserPasswordResetEmailInput!) {
  sendUserPasswordResetEmail(input: $input) {
    email
    id
  }
}
```

Variables

```
{"input": SendUserPasswordResetEmailInput}
```

Response

```
{"data": {"sendUserPasswordResetEmail": {"email": "abc123", "id": "xyz789"}}}
```

Mutations

`unlockConfigurationChanges`

Returns a `Boolean!`

Example

Query

```
mutation unlockConfigurationChanges {
  unlockConfigurationChanges
}
```

Response

```
{"data": {"unlockConfigurationChanges": false}}
```

Mutations

`updatePolicy`

Modify a policy

Returns an `UpdatePolicyOutput`

Name	Description

`input` - `UpdatePolicyInput!`

Example

Query

```
mutation updatePolicy($input: UpdatePolicyInput!) {
  updatePolicy(input: $input) {
    policy {
      ...PolicyFragment
    }
  }
}
```

Variables

```
{"input": UpdatePolicyInput}
```

Response

```
{"data": {"updatePolicy": {"policy": Policy}}}
```

Mutations

`updateProxy`

Modify a proxy
Returns an `UpdateProxyOutput`

Name	Description
`input` - `UpdateProxyInput!`	

Example

Query

```
mutation updateProxy($input: UpdateProxyInput!) {
  updateProxy(input: $input) {
    proxy {
      ...ProxyFragment
    }
  }
}
```

Variables

```
{"input": UpdateProxyInput}
```

Response

```
{"data": {"updateProxy": {"proxy": Proxy}}}
```

Mutations

updateRecurringExecutiveReportConfiguration

Updates a recurring report generation configuration
Returns an `UpdateRecurringExecutiveReportConfigurationOutput!`

Name	Description
`input` - `UpdateRecurringExecutiveReportConfigurationInput`	

Example

Query

```
mutation updateRecurringExecutiveReportConfiguration($input:
UpdateRecurringExecutiveReportConfigurationInput) {
  updateRecurringExecutiveReportConfiguration(input: $input) {
    configuration {
      ...RecurringExecutiveReportConfigurationFragment
    }
  }
}
```

Variables

```
{
  "input": UpdateRecurringExecutiveReportConfigurationInput
}
```

Response

```
{
  "data": {
    "updateRecurringExecutiveReportConfiguration": {
      "configuration": RecurringExecutiveReportConfiguration
    }
  }
```

```
}
```

Mutations

`updateUser`

Modify a user

Returns an `UpdateUserOutput`

Name	Description
`input` - `UpdateUserInput!`	

Example

Query

```
mutation updateUser($input: UpdateUserInput!) {
  updateUser(input: $input) {
    user {
      ...UserFragment
    }
  }
}
```

Variables

```
{"input": UpdateUserInput}
```

Response

```
{"data": {"updateUser": {"user": User}}}
```

Types

`APIAccess`

Specifies API Access configuration for company.

Field Name	Description
`enabled` - `Boolean!`	Whether API access is enabled for the Company.
`maxAPIClients` - `UnsignedInt32!`	Specifies the max number of API clients that can be configured for this company.

`openHybridEnabled` - `Boolean!`	Specifies if Open Hybrid access is enabled in portal for this company.

Example

```
{
  "enabled": true,
  "maxAPIClients": UnsignedInt32,
  "openHybridEnabled": false
}
```

Types

APIClient

Per-Company API Access settings.

Field Name	Description
`company` - `Company!`	Company Details.
`description` - `String!`	API Client Description.
`id` - `String!`	API Client ID.
`name` - `String!`	API Client Name.
`user` - `User`	User Details.

Example

```
{
  "company": Company,
  "description": "abc123",
  "id": "abc123",
  "name": "xyz789",
  "user": User
}
```

Types

AccountInfo

Contract-related information for a customer.

Field Name	Description

`accountExecutiveList` - `[Person!]`	List of Account Executives for customer.
`accountNumber` - `String!`	Account Number of customer.
`countryName` - `String`	Country customer is registered in.
`domain` - `String!`	Primary DNS name of customer.
`featureList` - `[Feature!]`	List of features purchased by customer.
`state` - `String`	State customer is registered in.

Example

```
{
  "accountExecutiveList": [Person],
  "accountNumber": "abc123",
  "countryName": "abc123",
  "domain": "abc123",
  "featureList": [Feature],
  "state": "xyz789"
}
```

Types

`ActivationStatus`

The status of a contract negotiated with customer.

Enum Value	Description
`ACTIVATED`	Indicates that the specified feature is purchased and activated for the company.
`EDIT_UNDER_REVIEW`	Indicates that the specified feature is under review but not purchased yet by the company.
`PENDING_CUSTOMER_SIGNATURE`	Indicates that the specified feature is pending signature by the company.
`SUBMISSION_UNDER_REVIEW`	Indicates that the specified feature is being reviewed post submission, for the company.

Types

`AppDataAggregateByField`

Allowed list of values for results to be grouped by.

Enum Value	Description
`METHOD`	
`VIP`	

Types

AppDataAggregateByInput

Define how the results should be grouped.

Input Field	Description
`field` - `AppDataAggregateByField!`	A value indicating how the results should be grouped.

Example

```
{"field": AppDataAggregateByField}
```

Types

AppDataAnalyticsResponse

Output application results.

Field Name	Description
`aggregateBy` - `AppDataAggregateByField!`	
`field` - `AppDataField!`	
`values` - `[AppDataValues!]`	

Example

```
{
  "aggregateBy": AppDataAggregateByField,
  "field": AppDataField,
  "values": [AppDataValues]
}
```

Types

AppDataField

Allowed list of request types for any given query.

Enum Value	Description
CONNECTIONS	
FAILURES	
INVALIDS	
VALIDS	

Types

AppDataFilterInput

Input required if extra criteria is needed to constrain the queried results.

Input Field	Description
vips - [IPAddressInput!]	If given, the queried results will only include those for the VIPs provided.

Example

```
{"vips": [IPAddressInput]}
```

Types

AppDataValues

Generic query type and result count.

Field Name	Description
count - UnsignedInt32!	
key - String!	

Example

```
{"count": UnsignedInt32, "key": "xyz789"}
```

Types

AppSecThreshold

An Application Security (AppSec) Threshold.

Field Name	Description
`bucketDurationSeconds` - `UnsignedInt32!`	Time period for max number of violations to occur before generating alerts.
`count` - `UnsignedInt32!`	Max number of violations allowed for this configuration before generating alerts.
`dimension` - `AppSecThresholdDimension!`	Dimension for this configuration from a valid list of dimensions.
`key` - `String!`	Key based on the Dimension. For instance, valid keys for REQUEST_BY_SOURCE_IP are , ||, */index.html*||., /index.html||153.18.34.1. Valid keys for for RESPONSE_BY_STATUS are *, /index.html||200.

Example

```
{
  "bucketDurationSeconds": UnsignedInt32,
  "count": UnsignedInt32,
  "dimension": AppSecThresholdDimension,
  "key": "abc123"
}
```

Types

AppSecThresholdDimension

Allowed values for a WAF Application Security (AppSec) Threshold Configuration Dimension.

Enum Value	Description
`BUFFER_OVERFLOW`	
`COMMAND`	

`CONTENT_TYPE`
`COOKIE`
`CSRF_TAG`
`DENY_URL`
`FIELD_CONSISTENCY`
`FIELD_FORMAT`
`INVALID_RFC`
`JSON_COMMAND`
`JSON_DENIAL_OF_SERVICE`
`JSON_SQL`
`JSON_XSS`
`MALFORMED_REQUEST_ERROR`
`POST_BODY_LIMIT`
`REQUEST_BY_ASN`
`REQUEST_BY_COUNTRY`
`REQUEST_BY_METHOD`
`REQUEST_BY_SOURCE_IP`
`REQUEST_BY_URI`
`REQUEST_BY_URI_SOURCE_IP`
`REQUEST_BY_USER_AGENT`
`RESPONSE_BY_COUNTRY`
`RESPONSE_BY_SOURCE_IP`
`RESPONSE_BY_STATUS`
`RESPONSE_BY_URI_STATUS`
`SIGNATURE_MATCH`
`SQL`
`XML_ERROR_NOT_WELL_FORMED`
`XML_ERROR_SOAP_FAULT`

`XML_SQL`
`XML_WSI`
`XML_XSS`
`XSS`

Types

AppSecThresholdDimensionInput

Allowed values for a policy level Application Security (AppSec) Threshold Configuration Dimension Input.

Enum Value	Description
`REQUEST_BY_ASN`	
`REQUEST_BY_COUNTRY`	
`REQUEST_BY_METHOD`	
`REQUEST_BY_SOURCE_IP`	
`REQUEST_BY_URI`	
`REQUEST_BY_URI_SOURCE_IP`	
`REQUEST_BY_USER_AGENT`	
`RESPONSE_BY_COUNTRY`	
`RESPONSE_BY_SOURCE_IP`	
`RESPONSE_BY_STATUS`	
`RESPONSE_BY_URI_STATUS`	

Types

AppSecThresholdInput

Specify a policy-level Application Security (AppSec) Threshold.

Input Field	Description
`bucketDurationSeconds` - `UnsignedInt32!` default = `60`	Time period within which the minimum number of violations

	need to occur in order to generate alerts. (allowed values : 60).
`count` - `UnsignedInt32!` default = `100`	Minimum number of violations for generating alerts.(allowed value range: 1-1000).
`dimension` - `AppSecThresholdDimensionInput!`	Dimension for this configuration from a valid list of dimensions.
`key` - `String!`	Key based on the Dimension. For instance, valid keys for REQUEST_BY_SOURCE_IP , ||, */index.html*||., /index.html||153.18.34.1, for RESPONSE_BY_STATUS *, /index.html||200.

Example

```
{
  "bucketDurationSeconds": 60,
  "count": 100,
  "dimension": AppSecThresholdDimensionInput,
  "key": "xyz789"
}
```

Types

AppViolationData

Represents the application violation data object.

Field Name	Description
`metric` - `AppViolationMetric!`	The metric for the data.
`value` - `Int!`	The value for the data.

Example

```
{"metric": AppViolationMetric, "value": 123}
```

Types

AppViolationMetric

One of the application violation metrics.

Enum Value	Description
`COUNT`	The count of application violations.

Types

`ApplicationService`

Application services that make up this virtual servers back end.

Field Name	Description
`monitor` - `Boolean!`	Whether or not to monitor this origin.
`origin` - `String!`	The back-end IP for this virtual server's origin.
`port` - `UnsignedInt16!`	The back-end port for this virtual server's origin.
`protocol` - `ProxyProtocol!`	Protocol type used for this virtual server's front and back ends.

Example

```
{
  "monitor": true,
  "origin": "abc123",
  "port": UnsignedInt16,
  "protocol": ProxyProtocol
}
```

Types

`ApplicationServiceInput`

Define a virtual server's back-end server.

Input Field	Description
`monitor` - `Boolean!` default = `true`	Whether or not to monitor this origin.
`origin` - `String!`	The back-end IP/hostname of this virtual server's origin.
`port` - `UnsignedInt16!`	The back-end port for this virtual server's origin.

`protocol` - `ProxyProtocol!`	Protocol type used for this virtual server's front and back ends.

Example

```
{
  "monitor": true,
  "origin": "abc123",
  "port": UnsignedInt16,
  "protocol": ProxyProtocol
}
```

Types

AuditLogAction

Allowed list of values indicating what type of action caused an audit log transaction to be written.

Enum Value	Description
`CHANGE_STATE`	
`CREATE`	
`DELETE`	
`UPDATE`	

Types

AuditLogImage

The before and after image of an object that was altered.

Field Name	Description
`newObj` - `RawJSON!`	A JSON string representing the image of an object before it was modified.
`oldObj` - `RawJSON`	A JSON string representing the image of an object after it was modified.

Example

```
{
  "newObj": RawJSON,
```

```
  "oldObj": RawJSON
}
```

Types

AuditLogOperation

A specific audit log operation. A given audit log transaction can contain many seperate operations.

Field Name	Description
`action` - `AuditLogAction!`	A value indicating what type of action caused an audit log transaction to be written.
`callerID` - `String`	Used internally to help identify what system component made a request to record the audit log operation.
`callerType` - `CallerType`	A string indicating what type of caller is recording an audit log transaction.
`company` - `Company!`	The owning company of the object represented in this audit log operation.
`description` - `String!`	A description describing the cause of the audit log operation.
`id` - `String!`	The identifier of an audit log operation.
`image` - `AuditLogImage`	A before and after image of an object that was altered.
`messages` - `[String!]`	A list of messages indicating useful information about the action that caused the audit log operation to be captured.
`resourceID` - `String!`	An ID value for internal reference indicating the key/ID value of the object being altered.
`resourceType` - `String!`	A string value for internal reference indicating what type of object was altered.
`serviceID` - `String!`	A string representing the name of the service that caused the audit log operation to be captured.
`status` - `AuditLogResultStatus!`	The result of the action that caused an audit log transaction to be written.

`timestamp` - `Time!`	The time reported by the caller for when the action occurred causing the audit log operation to be captured.
`transaction` - `AuditLogTransaction!`	Audit log transaction details associated with the operation.

Example


```
{
  "action": AuditLogAction,
  "callerID": "abc123",
  "callerType": CallerType,
  "company": Company,
  "description": "abc123",
  "id": "abc123",
  "image": AuditLogImage,
  "messages": ["abc123"],
  "resourceID": "xyz789",
  "resourceType": "abc123",
  "serviceID": "xyz789",
  "status": AuditLogResultStatus,
  "timestamp": Time,
  "transaction": AuditLogTransaction
}
```


Types

`AuditLogOperationDimension`

Allowed list of values indicating what field and order the results are to be sorted.

Enum Value	Description
`TIMESTAMP`	

Types

`AuditLogOperationFilterInput`

Input required if extra criteria is needed to constrain the queried results.

Input Field	Description
`action` - `AuditLogAction`	A value indicating what type of action caused an audit log transaction to be written.

`resourceID` - `String`	An ID value for internal reference indicating the key/ID value of the object being altered.
`resourceType` - `String`	A string value for internal reference indicating what type of object was altered.
`serviceID` - `String`	A string representing the name of the service that caused the audit log operation to be captured.
`status` - `AuditLogResultStatus`	The result of the action that caused an audit log transaction to be written.

Example

```
{
  "action": AuditLogAction,
  "resourceID": "xyz789",
  "resourceType": "abc123",
  "serviceID": "xyz789",
  "status": AuditLogResultStatus
}
```

Types

`AuditLogOperationSortBy`

Audit Log Operations log sorting.

Input Field	Description
`dimension` - `AuditLogOperationDimension!` default = `"TIMESTAMP"`	The dimension to sort by.
`direction` - `SortDirection!` default = `"DESCENDING"`	The direction to sort in.

Example

```
{
  "dimension": "TIMESTAMP",
  "direction": "DESCENDING"
}
```

Types

`AuditLogResultStatus`

Allowed list of values indicating the result of the action that caused an audit log transaction to be written.

Enum Value	Description
`ERROR`	
`INFO`	
`IN_PROGRESS`	
`SUCCESS`	

Types

`AuditLogTransaction`

A specific audit log transaction. A transaction can consist of many individual audit log operations.

Field Name	Description
`apiClient` - `APIClient`	API caller information.
`apiClientID` - `String`	Used internally to help identify what system user made a request to record the audit log operation.
`applicationID` - `String!`	Used internally to help identify what system component made a request to record the audit log operation.
`description` - `String!`	A description describing the cause of the audit log transaction.
`id` - `String!`	The identifier of an audit log transaction.
`messages` - `[String!]`	A list of messages indicating useful information about the action that caused the audit log operation to be captured.
`operations` - `[AuditLogOperation!]`	A list of audit log operations. A given audit log transaction may contain many individual operations.

Arguments
 	
`filter` - `AuditLogOperationFilterInput`
`sortBy` - `[AuditLogOperationSortBy!]`	

`status` - `AuditLogResultStatus!`	The result of the action that caused an audit log transaction to be written.

`timestamp` - `Time!`	The time reported by the caller for when the action occurred causing the audit log operation to be captured.
`traceID` - `String!`	An identifier that ties this audit log operation with a transaction.
`user` - `User`	User details.
`userID` - `String!`	The ID of the user who caused an audit log transaction to be written.

Example

```
{
  "apiClient": APIClient,
  "apiClientID": "abc123",
  "applicationID": "abc123",
  "description": "abc123",
  "id": "xyz789",
  "messages": ["xyz789"],
  "operations": [AuditLogOperation],
  "status": AuditLogResultStatus,
  "timestamp": Time,
  "traceID": "abc123",
  "user": User,
  "userID": "xyz789"
}
```

Types

AuditLogTransactionDimension

How to sort audit log transactions.

Enum Value	Description
`TIMESTAMP`	

Types

AuditLogTransactionFilterInput

Input required if extra criteria is needed to constrain the queried results.

Input Field	Description

`action` - `AuditLogAction`	A value indicating what type of action caused an audit log transaction to be written.
`apiClientID` - `String`	Used internally to help identify what system user made a request to record the audit log operation.
`applicationID` - `String`	Used internally to help identify what system component made a request to record the audit log operation.
`resourceID` - `String`	An ID value for internal reference indicating the key/ID value of the object being altered.
`resourceType` - `String`	A string value for internal reference indicating what type of object was altered.
`transactionResultStatus` - `AuditLogResultStatus`	A status representing the result of the action that caused an audit log transaction to be written.
`userID` - `String`	The ID of the user who caused an audit log transaction to be written.

Example

```
{
  "action": AuditLogAction,
  "apiClientID": "xyz789",
  "applicationID": "xyz789",
  "resourceID": "xyz789",
  "resourceType": "xyz789",
  "transactionResultStatus": AuditLogResultStatus,
  "userID": "abc123"
}
```

Types

`AuditLogTransactionSortBy`

Audit Log Transactions log sorting.

Input Field	Description

`dimension` - `AuditLogTransactionDimension!` default = `"TIMESTAMP"`	The dimension to sort by.
`direction` - `SortDirection!` default = `"DESCENDING"`	The direction to sort in.

Example

```
{
  "dimension": "TIMESTAMP",
  "direction": "DESCENDING"
}
```

Types

AuditLogTransactionsWithPagination

The list of audit log transactions along with pagination details.

Field Name	Description
`pageInfo` - `Pagination!`	The pagination details.
`results` - `[AuditLogTransaction!]`	The list of audit log transactions.

Example

```
{
  "pageInfo": Pagination,
  "results": [AuditLogTransaction]
}
```

Types

BGPCleanTrafficDeliveryMechanism

Enum Value	Description
`DIRECT_CONNECT`	
`LOAD_BALANCED`	
`REDUNDANT`	
`SINGLE_GRE`	

Types

BGPMitigationTriggerMechanism

Enum Value	Description
ROUTE_TRIGGERED_MITIGATION	
ROUTE_TRIGGERED_SUPPRESSION	
STANDARD	

Types

BGPPackage

Specifies BGP configuration for the company.

Field Name	Description
alertAuto - Boolean!	Auto Mitigation Enabled.
alwaysOn - Boolean!	Indicates whether company has BGP Always On DDoS mitigation enabled.
alwaysRouted - Boolean!	Whether traffic is always routed here.
cleanTrafficDeliveryMechanisms - [BGPCleanTrafficDeliveryMechanism!]	Mechanism(s) used to send clean traffic to back end.
companyDName - String!	The identifier of the owning company.

`enabled` - `Boolean!`	Whether BGP is enabled for the Company.
`hybridCloudSignalling` - `Boolean!`	Cloud Signalling Auto Mitigation Enabled.
`managedObjects` - `[ManagedObject!]`	List of BGP Managed Objects.
`mitigationTriggerMechanisms` - `[BGPMitigationTriggerMechanism!]`	Mechanism(s) used to trigger mitigations.
`onDemand` - `Boolean!`	Indicates whether company has BGP On Demand DDoS mitigation enabled.
`routing` - `BGPTrafficRouting`	Indicates what type of BGP routing is being used. This can be one of BGP IP, Traffic Engineering, Direct Connect, Direct Connect Traffic Engineering, or Group Routing Encapsulation (GRE).

`serviceTypes` - `[BGPServiceType!]`	BGP Service types configured.

Example

```
{
  "alertAuto": false,
  "alwaysOn": true,
  "alwaysRouted": true,
  "cleanTrafficDeliveryMechanisms": [
    BGPCleanTrafficDeliveryMechanism
  ],
  "companyDName": "abc123",
  "enabled": true,
  "hybridCloudSignalling": true,
  "managedObjects": [ManagedObject],
  "mitigationTriggerMechanisms": [
    BGPMitigationTriggerMechanism
  ],
  "onDemand": true,
  "routing": BGPTrafficRouting,
  "serviceTypes": [BGPServiceType]
}
```

Types

`BGPPackageFilterInput`

Ways of reducing output of Company queries.

Input Field	Description
`cleanTrafficDeliveryMechanisms` - `[BGPCleanTrafficDeliveryMechanism!]`	Mechanism(s) used to send clean traffic to back end.
`mitigationTriggerMechanisms` - `[BGPMitigationTriggerMechanism!]`	Mechanism(s) used to trigger mitigations.
`serviceTypes` - `[BGPServiceType!]`	BGP Service types configured.

Example

```
{
  "cleanTrafficDeliveryMechanisms": [
    BGPCleanTrafficDeliveryMechanism
  ],
  "mitigationTriggerMechanisms": [
    BGPMitigationTriggerMechanism
  ],
  "serviceTypes": [BGPServiceType]
}
```

Types

BGPServiceType

Enum Value	Description
ANYCAST_GRE	
BGP_IP	
BGP_TE	
DIRECT_CONNECT	
DIRECT_CONNECT_TE	

Types

BGPTrafficRouting

Specifies the type of BGP traffic routing configured for the company.

Enum Value	Description
BGP_IP	Specifies BGP IP routing.
BGP_TE	Specifies BGP Traffic Engineering routing.
DIRECT_CONNECT	Specifies BGP Direct Connect routing.
DIRECT_CONNECT_TE	Specifies BGP Direct Connect Traffic Engineering routing.
GRE	Specifies BGP Group Routing Encapsulation (GRE) routing.

Types

BaseBotSignature

A Bot Detection signature provided by the system. Can be configured to respond with a different action.

Field Name	Description
botType - BotType!	The signature bot type.
category - String!	The signature category.
defaultAction - BotSignatureAction!	The signature action taken by default.
defaultEnabled - Boolean!	Whether bot signature is enabled.
description - String!	Description of the signature.
id - String!	The signature unique ID.
version - String!	The signature version.

Example

```
{
  "botType": BotType,
  "category": "abc123",
  "defaultAction": BotSignatureAction,
  "defaultEnabled": true,
  "description": "xyz789",
  "id": "xyz789",
  "version": "xyz789"
}
```

Types

BaseWAFSignature

A WAF signature provided by the system. Can be configured to respond with a different action.

Field Name	Description
category - String!	Category of the signature.
createdAt - Time	The time that this base signature was added into the system.
defaultAction - WAFAction!	Default action to be taken.

`description` - `String!`	Description of the signature.
`id` - `String!`	Unique ID of the signature.
`refs` - `String`	Reference ID to the corresponding vulnerability lists. For instance: cve, bugtraq, nessus

Example

```
{
  "category": "abc123",
  "createdAt": Time,
  "defaultAction": WAFAction,
  "description": "abc123",
  "id": "abc123",
  "refs": "xyz789"
}
```

Types

`BaseWAFSignatureDimension`

Allowed values for sorting the Signature list.

Enum Value	Description
`CATEGORY`	
`CREATED_AT`	
`DESCRIPTION`	

Types

`BaseWAFSignatureSortBy`

Signature sorting input.

Input Field	Description
`dimension` - `BaseWAFSignatureDimension!`	The dimension to sort by.
`direction` - `SortDirection!`	The direction to sort in.

Example

```
{
```

```
  "dimension": BaseWAFSignatureDimension,
  "direction": SortDirection
}
```

Types

BaseWAFSignaturesResponse

A base signatures response object.

Field Name	Description
`lastCheckedTime` - `Time`	Represents the timestamp when the job ran to check for latest signature updates
`signatures` - `BaseWAFSignaturesWithPagination`	A paginated list of base signatures

Example

```
{
  "lastCheckedTime": Time,
  "signatures": BaseWAFSignaturesWithPagination
}
```

Types

BaseWAFSignaturesWithPagination

A paginated list of base WAF signatures.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BaseWAFSignature!]`	A list of signatures

Example

```
{
  "pageInfo": Pagination,
  "results": [BaseWAFSignature]
}
```

Types

Boolean

The `Boolean` scalar type represents `true` or `false`.

Example

```
true
```

Types

BotAnalyticsResponse

A Bot analytics response.

Field Name	Description
`groups` - `[ViolationLogGroup!]`	The list of aggregated group results satisfying the group by criteria.
`logs` - `BotViolationLogsWithPagination`	A paginated list of violation logs satisfying the filter criteria.
`timeSeriesData` - `[ViolationLogTimeSeries!]`	The time series information of the violation logs occurrences.

Example

```
{
  "groups": [ViolationLogGroup],
  "logs": BotViolationLogsWithPagination,
  "timeSeriesData": [ViolationLogTimeSeries]
}
```

Types

BotBlackList

A black list countermeasure.

Field Name	Description
`enabled` - `Boolean!`	Whether the black list countermeasure is enabled.
`types` - `BotBlackListTypesWithPagination`	A paginated list of black list bindings.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

Example

```
{
  "enabled": true,
  "types": BotBlackListTypesWithPagination
}
```

Types

`BotBlackListAction`

Allowed list of black list actions.

Enum Value	Description
`DROP`	
`REDIRECT`	
`RESET`	

Types

`BotBlackListBinding`

A black list binding.

Field Name	Description
`action` - `BotBlackListAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`active` - `Boolean!`	Whether the binding is active.

`expressionMatch` - `BotBlackWhiteListExpressionMatch`	The binding expression value. Can only be set if type is EXPRESSION.
`response` - `BotResponse!`	The binding response.
`type` - `BotBlackListType!`	The binding type.
`value` - `String`	The binding value. Can only be set if type is IPV4 or SUBNET.

Example

```
{
  "action": BotBlackListAction,
  "active": true,
  "expressionMatch": BotBlackWhiteListExpressionMatch,
  "response": BotResponse,
  "type": BotBlackListType,
  "value": "xyz789"
}
```

Types

`BotBlackListBindingInput`

A black list binding.

Input Field	Description
`action` - `BotBlackListAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`active` - `Boolean!`	Whether the binding is active.
`expressionMatch` - `BotBlackWhiteListExpressionMatchInput`	The binding expression value. Can only be set if type is EXPRESSION.
`response` - `BotResponse!`	The binding response.
`type` - `BotBlackListType!`	The binding type.

`value` - `String`	The binding value. Can only be set if type is IPV4 or SUBNET.

Example

```
{
  "action": BotBlackListAction,
  "active": false,
  "expressionMatch": BotBlackWhiteListExpressionMatchInput,
  "response": BotResponse,
  "type": BotBlackListType,
  "value": "abc123"
}
```

Types

BotBlackListType

Allowed list of black list types.

Enum Value	Description
`EXPRESSION`	
`IPV4`	
`SUBNET`	

Types

BotBlackListTypesWithPagination

A paginated list of black list bindings.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BotBlackListBinding!]`	List of black list bindings.

Example

```
{
  "pageInfo": Pagination,
  "results": [BotBlackListBinding]
```

```
}
```

Types

BotBlackWhiteListExpressionField

Allowed list of black and white list expression fields.

Enum Value	Description
`COOKIE`	
`HEADER`	
`HOSTNAME`	
`URL`	

Types

BotBlackWhiteListExpressionMatch

A black and white list expression match.

Field Name	Description
`field` - `BotBlackWhiteListExpressionField!`	The expression field.
`fieldValue` - `String`	The expression field value. Can only be set if field is HEADER.
`operand` - `BotBlackWhiteListExpressionOperand!`	The expression operand.
`operandValue` - `String!`	The expression operand value.

Example

```
{
  "field": BotBlackWhiteListExpressionField,
  "fieldValue": "abc123",
  "operand": BotBlackWhiteListExpressionOperand,
  "operandValue": "xyz789"
}
```

Types

BotBlackWhiteListExpressionMatchInput

A black and white list expression match.

Input Field	Description
`field` - `BotBlackWhiteListExpressionField!`	The expression field.
`fieldValue` - `String`	The expression field value. Can only be set if field is HEADER.
`operand` - `BotBlackWhiteListExpressionOperand!`	The expression operand.
`operandValue` - `String!`	The expression operand value.

Example

```
{
  "field": BotBlackWhiteListExpressionField,
  "fieldValue": "xyz789",
  "operand": BotBlackWhiteListExpressionOperand,
  "operandValue": "xyz789"
}
```

Types

BotBlackWhiteListExpressionOperand

Allowed list of black and white list expression operands.

Enum Value	Description
`CONTAINS`	
`DOES_NOT_CONTAIN`	
`DOES_NOT_EQUAL`	
`ENDS_WITH`	
`EQUALS`	
`STARTS_WITH`	

Types

BotCAPTCHA

A CAPTCHA countermeasure.

Field Name	Description

`resources` - `BotCAPTCHAResourcesWithPagination`	A paginated list of CAPTCHA bindings.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

Example

```
{"resources": BotCAPTCHAResourcesWithPagination}
```

Types

BotCAPTCHAAction

Allowed list of CAPTCHA actions.

Enum Value	Description
`DROP`	
`REDIRECT`	
`RESET`	

Types

BotCAPTCHABinding

A CAPTCHA binding.

Field Name	Description
`action` - `BotCAPTCHAAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`active` - `Boolean!`	Whether the binding is active.
`gracePeriod` - `UnsignedInt32!`	The binding grace period.
`mutePeriod` - `UnsignedInt32!`	The binding mute period.

`requestLengthLimit` - `UnsignedInt32!`	The binding request length limit.
`response` - `BotResponse!`	The binding response.
`retryAttempts` - `UnsignedInt32!`	The binding retry attempts.
`urlPath` - `String!`	The binding url.
`waitTime` - `UnsignedInt32!`	The binding wait time.

Example

```
{
  "action": BotCAPTCHAAction,
  "active": true,
  "gracePeriod": UnsignedInt32,
  "mutePeriod": UnsignedInt32,
  "requestLengthLimit": UnsignedInt32,
  "response": BotResponse,
  "retryAttempts": UnsignedInt32,
  "urlPath": "xyz789",
  "waitTime": UnsignedInt32
}
```

Types

`BotCAPTCHABindingInput`

A CAPTCHA binding.

Input Field	Description
`action` - `BotCAPTCHAAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`active` - `Boolean!`	Whether the binding is active.
`gracePeriod` - `UnsignedInt32!`	The binding grace period.
`mutePeriod` - `UnsignedInt32!`	The binding mute period.
`requestLengthLimit` - `UnsignedInt32!`	The binding request length limit.
`response` - `BotResponse!`	The binding response.
`retryAttempts` - `UnsignedInt32!`	The binding retry attempts.
`urlPath` - `String!`	The binding url.
`waitTime` - `UnsignedInt32!`	The binding wait time.

Example

```
{
  "action": BotCAPTCHAAction,
  "active": true,
  "gracePeriod": UnsignedInt32,
  "mutePeriod": UnsignedInt32,
  "requestLengthLimit": UnsignedInt32,
  "response": BotResponse,
  "retryAttempts": UnsignedInt32,
  "urlPath": "xyz789",
  "waitTime": UnsignedInt32
}
```

Types

BotCAPTCHAResourcesWithPagination

A paginated list of CAPTCHA bindings.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BotCAPTCHABinding!]`	List of CAPTCHA bindings.

Example

```
{
  "pageInfo": Pagination,
  "results": [BotCAPTCHABinding]
}
```

Types

BotDeviceFingerprint

A device fingerprint countermeasure.

Field Name	Description
`action` - `BotDeviceFingerprintAction`	Action to be taken. Can only be set if response is ACTION_AND_LOG.
`enabled` - `Boolean!`	Whether the device fingerprint countermeasure is enabled.

`response` - `BotResponse!`	Response to be taken.

Example

```
{
  "action": BotDeviceFingerprintAction,
  "enabled": true,
  "response": BotResponse
}
```

Types

BotDeviceFingerprintAction

Allowed list of device fingerprint actions.

Enum Value	Description
`DROP`	
`MITIGATION`	
`REDIRECT`	
`RESET`	

Types

BotIPReputation

An IP reputation countermeasure.

Field Name	Description
`categories` - `BotIPReputationCategoriesWithPagination`	A paginated list of IP reputation bindings.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`enabled` - `Boolean!`	Whether the IP reputation countermeasure is enabled.

Example

```
{
  "categories": BotIPReputationCategoriesWithPagination,
  "enabled": false
}
```

Types

`BotIPReputationAction`

Allowed list of IP reputation actions.

Enum Value	Description
`DROP`	
`MITIGATION`	
`REDIRECT`	
`RESET`	

Types

`BotIPReputationBinding`

An IP reputation binding.

Field Name	Description
`action` - `BotIPReputationAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`active` - `Boolean!`	Whether the binding is active.
`response` - `BotResponse!`	The binding response.
`type` - `BotIPReputationType!`	The binding type.

Example

```
{
  "action": BotIPReputationAction,
  "active": false,
  "response": BotResponse,
  "type": BotIPReputationType
}
```

Types

BotIPReputationBindingInput

An IP reputation binding.

Input Field	Description
`action` - `BotIPReputationAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`active` - `Boolean!`	Whether the binding is active.
`response` - `BotResponse!`	The binding response.
`type` - `BotIPReputationType!`	The binding type.

Example

```
{
  "action": BotIPReputationAction,
  "active": false,
  "response": BotResponse,
  "type": BotIPReputationType
}
```

Types

BotIPReputationCategoriesWithPagination

A paginated list of IP reputation bindings.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BotIPReputationBinding!]`	List of IP reputation bindings.

Example

```
{
  "pageInfo": Pagination,
  "results": [BotIPReputationBinding]
}
```

Types

BotIPReputationType

Allowed list of IP reputation types.

Enum Value	Description
BOTNETS	
DOS	
IP	
MOBILE_THREATS	
PHISHING	
PROXY	
REPUTATION	
SCANNERS	
SPAM_SOURCES	

Types

BotMitigation

Bot Mitigation.

Field Name	Description
company - Company!	
countermeasures - [BotViolation!]	The countermeasures associated with the mitigation.
destinationIPs - [CIDR!]	The destination IPs.
end - Time	The end time of the mitigation. A non-zero value of end time means that the mitigation has ended.
id - String!	The identifier of the mitigation.

`policy` - `Policy`	The Policy that triggered this mitigation.
`start` - `Time!`	The start time of the mitigation.

Example

```
{
  "company": Company,
  "countermeasures": [BotViolation],
  "destinationIPs": [CIDR],
  "end": Time,
  "id": "abc123",
  "policy": Policy,
  "start": Time
}
```

Types

BotProfile

A bot profile for a given policy.

Field Name	Description
`blackList` - `BotBlackList`	The black list countermeasure settings.
`botTrap` - `BotTrap`	The bot trap countermeasure settings.
`captcha` - `BotCAPTCHA`	The CAPTCHA countermeasure settings.
`deviceFingerprint` - `BotDeviceFingerprint`	The device fingerprint countermeasure settings.
`enabled` - `Boolean!`	Whether the bot profile is enabled.
`ipReputation` - `BotIPReputation`	The IP reputation countermeasure settings.
`rateLimit` - `BotRateLimit`	The rate limit countermeasure settings.
`signatures` - `BotSignatures`	The bot signatures settings.
`tps` - `BotTPS`	The TPS countermeasure settings.
`whiteList` - `BotWhiteList`	The white list countermeasure settings.

Example

```
{
  "blackList": BotBlackList,
  "botTrap": BotTrap,
  "captcha": BotCAPTCHA,
  "deviceFingerprint": BotDeviceFingerprint,
  "enabled": false,
  "ipReputation": BotIPReputation,
  "rateLimit": BotRateLimit,
  "signatures": BotSignatures,
  "tps": BotTPS,
  "whiteList": BotWhiteList
}
```

Types

BotRateLimit

A rate limit countermeasure.

Field Name	Description
`enabled` - `Boolean!`	Whether the rate limit countermeasure is enabled.
`resources` - `BotRateLimitResourcesWithPagination`	A paginated list of rate limit bindings.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

Example

```
{
  "enabled": true,
  "resources": BotRateLimitResourcesWithPagination
}
```

Types

BotRateLimitAction

Allowed list of rate limit actions.

Enum Value	Description
DROP	
REDIRECT	
RESET	

Types

BotRateLimitBinding

A rate limit binding.

Field Name	Description
action - BotRateLimitAction	The binding action. Can only be set if response is ACTION_AND_LOG.
active - Boolean!	Whether the binding is active.
cookieName - String	The binding cookie name. Can only be set if type is SESSION.
period - UnsignedInt32!	The binding period.
rate - UnsignedInt32!	The binding rate.
response - BotResponse!	The binding response.
type - BotRateLimitType!	The binding type.
urlPath - String	The binding URL path. Can only be set if type is URL.

Example

```
{
  "action": BotRateLimitAction,
  "active": false,
  "cookieName": "abc123",
  "period": UnsignedInt32,
  "rate": UnsignedInt32,
  "response": BotResponse,
  "type": BotRateLimitType,
```

```
  "urlPath": "xyz789"
}
```

Types

BotRateLimitBindingInput

A rate limit binding.

Input Field	Description
`action` - `BotRateLimitAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`active` - `Boolean!`	Whether the binding is active.
`cookieName` - `String`	The binding cookie name. Can only be set if type is SESSION.
`period` - `UnsignedInt32!`	The binding period.
`rate` - `UnsignedInt32!`	The binding rate.
`response` - `BotResponse!`	The binding response.
`type` - `BotRateLimitType!`	The binding type.
`urlPath` - `String`	The binding URL path. Can only be set if type is URL.

Example

```
{
  "action": BotRateLimitAction,
  "active": true,
  "cookieName": "xyz789",
  "period": UnsignedInt32,
  "rate": UnsignedInt32,
  "response": BotResponse,
  "type": BotRateLimitType,
  "urlPath": "abc123"
}
```

Types

BotRateLimitResourcesWithPagination

A paginated list of rate limit bindings.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BotRateLimitBinding!]`	List of rate limit bindings.

Example

```
{
  "pageInfo": Pagination,
  "results": [BotRateLimitBinding]
}
```

Types

`BotRateLimitType`

Allowed list of rate limit types.

Enum Value	Description
`SESSION`	
`SOURCE_IP`	
`URL`	

Types

`BotResponse`

Allowed list of countermeasure responses.

Enum Value	Description
`ACTION_AND_LOG`	
`LOG`	
`NONE`	

Types

`BotSignatureAction`

Allowed list of bot signature actions.

Enum Value	Description
`DROP_AND_LOG`	
`LOG`	
`NONE`	
`REDIRECT_AND_LOG`	
`RESET_AND_LOG`	

Types

`BotSignatureDimension`

Allowed values for sorting the bot signature list.

Enum Value	Description
`CATEGORY`	
`NAME`	

Types

`BotSignatureFilterInput`

Filter a list of bot signatures.

Input Field	Description
`category` - `String`	Category to filter the signatures by.
`name` - `String`	Name to filter the signatures by.
`search` - `String`	Substring to search in description and other text, etc.

Example

```
{"category": "xyz789", "name": "xyz789", "search": "xyz789"}
```

Types

`BotSignatureSortBy`

Sort options for the bot signature list.

Input Field	Description
`dimension` - `BotSignatureDimension!`	The dimension to sort by.
`direction` - `SortDirection!`	The direction to sort in.

Example

```
{
  "dimension": BotSignatureDimension,
  "direction": SortDirection
}
```

Types

BotSignatures

Bot signatures.

Field Name	Description
`configuredBaseSignatures` - `[ConfiguredBaseBotSignature!]`	List of bot signatures.
`enabled` - `Boolean!`	Whether bot signatures are enabled.

Example

```
{
  "configuredBaseSignatures": [
    ConfiguredBaseBotSignature
  ],
  "enabled": true
}
```

Types

BotSignaturesVersion

The version information for a bot signatures file.

Field Name	Description
`schemaVersion` - `String!`	The signature file schema version.

`version` - `String!`	The signature file version.

Example

```
{"schemaVersion": "abc123", "version": "xyz789"}
```

Types

BotSignaturesWithPagination

A paginated list of bot signatures.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BaseBotSignature!]`	List of bot signatures.
`version` - `BotSignaturesVersion`	The version of the default bot signatures file

Example

```
{
  "pageInfo": Pagination,
  "results": [BaseBotSignature],
  "version": BotSignaturesVersion
}
```

Types

BotTPS

A TPS countermeasure.

Field Name	Description
`enabled` - `Boolean!`	Whether the TPS countermeasure is enabled.
`resources` - `BotTPSResourcesWithPagination`	A paginated list of rate limit bindings.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

Example

```
{
  "enabled": true,
  "resources": BotTPSResourcesWithPagination
}
```

Types

BotTPSAction

Allowed list of TPS actions.

Enum Value	Description
`DROP`	
`MITIGATION`	
`REDIRECT`	
`RESET`	

Types

BotTPSBinding

A TPS binding.

Field Name	Description
`action` - `BotTPSAction`	The binding action. Can only be set if response is ACTION_AND_LOG.
`fixedThreshold` - `UnsignedInt32`	The binding fixed threshold. One or both of fixed and percentage threshold must be set.
`percentageThreshold` - `UnsignedInt32`	The binding percentage threshold. One or both of fixed and percentage threshold must be set.
`response` - `BotResponse!`	The binding response.
`type` - `BotTPSType!`	The binding type.

Example

```
{
  "action": BotTPSAction,
  "fixedThreshold": UnsignedInt32,
  "percentageThreshold": UnsignedInt32,
  "response": BotResponse,
  "type": BotTPSType
}
```

Types

BotTPSBindingInput

A TPS binding.

Input Field	Description
action - BotTPSAction	The binding action. Can only be set if response is ACTION_AND_LOG.
fixedThreshold - UnsignedInt32	The binding fixed threshold. One or both of fixed and percentage threshold must be set.
percentageThreshold - UnsignedInt32	The binding percentage threshold. One or both of fixed and percentage threshold must be set.
response - BotResponse!	The binding response.
type - BotTPSType!	The binding type.

Example

```
{
  "action": BotTPSAction,
  "fixedThreshold": UnsignedInt32,
  "percentageThreshold": UnsignedInt32,
  "response": BotResponse,
  "type": BotTPSType
}
```

Types

BotTPSResourcesWithPagination

A paginated list of TPS bindings.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BotTPSBinding!]`	List of TPS bindings.

Example

```
{
  "pageInfo": Pagination,
  "results": [BotTPSBinding]
}
```

Types

BotTPSType

Allowed list of TPS types.

Enum Value	Description
`GEOLOCATION`	
`HOST`	
`REQUEST_URL`	
`SOURCE_IP`	

Types

BotTrap

A bot trap countermeasure.

Field Name	Description
`action` - `BotTrapAction`	Action to be taken. Can only be set if response is ACTION_AND_LOG.
`enabled` - `Boolean!`	Whether the bot trap countermeasure is enabled.
`insertionURLs` - `[BotTrapBinding!]`	List of bot trap bindings.
`response` - `BotResponse!`	Response to be taken.

Example

```
{
  "action": BotTrapAction,
  "enabled": false,
  "insertionURLs": [BotTrapBinding],
  "response": BotResponse
}
```

Types

BotTrapAction

Allowed list of bot trap actions.

Enum Value	Description
DROP	
REDIRECT	
RESET	

Types

BotTrapBinding

A bot trap binding.

Field Name	Description
active - Boolean!	Whether the binding is active.
urlPath - String!	The binding insertion URL.

Example

```
{"active": true, "urlPath": "xyz789"}
```

Types

BotTrapBindingInput

A bot trap binding.

Input Field	Description
active - Boolean!	Whether the binding is active.

`urlPath` - `String!`	The binding insertion URL.

Example

```
{"active": false, "urlPath": "xyz789"}
```

Types

BotType

Allowed list of bot types.

Enum Value	Description
`BAD_BOT`	
`GOOD_BOT`	

Types

BotViolation

Represents Bot violation.

Field Name	Description
`company` - `Company!`	The company object.
`id` - `String!`	The id of a bot violation.
`name` - `String!`	The signature name.
`violationsDetails` - `[AppViolationData!]`	The details of the violations.

Arguments

`metrics` - `[AppViolationMetric!]`

Example

```
{
  "company": Company,
  "id": "abc123",
  "name": "abc123",
  "violationsDetails": [AppViolationData]
}
```

Types

BotViolationLog

A Bot violation log.

Field Name	Description
action - String	The action that caused this violation log.
cookies - String	The cookies in the original request.
customer - String	The customer account dname.
destinationIP - IPAddress	The destination IP the request was intended for.
domain - String	The domain the request was intended for.
host - String	The hostname in the request.
httptxID - String	The HTTP transaction ID from the engine.
logType - BotViolationLogType	The type of the log message.
node - NetworkNode	The network node that detected the violation.
profile - String	The policy key generating this violation.
protocol - String	The protocol used.
rawHeaders - String	The raw headers in the original request.
reason - String	The reason for the violation to occur.
signatureName - String	The protection / signature name which triggered the violation.
sourceASN - UnsignedInt32	The source ASN (autonomous system number) of the request.
sourceIP - IPAddress	The source IP of the request.
sourceLocation - GeoLocation	The location where the request originated.
timestamp - LogTime	The timestamp of the violation log.
timestampEvent - LogTime	The log timestamp event.
type - String	The type of the violation.
uri - String	The uri which cause the violation.
userAgent - String	The user agent in the original request header.
version - String	The version.

`wafVersion` - `String` The WAF version.

Example

```
{
  "action": "xyz789",
  "cookies": "abc123",
  "customer": "abc123",
  "destinationIP": IPAddress,
  "domain": "abc123",
  "host": "xyz789",
  "httptxID": "xyz789",
  "logType": BotViolationLogType,
  "node": NetworkNode,
  "profile": "xyz789",
  "protocol": "xyz789",
  "rawHeaders": "xyz789",
  "reason": "abc123",
  "signatureName": "xyz789",
  "sourceASN": UnsignedInt32,
  "sourceIP": IPAddress,
  "sourceLocation": GeoLocation,
  "timestamp": LogTime,
  "timestampEvent": LogTime,
  "type": "abc123",
  "uri": "abc123",
  "userAgent": "xyz789",
  "version": "xyz789",
  "wafVersion": "xyz789"
}
```

Types

`BotViolationLogDimension`

Allowed list of Bot violation log sort fields.

Enum Value	Description
`DESTINATION_IP`	
`DOMAIN`	
`NODE_IATA_CODE`	
`SIGNATURE_NAME`	

`SOURCE_COUNTRY`
`SOURCE_IP`
`TIMESTAMP`
`URI`

Types

`BotViolationLogFilterInput`

A Bot violation log filter input.

Input Field	Description
`action` - `String`	The violation log action.
`all` - `String`	The All filters looks at all the filters mentioned above, with the exception of profile.
`destinationIP` - `IPAddressInput`	The destination IP of the request.
`domain` - `String`	The domain the request was intended for.
`host` - `String`	The host of the request.
`httptxID` - `String`	The HTTP transaction ID from the engine.
`logType` - `BotViolationLogType`	The type of the log message.
`nodeIATACode` - `String`	The IATA code for the processing node (site).
`profile` - `String`	The policy key generating this violation.
`reason` - `String`	The reason for the violation to occur.
`signatureName` - `String`	The signature name which triggered the violation.
`sourceCity` - `String`	The source city name.
`sourceCountryName` - `String`	The source country name.
`sourceIP` - `IPAddressInput`	The source IP of the request.
`timestamp` - `String`	The timestamp of the violation log.
`uri` - `String`	The uri which cause the violation.
`userAgent` - `String`	The user agent in the original request header.

Example

```
{
  "action": "xyz789",
  "all": "xyz789",
  "destinationIP": IPAddressInput,
  "domain": "xyz789",
  "host": "abc123",
  "httptxID": "abc123",
  "logType": BotViolationLogType,
  "nodeIATACode": "xyz789",
  "profile": "abc123",
  "reason": "abc123",
  "signatureName": "xyz789",
  "sourceCity": "abc123",
  "sourceCountryName": "xyz789",
  "sourceIP": IPAddressInput,
  "timestamp": "xyz789",
  "uri": "xyz789",
  "userAgent": "xyz789"
}
```

Types

BotViolationLogGroupByField

Allowed list of Bot violation log group by fields.

Enum Value	Description
DESTINATION_IP	
DOMAIN	
PROFILE	
SIGNATURE_NAME	
SOURCE_COUNTRY	
SOURCE_IP	
URI	

Types

BotViolationLogGroupByInput

A Bot violation log group by input.

Input Field	Description
`direction` - `SortDirection`	The order of the groups listed (ascending or descending).
`field` - `BotViolationLogGroupByField!`	The field that will be used to group the logs.
`timeInterval` - `TimeInterval`	The time interval when the group of logs occurred.

Example

```
{
  "direction": SortDirection,
  "field": BotViolationLogGroupByField,
  "timeInterval": TimeInterval
}
```

Types

`BotViolationLogSortBy`

Bot violation log sorting.

Input Field	Description
`dimension` - `BotViolationLogDimension!`	The dimension to sort by.
`direction` - `SortDirection!` default = `"DESCENDING"`	The direction to sort in.

Example

```
{
  "dimension": BotViolationLogDimension,
  "direction": "DESCENDING"
}
```

Types

`BotViolationLogType`

Allowed list of Bot violation log types.

Enum Value	Description
`ALL`	

`INFO`

`VIOLATION`

Types

`BotViolationLogsWithPagination`

A paginated list of Bot violation logs.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[BotViolationLog!]`	Violation log entries.

Example

```
{
  "pageInfo": Pagination,
  "results": [BotViolationLog]
}
```

Types

`BotWhiteList`

A white list countermeasure.

Field Name	Description
`enabled` - `Boolean!`	Whether the white list countermeasure is enabled.
`types` - `BotWhiteListTypesWithPagination`	A paginated list of white list bindings.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

Example

```
{
  "enabled": false,
  "types": BotWhiteListTypesWithPagination
}
```

Types

BotWhiteListBinding

A white list binding.

Field Name	Description
active - Boolean!	Whether the binding is active.
expressionMatch - BotBlackWhiteListExpressionMatch	The binding expression value. Can only be set if type is EXPRESSION.
response - BotWhiteListResponse!	The binding response.
type - BotWhiteListType!	The binding type.
value - String	The binding value. Can only be set if type is IPV4 or SUBNET.

Example

```
{
  "active": true,
  "expressionMatch": BotBlackWhiteListExpressionMatch,
  "response": BotWhiteListResponse,
  "type": BotWhiteListType,
  "value": "abc123"
}
```

Types

BotWhiteListBindingInput

A white list binding.

Input Field	Description

`active` - `Boolean!`	Whether the binding is active.
`expressionMatch` - `BotBlackWhiteListExpressionMatchInput`	The binding expression value. Can only be set if type is EXPRESSION.
`response` - `BotWhiteListResponse!`	The binding response.
`type` - `BotWhiteListType!`	The binding type.
`value` - `String`	The binding value. Can only be set if type is IPV4 or SUBNET.

Example

```
{
  "active": false,
  "expressionMatch": BotBlackWhiteListExpressionMatchInput,
  "response": BotWhiteListResponse,
  "type": BotWhiteListType,
  "value": "xyz789"
}
```

Types

`BotWhiteListResponse`

Allowed list of white list responses.

Enum Value	Description
`LOG`	
`NONE`	

Types

`BotWhiteListType`

Allowed list of white list types.

Enum Value	Description
`EXPRESSION`	
`IPV4`	
`SUBNET`	

Types

`BotWhiteListTypesWithPagination`

A paginated list of white list bindings.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[BotWhiteListBinding!]`	List of white list bindings.

Example

```
{
  "pageInfo": Pagination,
  "results": [BotWhiteListBinding]
}
```

Types

`BufferOverflow`

Buffer overflow countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`maxCookieLength` - `UnsignedInt16!`	Maximum cookie length (in characters) in requests to the protected web sites. Requests with longer cookie lengths will be blocked.
`maxHeaderLength` - `UnsignedInt16!`	Maximum HTTP header length (in characters) in requests to the protected web sites. Requests with longer headers will be blocked.
`maxURLLength` - `UnsignedInt16!`	Maximum URL length allowed on the protected web sites. Requests with longer URLs will be blocked.

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for buffer overflow violations.

Example

```
{
  "action": WAFAction,
  "maxCookieLength": UnsignedInt16,
  "maxHeaderLength": UnsignedInt16,
  "maxURLLength": UnsignedInt16,
  "threshold": AppSecThreshold
}
```

Types

`CIDR`

CIDR represents an IP address range, either IPv4 or IPv6.

Example

```
object
```

Types

`CSRFRelaxationRule`

A CSRF relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`formActionURL` - `String!`	The action URL for the web form.
`formOriginURL` - `String!`	The web form originating URL.

Example

```
{"enabled": true, "formActionURL": "abc123", "formOriginURL": "xyz789"}
```

Types

`CSRFRelaxationRuleInput`

A CSRF relaxation rule. Form tagging must be enabled to use this feature.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.
`formActionURL` - `String!`	The action URL for the web form.
`formOriginURL` - `String!`	The web form originating URL.

Example

```
{"enabled": true, "formActionURL": "xyz789", "formOriginURL": "abc123"}
```

Types

CSRFRelaxationRulesWithPagination

A paginated list of CSRF relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[CSRFRelaxationRule!]`	A list of CSRF relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [CSRFRelaxationRule]
}
```

Types

CSRFSettings

A cross-site request forgery countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`learn` - `Boolean!`	A flag to enable or disable learning.
`relaxationRules` - `CSRFRelaxationRulesWithPagination`	A paginated list of CSRF relaxation rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for CSRF violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "relaxationRules": CSRFRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

`CSRFSettingsRuleCount`

CSRF settings rule count.

Field Name	Description
`count` - `UnsignedInt32!`	
`rule` - `LearnedCSRFSettingsRule!`	

Example

```
{
  "count": UnsignedInt32,
  "rule": LearnedCSRFSettingsRule
}
```

Types

`CSRFSettingsRuleCountsWithPagination`

CSRF settings learning rules.

Field Name	Description
`pageInfo` - `Pagination!`	
`results` - `[CSRFSettingsRuleCount!]`	

Example

```
{
  "pageInfo": Pagination,
  "results": [CSRFSettingsRuleCount]
}
```

Types

`CallerType`

Allowed list of values indicating what type of caller is recording an audit log transaction.

Enum Value	Description
`APPLICATION`	
`SERVICE`	

Types

`Certificate`

An SSL certificate.

Field Name	Description
`commonName` - `String!`	The common name of the certificate.
`company` - `Company!`	The name of the company.
`createdAt` - `Time!`	The time at which the certificate was created.
`expiration` - `Time!`	The time at which the certificate will expire.
`fingerprint` - `String!`	The hash of the certificate.
`id` - `String!`	The ID of the certificate.
`isIntermediate` - `Boolean!`	Whether or not the certificate is an intermediate.
`issued` - `Time!`	The time at which the certificate was issued.

`issuer` - `String!`	The issuer name of the certificate.
`linksTo` - `String`	The intermediate certificate that links to the SSL certificate.
`name` - `String!`	The name of the certificate.
`nod` - `String!`	The name of the certificate on the devices.
`root` - `String!`	The root certificate name.
`sanNames` - `[String!]`	SAN Names belonging to the certificate.
`updatedAt` - `Time!`	The time at which the certificate was updated.

Example

```
{
  "commonName": "abc123",
  "company": Company,
  "createdAt": Time,
  "expiration": Time,
  "fingerprint": "abc123",
  "id": "abc123",
  "isIntermediate": true,
  "issued": Time,
  "issuer": "xyz789",
  "linksTo": "abc123",
  "name": "abc123",
  "nod": "abc123",
  "root": "abc123",
  "sanNames": ["xyz789"],
  "updatedAt": Time
}
```

Types

`CertificateBinding`

Certificate information for a back end.

Field Name	Description
`certificateID` - `String!`	Common name used for SNI initiation.
`sni` - `Boolean!`	Forces back-end SNI support between the proxy and the origin, sending the specified common name to initiate SNI to the back end.

Example

```
{"certificateID": "xyz789", "sni": false}
```

Types

CertificateBindingInput

Associate a certificate with a virtual server.

Input Field	Description
certificateID - String!	Internal ID for a defined certficiate.

Example

```
{"certificateID": "xyz789"}
```

Types

CipherSelectionMode

Allowed list of TLS cipher user selection mode.

Enum Value	Description
CUSTOM	
DEFAULT	

Types

CommandInjection

An Command injection countermeasure.

Field Name	Description
action - WAFAction!	Action to be taken.
commandInjectionType - CommandInjectionType!	A command injection type.
relaxationRules - CommandInjectionRelaxationRulesWithPagination	A paginated list of SQL

	Injection rules.

Arguments
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `1000`
 	
The maximum number of results to show per page.	

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for command injection violations.

Example

```
{
  "action": WAFAction,
  "commandInjectionType": CommandInjectionType,
  "relaxationRules": CommandInjectionRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

`CommandInjectionRelaxationRule`

A Command injection relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!`	Whether the name is in regex format.
`isValueExpressionRegex` - `Boolean`	Whether the value expression is in regex format.
`location` - `HTMLLocation`	Location that should be examined by the rule.

`name` - `String!`	Name of the web form field, cookie, or HTTP header to relax.
`url` - `String!`	If the item to be exempted is a web form field, the action URL for the web form.
`valueExpression` - `String`	The value expression.
`valueType` - `CommandInjectionValueType`	The value type.

Example

```
{
  "enabled": true,
  "isNameRegex": false,
  "isValueExpressionRegex": false,
  "location": HTMLLocation,
  "name": "xyz789",
  "url": "abc123",
  "valueExpression": "abc123",
  "valueType": CommandInjectionValueType
}
```

Types

`CommandInjectionRelaxationRuleInput`

A Command injection relaxation rule input.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!` default = `false`	Whether the name is in regex format.
`isValueExpressionRegex` - `Boolean` default = `false`	Whether the value expression is in regex format.
`location` - `HTMLLocation`	The location that should be examined by the rule.
`name` - `String!`	Name of the web form field, cookie, or HTTP header to relax.
`url` - `String!`	If the item to be exempted is a web form field, the action URL for the web form.
`valueExpression` - `String`	The value expression.

`valueType` - `CommandInjectionValueType`	The value type.

Example

```
{
  "enabled": true,
  "isNameRegex": false,
  "isValueExpressionRegex": false,
  "location": HTMLLocation,
  "name": "xyz789",
  "url": "abc123",
  "valueExpression": "abc123",
  "valueType": CommandInjectionValueType
}
```

Types

`CommandInjectionRelaxationRulesWithPagination`

A paginated list of SQL injection relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[CommandInjectionRelaxationRule!]`	A list of relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [CommandInjectionRelaxationRule]
}
```

Types

`CommandInjectionType`

Allowed list of command injection types.

Enum Value	Description
`COMMAND_KEYWORD`	
`COMMAND_SPECIAL_CHARACTER`	

`COMMAND_SPECIAL_CHARACTER_AND_KEYWORD`	
`COMMAND_SPECIAL_CHARACTER_OR_KEYWORD`	

Types

CommandInjectionValueType

Allowed list of values for command injection value types.

Enum Value	Description
`KEYWORD`	
`SPECIAL_STRING`	

Types

CommentExemption

Allowed list of types of comment which can be exmpted.

Enum Value	Description
`ANSI`	
`ANSI_NESTED`	
`CHECK_ALL`	
`NESTED`	

Types

CompaniesWithPagination

A paginated list of Companies.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[Company!]`	Set of companies returned by query.

Example

```
{
```

```
  "pageInfo": Pagination,
  "results": [Company]
}
```

Types

Company

A Customer or Reseller

Field Name	Description
`accountID` - `String!`	Unique account ID of Company.
`accountInfo` - `AccountInfo`	Account and Contract Details of Company.
`accountManagerEmail` - `String!`	Company Account Manager email.
`accountManagerName` - `String!`	Company Account Manager Name.
`allCustomers` - `CompaniesWithPagination!`	Returns all companies that are customers of (resold by) this company and those resold by other reseller.

Arguments

`filter` - `CustomerFilterInput`

Input search criteria to filter results.

`page` - `UnsignedInt32!` default = `1`

Page number.

`perPage` - `UnsignedInt32!` default = `50`

Entries per page.

`apiPackage` - `APIAccess`	API access settings users belonging to this company.
`appDataAnalytics` - `[AppDataAnalyticsResponse!]`	Application-level traffic data.

Arguments

`aggregateBy` - `AppDataAggregateByInput!`

A value indicating how the results should be grouped.

`fields` - `[AppDataField!]`

A list of result types that should be included in the results.

`filter` - `AppDataFilterInput`

If given, criteria to constrain the results queried.

`from` - `Time!`

The start time (inclusive) of the results to fetch.

`to` - `Time`

The end time (exclusive) of the results to fetch. Defaults to the current time.

`auditLogTransactions` - `AuditLogTransactionsWithPagination!`

A list of audit log transactions that occurred between UTC time (from) to UTC time (to).

Arguments

`filter` - `AuditLogTransactionFilterInput`

The filters that can be applied to scope the specific list of audit log transactions.

`from` - `Time`

Earliest time to show transactions from. If not given, will use earliest recorded transaction date.

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results. It takes a non-zero number.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`sortBy` - `[AuditLogTransactionSortBy!]`

The sortBy sorts the results based on the specific sort field selected and order. If omitted, results are sorted based on the descending order of the transaction timestamp.

`to` - `Time`

Latest time to show transactions from. If not given, most recent transactions will be included.

`bgpPackage` - `BGPPackage`

BGP Configuration, if any.

Arguments

`filter` - `BGPPackageFilterInput`

`botAnalytics` - `BotAnalyticsResponse`	Bot Violation Log details.

Arguments
 	
`filter` - `BotViolationLogFilterInput`
 	
If given, criteria to constrain the results queried.
 	
`from` - `Time!`
 	
The start time (inclusive) of the violations to fetch.
 	
`groupBy` - `BotViolationLogGroupByInput`
 	
If given, result will be grouped by the given criteria.
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `50`
 	
The maximum number of results to show per page.
 	
`sortBy` - `[BotViolationLogSortBy!]`
 	
If given, result will be sorted in the given order.
 	
`to` - `Time`
 	
The end time (exclusive) of the violations to fetch. Defaults to the current time.	

`certificates` - `[Certificate!]`	TLS Certificates configured for the Company.
`configurationChanges` - `[ConfigurationChange!]`	Recent changes to Policies

	and/or Proxies.
Arguments	
`filter` - `ConfigurationChangeFilterInput`	
`corporateDomain` - `String!`	Corporate Domain name of the company.
`corporateName` - `String!`	Corporate Name of the company.
`createdAt` - `Time!`	Timestamp the company entry was created at.
`customers` - `[Company!]`	Companies that are direct customers of this company.
`dName` - `String!`	The unique, primary identifier for the company.
`deleted` - `Boolean!`	Indicates whether company is deleted.
`destinationIPs` - `[CIDR!]`	IP Addresses that could be getting traffic.

`details` - `CompanyDetails!`	Contains Company details like Name, Account Name and ID, DNS account, among others.
`detectionAndAlertingPackage` - `DetectionAndAlertingPackage`	Detection and Alerting Package.
`enabled` - `Boolean!`	Whether the Company and its users are able to access the system.
`event` - `Event`	Details of a specific event.
Arguments `id` - `String!`	
`events` - `EventsWithPagination!`	The list of events.

Arguments
 	
`filter` - `EventFilterInput`
 	
The filters that can be applied to scope the specific list of events.
 	
`from` - `Time!`
 	
The time to fetch events from(inclusive).
 	
`page` - `UnsignedInt32!` default = `1`	

The page number to fetch results. It takes a non-zero number. If omitted, default value of 1 is applied.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page. If omitted, default value of 50 is applied.

`sortBy` - `[EventSortBy!]`

The sortBy sorts the results based on the specific sort field order.

`to` - `Time`

The time to fetch events until this time(exclusive). If **to** is skipped, then **to** defaults to the current time.

`executiveReports` - `ExecutiveReportsWithPagination!`
 	
Arguments
 	
`filter` - `ExecutiveReportFilterInput`
 	
Input search criteria to filter results.
 	
`page` - `UnsignedInt32!` default = `1`
 	
Page number.
 	
`perPage` - `UnsignedInt32!` default = `50`
 	
Entries per page.
	Retrieves Executive Reports.

`formerlyKnownAs` - `String!`	Former Name of Company if applicable.
`id` - `String!`	Company ID.
`isReseller` - `Boolean!`	Indicates whether the company

	resells other companies.
`legacyProxies` - `[LegacyProxy!]`	List of legacy proxies based on filter options.
Arguments `filter` - `ProxyFilterInput`	
`managedObjects` - `[ManagedObject!]`	List of Managed Objects.
Arguments `filter` - `ManagedObjectFilterInput`	
`managementDomain` - `String!`	Management Domain name of the company.
`mfaPackage` - `MFAPackage`	Specifies Multi Factor Authentication configuration and Enablement for this company's users.
`oneTimeExecutiveReportConfigurations` - `OneTimeExecutiveReportConfigurationsWithPagination!`	Retrieves One time Executive Report Configurations.

Arguments
 	
`filter` - `ExecutiveReportConfigurationFilterInput`
 	
Input search criteria to filter results.
 	
`page` - `UnsignedInt32!` default = `1`
 	
Page number.
 	
`perPage` - `UnsignedInt32!` default = `50`
 	
Entries per page.	

`policies` - `[Policy!]`
 	
Arguments
 	
`filter` - `PolicyFilterInput`
	A list of policies based on filter options.

`proxies` - `[Proxy!]`
 	
Arguments
 	
`filter` - `ProxyFilterInput`
	A list of proxies based on filter options.

`proxyPackage` - `ProxyPackage`	Proxy Related information for the company.
`recurringExecutiveReportConfigurations` - `RecurringExecutiveReportConfigurationsWithPagination!`	Retrieves Recurring Executive Report Configurations.

Arguments

`filter` - `ExecutiveReportConfigurationFilterInput`

Input search criteria to filter results.

`page` - `UnsignedInt32!` default = `1`

Page number.

`perPage` - `UnsignedInt32!` default = `50`

Entries per page.

`resellBGP` - `Boolean!`	Indicates whether this company is a reseller of BGP related offerings.
`resellBot` - `Boolean!`	Indicates whether this company is a reseller of Bot related offerings.
`resellDetectionAndAlerting` - `Boolean!`	Indicates whether this company is a reseller of Detection and Alerting related offerings.
`resellProxy` - `Boolean!`	Indicates whether

	this company is a reseller of Proxy offerings.
`resellWAF` - `Boolean!`	Indicates whether this company is a reseller of Web Application Firewall related offerings.
`reseller` - `Company`	Details of company that is the reseller of this company.
`responderAnalytics` - `ResponderAnalyticsResponse`	WAF Responder Policy Log details.

Arguments

`filter` - `ResponderLogFilterInput`

If given, criteria to constrain the results queried.

`from` - `Time!`

The start time (inclusive) of the data to fetch.

`groupBy` - `ResponderLogGroupByInput`

If given, result will be grouped by the given criteria.

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`sortBy` - `[ResponderLogSortBy!]`

If given, result will be sorted in the given order.

`to` - `Time`

The end time (exclusive) of the data to fetch. Defaults to the current time.

`serviceProvider` - `String!`	Service Provider for the company.
`shortname` - `String!`	Short name of Company.
`technicalEmail` - `String!`	Company Technical contact Email.
`technicalFirstName` - `String!`	Company Technical contact First Name.
`technicalJobTitle` - `String!`	Company Technical contact Job Title.
`technicalLastName` - `String!`	Company Technical contact Last Name.
`technicalMobile` - `String!`	Company Technical contact

	Mobile number.
`technicalPhone` - `String!`	Company Technical contact phone number.
`tunnels` - `[Tunnel!]`	Tunnels connecting to the customer origin.
`updatedAt` - `Time!`	Timestamp the company entry was last updated at.
`users` - `UsersWithPagination!`	Returns all Users associated with this company.

Arguments
 	
`filter` - `CompanyUsersFilterInput`
 	
Reduce the list based on filtering criteria.
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `50`
 	
The maximum number of results to show per page.	

`wafAnalytics` - `WAFAnalyticsResponse`	WAF Violation Log details.

Arguments

`filter` - `ViolationLogFilterInput`

If given, criteria to constrain the results queried.

`from` - `Time!`

The start time (inclusive) of the events to fetch.

`groupBy` - `ViolationLogGroupByInput`

If given, result will be grouped by the given criteria.

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`sortBy` - `[ViolationLogSortBy!]`

If given, result will be sorted in the given order.

`to` - `Time`

The end time (exclusive) of the events to fetch. Defaults to the current time.

`whiteLabel` - `WhiteLabel`

Contains whitelabel specifications for this company.

Example

```
{
  "accountID": "abc123",
  "accountInfo": AccountInfo,
  "accountManagerEmail": "abc123",
  "accountManagerName": "xyz789",
  "allCustomers": CompaniesWithPagination,
  "apiPackage": APIAccess,
  "appDataAnalytics": [AppDataAnalyticsResponse],
```

```
  "auditLogTransactions": AuditLogTransactionsWithPagination,
  "bgpPackage": BGPPackage,
  "botAnalytics": BotAnalyticsResponse,
  "certificates": [Certificate],
  "configurationChanges": [ConfigurationChange],
  "corporateDomain": "abc123",
  "corporateName": "xyz789",
  "createdAt": Time,
  "customers": [Company],
  "dName": "abc123",
  "deleted": false,
  "destinationIPs": [CIDR],
  "details": CompanyDetails,
  "detectionAndAlertingPackage": DetectionAndAlertingPackage,
  "enabled": true,
  "event": Event,
  "events": EventsWithPagination,
  "executiveReports": ExecutiveReportsWithPagination,
  "formerlyKnownAs": "abc123",
  "id": "xyz789",
  "isReseller": true,
  "legacyProxies": [LegacyProxy],
  "managedObjects": [ManagedObject],
  "managementDomain": "xyz789",
  "mfaPackage": MFAPackage,
  "oneTimeExecutiveReportConfigurations":
OneTimeExecutiveReportConfigurationsWithPagination,
  "policies": [Policy],
  "proxies": [Proxy],
  "proxyPackage": ProxyPackage,
  "recurringExecutiveReportConfigurations":
RecurringExecutiveReportConfigurationsWithPagination,
  "resellBGP": true,
  "resellBot": false,
  "resellDetectionAndAlerting": false,
  "resellProxy": true,
  "resellWAF": false,
  "reseller": Company,
  "responderAnalytics": ResponderAnalyticsResponse,
  "serviceProvider": "abc123",
  "shortname": "abc123",
  "technicalEmail": "abc123",
  "technicalFirstName": "abc123",
  "technicalJobTitle": "abc123",
  "technicalLastName": "xyz789",
  "technicalMobile": "xyz789",
```

```
  "technicalPhone": "abc123",
  "tunnels": [Tunnel],
  "updatedAt": Time,
  "users": UsersWithPagination,
  "wafAnalytics": WAFAnalyticsResponse,
  "whiteLabel": WhiteLabel
}
```

Types

CompanyDetails

Company configuration details.

Field Name	Description
`dName` - `String!`	The unique, primary identifier for the company.
`ipiID` - `String`	Neustar IP Intelligence ID for this company.
`recursiveAccountID` - `String`	Neustar Recursive DNS Account ID for this company.
`recursiveSponsorID` - `String`	Neustar Recursive DNS Sponsor server ID for this company.
`ultraDNSAccountName` - `String`	Ultra DNS Account name for this company.
`ultraSecurityAccountID` - `String!`	Company portal Account ID.
`wpmAPIKey` - `String`	Web Performance Management API key for this company.

Example

```
{
  "dName": "abc123",
  "ipiID": "xyz789",
  "recursiveAccountID": "abc123",
  "recursiveSponsorID": "abc123",
  "ultraDNSAccountName": "xyz789",
  "ultraSecurityAccountID": "xyz789",
  "wpmAPIKey": "abc123"
}
```

Types

CompanyFilterInput

Filters queries for companies.

Input Field	Description
dName - String	A unique, primary identifier for a company.

Example

```
{"dName": "xyz789"}
```

Types

CompanyUsersFilterInput

Specify how to search Company users.

Input Field	Description
emailSubstring - String	Filter users by a specified substring in their email IDs.
includeDescendants - Boolean default = false	Indicates whether users from descendant companies should be included in query results.
includeDisabled - Boolean	Specifies whether disabled users belonging to company should be included in query results.
userNameSubstring - String	Filter users by a specified substring in their name (first and/or last name).

Example

```
{
  "emailSubstring": "xyz789",
  "includeDescendants": false,
  "includeDisabled": false,
  "userNameSubstring": "abc123"
}
```

Types

ConfigurationChange

A configuration change submitted to the controlling system(s).

Field Name	Description
company - Company!	Company the change belongs to.
createdAt - Time!	Time at which the change was created.
ended - Time	Time at which the change finished provisioning to devices.
id - String!	ID of the change.
started - Time	Time at which the change began provisioning to devices.
status - ConfigurationChangeStatus!	Current status of the config change.
statusText - String!	Additional status infomation about the config change.
updatedAt - Time!	Time at which the change was last updated.

Example

```
{
  "company": Company,
  "createdAt": Time,
  "ended": Time,
  "id": "xyz789",
  "started": Time,
  "status": ConfigurationChangeStatus,
  "statusText": "abc123",
  "updatedAt": Time
}
```

Types

ConfigurationChangeFilterInput

Input needed to get config changes.

Input Field	Description
latest - Boolean	Whether to only return the latest config change.

Example

```
{"latest": false}
```

Types

ConfigurationChangeStatus

List of possible ConfigurationChange statuses.

Enum Value	Description
COMPLETED_FAILURE	Completed, but failed.
COMPLETED_SUCCESS	Completed successfully.
IN_PROGRESS	In progress.
SUBMITTED	Submitted, but not yet processing.
UNKNOWN	Should never be encountered, used in manual adjustments only.

Types

ConfigurationChangesLock

The lock status of the configuration engine.

Field Name	Description
createdAt - Time!	Time at which the lock was created.
ended - Time	Time at which the lock ended.
id - String!	ID of the lock.
lockedBy - String!	User that created this lock.
started - Time!	Time at which the lock started.
unlockedBy - String	User that unlocked this lock.
updatedAt - Time!	Time at which the lock was updated.

Example

```
{
  "createdAt": Time,
  "ended": Time,
```

```
  "id": "abc123",
  "lockedBy": "abc123",
  "started": Time,
  "unlockedBy": "xyz789",
  "updatedAt": Time
}
```

Types

ConfigurationChangesLockResponse

The lock status of the configuration engine.

Field Name	Description
`status` - `ConfigurationChangesLockStatus!`	User that unlocked this lock.
`timestamp` - `Time!`	Time at which the status last changed.

Example

```
{
  "status": ConfigurationChangesLockStatus,
  "timestamp": Time
}
```

Types

ConfigurationChangesLockStatus

List of possible ConfigurationChangesLockResponse statuses.

Enum Value	Description
`LOCKED`	Locked
`UNKNOWN`	Should never be encountered, used in manual adjustments only.
`UNLOCKED`	Unlocked

Types

ConfiguredBaseBotSignature

A base Bot Detection signature configured to respond with a different action.

Field Name	Description
`action` - `BotSignatureAction!`	The signature action.
`enabled` - `Boolean!`	Whether the signature is enabled.
`signature` - `BaseBotSignature!`	The base signature being configured.

Example

```
{
  "action": BotSignatureAction,
  "enabled": false,
  "signature": BaseBotSignature
}
```

Types

`ConfiguredBaseBotSignatureInput`

Configure an action for a base Bot signature.

Input Field	Description
`action` - `BotSignatureAction!`	Action to be taken.
`enabled` - `Boolean!`	Whether the signature is enabled.
`id` - `String!`	ID of the signature.

Example

```
{
  "action": BotSignatureAction,
  "enabled": true,
  "id": "xyz789"
}
```

Types

`ConfiguredBaseWAFSignature`

A base WAF signature configured to respond with a different action.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.

`enabled` - `Boolean!`	Whether the signature is enabled.
`signature` - `BaseWAFSignature!`	The base signature being configured.

Example

```
{
  "action": WAFAction,
  "enabled": true,
  "signature": BaseWAFSignature
}
```

Types

`ConfiguredBaseWAFSignatureInput`

Configure an action for a base WAF signature.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`id` - `String!`	ID of the signature.

Example

```
{"action": WAFAction, "id": "xyz789"}
```

Types

`ConfiguredBaseWAFSignaturesWithPagination`

A paginated list of base WAF signatures with configured actions.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[ConfiguredBaseWAFSignature!]`	A list of signatures

Example

```
{
  "pageInfo": Pagination,
  "results": [ConfiguredBaseWAFSignature]
}
```

Types

ContentType

A content type countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`learn` - `Boolean!`	A flag to enable or disable learning.
`relaxationRules` - `ContentTypeRelaxationRulesWithPagination`	A paginated list of content type relaxation rules.

Arguments
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `1000`
 	
The maximum number of results to show per page.	

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for content type violations.

Example

```
{
  "action": WAFAction,
  "learn": true,
  "relaxationRules": ContentTypeRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

ContentTypeRelaxationRule

A content type relaxation rule.

Field Name	Description
`contentType` - `String!`	The content type to be exempted.
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.

Example

```
{"contentType": "abc123", "enabled": true}
```

Types

ContentTypeRelaxationRuleInput

A content type relaxation rule.

Input Field	Description
`contentType` - `String!`	The content type to be exempted.
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.

Example

```
{"contentType": "xyz789", "enabled": true}
```

Types

ContentTypeRelaxationRulesWithPagination

A paginated list for content type relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	Contains the current page information.
`results` - `[ContentTypeRelaxationRule!]`	A list of content type relaxation rules.

Example

```
{
  "pageInfo": Pagination,
```

```
  "results": [ContentTypeRelaxationRule]
}
```

Types

ContentTypeRuleCount

Content type rule count.

Field Name	Description
`count` - `UnsignedInt32!`	
`rule` - `LearnedContentTypeRule!`	

Example

```
{
  "count": UnsignedInt32,
  "rule": LearnedContentTypeRule
}
```

Types

ContentTypeRuleCountsWithPagination

Content type learning rules.

Field Name	Description
`pageInfo` - `Pagination!`	
`results` - `[ContentTypeRuleCount!]`	

Example

```
{
  "pageInfo": Pagination,
  "results": [ContentTypeRuleCount]
}
```

Types

CookieConsistency

Cookie consistency countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`learn` - `Boolean!`	A flag to enable or disable learning.
`relaxationRules` - `CookieConsistencyRelaxationRulesWithPagination`	A paginated list of relaxation rules.

Arguments
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `1000`
 	
The maximum number of results to show per page.	

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for cookie consistency violations.

Example

```
{
  "action": WAFAction,
  "learn": true,
  "relaxationRules": CookieConsistencyRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

`CookieConsistencyRelaxationRule`

A cookie consistency relaxation rule.

Field Name	Description
`cookieName` - `String`	The cookie name to be exempted.
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`isRegex` - `Boolean!`	Whether the cookie name is in regex format.

Example

```
{"cookieName": "xyz789", "enabled": true, "isRegex": false}
```

Types

`CookieConsistencyRelaxationRuleInput`

A cookie consistency relaxation rule.

Input Field	Description
`cookieName` - `String`	The cookie name to be exempted.
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.
`isRegex` - `Boolean!` default = `false`	Whether the cookie name is in regex format.

Example

```
{"cookieName": "xyz789", "enabled": true, "isRegex": false}
```

Types

`CookieConsistencyRelaxationRulesWithPagination`

A paginated list of cookie consistency relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[CookieConsistencyRelaxationRule!]`	A paginated list of relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [CookieConsistencyRelaxationRule]
}
```

Types

CookieConsistencyRuleCount

Cookie consistency rule count.

Field Name	Description
count - UnsignedInt32!	
rule - LearnedCookieConsistencyRule!	

Example

```
{
  "count": UnsignedInt32,
  "rule": LearnedCookieConsistencyRule
}
```

Types

CookieConsistencyRuleCountsWithPagination

Cookie consistency learning rules.

Field Name	Description
pageInfo - Pagination!	
results - [CookieConsistencyRuleCount!]	

Example

```
{
  "pageInfo": Pagination,
  "results": [CookieConsistencyRuleCount]
}
```

Types

CookieSignatureRule

A WAF custom signature cookie rule.

Field Name	Description

`cookieName` - `String`	The cookie name used in this rule.
`cookieNameFormat` - `SignatureRuleFormat!`	A cookie name format from the allowed list of formats.

Example

```
{
  "cookieName": "abc123",
  "cookieNameFormat": SignatureRuleFormat
}
```

Types

`CookieSignatureRuleInput`

Create a WAF custom signature cookie rule.

Input Field	Description
`cookieName` - `String`	The cookie name used in this rule.
`cookieNameFormat` - `SignatureRuleFormat!` default = `"ANY"`	A cookie name format from the allowed list of formats.

Example

```
{
  "cookieName": "abc123",
  "cookieNameFormat": "ANY"
}
```

Types

`Countermeasure`

Field Name	Description
`company` - `Company!`	The company object.
`id` - `String!`	The internal identifier for identifying a countermeasure.
`name` - `String!`	The name of the countermeasure.

Example

{"company": Company, "id": "abc123", "name": "abc123"}

Types

CountryCode

ISO 3166-1 alpha-2 country codes

Enum Value	Description
AD	Andorra
AE	United Arab Emirates
AF	Afghanistan
AG	Antigua and Barbuda
AI	Anguilla
AL	Albania
AM	Armenia
AN	Angola
AO	Netherlands Antilles
AQ	Antarctica
AR	Argentina
AS	American Samoa
AT	Austria
AU	Australia
AW	Aruba
AX	Åland Islands
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BD	Bangladesh
BE	Belgium
BF	Burkina Faso

BG	Bulgaria
BH	Bahrain
BI	Burundi
BJ	Benin
BL	Saint Barthélemy
BM	Bermuda
BN	Brunei Darussalam
BO	Bolivia (Plurinational State of)
BQ	Bonaire, Sint Eustatius and Saba
BR	Brazil
BS	Bahamas
BT	Bhutan
BV	Bouvet Island
BW	Botswana
BY	Belarus
BZ	Belize
CA	Canada
CC	Cocos (Keeling) Islands
CD	Congo, Democratic Republic of the
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CK	Cook Islands
CL	Chile
CM	Cameroon
CN	China
CO	Colombia

CR	Costa Rica
CU	Cuba
CV	Cabo Verde
CW	Curaçao
CX	Christmas Island
CY	Cyprus
CZ	Czechia
DE	Germany
DJ	Djibouti
DK	Denmark
DM	Dominica
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
EH	Western Sahara
ER	Eritrea
ES	Spain
ET	Ethiopia
FI	Finland
FJ	Fiji
FK	Falkland Islands (Malvinas)
FM	Micronesia (Federated States of)
FO	Faroe Islands
FR	France
FX	Gabon
GA	France, Metropolitan

GB	United Kingdom of Great Britain and Northern Ireland
GD	Grenada
GE	Georgia
GF	French Guiana
GG	Guernsey
GH	Ghana
GI	Gibraltar
GL	Greenland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Equatorial Guinea
GR	Greece
GS	South Georgia and the South Sandwich Islands
GT	Guatemala
GU	Guam
GW	Guinea-Bissau
GY	Guyana
HK	Hong Kong
HM	Heard Island and McDonald Islands
HN	Honduras
HR	Croatia
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IM	Isle of Man

IN	India
IO	British Indian Ocean Territory
IQ	Iraq
IR	Iran (Islamic Republic of)
IS	Iceland
IT	Italy
JE	Jersey
JM	Jamaica
JO	Jordan
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KH	Cambodia
KI	Kiribati
KM	Comoros
KN	Saint Kitts and Nevis
KP	Korea (Democratic People's Republic of)
KR	Korea, Republic of
KW	Kuwait
KY	Cayman Islands
KZ	Kazakhstan
LA	Lao People's Democratic Republic
LB	Lebanon
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho

LT	Lithuania
LU	Luxembourg
LV	Latvia
LY	Libya
MA	Morocco
MC	Monaco
MD	Moldova, Republic of
ME	Montenegro
MF	Saint Martin (French part)
MG	Madagascar
MH	Marshall Islands
MK	North Macedonia
ML	Mali
MM	Myanmar
MN	Mongolia
MO	Macao
MP	Northern Mariana Islands
MQ	Martinique
MR	Mauritania
MS	Montserrat
MT	Malta
MU	Mauritius
MV	Maldives
MW	Malawi
MX	Mexico
MY	Malaysia
MZ	Mozambique
NA	Namibia

NC	New Caledonia
NE	Niger
NF	Norfolk Island
NG	Nigeria
NI	Nicaragua
NL	Netherlands
NO	Norway
NP	Nepal
NR	Nauru
NU	Niue
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PF	French Polynesia
PG	Papua New Guinea
PH	Philippines
PK	Pakistan
PL	Poland
PM	Saint Pierre and Miquelon
PN	Pitcairn
PR	Puerto Rico
PS	Palestine, State of
PT	Portugal
PW	Palau
PY	Paraguay
QA	Qatar
RE	Réunion

RO	Romania
RS	Serbia
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
SB	Solomon Islands
SC	Seychelles
SD	Sudan
SE	Sweden
SG	Singapore
SH	Saint Helena, Ascension and Tristan da Cunha
SI	Slovenia
SJ	Svalbard and Jan Mayen
SK	Slovakia
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia
SR	Suriname
SS	South Sudan
ST	Sao Tome and Principe
SV	El Salvador
SX	Sint Maarten (Dutch part)
SY	Syrian Arab Republic
SZ	Eswatini
TC	Turks and Caicos Islands
TD	Chad
TF	French Southern Territories

TG	Togo
TH	Thailand
TJ	Tajikistan
TK	Tokelau
TL	Timor-Leste
TM	Turkmenistan
TN	Tunisia
TO	Tonga
TP	Turkey
TR	East Timor
TT	Trinidad and Tobago
TV	Tuvalu
TW	Taiwan, Province of China
TZ	Tanzania, United Republic of
UA	Ukraine
UG	Uganda
UM	United States Minor Outlying Islands
US	United States of America
UY	Uruguay
UZ	Uzbekistan
VA	Holy See
VC	Saint Vincent and the Grenadines
VE	Venezuela (Bolivarian Republic of)
VG	Virgin Islands (British)
VI	Virgin Islands (U.S.)
VN	Viet Nam
VU	Vanuatu
WF	Wallis and Futuna

`WS`	Samoa
`YE`	Yemen
`YT`	Mayotte
`ZA`	South Africa
`ZM`	Zambia
`ZW`	Zimbabwe

Types

`CreateBotBlackListInput`

Create a black list countermeasure.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the black list countermeasure is enabled.
`types` - `[BotBlackListBindingInput!]`	List of black list bindings.

Example

```
{"enabled": true, "types": [BotBlackListBindingInput]}
```

Types

`CreateBotCAPTCHAInput`

Create a CAPTCHA countermeasure.

Input Field	Description
`resources` - `[BotCAPTCHABindingInput!]`	List of CAPTCHA bindings.

Example

```
{"resources": [BotCAPTCHABindingInput]}
```

Types

`CreateBotDeviceFingerprintInput`

Create a device fingerprint countermeasure.

Input Field	Description
`action` - `BotDeviceFingerprintAction`	Action to be taken. Can only be set if response is ACTION_AND_LOG.
`enabled` - `Boolean!` default = `true`	Whether the device fingerprint countermeasure is enabled.
`response` - `BotResponse!`	Response to be taken.

Example

```
{
  "action": BotDeviceFingerprintAction,
  "enabled": true,
  "response": BotResponse
}
```

Types

`CreateBotIPReputationInput`

Create an IP reputation countermeasure.

Input Field	Description
`categories` - `[BotIPReputationBindingInput!]`	List of IP reputation bindings.
`enabled` - `Boolean!` default = `true`	Whether the IP reputation countermeasure is enabled.

Example

```
{
  "categories": [BotIPReputationBindingInput],
  "enabled": true
}
```

Types

`CreateBotProfileInput`

Create a new bot profile.

Input Field	Description

`blackList` - `CreateBotBlackListInput`	The black list countermeasure settings.
`botTrap` - `CreateBotTrapInput`	The bot trap countermeasure settings.
`captcha` - `CreateBotCAPTCHAInput`	The CAPTCHA countermeasure settings.
`deviceFingerprint` - `CreateBotDeviceFingerprintInput`	The device fingerprint countermeasure settings.
`enabled` - `Boolean!` default = `true`	Whether the bot profile is enabled.
`ipReputation` - `CreateBotIPReputationInput`	The IP reputation countermeasure settings.
`rateLimit` - `CreateBotRateLimitInput`	The rate limit countermeasure settings.
`signatures` - `CreateBotSignaturesInput`	The bot signatures settings.
`tps` - `CreateBotTPSInput`	The TPS countermeasure settings.
`whiteList` - `CreateBotWhiteListInput`	The white list countermeasure settings.

Example

```
{
  "blackList": CreateBotBlackListInput,
  "botTrap": CreateBotTrapInput,
  "captcha": CreateBotCAPTCHAInput,
  "deviceFingerprint": CreateBotDeviceFingerprintInput,
  "enabled": true,
  "ipReputation": CreateBotIPReputationInput,
  "rateLimit": CreateBotRateLimitInput,
  "signatures": CreateBotSignaturesInput,
  "tps": CreateBotTPSInput,
  "whiteList": CreateBotWhiteListInput
}
```

Types

`CreateBotRateLimitInput`

Create a rate limit countermeasure.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the rate limit countermeasure is enabled.
`resources` - `[BotRateLimitBindingInput!]`	List of rate limit bindings.

Example

```
{"enabled": true, "resources": [BotRateLimitBindingInput]}
```

Types

CreateBotSignaturesInput

Create bot signatures.

Input Field	Description
`configuredBaseSignatures` - `[ConfiguredBaseBotSignatureInput!]`	List of bot signatures.
`enabled` - `Boolean!` default = `true`	Whether bot signatures are enabled.

Example

```
{
  "configuredBaseSignatures": [
    ConfiguredBaseBotSignatureInput
  ],
  "enabled": true
}
```

Types

CreateBotTPSInput

Create a TPS countermeasure.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the TPS countermeasure is enabled.
`resources` - `[BotTPSBindingInput!]`	List of TPS bindings.

Example

```
{"enabled": true, "resources": [BotTPSBindingInput]}
```

Types

CreateBotTrapInput

Create a bot trap countermeasure.

Input Field	Description
`action` - `BotTrapAction`	Action to be taken. Can only be set if response is ACTION_AND_LOG.
`enabled` - `Boolean!` default = `true`	Whether the bot trap countermeasure is enabled.
`insertionURLs` - `[BotTrapBindingInput!]`	List of bot trap bindings.
`response` - `BotResponse!`	Response to be taken.

Example

```
{
  "action": BotTrapAction,
  "enabled": true,
  "insertionURLs": [BotTrapBindingInput],
  "response": BotResponse
}
```

Types

CreateBotWhiteListInput

Create a white list countermeasure.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the white list countermeasure is enabled.
`types` - `[BotWhiteListBindingInput!]`	List of white list bindings.

Example

```
{"enabled": true, "types": [BotWhiteListBindingInput]}
```

Types

CreateBufferOverflowInput

Create a buffer overflow countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`maxCookieLength` - `UnsignedInt16!` default = `4096`	Maximum cookie length (in character, allowed range 0-65535) in requests to the protected web sites. Requests with longer cookie lengths will be blocked.
`maxHeaderLength` - `UnsignedInt16!` default = `4096`	Maximum HTTP header length (in characters, allowed range 0-65535) in requests to the protected web sites. Requests with longer headers will be blocked.
`maxURLLength` - `UnsignedInt16!` default = `1024`	Maximum URL length (in characters, allowed range 0-65535) of the protected web sites. Requests with longer URLs will be blocked.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for buffer overflow violations.

Example

```
{
  "action": WAFAction,
  "maxCookieLength": 4096,
  "maxHeaderLength": 4096,
  "maxURLLength": 1024,
  "threshold": ThresholdInput
}
```

Types

CreateCSRFSettingsInput

Create a cross-site request forgery countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.

`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`relaxationRules` - `[CSRFRelaxationRuleInput!]`	A list of CSRF relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for CSRF violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "relaxationRules": [CSRFRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

`CreateCertificateInput`

Create a certificate.

Input Field	Description
`certPEM` - `String!`	Public certificate, and any intermediate, together in PEM format.
`companyDName` - `String`	The identifier of the owning company.
`keyPEM` - `String!`	Private key, in PEM format.
`keyPass` - `String`	Password, only required if keyPEM is encrypted.
`name` - `String!`	Name of the certificate.

Example

```
{
  "certPEM": "abc123",
  "companyDName": "xyz789",
  "keyPEM": "abc123",
  "keyPass": "xyz789",
  "name": "xyz789"
}
```

Types

CreateCertificateOutput

Output from creating a certificate.

Field Name	Description
`certificate` - `Certificate!`	The created Certificate.

Example

```
{"certificate": Certificate}
```

Types

CreateCommandInjectionInput

Create a command injection countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`commandInjectionType` - `CommandInjectionType!`	A command injection type.
`relaxationRules` - `[CommandInjectionRelaxationRuleInput!]`	A list of command injection relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for command injection violations.

Example

```
{
  "action": WAFAction,
  "commandInjectionType": CommandInjectionType,
  "relaxationRules": [
    CommandInjectionRelaxationRuleInput
  ],
  "threshold": ThresholdInput
}
```

Types

CreateContentTypeInput

Create a content type countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`relaxationRules` - `[ContentTypeRelaxationRuleInput!]`	A list of content type relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for content type violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "relaxationRules": [ContentTypeRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

CreateCookieConsistencyInput

Create a cookie consistency countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`relaxationRules` - `[CookieConsistencyRelaxationRuleInput!]`	A list of relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for cookie consistency violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "relaxationRules": [
    CookieConsistencyRelaxationRuleInput
  ],
  "threshold": ThresholdInput
}
```

Types

`CreateDenyURLInput`

Create a deny URL countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`regexRules` - `[DenyURLRuleInput!]`	A list of deny URL regex rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for deny URL violations.

Example

```
{
  "action": WAFAction,
  "regexRules": [DenyURLRuleInput],
  "threshold": ThresholdInput
}
```

Types

`CreateFieldFormatInput`

Create a field format countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`enforcementRules` - `[FieldFormatEnforcementRuleInput!]`	A list of enforcement rules. These are tightening rules, in

	order to relax some rules you need to remove them from this list.
`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`maxLength` - `UnsignedInt16!` default = `65535`	Maximum length of the field (in characters, allowed range 0-65535). Please note that distinguishing an integer from an alpha character requires at least one character.
`minLength` - `UnsignedInt16!` default = `0`	Minimum length of the field (in characters, allowed range 0-65535). Please note that distinguishing an integer from an alpha character requires at least one character.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for field format violations.
`type` - `FieldFormatType!`	Allowed types for this field.

Example

```
{
  "action": WAFAction,
  "enforcementRules": [FieldFormatEnforcementRuleInput],
  "learn": false,
  "maxLength": 65535,
  "minLength": 0,
  "threshold": ThresholdInput,
  "type": FieldFormatType
}
```

Types

CreateFormFieldConsistencyInput

Create a form field consistency countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`fieldConsistencyExemptions` - `[FormFieldConsistencyRuleInput!]`	A list of exemption rules.
`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`sessionlessFieldConsistency` - `SessionlessFieldConsistency!`	When turned on, it checks only the web form structure.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for form field consistency violations.

Example

```
{
  "action": WAFAction,
  "fieldConsistencyExemptions": [
    FormFieldConsistencyRuleInput
  ],
  "learn": false,
  "sessionlessFieldConsistency": SessionlessFieldConsistency,
  "threshold": ThresholdInput
}
```

Types

CreateHTMLSQLInjectionInput

Create an HTML SQL injection countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`checkSQLWildChars` - `Boolean!`	Whether to check for form fields that contain SQL wild chars.
`exemptCommentsWith` - `CommentExemption!`	Exempts all comments of the given type.
`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`relaxationRules` - `[HTMLSQLInjectionRelaxationRuleInput!]`	A list of XML SQL injection relaxation rules.
`sqlInjectionType` - `SQLInjectionType!`	A SQL injection type.
`sqliGrammar` - `Boolean!`	Enable SQL Injection grammar
`threshold` - `ThresholdInput`	Appsec Threshold configuration for HTML SQL injection violations.

Example

```
{
  "action": WAFAction,
  "checkSQLWildChars": true,
  "exemptCommentsWith": CommentExemption,
  "learn": false,
  "relaxationRules": [
    HTMLSQLInjectionRelaxationRuleInput
  ],
  "sqlInjectionType": SQLInjectionType,
  "sqliGrammar": true,
  "threshold": ThresholdInput
}
```

Types

CreateHTMLXSSInput

Create an HTML cross-site scripting countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`checkCompleteURLs` - `Boolean!` default = `false`	A flag to enforce checks for complete URLs for cross-site scripts, instead of just the query portions of URLs.
`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`relaxationRules` - `[HTMLXSSRelaxationRuleInput!]`	A list of HTML cross-site scripting relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for HTML cross-site scripting violations.

Example

```
{
  "action": WAFAction,
  "checkCompleteURLs": false,
  "learn": false,
  "relaxationRules": [HTMLXSSRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

CreateHTTPRFCProfileInput

Create an HTTP RFC Profile countermeasure.

Input Field	Description
`action` - `HTTPRFCProfileAction!` default = `"BLOCK"`	Action to be taken when there is a non-compliant request.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for HTTP RFC violations.

Example

```
{
  "action": "BLOCK",
  "threshold": ThresholdInput
}
```

Types

CreateJSONCommandInjectionSettingsInput

Create a JSON command injection Settings Input.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`commandInjectionType` - `CommandInjectionType!`	A Command injection type.
`relaxationRules` - `[JSONCommandInjectionRelaxationRuleInput!]`	A list of command injection rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for json command injection violations.

Example

```
{
  "action": WAFAction,
  "commandInjectionType": CommandInjectionType,
  "relaxationRules": [
    JSONCommandInjectionRelaxationRuleInput
  ],
  "threshold": ThresholdInput
}
```

Types

CreateJSONCrossSiteScriptingSettingsInput

Create a JSON cross-site scripting settings input to protect applications from XSS Attacks through JSON requests

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`relaxationRules` - `[JSONXSSRelaxationRuleInput!]`	A list of JSON XSS rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for JSON XSS violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": [JSONXSSRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

CreateJSONDenialOfServiceSettingsInput

Create a JSON Denial of Service Settings input to protect applications from Denial of Service Attacks through JSON requests

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`enforcementRule` - `JSONDoSEnforcementRuleInput`	A paginated list of SQL Injection rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for JSON DOS violations.

Example

```
{
  "action": WAFAction,
  "enforcementRule": JSONDoSEnforcementRuleInput,
  "threshold": ThresholdInput
}
```

Types

CreateJSONSQLInjectionSettingsInput

Create a JSON SQL Injection Settings input to protect applications from SQL Injection attacks through JSON requests

Input Field	Description
action - WAFAction!	Action to be taken.
relaxationRules - [JSONSQLInjectionRelaxationRuleInput!]	A paginated list of SQL Injection rules.
sqlInjectionType - SQLInjectionType!	A SQL injection type.
sqliGrammar - Boolean!	Enable SQL Injection grammar.
threshold - ThresholdInput	Appsec Threshold configuration for JSON SQL injection violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": [
    JSONSQLInjectionRelaxationRuleInput
  ],
  "sqlInjectionType": SQLInjectionType,
  "sqliGrammar": true,
  "threshold": ThresholdInput
}
```

Types

CreateJSONSettingsInput

Create a JSON Security Settings input to protect JSON Applications

Input Field	Description

`jsonCommandInjectionSettings` - `CreateJSONCommandInjectionSettingsInput`	JSON Command Injection Settings.
`jsonCrossSiteScriptingSettings` - `CreateJSONCrossSiteScriptingSettingsInput`	JSON Cross Site Scripting Settings.
`jsonDenialOfServiceSettings` - `CreateJSONDenialOfServiceSettingsInput`	JSON Denial Of Service Settings.
`jsonSQLInjectionSettings` - `CreateJSONSQLInjectionSettingsInput`	JSON SQL Injection Settings.

Example

```
{
  "jsonCommandInjectionSettings": CreateJSONCommandInjectionSettingsInput,
  "jsonCrossSiteScriptingSettings": CreateJSONCrossSiteScriptingSettingsInput,
  "jsonDenialOfServiceSettings": CreateJSONDenialOfServiceSettingsInput,
  "jsonSQLInjectionSettings": CreateJSONSQLInjectionSettingsInput
}
```

Types

`CreateNetworkControlsInput`

Create network controls.

Input Field	Description
`blockedCountries` - `[CountryCode!]`	A list of blocked countries.
`ipFilterList` - `[IPFilterInput!]`	A list of ip filters.

Example

```
{
  "blockedCountries": [CountryCode],
  "ipFilterList": [IPFilterInput]
}
```

Types

CreateOneTimeExecutiveReportConfigurationInput

Input Configuration to create a one time reporting job.

Input Field	Description
dName - String!	The unique, primary identifier for the company.
description - String	Description of Report Configuration.
enabled - Boolean default = true	Specifies whether this configuration should generate reports or not.
from - Time!	Specifies the start of time range from when to pull metrics data for the requested features.
includeBot - Boolean	Specifies whether to include Bot detection/mitigation metrics in generated report.
includeDDOS - Boolean	Specifies whether to include DDOS mitigation metrics in generated report.
includeWAF - Boolean	Specifies whether to include WAF violation metrics in generated report.
name - String!	Name of Report Configuration.
notification - ExecutiveReportNotificationDetailsInput	Contains email addresses of recipients of generated report.
to - Time!	Specifies the end of time range until when

	to pull metrics data for the requested features.

Example

```
{
  "dName": "xyz789",
  "description": "xyz789",
  "enabled": true,
  "from": Time,
  "includeBot": true,
  "includeDDOS": true,
  "includeWAF": false,
  "name": "xyz789",
  "notification": ExecutiveReportNotificationDetailsInput,
  "to": Time
}
```

Types

`CreateOneTimeExecutiveReportConfigurationOutput`

Output of creation of a one time report configuration.

Field Name	Description
`configuration` - `OneTimeExecutiveReportConfiguration!`	One time reporting configuration

Example

```
{"configuration": OneTimeExecutiveReportConfiguration}
```

Types

`CreatePOSTBodyInput`

Create a POST BODY limit countermeasure.

Input Field	Description
`limit` - `UnsignedInt32!` default = `4294967295`	A post body size limit value.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for post body limit violations.

Example

```
{"limit": 4294967295, "threshold": ThresholdInput}
```

Types

CreatePolicyInput

Create a Policy.

Input Field	Description
appSecThresholds - [AppSecThresholdInput!]	The appsec thresholds associated to this policy.
botProfile - CreateBotProfileInput	The bot profile associated to this policy.
companyDName - String	The identifier of the owning company.
name - String!	The name of the policy.
networkControls - CreateNetworkControlsInput	The network controls associated to this policy.
responderPolicies - [ResponderPolicyInput!]	The responder polices associated to this policy.
trustedSources - [TrustedSourceInput!]	The trusted IP sources associated to this policy. Traffic at these sources are used by the learning feature to generate recommendations.
wafProfile - CreateWAFProfileInput	The WAF profile associated to this policy.

Example

```
{
  "appSecThresholds": [AppSecThresholdInput],
  "botProfile": CreateBotProfileInput,
  "companyDName": "xyz789",
  "name": "abc123",
  "networkControls": CreateNetworkControlsInput,
  "responderPolicies": [ResponderPolicyInput],
  "trustedSources": [TrustedSourceInput],
  "wafProfile": CreateWAFProfileInput
```

```
}
```

Types

CreatePolicyOutput

Returned when creating a policy.

Field Name	Description
`policy` - `Policy!`	The created policy.

Example

```
{"policy": Policy}
```

Types

CreateProxyInput

Create a proxy.

Input Field	Description
`companyDName` - `String`	Company the proxy configuration belongs to.
`ipVersion` - `IPVersion!`	The IP version of this host.
`name` - `String!`	Friendly name of the proxy configuration. Typically set to the hostname being proxied to the service.
`policyIDs` - `[String!]`	A list of policies associated with this proxy.
`vServers` - `[VServerInput!]`	The back-end origin servers, ports and protocols that bind it to the front-end port.

Example

```
{
  "companyDName": "abc123",
  "ipVersion": IPVersion,
  "name": "xyz789",
  "policyIDs": ["xyz789"],
  "vServers": [VServerInput]
}
```

Types

`CreateProxyOutput`

Output from creating a proxy.

Field Name	Description
`proxy` - `Proxy!`	The created proxy.

Example

```
{"proxy": Proxy}
```

Types

`CreateRecurringExecutiveReportConfigurationInput`

Input for a create recurring report configuration operation.

Input Field	Description
`dName` - `String!`	The unique, primary identifier for the company.
`description` - `String`	Description of Report Configuration.
`enabled` - `Boolean` default = `true`	Specifies whether this configuration should generate reports or not.
`from` - `Time`	Specifies the time when the first report should be generated.
`includeBot` - `Boolean`	Specifies whether to include Bot detection/mitigation metrics in generated report.
`includeDDOS` - `Boolean`	Specifies whether to include DDOS mitigation metrics in generated report.

`includeWAF` - `Boolean`	Specifies whether to include WAF violation metrics in generated report.
`name` - `String!`	Name of Report Configuration.
`notification` - `ExecutiveReportNotificationDetailsInput`	Contains email addresses of recipients of generated report.
`period` - `ExecutiveReportPeriodInput!`	Specifies the time period for which metrics need to be looked up for the requested features.
`to` - `Time`	Specifies the time when the last report in this series should be generated. The configuration expires after this time.

Example

```
{
  "dName": "abc123",
  "description": "xyz789",
  "enabled": true,
  "from": Time,
  "includeBot": true,
  "includeDDOS": true,
  "includeWAF": false,
  "name": "xyz789",
  "notification": ExecutiveReportNotificationDetailsInput,
  "period": ExecutiveReportPeriodInput,
  "to": Time
}
```

Types

`CreateRecurringExecutiveReportConfigurationOutput`

Represents output of a create recurring executive report configuration operation.

Field Name	Description
`configuration` - `RecurringExecutiveReportConfiguration!`	Configuration of recurring report job.

Example

```
{"configuration": RecurringExecutiveReportConfiguration}
```

Types

`CreateSemicolonFieldSeparatorInput`

Create a Semicolon field separator countermeasure.

Input Field	Description
`enabled` - `Boolean!` default = `false`	Whether the countermeasure is enabled.

Example

```
{"enabled": false}
```

Types

`CreateUserInput`

Create a User.

Input Field	Description
`company` - `String!`	Company.
`email` - `String!`	User email.
`firstName` - `String!`	First name.
`jobTitle` - `String`	Job title.
`lastName` - `String!`	Last name.
`mobile` - `String`	Mobile number.
`phone` - `String`	Phone number.
`roles` - `[UserRole!]!`	Roles.

Example

```
{
  "company": "xyz789",
  "email": "xyz789",
  "firstName": "abc123",
  "jobTitle": "xyz789",
  "lastName": "xyz789",
  "mobile": "abc123",
  "phone": "abc123",
  "roles": [UserRole]
}
```

Types

`CreateUserOutput`

Returned when creating a user.

Field Name	Description
`user` - `User!`	The created user.

Example

```
{"user": User}
```

Types

`CreateWAFProfileInput`

Create a WAF profile.

Input Field	Description
`bufferOverflow` - `CreateBufferOverflowInput`	The buffer overflow countermeasure settings.
`commandInjection` - `CreateCommandInjectionInput`	The Command Injection countermeasure settings.
`contentType` - `CreateContentTypeInput`	The content type countermeasure settings.

`cookieConsistency` - `CreateCookieConsistencyInput`	The cookie consistency countermeasure settings.
`crossSiteScripting` - `CreateHTMLXSSInput`	The HTML cross-site scripting countermeasure settings.
`csrfSettings` - `CreateCSRFSettingsInput`	The CSRF countermeasure settings.
`denyURL` - `CreateDenyURLInput`	The deny URL countermeasure settings.
`enabled` - `Boolean!` default = `true`	Whether the WAF profile is enabled.
`fieldConsistency` - `CreateFormFieldConsistencyInput`	The form field consistency countermeasure settings.
`fieldFormat` - `CreateFieldFormatInput`	The field format countermeasure settings.
`htmlSQLInjection` - `CreateHTMLSQLInjectionInput`	The HTML SQL Injection countermeasure settings.
`httpRFCProfile` - `CreateHTTPRFCProfileInput`	Check requests for HTTP RFC non compliance.
`jsonSettings` - `CreateJSONSettingsInput`	The JSON related countermeasure settings.

`postBody` - `CreatePOSTBodyInput`	Limits the request payload size.
`semicolonFieldSeparator` - `CreateSemicolonFieldSeparatorInput`	Allow or disallow semicolon field separator between request fields.
`signatures` - `CreateWAFSignaturesInput`	The WAF signatures settings.
`wsiSettings` - `CreateWSISettingsInput`	The web service interoperability countermeasure settings.
`xmlCrossSiteScripting` - `CreateXMLXSSInput`	The XML cross-site scripting countermeasure settings.
`xmlFormat` - `CreateXMLFormatInput`	The XML format countermeasure settings.
`xmlSOAPFault` - `CreateXMLSOAPFaultInput`	The XML SOAP fault countermeasure settings.
`xmlSQLInjection` - `CreateXMLSQLInjectionInput`	The XML SQL Injection countermeasure settings.

Example

```
{
  "bufferOverflow": CreateBufferOverflowInput,
  "commandInjection": CreateCommandInjectionInput,
  "contentType": CreateContentTypeInput,
  "cookieConsistency": CreateCookieConsistencyInput,
```

```
  "crossSiteScripting": CreateHTMLXSSInput,
  "csrfSettings": CreateCSRFSettingsInput,
  "denyURL": CreateDenyURLInput,
  "enabled": true,
  "fieldConsistency": CreateFormFieldConsistencyInput,
  "fieldFormat": CreateFieldFormatInput,
  "htmlSQLInjection": CreateHTMLSQLInjectionInput,
  "httpRFCProfile": CreateHTTPRFCProfileInput,
  "jsonSettings": CreateJSONSettingsInput,
  "postBody": CreatePOSTBodyInput,
  "semicolonFieldSeparator": CreateSemicolonFieldSeparatorInput,
  "signatures": CreateWAFSignaturesInput,
  "wsiSettings": CreateWSISettingsInput,
  "xmlCrossSiteScripting": CreateXMLXSSInput,
  "xmlFormat": CreateXMLFormatInput,
  "xmlSOAPFault": CreateXMLSOAPFaultInput,
  "xmlSQLInjection": CreateXMLSQLInjectionInput
}
```

Types

CreateWAFSignaturesInput

Create WAF signatures for a Policy.

Input Field	Description
`configuredBaseSignatures` - `[ConfiguredBaseWAFSignatureInput!]`	A list of signatures for a policy configured from a list of available base signatures.
`customSignatures` - `[CustomWAFSignatureInput!]`	A list of custom signatures created for a policy.

Example

```
{
  "configuredBaseSignatures": [
    ConfiguredBaseWAFSignatureInput
  ],
```

```
  "customSignatures": [CustomWAFSignatureInput]
}
```

Types

CreateWSISettingsInput

Create a web services interoperability countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`learn` - `Boolean!` default = `false`	A flag to enable or disable learning.
`standards` - `[WSIStandardInput!]`	A list of WSI standards.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for WSI violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "standards": [WSIStandardInput],
  "threshold": ThresholdInput
}
```

Types

CreateXMLFormatInput

Create an XML format countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML format violations.

Example

```
{
  "action": WAFAction,
  "threshold": ThresholdInput
```

```
}
```

Types

CreateXMLSOAPFaultInput

Create an XML SOAP fault countermeasure.

Input Field	Description
`action` - `XMLSOAPFaultAction!`	Action to be taken.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML format violations.

Example

```
{
  "action": XMLSOAPFaultAction,
  "threshold": ThresholdInput
}
```

Types

CreateXMLSQLInjectionInput

Create an HTML SQL injection countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`checkSQLWildChars` - `Boolean!`	Whether to check for form fields that contain SQL wild chars.
`exemptCommentsWith` - `CommentExemption!`	Exempts all comments of the given type.
`relaxationRules` - `[XMLSQLInjectionRelaxationRuleInput!]`	A list of XML SQL injection relaxation rules.
`sqlInjectionType` - `SQLInjectionType!`	An XML SQL injection type.

`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML SQL injection violations.

Example

```
{
  "action": WAFAction,
  "checkSQLWildChars": true,
  "exemptCommentsWith": CommentExemption,
  "relaxationRules": [XMLSQLInjectionRelaxationRuleInput],
  "sqlInjectionType": SQLInjectionType,
  "threshold": ThresholdInput
}
```

Types

`CreateXMLXSSInput`

Create an XML cross-site scripting countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`relaxationRules` - `[XMLXSSRelaxationRuleInput!]`	A list of XML cross-site scripting relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML cross-site scripting violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": [XMLXSSRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

`CustomWAFSignature`

A WAF custom signature.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`category` - `String!`	Category of the signature.
`description` - `String!`	Description of the signature.
`requestRules` - `[SignatureRequestRule!]`	List of request rules.
`responseRules` - `[SignatureResponseRule!]`	List of response rules.

Example

```
{
  "action": WAFAction,
  "category": "xyz789",
  "description": "abc123",
  "requestRules": [SignatureRequestRule],
  "responseRules": [SignatureResponseRule]
}
```

Types

`CustomWAFSignatureFilterInput`

Filter a list of custom WAF signatures.

Input Field	Description
`category` - `String`	Category to filter the signatures by.
`search` - `String`	Substring to search in description and other text, etc.

Example

```
{"category": "abc123", "search": "abc123"}
```

Types

`CustomWAFSignatureInput`

Specify a WAF custom signature.

Input Field	Description

`action` - `WAFAction!`	Action to be taken.
`category` - `String!`	Category of the signature.
`description` - `String!`	Description of the signature.
`requestRules` - `[SignatureRequestRuleInput!]`	List of request rules.
`responseRules` - `[SignatureResponseRuleInput!]`	List of response rules.

Example

```
{
  "action": WAFAction,
  "category": "abc123",
  "description": "abc123",
  "requestRules": [SignatureRequestRuleInput],
  "responseRules": [SignatureResponseRuleInput]
}
```

Types

`CustomWAFSignaturesWithPagination`

A list of WAF custom signatures with pagination.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[CustomWAFSignature!]`	A list of custom signatures.

Example

```
{
  "pageInfo": Pagination,
  "results": [CustomWAFSignature]
}
```

Types

`CustomerFilterInput`

Filters queries for customers.

Input Field	Description

`activationState` - `FeatureActivationState`	Filter to specify whether the requested feature on which search is carried out is purchased and/or enabled in the portal.
`bgpAlwaysOn` - `FeatureActivationState`	Filter to include companies that have the BGP Always On offering purchased and/or enabled in the portal.
`bgpOnDemand` - `FeatureActivationState`	Filter to include companies that have the BGP On Demand offering purchased and/or enabled in the portal.
`corporateNameSubstring` - `String`	Search for companies with the same substring in their corporateName.
`dNamePrefix` - `String`	Prefix to search for companies with the same substring prefix in their dNames.
`detectionAndAlertingActivation` - `FeatureActivationState`	Filter to include companies that have the Detection and Alerting offering purchased and/or enabled in the portal.
`includeDeleted` - `Boolean!` default = `false`	Specifies whether deleted companies should be included in the query results.
`includeDisabled` - `Boolean!` default = `false`	Specifies whether companies disabled in the portal should be included in the query results.

`maxDepth` - `Int!` default = `0`	Specifies how many levels of resellers or companies of resellers should be retrieved. A value of zero will retrieve all levels.
`proxyActivation` - `FeatureActivationState`	Filter to include companies that have the L7 Proxy offering purchased and/or enabled in the portal.
`wafActivation` - `FeatureActivationState`	Filter to include companies that have the Web Application Firewall offering purchased and/or enabled in the portal.

Example

```
{
  "activationState": FeatureActivationState,
  "bgpAlwaysOn": FeatureActivationState,
  "bgpOnDemand": FeatureActivationState,
  "corporateNameSubstring": "abc123",
  "dNamePrefix": "abc123",
  "detectionAndAlertingActivation": FeatureActivationState,
  "includeDeleted": false,
  "includeDisabled": false,
  "maxDepth": 0,
  "proxyActivation": FeatureActivationState,
  "wafActivation": FeatureActivationState
}
```

Types

`DDOSCountermeasure`

Represents a DDOS countermeasure.

Field Name	Description

`company` - `Company!`	The company object.
`id` - `String!`	The internal identifier for identifying a countermeasure.
`name` - `String!`	The name of the countermeasure.
`trafficData` - `[TrafficData!]`	The DDOS countermeasure traffic data.

Example

```
{
  "company": Company,
  "id": "xyz789",
  "name": "abc123",
  "trafficData": [TrafficData]
}
```

Types

DDOSFilter

Filters used with Mitigations

Field Name	Description
`id` - `String!`	Identifier of the filter.
`name` - `String!`	DDOS filter name.

Example

```
{"id": "abc123", "name": "abc123"}
```

Types

DDOSMitigation

Mitigations for DDOS attacks.

Field Name	Description
`activeDestinationIPs` - `[CIDR!]`	The active destinations.
`company` - `Company!`	

`countermeasures` - `[DDOSCountermeasure!]`	The countermeasures associated with the mitigation.
`end` - `Time`	The end time of the mitigation. A non-zero value of end time means that the mitigation has ended.
`historicalDestinationIPs` - `[CIDR!]`	The historical destinations.
`id` - `String!`	The identifier of the mitigation.
`mitigationTemplate` - `MitigationTemplate!`	The mitigation template used for the mitigation.
`start` - `Time!`	The start time of the mitigation.

Example

```
{
  "activeDestinationIPs": [CIDR],
  "company": Company,
  "countermeasures": [DDOSCountermeasure],
  "end": Time,
  "historicalDestinationIPs": [CIDR],
  "id": "abc123",
  "mitigationTemplate": MitigationTemplate,
  "start": Time
}
```

Types

`DeleteCertificateInput`

Input for deleting a certificate.

Input Field	Description
`id` - `String!`	ID of the certificate to delete.

Example

```
{"id": "abc123"}
```

Types

`DeleteCertificateOutput`

Output from deleting a certificate.

Field Name	Description
`deletedCertificateID` - `String!`	ID of the deleted certificate.

Example

```
{"deletedCertificateID": "xyz789"}
```

Types

`DeleteExecutiveReportInput`

Input required to delete a generated executive report.

Input Field	Description
`id` - `String!`	ID of the generated executive report to be deleted.

Example

```
{"id": "abc123"}
```

Types

`DeleteExecutiveReportOutput`

Represents a deleted executive report.

Field Name	Description
`deletedExecutiveReportID` - `String!`	ID of the generated executive report that was deleted.

Example

```
{"deletedExecutiveReportID": "abc123"}
```

Types

`DeleteOneTimeExecutiveReportConfigurationInput`

Input required to delete a one time executive report configuration.

Input Field	Description

`id` - `String!`	ID of the executive report configuration to be deleted.

Example

```
{"id": "xyz789"}
```

Types

DeleteOneTimeExecutiveReportConfigurationOutput

One time executive report configuration that was deleted.

Field Name	Description
`deletedOneTimeExecutiveReportConfigurationID` - `String!`	ID of the deleted one time executive report configuration.

Example

```
{"deletedOneTimeExecutiveReportConfigurationID": "abc123"}
```

Types

DeletePolicyInput

Delete a policy.

Input Field	Description
`id` - `String!`	ID of the policy to be deleted.

Example

```
{"id": "xyz789"}
```

Types

DeletePolicyOutput

A deleted policy response.

Field Name	Description
`deletedPolicyID` - `String!`	ID of the policy deleted.

Example

```
{"deletedPolicyID": "abc123"}
```

Types

DeleteProxyInput

Delete a proxy.

Input Field	Description
`deletePermanently` - `Boolean!` default = `false`	If provided and true, the proxy will be permanently deleted from the database.
`id` - `String!`	ID of the proxy to be deleted.

Example

```
{"deletePermanently": false, "id": "xyz789"}
```

Types

DeleteProxyOutput

Output from deleting a proxy.

Field Name	Description
`deletedProxyID` - `String!`	ID of the proxy that was deleted.
`permanentlyDeleted` - `Boolean!`	Flag indicating if the proxy was permanently deleted from the database or not.

Example

```
{"deletedProxyID": "xyz789", "permanentlyDeleted": true}
```

Types

DeleteRecurringExecutiveReportConfigurationInput

Input required to delete a recurring executive report configuration.

Input Field	Description

`id` - `String!`	ID of the one time executive report configuration to be deleted.

Example

```
{"id": "xyz789"}
```

Types

DeleteRecurringExecutiveReportConfigurationOutput

Represents a deleted recurring executive report configuration.

Field Name	Description
`deletedRecurringExecutiveReportConfigurationID` - `String!`	ID of the deleted recurring executive report configuration.

Example

```
{"deletedRecurringExecutiveReportConfigurationID": "abc123"}
```

Types

DeleteUserInput

Delete a user.

Input Field	Description
`id` - `String!`	ID of the user to be deleted.

Example

```
{"id": "xyz789"}
```

Types

DeleteUserOutput

A deleted user response.

Field Name	Description

`deletedUserID` - `String!`	ID of the user deleted.

Example

```
{"deletedUserID": "xyz789"}
```

Types

DenyURL

A deny URL countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`regexRules` - `DenyURLRulesWithPagination`	A paginated list of deny URL regex rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for deny URL violations.

Example

```
{
  "action": WAFAction,
  "regexRules": DenyURLRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

DenyURLRule

A Deny URL Regex Rule.

Field Name	Description

`denyURL` - `String`	The Deny URL text value. Value will be empty in case of ALL Deny URL Type.
`enabled` - `Boolean!`	Whether the rule is enabled.
`type` - `DenyURLType!`	Type of the Deny URL.

Example

```
{
  "denyURL": "xyz789",
  "enabled": true,
  "type": DenyURLType
}
```

Types

`DenyURLRuleInput`

Create a Deny URL Regex Rule.

Input Field	Description
`denyURL` - `String`	The Deny URL text value. Value will be null in case of ALL Deny URL Type.
`enabled` - `Boolean!` default = `true`	Whether the rule is enabled.
`type` - `DenyURLType!`	Type of the Deny URL.

Example

```
{
  "denyURL": "xyz789",
  "enabled": true,
  "type": DenyURLType
}
```

Types

`DenyURLRulesWithPagination`

A paginated list for deny URL rules.

Field Name	Description

`pageInfo` - `Pagination!`	The results paging information.
`results` - `[DenyURLRule!]`	A list of deny URL rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [DenyURLRule]
}
```

Types

DenyURLType

Allowed list of values for the Deny URL Regex Rule Type.

Enum Value	Description
`ACCESS_ATTACKS`	
`ALL`	
`APACHE_POSSIBLE_DIRECTORY_INDEX_DISCLOSURE_VULNERABILITY`	
`CODE_RED`	
`COMMAND_INJECTION_ATTACK`	
`CUSTOM`	
`DEBUG_ATTACKS`	
`FRONT_PAGE_SERVER_EXTENSIONS_BUFFER_OVERFLOW_1`	
`FRONT_PAGE_SERVER_EXTENSIONS_BUFFER_OVERFLOW_2`	
`FRONT_PAGE_SERVER_EXTENSIONS_PATH_DISCLOSURE_VULNERABILITY`	
`HTR_SOURCE_DISCLOSURE`	
`IIS_EXECUTABLE_FILE_PARSING_VULNERABILITY_1`	
`IIS_EXECUTABLE_FILE_PARSING_VULNERABILITY_2`	
`IIS_EXECUTABLE_FILE_PARSING_VULNERABILITY_3`	
`INDEX_SERVER_BUFFER_OVERFLOW`	
`MICROSOFT_IIS_UNC_MAPPED_VIRTUAL_HOST_VULNERABILITY`	
`MICROSOFT_IIS_UNC_PATH_DISCLOSURE_VULNERABILITY`	

NETSCAPE_ENTERPRISE_SERVER_DIRECTORY_INDEXING_VULNERABILITY
NETSCAPE_ENTERPRISE_SERVER_WEB_PUBLISHING_VULNERABILITY
NIMBDA_3
NIMBDA_4
PASSWORD_FILE_ATTACKS
PRINTER_BUFFER_OVERFLOW
SCRIPT_EXPLOIT
SYSTEM_COMMAND_ATTACKS
UNIX_CORE_FILE_ATTACKS
UNIX_FILE_ATTACKS
WEB_HITS_SOURCE_DISCLOSURE
WSDL_SCANNING_ATTACK_DOT_WSDL
WSDL_SCANNING_ATTACK_QUERY_PARAM_WSDL
WSDL_SCANNING_ATTACK_SLASH_WSDL

Types

DetectionAndAlertingPackage

Specifies Detection and Alerting configuration for company.

Field Name	Description
companyDName - String!	The identifier of the owning company.
enabled - Boolean!	Whether D&A is enabled for the Company.
escalationNotes - String	Useful notes about this configuration.
managedObjects - [ManagedObject!]	List of managed objects configured for detection and alerting.
routers - [Router!]	List of routers configured for detection and alerting.

Example


```
{
  "companyDName": "xyz789",
```

```
  "enabled": true,
  "escalationNotes": "xyz789",
  "managedObjects": [ManagedObject],
  "routers": [Router]
}
```

Types

DeviceGroup

Device Group

Field Name	Description
`id` - `String!`	Identifier for the device group.
`name` - `String!`	User friendly name for the device group.

Example

```
{"id": "xyz789", "name": "abc123"}
```

Types

EMail

Email elements

Field Name	Description
`fromAddr` - `String!`	From Address to display for company.
`resetIntroText` - `String!`	Reset Intro text for company.
`resetOutroText` - `String!`	Reset Outro text for company.
`resetSignatureText` - `String!`	Reset Signature to display for company.
`welcomeIntroText` - `String!`	Welcome Intro text for company that marks the beginnig of page content.
`welcomeOutroText` - `String!`	Welcome Outro text for company that marks the end of page content.
`welcomeSignatureText` - `String!`	Welcome signature text to display for company.

Example

```
{
  "fromAddr": "abc123",
  "resetIntroText": "xyz789",
  "resetOutroText": "abc123",
  "resetSignatureText": "xyz789",
  "welcomeIntroText": "abc123",
  "welcomeOutroText": "xyz789",
  "welcomeSignatureText": "abc123"
}
```

Types

Event

Represents the event object.

Field Name	Description
`company` - `Company!`	The company object.
`destinationIPs` - `[CIDR!]`	The list of destinations.
`end` - `Time`	The end time of the event. A non-zero value of end time means that the event has ended or finished.
`id` - `String!`	The identifier of the event.
`mitigation` - `Mitigation`	Details of a specific mitigation.
Arguments `id` - `String!`	
`mitigations` - `MitigationsWithPagination!`	The list of mitigations associated with an event.

Arguments
 	
`filter` - `MitigationFilterInput`
 	
The filters that can be applied to scope the specific list of mitigations.
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results. It takes a non-zero number. If omitted, default value of 1 is applied.	

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page. If omitted, default value of 50 is applied.

`sortBy` - `[MitigationSortBy!]`

The sortBy sorts the results based on the specific sort field order.

`start` - `Time!`	The start time of the event
`trafficData` - `[TrafficData!]`	The traffic data associated with an event.

Example

```
{
  "company": Company,
  "destinationIPs": [CIDR],
  "end": Time,
  "id": "abc123",
  "mitigation": Mitigation,
  "mitigations": MitigationsWithPagination,
  "start": Time,
  "trafficData": [TrafficData]
}
```

Types

`EventDimension`

Event dimensions to sort by.

Enum Value	Description
`END`	
`START`	

Types

`EventFilterInput`

The filters that can be applied to scope the list of events.

Input Field	Description

`active` - `Boolean`	The filter to fetch active or finished events. By default all events are retrieved. When active is set to true, only active events are fetched. When active is set to false, only finished events are fetched.
`destinationIPs` - `[CIDR!]`	The destinations to filter events.

Example

```
{"active": true, "destinationIPs": [CIDR]}
```

Types

EventSortBy

How to sort Events.

Input Field	Description
`dimension` - `EventDimension!` default = `"START"`	The dimension to sort by.
`direction` - `SortDirection!` default = `"DESCENDING"`	The direction to sort in.

Example

```
{
  "dimension": "START",
  "direction": "DESCENDING"
}
```

Types

EventsWithPagination

Represents the list of events along with pagination details.

Field Name	Description
`pageInfo` - `Pagination!`	The pagination details.
`results` - `[Event!]`	The list of events.

Example

```
{
  "pageInfo": Pagination,
```

```
  "results": [Event]
}
```

Types

ExecutiveReport

Defines a Report.

Field Name	Description
`generatedTimestamp` - `Time`	Timestamp when report was generated successfully or was marked as failed.
`id` - `String!`	ID of the generated report.
`reportBody` - `String!`	Generated report.
`status` - `ExecutiveReportStatus!`	Status of report generation.
`statusDetails` - `[String!]`	Additional information if any on report generation status, like notification errors etc.

Example

```
{
  "generatedTimestamp": Time,
  "id": "abc123",
  "reportBody": "xyz789",
  "status": ExecutiveReportStatus,
  "statusDetails": ["abc123"]
}
```

Types

ExecutiveReportConfiguration

Union type combining one time and recurring report configurations.

Union Types
`OneTimeExecutiveReportConfiguration`
`RecurringExecutiveReportConfiguration`

Types

`ExecutiveReportConfigurationFilterInput`

Report configuration filter input for report configuration queries.

Input Field	Description
`excludeBot` - `Boolean` default = `false`	If true, will exclude configurations generating a Bot mitigation summary in their reports.
`excludeDDoS` - `Boolean` default = `false`	If true, will exclude configurations generating a DDoS mitigation summary in their reports.
`excludeWAF` - `Boolean` default = `false`	If true, will exclude configurations generating a WAF violation summary in their reports.
`from` - `Time`	Will include report configurations created from and after this timestamp.
`id` - `String`	Report config ID to search on.
`includeDisabled` - `Boolean` default = `false`	If true, will include disabled report configurations in the result set.
`includeExpired` - `Boolean` default = `false`	If true, will include expired report configurations in the result set.
`name` - `String`	Substring search of name
`reportType` - `ExecutiveReportType`	Type of report generated by requested configuration.
`to` - `Time`	Will include report configuration created until this timestamp.

Example

```
{
  "excludeBot": false,
  "excludeDDoS": false,
  "excludeWAF": false,
  "from": Time,
  "id": "xyz789",
  "includeDisabled": false,
  "includeExpired": false,
  "name": "xyz789",
  "reportType": ExecutiveReportType,
  "to": Time
}
```

Types

ExecutiveReportFilterInput

Input filter for Report queries.

Input Field	Description
endDate - Time	Query for reports by date range end timestamp.
id - String	Report ID to search on.
reportConfigurationName - String	Query by the report configuration name.
reportType - ExecutiveReportType	Query by report type (one-time/recurring).
startDate - Time	Query for reports by date range start timestamp.

Example

```
{
  "endDate": Time,
  "id": "abc123",
  "reportConfigurationName": "abc123",
  "reportType": ExecutiveReportType,
  "startDate": Time
}
```

Types

ExecutiveReportNotificationDetails

Notification configuration for report recipients.

Field Name	Description
emailList - [String!]	List of email recipients

Example

```
{"emailList": ["abc123"]}
```

Types

ExecutiveReportNotificationDetailsInput

Input notification configuration for report receipients.

Input Field	Description
`emailList` - `[String!]`	List of email recipients

Example

```
{"emailList": ["xyz789"]}
```

Types

`ExecutiveReportPeriod`

Periodicity of report generation.

Enum Value	Description
`CALENDAR_MONTHLY`	
`PRIOR_BIWEEKLY`	
`PRIOR_MONTHLY`	
`PRIOR_QUARTERLY`	
`PRIOR_WEEKLY`	

Types

`ExecutiveReportPeriodInput`

Periodicity of report generation supplied as input.

Enum Value	Description
`CALENDAR_MONTHLY`	
`PRIOR_BIWEEKLY`	
`PRIOR_MONTHLY`	
`PRIOR_QUARTERLY`	
`PRIOR_WEEKLY`	

Types

ExecutiveReportStatus

Status of report generation.

Enum Value	Description
IN_PROGRESS	Indicates report generation is in progress.
NOTIFICATION_FAILED	Indicates successful report generation but failed notification.
REPORT_FAILED	Indicates failed report generation.
SUCCESS	Indicates successful report generation and notification.

Types

ExecutiveReportType

Type of report.

Enum Value	Description
ONE_TIME	One time report.
RECURRING	Recurring report.

Types

ExecutiveReportsWithPagination

Paginated reports.

Field Name	Description
pageInfo - Pagination!	Pagination settings.
results - [ExecutiveReport!]	List of report configurations.

Example

```
{
  "pageInfo": Pagination,
  "results": [ExecutiveReport]
}
```

Types

Feature

Feature type along with its negotiation status.

Field Name	Description
`activationStatus` - `ActivationStatus!`	Specifies a combination of whether the offering is purchased and/or enabled in the portal.
`name` - `FeatureType!`	Specifies a feature/offering (DDOS/BGP On Demand/etc) to filter search results on.

Example

```
{
  "activationStatus": ActivationStatus,
  "name": FeatureType
}
```

Types

FeatureActivationState

Filter for a feature's enabled and contract statuses.

Input Field	Description
`enabled` - `Boolean`	When set to true, it means customer has this feature enabled.
`entitled` - `Boolean`	When set to true, it means customer has an activated contract for this feature.

Example

```
{"enabled": true, "entitled": true}
```

Types

FeatureType

A feature purchased by a customer.

Enum Value	Description

`ADDITIONAL_ROUTER`	Represents Additional Router for BGP routes for customer.
`ADDITIONAL_ROUTER_DNA`	Additional Router for BGP routes for customer.
`ASSURANCE_1`	Assures one free mitigation contract for customer.
`ASSURANCE_3`	Assures three free mitigation contracts for customer.
`BGP_ALWAYS_ON`	Represents that BGP mitigation is always on for customer.
`BGP_ON_DEMAND`	Represents that BGP mitigation is available upon demand for customer.
`DDOS_AND_APPLICATION_SECURITY`	Represents Web Application Firewall feature for customer.
`HYBRID_APPLIANCE_ONLY`	Represents Hybrid Appliance for DDoS mitigation for customer.
`PROXY`	Represents Web proxy (Virtual IPs) feature for customer.
`UNLIMITED_MITIGATIONS`	Assures unlimited mitigations for customer.

Types

`FieldConsistencyRuleCountsWithPagination`

Field consistency learning rule counts.

Field Name	Description
`pageInfo` - `Pagination!`	
`results` - `[FormFieldConsistencyRuleCount!]`	

Example

```
{
  "pageInfo": Pagination,
  "results": [FormFieldConsistencyRuleCount]
}
```

Types

`FieldConsistencyRulesWithPagination`

A paginated list of Form Field consistency exemption rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[FormFieldConsistencyRule!]`	A list of exemption rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [FormFieldConsistencyRule]
}
```

Types

`FieldFormat`

A field format countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`enforcementRules` - `FieldFormatEnforcementRulesWithPagination`	A paginated list of enforcement rules. These are tightening rules, in order to relax some rules you need to remove them from this list.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`learn` - `Boolean!`	A flag to enable or disable learning.
`maxLength` - `UnsignedInt16`	Maximum length of the field (in characters).
`minLength` - `UnsignedInt16`	Minimum length of the field (in characters).
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for field format violations.
`type` - `FieldFormatType!`	Allowed types for this field.

Example

```
{
  "action": WAFAction,
  "enforcementRules": FieldFormatEnforcementRulesWithPagination,
  "learn": true,
  "maxLength": UnsignedInt16,
  "minLength": UnsignedInt16,
  "threshold": AppSecThreshold,
  "type": FieldFormatType
}
```

Types

`FieldFormatEnforcementRule`

A field format enforcement rule.

Field Name	Description
`actionURL` - `String!`	The action URL of the web form.
`enabled` - `Boolean!`	Whether the field format is enabled.

`fieldType` - `FieldFormatType!`	The field type from the allowed list.
`formFieldName` - `String!`	The form field name.
`isFormFieldRegex` - `Boolean!`	Whether a form field name is in regex format.
`maxLength` - `UnsignedInt16`	Maximum length of the field (in characters). This field is set ONLY when field type is present.
`minLength` - `UnsignedInt16`	Minimum length of the field (in characters). This field is set ONLY when field type is present.

Example

```
{
  "actionURL": "xyz789",
  "enabled": true,
  "fieldType": FieldFormatType,
  "formFieldName": "xyz789",
  "isFormFieldRegex": true,
  "maxLength": UnsignedInt16,
  "minLength": UnsignedInt16
}
```

Types

`FieldFormatEnforcementRuleInput`

Create a field format enforcement rule.

Input Field	Description
`actionURL` - `String!`	The action URL of the web form.
`enabled` - `Boolean!` default = `true`	Whether the field format is enabled.
`fieldType` - `FieldFormatType!`	The field type from the allowed list.
`formFieldName` - `String!`	The form field name.
`isFormFieldRegex` - `Boolean!` default = `false`	Whether the form field name is in regex format
`maxLength` - `UnsignedInt16!` default = `65535`	Maximum length of the field (in characters).
`minLength` - `UnsignedInt16!` default = `0`	Minimum length of the field (in characters).

Example

```
{
  "actionURL": "abc123",
  "enabled": true,
  "fieldType": FieldFormatType,
  "formFieldName": "abc123",
  "isFormFieldRegex": false,
  "maxLength": 65535,
  "minLength": 0
}
```

Types

FieldFormatEnforcementRulesWithPagination

A paginated list of field format enforcement rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[FieldFormatEnforcementRule!]`	List of field format rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [FieldFormatEnforcementRule]
}
```

Types

FieldFormatRuleCount

Field format rule count.

Field Name	Description
`count` - `UnsignedInt32!`	
`rule` - `LearnedFieldFormatRule!`	

Example

```
{
  "count": UnsignedInt32,
```

```
  "rule": LearnedFieldFormatRule
}
```

Types

FieldFormatRuleCountsWithPagination

Field format learning rule counts.

Field Name	Description
pageInfo - Pagination!	
results - [FieldFormatRuleCount!]	

Example

```
{
  "pageInfo": Pagination,
  "results": [FieldFormatRuleCount]
}
```

Types

FieldFormatType

Allowed list of field format types.

Enum Value	Description
ALPHA	
ALPHANUMERIC	
ANY	
INTEGER	
NO_HTML	

Types

Float

The Float scalar type represents signed double-precision fractional values as specified by IEEE 754.

Example

```
987.65
```

Types

FlowConfig

Flow Configuration

Field Name	Description
`alertEnabled` - `Boolean!`	Flow up/down notification.
`alertTimeout` - `String!`	Configured flow alert timeout.
`exportIP` - `IPAddress!`	Flow export IP address.

Example

```
{
  "alertEnabled": false,
  "alertTimeout": "abc123",
  "exportIP": IPAddress
}
```

Types

FormFieldConsistency

Represents Form field consistency countermeasure. It verifies that the web forms were not modified inappropriately by the client.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`fieldConsistencyExemptions` - `FieldConsistencyRulesWithPagination`	A paginated list of exemption rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`learn` - `Boolean!`	A flag to enable or disable learning.
`sessionlessFieldConsistency` - `SessionlessFieldConsistency!`	When turned on, it checks only the web form structure.
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for form field consistency violations.

Example

```
{
  "action": WAFAction,
  "fieldConsistencyExemptions": FieldConsistencyRulesWithPagination,
  "learn": true,
  "sessionlessFieldConsistency": SessionlessFieldConsistency,
  "threshold": AppSecThreshold
}
```

Types

`FormFieldConsistencyRule`

A form field consistency exemption rule.

Field Name	Description
`actionURL` - `String!`	The action URL of the web form.
`enabled` - `Boolean!`	Whether the field consistency exemption is enabled.

`formFieldName` - `String!`	The form field name.
`isFormFieldRegex` - `Boolean!`	Whether the form field name is in regex format.

Example

```
{
  "actionURL": "xyz789",
  "enabled": false,
  "formFieldName": "xyz789",
  "isFormFieldRegex": false
}
```

Types

FormFieldConsistencyRuleCount

Field consistency rule count.

Field Name	Description
`count` - `UnsignedInt32!`	
`rule` - `LearnedFormFieldConsistencyRule!`	

Example

```
{
  "count": UnsignedInt32,
  "rule": LearnedFormFieldConsistencyRule
}
```

Types

FormFieldConsistencyRuleInput

A form field consistency exemption rule.

Input Field	Description
`actionURL` - `String!`	The action URL of the web form.
`enabled` - `Boolean!` default = `true`	Whether the field consistency exemption is enabled.
`formFieldName` - `String!`	The form field name.

`isFormFieldRegex` - `Boolean!` default = `false`	Whether the form field name is in regex format.

Example

```
{
  "actionURL": "xyz789",
  "enabled": true,
  "formFieldName": "abc123",
  "isFormFieldRegex": false
}
```

Types

`FormFieldSignatureRule`

A WAF custom signature form field rule.

Field Name	Description
`fieldName` - `String`	The field name used in this rule.
`fieldNameFormat` - `SignatureRuleFormat!`	A form field name format from the allowed list of formats.
`url` - `String`	The url used in this rule.
`urlFormat` - `SignatureRuleFormat!`	A url format from the allowed list of formats.

Example

```
{
  "fieldName": "xyz789",
  "fieldNameFormat": SignatureRuleFormat,
  "url": "xyz789",
  "urlFormat": SignatureRuleFormat
}
```

Types

`FormFieldSignatureRuleInput`

Create a WAF custom signature form field rule.

Input Field	Description

`fieldName` - `String`	The field name used in this rule.
`fieldNameFormat` - `SignatureRuleFormat!` default = `"ANY"`	A form field name format from the allowed list of formats.
`url` - `String`	The url used in this rule.
`urlFormat` - `SignatureRuleFormat!` default = `"ANY"`	A url format from the allowed list of formats.

Example

```
{
  "fieldName": "xyz789",
  "fieldNameFormat": "ANY",
  "url": "abc123",
  "urlFormat": "ANY"
}
```

Types

GeoLocation

Represents a geographic location.

Field Name	Description
`areaCode` - `String`	The area code of the location.
`city` - `String`	The city of the location.
`continent` - `String`	The continent of the location.
`countryCode` - `CountryCode`	The country code of the location.
`countryName` - `String`	The country name of the location.
`latitude` - `Float`	The latitude of the location.
`longitude` - `Float`	The longitude of the location.
`postal` - `String`	The postal code of the location.
`region` - `String`	The region of the location.
`state` - `String`	The state of the location.
`stateCode` - `String`	The state code of the location.

`timezone` - `String`	The timezone of the location.

Example

```
{
  "areaCode": "xyz789",
  "city": "abc123",
  "continent": "abc123",
  "countryCode": CountryCode,
  "countryName": "abc123",
  "latitude": 987.65,
  "longitude": 987.65,
  "postal": "abc123",
  "region": "abc123",
  "state": "abc123",
  "stateCode": "xyz789",
  "timezone": "xyz789"
}
```

Types

HTMLLocation

Allowed list of values for an HTML location.

Enum Value	Description
`COOKIE`	
`FORM_FIELD`	
`HEADER`	

Types

HTMLSQLInjection

An HTML SQL injection countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`checkSQLWildChars` - `Boolean!`	Whether to check for

	form fields that contain SQL wild chars.
`exemptCommentsWith` - `CommentExemption!`	Exempt all comments of the given type.
`learn` - `Boolean!`	A flag to enable or disable learning.
`relaxationRules` - `HTMLSQLInjectionRelaxationRulesWithPagination`	A paginated list of SQL Injection rules.

Arguments
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `1000`
 	
The maximum number of results to show per page.	

`sqlInjectionType` - `SQLInjectionType!`	A SQL injection type.
`sqliGrammar` - `Boolean!`	Enable SQL Injection grammar
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for HTML SQL injection violations.

Example

```
{
```

```
  "action": WAFAction,
  "checkSQLWildChars": false,
  "exemptCommentsWith": CommentExemption,
  "learn": true,
  "relaxationRules": HTMLSQLInjectionRelaxationRulesWithPagination,
  "sqlInjectionType": SQLInjectionType,
  "sqliGrammar": false,
  "threshold": AppSecThreshold
}
```

Types

HTMLSQLInjectionRelaxationRule

An HTML SQL injection relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!`	Whether the name is in regex format.
`isValueExpressionRegex` - `Boolean`	Whether the value expression is in regex format.
`location` - `HTMLLocation`	Location that should be examined by the rule.
`name` - `String!`	Name of the web form field, cookie, or HTTP header to relax.
`url` - `String!`	If the item to be exempted is a web form field, the action URL for the web form.
`valueExpression` - `String`	The value expression.
`valueType` - `ValueType`	The HTML value type.

Example

```
{
  "enabled": false,
  "isNameRegex": false,
  "isValueExpressionRegex": false,
  "location": HTMLLocation,
  "name": "xyz789",
  "url": "abc123",
  "valueExpression": "abc123",
  "valueType": ValueType
}
```

Types

HTMLSQLInjectionRelaxationRuleInput

An HTML SQL injection relaxation rule.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!` default = `false`	Whether the name is in regex format.
`isValueExpressionRegex` - `Boolean` default = `false`	Whether the value expression is in regex format.
`location` - `HTMLLocation`	The location that should be examined by the rule.
`name` - `String!`	Name of the web form field, cookie, or HTTP header to relax.
`url` - `String!`	If the item to be exempted is a web form field, the action URL for the web form.
`valueExpression` - `String`	The value expression.
`valueType` - `ValueType`	The HTML value type.

Example

```
{
  "enabled": true,
  "isNameRegex": false,
  "isValueExpressionRegex": false,
  "location": HTMLLocation,
  "name": "xyz789",
  "url": "xyz789",
  "valueExpression": "abc123",
  "valueType": ValueType
}
```

Types

HTMLSQLInjectionRelaxationRulesWithPagination

A paginated list of SQL injection relaxation rules.

Field Name	Description

`pageInfo` - `Pagination!`	The returned page information.
`results` - `[HTMLSQLInjectionRelaxationRule!]`	A list of relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [HTMLSQLInjectionRelaxationRule]
}
```

Types

HTMLSQLInjectionRuleCount

HTML SQL injection rule count.

Field Name	Description
`count` - `UnsignedInt32!`	
`rule` - `LearnedHTMLSQLInjectionRule!`	

Example

```
{
  "count": UnsignedInt32,
  "rule": LearnedHTMLSQLInjectionRule
}
```

Types

HTMLSQLInjectionRuleCountsWithPagination

Counts of learned HTML SQL injection relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	
`results` - `[HTMLSQLInjectionRuleCount!]`	

Example

```
{
  "pageInfo": Pagination,
```

```
  "results": [HTMLSQLInjectionRuleCount]
}
```

Types

HTMLXSS

An HTML cross-site scripting countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`checkCompleteURLs` - `Boolean`	A flag to enforce checks for complete URLs for cross-site scripts, instead of just the query portions of URLs.
`learn` - `Boolean!`	A flag to enable or disable learning.
`relaxationRules` - `HTMLXSSRelaxationRulesWithPagination`	A paginated list of HTML XSS relaxation rules.

Arguments
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `1000`
 	
The maximum number of results to show per page.	

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for HTML cross-site scripting violations.

Example

```
{
  "action": WAFAction,
  "checkCompleteURLs": false,
  "learn": true,
```

```
  "relaxationRules": HTMLXSSRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

HTMLXSSLocation

Allowed list of values for an HTML location in case of HTML XSS.

Enum Value	Description
COOKIE	
FORM_FIELD	
HEADER	
URL	

Types

HTMLXSSRelaxationRule

An HTML XSS relaxation rule.

Field Name	Description
enabled - Boolean!	Whether the relaxation rule is enabled.
isNameRegex - Boolean!	Whether the name is in regex format.
isValueExpressionRegex - Boolean	Whether the value expression is in regex format.
location - HTMLXSSLocation	The location that should be examined by the rule.
name - String!	Name of the web form field, cookie, or HTTP header to relax.
url - String!	If the item to be exempted is a web form field, the action URL for the web form.
valueExpression - String	The value expression.
valueType - XSSValueType	The XSS value type.

Example

```
{
```

```
  "enabled": true,
  "isNameRegex": true,
  "isValueExpressionRegex": true,
  "location": HTMLXSSLocation,
  "name": "abc123",
  "url": "abc123",
  "valueExpression": "xyz789",
  "valueType": XSSValueType
}
```

Types

HTMLXSSRelaxationRuleInput

An HTML XSS relaxation rule.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!` default = `false`	Whether the name is in regex format.
`isValueExpressionRegex` - `Boolean` default = `false`	Whether the value expression is in regex format.
`location` - `HTMLXSSLocation`	The location that should be examined by the rule.
`name` - `String!`	Name of the web form field, cookie, or HTTP header to relax.
`url` - `String!`	If the item to be exempted is a web form field, the action URL for the web form.
`valueExpression` - `String`	The value expression.
`valueType` - `XSSValueType`	The HTML value type.

Example

```
{
  "enabled": true,
  "isNameRegex": false,
  "isValueExpressionRegex": false,
  "location": HTMLXSSLocation,
  "name": "abc123",
  "url": "xyz789",
  "valueExpression": "abc123",
```

```
  "valueType": XSSValueType
}
```
Types

HTMLXSSRelaxationRulesWithPagination

A paginated list of HTML cross-site scripting relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[HTMLXSSRelaxationRule!]`	A list of HTML XSS relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [HTMLXSSRelaxationRule]
}
```
Types

HTMLXSSRuleCount

HTML XSS rule count.

Field Name	Description
`count` - `UnsignedInt32!`	
`rule` - `LearnedHTMLXSSRule!`	

Example

```
{
  "count": UnsignedInt32,
  "rule": LearnedHTMLXSSRule
}
```
Types

HTMLXSSRuleCountsWithPagination

HTML XSS learning rules.

Field Name	Description
`pageInfo` - `Pagination!`	
`results` - `[HTMLXSSRuleCount!]`	

Example

```
{
  "pageInfo": Pagination,
  "results": [HTMLXSSRuleCount]
}
```

Types

HTTPRFCProfile

A HTTP RFC Profile countermeasure. This setting is used when certain scenarios might need to bypass or block non RFC compliant request.

Field Name	Description
`action` - `HTTPRFCProfileAction!`	Action to be taken when there is a non compliant request.
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for HTTP RFC violations.

Example

```
{
  "action": HTTPRFCProfileAction,
  "threshold": AppSecThreshold
}
```

Types

HTTPRFCProfileAction

Allowed list of values for HTTP RFC Profile action.

Enum Value	Description
`BLOCK`	
`BYPASS`	

Types

HeaderSignatureRule

A WAF custom signature header rule.

Field Name	Description
`headerName` - `String`	The header name used in this rule.
`headerNameFormat` - `SignatureRuleFormat!`	A header name format from the allowed list of formats.

Example

```
{
  "headerName": "abc123",
  "headerNameFormat": SignatureRuleFormat
}
```

Types

HeaderSignatureRuleInput

Create a WAF custom signature header rule.

Input Field	Description
`headerName` - `String`	The header name used in this rule.
`headerNameFormat` - `SignatureRuleFormat!` default = `"ANY"`	A header name format from the allowed list of formats.

Example

```
{
  "headerName": "abc123",
  "headerNameFormat": "ANY"
}
```

Types

ID

The `ID` scalar type represents a unique identifier, often used to refetch an object or as key for a cache. The ID type appears in a JSON response as a String; however, it is not intended to be human-readable. When expected as an input type, any string (such as `"4"`) or integer (such as `4`) input value will be accepted as an ID.

Example

```
object
```

Types

IPAddress

IPAddress represents a generic IP address

Field Name	Description
`strictVersion` - `IPVersion!`	The reduced IP version of the address. V4 addresses encoded in v6 format will report IPV4
`string` - `String!`	A string representation of the IP address.
`version` - `IPVersion!`	The nominal IP version of the address. Note that v4 addresses encoded in v6 format will report IPV6

Example

```
{
  "strictVersion": IPVersion,
  "string": "xyz789",
  "version": IPVersion
}
```

Types

IPAddressInput

IPAddressInput is used to specify a generic IP address. One and only one field can be specified.

Input Field	Description
`ipv4Address` - `IPv4Address`	for an IPV4 version address
`ipv6Address` - `IPv6Address`	for an IPV6 version address

Example

```
{
  "ipv4Address": IPv4Address,
  "ipv6Address": IPv6Address
}
```

Types

IPFilter

Filters by IP address(es).

Field Name	Description
`cidr` - `CIDR!`	CIDR which is blacklisted or whitelisted.
`isBlocked` - `Boolean!`	Flag which shows if the CIDR is blacklisted (true) or whitelisted (false).

Example

```
{"cidr": CIDR, "isBlocked": true}
```

Types

IPFilterFilterInput

Represents properties we can filter the IP filter list by.

Input Field	Description
`cidr` - `CIDR`	CIDR which is blacklisted or whitelisted.
`isBlocked` - `Boolean`	Flag which shows if the CIDR is blacklisted (true) or whitelisted (false).
`version` - `IPVersion`	IP Version of the CIDR.

Example

```
{
  "cidr": CIDR,
  "isBlocked": false,
  "version": IPVersion
}
```

Types

IPFilterInput

Create an IP filter.

Input Field	Description
`cidr` - `CIDR!`	CIDR to be blacklisted or whitelisted.
`isBlocked` - `Boolean!`	Flag representing if the CIDR needs to be blacklisted (true) or whitelisted (false).

Example

```
{"cidr": CIDR, "isBlocked": true}
```

Types

IPFiltersWithPagination

Contains the paginated list of IP filters.

Field Name	Description
`pageInfo` - `Pagination!`	The results paging information.
`results` - `[IPFilter!]`	List of IP filters.

Example

```
{
  "pageInfo": Pagination,
  "results": [IPFilter]
}
```

Types

IPInfo

Represents IP Intelligence information for a given IP address.

Field Name	Description
`address` - `IPAddress`	The IP address of interest.
`location` - `GeoLocation`	The IP location metadata.

`network` - `IPNetwork`	The IP network.
`reputation` - `IPReputation`	The IP reputation.

Example

```
{
  "address": IPAddress,
  "location": GeoLocation,
  "network": IPNetwork,
  "reputation": IPReputation
}
```

Types

`IPNetwork`

IP Network information.

Field Name	Description
`asn` - `UnsignedInt32`	The ASN number.
`carrier` - `String`	The carrier of the network.
`organization` - `String`	The organization of the network.

Example

```
{
  "asn": UnsignedInt32,
  "carrier": "abc123",
  "organization": "abc123"
}
```

Types

`IPReputation`

IP Reputation score.

Field Name	Description
`classification` - `[String!]`	IP classifications are a list of strings which indicate additional analytical information about the IP .
`realScore` - `Float`	IP reputation real score.

`riskScore` - `Float`		IP reputation risk score.

Example

```
{"classification": ["xyz789"], "realScore": 987.65, "riskScore": 123.45}
```

Types

`IPVersion`

IP version

Enum Value	Description
`IPV4`	IP v4 (32 bits, Four dot-separated octets)
`IPV6`	IP v6 (128 bits, Eight colon-separated hextets, with shorthand for expressing IPv4 addresses)

Types

`IPv4Address`

An IPv4 address.

Example

```
object
```

Types

`IPv6Address`

An IPv6 address.

Example

```
object
```

Types

`Int`

The `Int` scalar type represents non-fractional signed whole numeric values. Int can represent values between -(2^31) and 2^31 - 1.

Example

```
987
```

Types

`Int64`

Example

```
object
```

Types

`JSONCommandInjectionRelaxationRule`

A JSON command injection relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`exemptURL` - `String!`	URL to exempt from JSON command injection check.

Example

```
{"enabled": true, "exemptURL": "abc123"}
```

Types

`JSONCommandInjectionRelaxationRuleInput`

A JSON command injection relaxation rule input.

Input Field	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`exemptURL` - `String!`	URL to exempt from JSON command injection check.

Example

```
{"enabled": false, "exemptURL": "abc123"}
```

Types

JSONCommandInjectionRelaxationRulesWithPagination

A paginated list of JSON command injection relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[JSONCommandInjectionRelaxationRule!]`	A list of relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [JSONCommandInjectionRelaxationRule]
}
```

Types

JSONCommandInjectionSettings

JSON command injection Settings

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`commandInjectionType` - `CommandInjectionType!`	A Command injection type.
`relaxationRules` - `JSONCommandInjectionRelaxationRulesWithPagination`	A paginated list of command injection rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for JSON command injection violations.

Example

```
{
  "action": WAFAction,
  "commandInjectionType": CommandInjectionType,
  "relaxationRules": JSONCommandInjectionRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

`JSONCrossSiteScriptingSettings`

JSON cross-site scripting settings to protect applications from XSS Attacks through JSON requests

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`relaxationRules` - `JSONXSSRelaxationRulesWithPagination`	A paginated list of SQL Injection rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for JSON XSS violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": JSONXSSRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

`JSONDenialOfServiceSettings`

JSON Denial of Service Settings to protect applications from Denial of Service Attacks through JSON requests

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`enforcementRule` - `JSONDoSEnforcementRule`	A DOS Enforcement rules.
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for JSON DOS violations.

Example

```
{
  "action": WAFAction,
  "enforcementRule": JSONDoSEnforcementRule,
  "threshold": AppSecThreshold
}
```

Types

`JSONDoSEnforcementRule`

A JSON Denial of Service enforcement rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.

`jsonMaxArrayLength` - `UnsignedInt32`	JSON maximum array length in bytes.
`jsonMaxContainerDepth` - `UnsignedInt32`	JSON maximum container depth in bytes.
`jsonMaxDocumentLength` - `UnsignedInt32`	JSON maximum document length in bytes.
`jsonMaxObjectKeyCount` - `UnsignedInt32`	JSON maximum object key count in bytes.
`jsonMaxObjectKeyLength` - `UnsignedInt32`	JSON maximum object key length in bytes.
`jsonMaxStringLength` - `UnsignedInt32`	JSON maximum object string length in bytes.

Example

```
{
  "enabled": false,
  "jsonMaxArrayLength": UnsignedInt32,
  "jsonMaxContainerDepth": UnsignedInt32,
  "jsonMaxDocumentLength": UnsignedInt32,
  "jsonMaxObjectKeyCount": UnsignedInt32,
  "jsonMaxObjectKeyLength": UnsignedInt32,
  "jsonMaxStringLength": UnsignedInt32
}
```

Types

`JSONDoSEnforcementRuleInput`

A JSON Denial of Service enforcement rule input.

Input Field	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`jsonMaxArrayLength` - `UnsignedInt32`	JSON maximum array length in bytes.
`jsonMaxContainerDepth` - `UnsignedInt32`	JSON maximum container depth in bytes.
`jsonMaxDocumentLength` - `UnsignedInt32`	JSON maximum document length in bytes.
`jsonMaxObjectKeyCount` - `UnsignedInt32`	JSON maximum object key count in bytes.
`jsonMaxObjectKeyLength` - `UnsignedInt32`	JSON maximum object key length in bytes.
`jsonMaxStringLength` - `UnsignedInt32`	JSON maximum object string length in bytes.

Example

```
{
  "enabled": true,
  "jsonMaxArrayLength": UnsignedInt32,
  "jsonMaxContainerDepth": UnsignedInt32,
  "jsonMaxDocumentLength": UnsignedInt32,
  "jsonMaxObjectKeyCount": UnsignedInt32,
  "jsonMaxObjectKeyLength": UnsignedInt32,
  "jsonMaxStringLength": UnsignedInt32
}
```

Types

`JSONSQLInjectionRelaxationRule`

A JSON SQL injection relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`exemptURL` - `String!`	URL to exempt from JSON SQLInjection check.

Example

```
{"enabled": false, "exemptURL": "abc123"}
```

Types

`JSONSQLInjectionRelaxationRuleInput`

A JSON SQL injection relaxation rule input.

Input Field	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`exemptURL` - `String!`	URL to exempt from JSON SQLInjection check.

Example

```
{"enabled": true, "exemptURL": "abc123"}
```

Types

JSONSQLInjectionRelaxationRulesWithPagination

A paginated list of JSON SQL injection relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[JSONSQLInjectionRelaxationRule!]`	A list of relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [JSONSQLInjectionRelaxationRule]
}
```

Types

JSONSQLInjectionSettings

JSON SQL Injection Settings to protect applications from SQL Injection attacks through JSON requests

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`relaxationRules` - `JSONSQLInjectionRelaxationRulesWithPagination`	A paginated list of SQL Injection rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`sqlInjectionType` - `SQLInjectionType!`	A SQL injection type.
`sqliGrammar` - `Boolean!`	Enable SQL Injection grammar
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for JSON SQL injection violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": JSONSQLInjectionRelaxationRulesWithPagination,
  "sqlInjectionType": SQLInjectionType,
  "sqliGrammar": true,
  "threshold": AppSecThreshold
}
```

Types

`JSONSettings`

JSON Security Settings to protect JSON Applications

Field Name	Description
`jsonCommandInjectionSettings` - `JSONCommandInjectionSettings`	JSON Command Injection Settings.
`jsonCrossSiteScriptingSettings` - `JSONCrossSiteScriptingSettings`	JSON Cross Site Scripting Settings.
`jsonDenialOfServiceSettings` - `JSONDenialOfServiceSettings`	JSON Denial of

	Service Settings.
`jsonSQLInjectionSettings` - `JSONSQLInjectionSettings`	JSON SQL Injection Settings.

Example

```
{
  "jsonCommandInjectionSettings": JSONCommandInjectionSettings,
  "jsonCrossSiteScriptingSettings": JSONCrossSiteScriptingSettings,
  "jsonDenialOfServiceSettings": JSONDenialOfServiceSettings,
  "jsonSQLInjectionSettings": JSONSQLInjectionSettings
}
```

Types

`JSONXSSRelaxationRule`

A JSON XSS relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`exemptURL` - `String!`	URL to exempt from JSON XSS check.

Example

```
{"enabled": false, "exemptURL": "abc123"}
```

Types

`JSONXSSRelaxationRuleInput`

A JSON XSS relaxation rule input.

Input Field	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`exemptURL` - `String!`	URL to exempt from JSON XSS check.

Example

```
{"enabled": true, "exemptURL": "abc123"}
```

Types

JSONXSSRelaxationRulesWithPagination

A paginated list of JSON XSS relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[JSONXSSRelaxationRule!]`	A list of relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [JSONXSSRelaxationRule]
}
```

Types

LearnedCSRFSettingsRule

A learned CSRF settings rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the rule is enabled.
`formActionURL` - `String!`	Action URL.
`formOriginURL` - `String!`	Origin URL.

Example

```
{"enabled": false, "formActionURL": "xyz789", "formOriginURL": "abc123"}
```

Types

LearnedContentTypeRule

A learned content type rule.

Field Name	Description
`contentType` - `String!`	Content type.

`enabled` - `Boolean!`	Whether the rule is enabled.

Example

```
{"contentType": "xyz789", "enabled": false}
```

Types

`LearnedCookieConsistencyRule`

A learned cookie consistency rule.

Field Name	Description
`cookieName` - `String!`	Name of the cookie.
`enabled` - `Boolean!`	Whether the rule is enabled.

Example

```
{"cookieName": "abc123", "enabled": true}
```

Types

`LearnedFieldFormatRule`

A learned field format rule.

Field Name	Description
`actionURL` - `String!`	Action URL.
`enabled` - `Boolean!`	Whether the rule is enabled.
`fieldType` - `String!`	Type of field.
`formFieldName` - `String!`	Name of the form field.
`maxLength` - `UnsignedInt32!`	Maximum length.
`minLength` - `UnsignedInt32!`	Minimum length.

Example

```
{
  "actionURL": "xyz789",
  "enabled": false,
```

```
  "fieldType": "abc123",
  "formFieldName": "xyz789",
  "maxLength": UnsignedInt32,
  "minLength": UnsignedInt32
}
```

Types

LearnedFormFieldConsistencyRule

A learned form field consistency rule.

Field Name	Description
`actionURL` - `String!`	Action URL.
`enabled` - `Boolean!`	Whether the rule is enabled.
`formFieldName` - `String!`	Name of the form field.

Example

```
{"actionURL": "xyz789", "enabled": true, "formFieldName": "abc123"}
```

Types

LearnedHTMLSQLInjectionRule

A learned HTML SQL injection rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the rule is enabled.
`location` - `String!`	Location.
`name` - `String!`	Name of the rule.
`url` - `String!`	URL.
`valueExpression` - `String!`	Value expression.
`valueType` - `String!`	Value type.

Example

```
{
  "enabled": true,
```

```
  "location": "abc123",
  "name": "xyz789",
  "url": "abc123",
  "valueExpression": "xyz789",
  "valueType": "abc123"
}
```


Types

LearnedHTMLXSSRule

A learned HTML XSS rule.

Field Name	Description
enabled - Boolean!	Whether the rule is enabled.
location - String!	Location.
name - String!	Name of the rule.
url - String!	URL.
valueExpression - String!	Value expression.
valueType - String!	Value type.

Example


```
{
  "enabled": true,
  "location": "xyz789",
  "name": "abc123",
  "url": "abc123",
  "valueExpression": "xyz789",
  "valueType": "xyz789"
}
```


Types

LearnedWSISettingsRule

A learned WSI settings rule.

Field Name	Description
code - String!	Code.

`description` - `String!`	Description.
`enabled` - `Boolean!`	Whether the rule is enabled.
`ruleID` - `String!`	ID of the rule.

Example

```
{
  "code": "abc123",
  "description": "xyz789",
  "enabled": false,
  "ruleID": "xyz789"
}
```

Types

`LearningRules`

Rules that are being learned, from items that were set to 'Learn' mode.

Field Name	Description
`contentTypeRules` - `ContentTypeRuleCountsWithPagination`	

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`cookieConsistencyRules` - `CookieConsistencyRuleCountsWithPagination`	

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`crossSiteScriptingRules` - `HTMLXSSRuleCountsWithPagination`

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`csrfSettingsRules` - `CSRFSettingsRuleCountsWithPagination`

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`fieldConsistencyRules` - `FieldConsistencyRuleCountsWithPagination`

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`fieldFormatRules` - `FieldFormatRuleCountsWithPagination`

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`htmlSQLInjectionRules` - `HTMLSQLInjectionRuleCountsWithPagination`

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

`wsiSettingsRules` - `WSISettingsRuleCountsWithPagination`

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `50`

The maximum number of results to show per page.

Example

```
{
  "contentTypeRules": ContentTypeRuleCountsWithPagination,
  "cookieConsistencyRules": CookieConsistencyRuleCountsWithPagination,
  "crossSiteScriptingRules": HTMLXSSRuleCountsWithPagination,
  "csrfSettingsRules": CSRFSettingsRuleCountsWithPagination,
  "fieldConsistencyRules": FieldConsistencyRuleCountsWithPagination,
  "fieldFormatRules": FieldFormatRuleCountsWithPagination,
  "htmlSQLInjectionRules": HTMLSQLInjectionRuleCountsWithPagination,
  "wsiSettingsRules": WSISettingsRuleCountsWithPagination
}
```

Types

`LegacyApplicationService`

Application services that make up the back end of the virtual server.

Field Name	Description
`origin` - `String!`	The IP address for the application service.

`port` - `UnsignedInt16!`	The port number for the application service.
`protocol` - `ProxyProtocol!`	The protocol type used for this virtual server's front and back ends.

Example

```
{
  "origin": "abc123",
  "port": UnsignedInt16,
  "protocol": ProxyProtocol
}
```

Types

LegacyCertificateBinding

Certificate information for a back end.

Field Name	Description
`certificateID` - `String!`	Common name used for SNI initiation.
`sni` - `Boolean!`	Forces back-end SNI support between the proxy and the origin, sending the specified common name to initiate SNI to the back end.

Example

```
{"certificateID": "xyz789", "sni": false}
```

Types

LegacyProxy

A proxy configured on hardware appliances.

Field Name	Description
`company` - `Company!`	Company for which this proxy is configured.
`createdAt` - `Time!`	Time when this proxy was created.
`deletedAt` - `Time`	Time when this proxy was deleted.
`id` - `String!`	ID of this proxy.

`ip` - `IPAddress!`	IP or hostname.
`ipVersion` - `IPVersion!`	The IP version of this host.
`name` - `String!`	Friendly name of the proxy configuration. Typically set to the hostname being proxied to the services.
`provisioningStatus` - `ProxyProvisioningStatus`	The provisioning status of this proxy.
`readOnly` - `Boolean!`	Indicates whether the configuration of this proxy can be updated by the customer.
`updatedAt` - `Time!`	Time when this proxy was last updated.
`vServers` - `[LegacyVServer!]`	List of virtual servers configured for this proxy for delivering services.

Example

```
{
  "company": Company,
  "createdAt": Time,
  "deletedAt": Time,
  "id": "xyz789",
  "ip": IPAddress,
  "ipVersion": IPVersion,
  "name": "xyz789",
  "provisioningStatus": ProxyProvisioningStatus,
  "readOnly": false,
  "updatedAt": Time,
  "vServers": [LegacyVServer]
}
```

Types

`LegacyTLSOptions`

TLS settings for the virtual server that is using TLS/SSL.

Field Name	Description

`commonName` - `String`	Common name to be sent with request to back-end origin(s).
`forceBackendSNI` - `Boolean!`	Forces back-end SNI support between the proxy and the origin, sending the specified common name to initiate SNI to the back end.
`hstsEnabled` - `Boolean!`	Flag indicating whether or not to follow HTTP Strict Transport Security.
`hstsIncludeSubdomains` - `Boolean!`	Flag indicating whether to include subdomains parameter in HSTS.
`hstsMaxAge` - `UnsignedInt32!`	MaxAge parameter for HSTS.
`hstsPreload` - `Boolean!`	Flag indicating whether to include preload parameter in HSTS.
`minTLSVersion` - `MinTLSVersion!`	Minimum TLS versions to support.

Example

```
{
  "commonName": "xyz789",
  "forceBackendSNI": true,
  "hstsEnabled": false,
  "hstsIncludeSubdomains": false,
  "hstsMaxAge": UnsignedInt32,
  "hstsPreload": true,
  "minTLSVersion": MinTLSVersion
}
```

Types

LegacyVServer

A virtual server, part of a legacy hardward proxy configuration.

Field Name	Description
`applicationServices` - `[LegacyApplicationService!]`	Application services that make up this virtual server's back end.
`certificateBindings` - `[LegacyCertificateBinding!]`	Certficate(s) for this virtual server.
`company` - `Company!`	Company the proxy configuration belongs to.

`loadBalanceMethod` - `ProxyLoadBalanceMethod!`	Method used to load-balance connections to application services.
`persistenceType` - `ProxyLoadBalancePersistenceType!`	A session persistence type to apply to requests.
`port` - `UnsignedInt16!`	The virtual server's front-end port.
`protocol` - `ProxyProtocol!`	Protocol type used for the front and back ends.
`sp` - `Boolean!`	Ensure connections to the server occur at a rate that the server can handle.
`tcpb` - `Boolean!`	Use TCP Buffering for the service.
`tlsOptions` - `LegacyTLSOptions`	TLS/SSL protocol options.
`xffHeader` - `String!`	The name of the 'forwarded-for' header.

Example

```
{
  "applicationServices": [LegacyApplicationService],
  "certificateBindings": [LegacyCertificateBinding],
  "company": Company,
  "loadBalanceMethod": ProxyLoadBalanceMethod,
  "persistenceType": ProxyLoadBalancePersistenceType,
  "port": UnsignedInt16,
  "protocol": ProxyProtocol,
  "sp": false,
  "tcpb": true,
  "tlsOptions": LegacyTLSOptions,
  "xffHeader": "abc123"
}
```

Types

`Link`

A URL and Label.

Field Name	Description

`label` - `String!`	Company label.
`url` - `String!`	Company URL to be displayed.

Example

```
{"label": "xyz789", "url": "abc123"}
```

Types

LogTime

The Date/Time format used for Violation logs time fields is UTC time with trailing zeroes for subfraction millseconds value.

Example

```
object
```

Types

MFAPackage

Specifies Multi Factor Authentication configuration for company.

Field Name	Description
`enabled` - `Boolean!`	Whether multi-factor authentication (MFA) is enabled for the Company.

Example

```
{"enabled": true}
```

Types

ManagedObject

Managed Objects

Field Name	Description
`company` - `Company!`	

`elementType` - `ManagedObjectElementType`	The type of traffic association criteria for the elements.
`id` - `String!`	Identifier of the managed object.
`mitigationTemplates` - `[MitigationTemplate!]`	List of mitigation templates associated
`name` - `String!`	
`types` - `[ManagedObjectType!]`	List of managed object type.

Example

```
{
  "company": Company,
  "elementType": ManagedObjectElementType,
  "id": "xyz789",
  "mitigationTemplates": [MitigationTemplate],
  "name": "abc123",
  "types": [ManagedObjectType]
}
```

Types

ManagedObjectElement

The type of the element for associating traffic with the managed object.

Union Types

`ManagedObjectElementGroup`
`ManagedObjectElementSimple`

Types

ManagedObjectElementGroup

The type of the element that contains a list of values and an associated tag.

Field Name	Description
`tag` - `String`	The tag for the list of values.
`values` - `[String!]`	List of values for the element.

Example

```
{"tag": "xyz789", "values": ["xyz789"]}
```

Types

ManagedObjectElementSimple

The type of the element that contains only a single value.

Field Name	Description
`value` - `String!`	The single value of the element.

Example

```
{"value": "abc123"}
```

Types

ManagedObjectElementType

The type of traffic association criteria for an element.

Enum Value	Description
`ADVANCED`	
`APP_ID`	
`AS_REGEX`	
`CIDR_BLOCKS`	
`CIDR_GROUPS`	
`CIDR_V6_BLOCKS`	
`COMMUNITY`	
`DDOS_DEVICE_PORTS`	
`EXTENDED_COMMUNITY`	
`INTERFACE`	
`PEER_AS`	
`PROFILED_INTERFACE_GROUP`	

SUB_AS

Types

ManagedObjectFilterInput

Input Field	Description
types - [ManagedObjectType!]	

Example

```
{"types": [ManagedObjectType]}
```

Types

ManagedObjectType

Types of Managed Objects.

Enum Value	Description
BGP	
DNA	
PROXY	

Types

Map

Example

```
object
```

Types

MinTLSVersion

Supported Minimum TLS version.

Enum Value	Description

`V_1_0`
`V_1_1`
`V_1_1_PFS`
`V_1_2`
`V_1_3`

Types

`Mitigation`

Fields shared among Mitigation types.

Field Name	Description
`company` - `Company!`	The company object.
`end` - `Time`	The end time of the mitigation. A non-zero value of end time means that the mitigation has ended.
`id` - `String!`	The identifier of the mitigation.
`start` - `Time!`	The start time of the mitigation.

Example

```
{
  "company": Company,
  "end": Time,
  "id": "abc123",
  "start": Time
}
```

Types

`MitigationDimension`

Mitigation dimensions to sort by.

Enum Value	Description
`END`	
`START`	

Types

MitigationFilterInput

The filters that can be applied to scope the list of mitigations.

Input Field	Description
`active` - `Boolean`	Include active mitigations when set to true or inactive when set to false. By default, all mitigations are fetched regardless of whether they are active or not.

Example

```
{"active": true}
```

Types

MitigationSortBy

How to sort Mitigations.

Input Field	Description
`dimension` - `MitigationDimension!` default = `"START"`	The dimension to sort by.
`direction` - `SortDirection!` default = `"DESCENDING"`	The direction to sort in.

Example

```
{
  "dimension": "START",
  "direction": "DESCENDING"
}
```

Types

MitigationTemplate

Mitigation Templates

Field Name	Description
`company` - `Company!`	
`deviceGroup` - `DeviceGroup`	Device group
`filterList` - `[DDOSFilter!]`	List of filters configured for this template

`id` - `String!`	Identifier for this Mitigation Template.
`ipVersion` - `IPVersion`	

Example

```
{
  "company": Company,
  "deviceGroup": DeviceGroup,
  "filterList": [DDOSFilter],
  "id": "xyz789",
  "ipVersion": IPVersion
}
```

Types

`MitigationsWithPagination`

Represents the list of mitigations along with pagination details.

Field Name	Description
`pageInfo` - `Pagination!`	The pagination details.
`results` - `[Mitigation!]`	The list of mitigations.

Example

```
{
  "pageInfo": Pagination,
  "results": [Mitigation]
}
```

Types

`NetworkControls`

Network controls for a given policy.

Field Name	Description
`blockedCountries` - `[CountryCode!]`	A list of blocked countries.
`ipFilterList` - `IPFiltersWithPagination`	A paginated list of ip filters.

Arguments

`filter` - `IPFilterFilterInput`

Ways to filter the list of IPFilters.

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

Example

```
{
  "blockedCountries": [CountryCode],
  "ipFilterList": IPFiltersWithPagination
}
```

Types

NetworkNode

A collection of devices and services located together in one physical location.

Field Name	Description
`description` - `String!`	A user-friendly description.
`iataCode` - `String!`	An identifier for the node. Based on IATA code for the nearest (major) airport.

Example

```
{"description": "abc123", "iataCode": "abc123"}
```

Types

NetworkNodeFilterInput

Reducing list of or choosing specific nodes.

Input Field	Description
`iataCode` - `String`	An identifier for the node. Based on IATA code for the nearest (major) airport.

`includeDeleted` - `Boolean`	Whether to include previously-deleted ones.

Example

```
{"iataCode": "abc123", "includeDeleted": false}
```

Types

`OneTimeExecutiveReportConfiguration`

One time report configuration.

Field Name	Description
`createdAt` - `Time`	Timestamp when report is created.
`description` - `String`	Description of Report Configuration.
`enabled` - `Boolean`	If enabled, this configuration will generate a report.
`from` - `Time`	Starting timestamp for metrics to be pulled from.
`id` - `String!`	ID of one time report configuration.
`includeBot` - `Boolean`	If true, includes Bot mitigation summary in report.
`includeDDOS` - `Boolean`	If true, includes DDOS mitigation summary in report.
`includeWAF` - `Boolean`	If true, includes WAF violation summary in report.
`name` - `String!`	Name of one time report configuration.
`notification` - `ExecutiveReportNotificationDetails`	Email recepient list to send reports to.
`reportType` - `ExecutiveReportType!`	Type of report.
`to` - `Time`	Ending timestamp for metrics to be pulled from.

Example

```
{
  "createdAt": Time,
  "description": "abc123",
  "enabled": false,
  "from": Time,
  "id": "abc123",
  "includeBot": true,
  "includeDDOS": true,
  "includeWAF": false,
  "name": "xyz789",
  "notification": ExecutiveReportNotificationDetails,
  "reportType": ExecutiveReportType,
  "to": Time
}
```

Types

OneTimeExecutiveReportConfigurationsWithPagination

Paginated One time report configurations.

Field Name	Description
`pageInfo` - `Pagination!`	Pagination settings.
`results` - `[OneTimeExecutiveReportConfiguration!]`	List of one time report configurations.

Example

```
{
  "pageInfo": Pagination,
  "results": [OneTimeExecutiveReportConfiguration]
}
```

Types

POSTBody

A POST BODY limit countermeasure.

Field Name	Description
`limit` - `UnsignedInt32!`	A post body size limit value.

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for post body limit violations.

Example

```
{
  "limit": UnsignedInt32,
  "threshold": AppSecThreshold
}
```

Types

Pagination

Pagination base type.

Field Name	Description
`itemsPerPage` - `UnsignedInt32!`	Number of items per page.
`pageNumber` - `UnsignedInt32!`	Current page number.
`totalItems` - `UnsignedInt64!`	The number of items that would have been returned if pagination hadn't been applied.

Example

```
{
  "itemsPerPage": UnsignedInt32,
  "pageNumber": UnsignedInt32,
  "totalItems": UnsignedInt64
}
```

Types

Person

Details of a contact, such as an Account Executive.

Field Name	Description
`email` - `String!`	Email of contact Person.
`name` - `String!`	Name of contact Person.
`phone` - `String!`	Phone number of contact Person.

Example

```
{"email": "abc123", "name": "xyz789", "phone": "abc123"}
```

Types

Policy

A configurable set of options that can be employed to secure Company assets.

Field Name	Description
`appSecThresholds` - `[AppSecThreshold!]`	The appsec thresholds associated to this policy.
`botProfile` - `BotProfile`	The bot profile associated to this policy.
`company` - `Company!`	The name of the company.
`createdAt` - `Time!`	The time at which the policy was created.
`deletedAt` - `Time`	The time at which the policy was deleted.
`id` - `String!`	ID of the policy.
`key` - `String!`	A unique string representing a policy.
`learningRules` - `LearningRules`	Learning rules associated with the Policy.
`name` - `String!`	The name of the policy.
`networkControls` - `NetworkControls`	The network controls associated to this policy.
`proxies` - `[Proxy!]`	A list of proxies using this policy.
Arguments	
`filter` - `ProxyFilterInput`	
`responderPolicies` - `[ResponderPolicy!]`	The responder polices associated to this policy.
`trustedSources` - `TrustedSourcesWithPagination`	The trusted IP sources associated to this policy. Traffic at these sources are used by the learning

	feature to generate recommendations.

Arguments
 	
`page` - `UnsignedInt32!` default = `1`
 	
The page number to fetch results for.
 	
`perPage` - `UnsignedInt32!` default = `1000`
 	
The maximum number of results to show per page.	

`updatedAt` - `Time!`	The time at which the policy was updated.
`wafProfile` - `WAFProfile`	The WAF profile associated to this policy.

Example

```
{
  "appSecThresholds": [AppSecThreshold],
  "botProfile": BotProfile,
  "company": Company,
  "createdAt": Time,
  "deletedAt": Time,
  "id": "abc123",
  "key": "abc123",
  "learningRules": LearningRules,
  "name": "abc123",
  "networkControls": NetworkControls,
  "proxies": [Proxy],
  "responderPolicies": [ResponderPolicy],
  "trustedSources": TrustedSourcesWithPagination,
  "updatedAt": Time,
  "wafProfile": WAFProfile
}
```

Types

`PolicyFilterInput`

Filter a list of policies.

Input Field	Description

`id` - `String`	ID of the policy.
`includeDeleted` - `Boolean!` default = `false`	Flag to indicate if we need to include the deleted policies as part of this search.
`key` - `String`	A unique string representing a policy.

Example

```
{"id": "abc123", "includeDeleted": false, "key": "xyz789"}
```

Types

Proxy

A proxy configuration.

Field Name	Description
`company` - `Company!`	Company the proxy configuration belongs to.
`createdAt` - `Time!`	Time proxy was created.
`deletedAt` - `Time`	Time proxy was deleted.
`id` - `String!`	ID of this proxy.
`ip` - `IPAddress!`	IP or hostname.
`ipVersion` - `IPVersion!`	The IP version of this host.
`name` - `String!`	Friendly name of the proxy configuration. Typically set to the hostname being proxied to the service.
`policies` - `[Policy!]`	A list of policies associated with this proxy.
`updatedAt` - `Time!`	Time proxy was updated.
`vServerStatus` - `[VServerStatus!]`	Status values for the vServers.
`vServers` - `[VServer!]`	The back-end origin servers, ports and protocols that bind it to the front-end port.

Example

```
{
  "company": Company,
  "createdAt": Time,
  "deletedAt": Time,
```

```
  "id": "xyz789",
  "ip": IPAddress,
  "ipVersion": IPVersion,
  "name": "xyz789",
  "policies": [Policy],
  "updatedAt": Time,
  "vServerStatus": [VServerStatus],
  "vServers": [VServer]
}
```

Types

ProxyFilterInput

Input required if extra criteria are needed to constrain the queried results.

Input Field	Description
`id` - `String`	If provided, ID of proxy to be queried.
`includeDeleted` - `Boolean!` default = `false`	If true is provided, proxies returned will include deleted Proxies.

Example

```
{"id": "abc123", "includeDeleted": false}
```

Types

ProxyLoadBalanceMethod

Load-balancing options.

Enum Value	Description
`DESTINATION_IP_HASH`	
`DOMAIN_HASH`	
`LEAST_BANDWIDTH`	
`LEAST_CONNECTION`	
`LEAST_PACKETS`	
`LEAST_REQUEST`	
`LEAST_RESPONSE_TIME`	

`LRTM`	
`ROUND_ROBIN`	
`SOURCE_DEST_IP_HASH`	
`SOURCE_IP_HASH`	
`SOURCE_IP_SOURCE_PORT_HASH`	
`URL_HASH`	

Types

ProxyLoadBalancePersistenceType

Type of session persistence to apply to requests.

Enum Value	Description
`COOKIE_INSERT`	
`SOURCE_IP`	

Types

ProxyPackage

Per-Company Proxy settings.

Field Name	Description
`basicWAFEnabled` - `Boolean!`	Specifies whether the basic Web Application Firewall offering is enabled for this company's VIPs.
`botEnabled` - `Boolean!`	Specifies whether the Bot Management offering is enabled for this company's VIPs.
`dName` - `String!`	The identifier of the owning company.
`enableHTTPSPacketInspection` - `Boolean!`	Specifies whether HTTPS packet introspection is turned on.
`enabled` - `Boolean!`	Whether proxy access is enabled for the Company.
`managedObjects` - `[ManagedObject!]`	List of proxy managed objects.

`maxSSLCertificates` - `UnsignedInt16!`	Specifies the max number of SSL certificates that can be configured for this company on all its VIPs combined.
`maxWAFSignatures` - `UnsignedInt16!`	Specifies the max number of signatures allowed for this company for its Web Application Firewall.
`networkEnabled` - `Boolean!`	Specifies whether the VIP network is enabled.
`policyEnabled` - `Boolean!`	Specifies whether L7 policies are enabled for Virtual IPs.
`proxyType` - `ProxyType`	Specifies type of proxy (hardware/cloud/none) for this company.
`ultraWAFEnabled` - `Boolean!`	Specifies whether the Ultra Web Application Firewall offering is enabled for this company's VIPs.
`vipCategory` - `String!`	Specifies the Virtual IP Category for this company.
`vipPoolAllocationLimit` - `UnsignedInt32!`	Specifies the max number of Virtual IPs that can be allocated to this company.
`wafEnabled` - `Boolean!`	Specifies whether Web Application Firewall is enabled for this company's Virtual IPs.

Example


```
{
  "basicWAFEnabled": true,
  "botEnabled": false,
  "dName": "xyz789",
  "enableHTTPSPacketInspection": true,
  "enabled": true,
  "managedObjects": [ManagedObject],
  "maxSSLCertificates": UnsignedInt16,
  "maxWAFSignatures": UnsignedInt16,
  "networkEnabled": true,
  "policyEnabled": true,
  "proxyType": ProxyType,
  "ultraWAFEnabled": true,
  "vipCategory": "abc123",
  "vipPoolAllocationLimit": UnsignedInt32,
  "wafEnabled": false
```

```
}
```

Types

ProxyProtocol

Allowed list of values for the front end protocol of a proxy.

Enum Value	Description
DNS	
DNS_TCP	
HTTP	
SSL	
SSL_BRIDGE	
TCP	
UDP	

Types

ProxyProvisioningStatus

Possible states of a proxy provisioning.

Enum Value	Description
COMPLETE	
FAILED	
IN_PROGRESS	

Types

ProxyType

Defines type of proxy virtual IP offering.

Enum Value	Description
CLOUD	Indicates VIPs on a cloud load balancer offering.
HARDWARE	Indicates VIPs on a hardware load balancer offering.

`NONE`	Indicates no Proxy.

Types

`RawJSON`

Example

```
object
```

Types

`RecurringExecutiveReportConfiguration`

Recurring report configuration.

Field Name	Description
`createdAt` - `Time`	Timestamp the report configuration was created at.
`description` - `String`	Description of Report Configuration.
`enabled` - `Boolean`	If true, this report configuration generates reports.
`from` - `Time`	Timestamp from when the first report is generated by this configuration.
`id` - `String!`	ID of recurring report configuration.
`includeBot` - `Boolean`	If true, includes Bot mitigation summary in the report.
`includeDDOS` - `Boolean`	If true, includes DDOS mitigation summary in the report.
`includeWAF` - `Boolean`	If true, includes WAF violation summary in the report.

`name` - `String!`	Name of recurring report configuration.
`notification` - `ExecutiveReportNotificationDetails`	List of email recepients of generated reports.
`period` - `ExecutiveReportPeriod!`	Metric summary interval of report.
`reportType` - `ExecutiveReportType!`	Type of report.
`to` - `Time`	Timestamp when this report configuration will expire and won't be run after.

Example

```
{
  "createdAt": Time,
  "description": "xyz789",
  "enabled": false,
  "from": Time,
  "id": "abc123",
  "includeBot": true,
  "includeDDOS": true,
  "includeWAF": false,
  "name": "abc123",
  "notification": ExecutiveReportNotificationDetails,
  "period": ExecutiveReportPeriod,
  "reportType": ExecutiveReportType,
  "to": Time
}
```

Types

`RecurringExecutiveReportConfigurationsWithPagination`

Paginated recurring report configurations.

Field Name	Description
`pageInfo` - `Pagination!`	Pagination settings.
`results` - `[RecurringExecutiveReportConfiguration!]`	List of recurring report configurations.

Example

```
{
  "pageInfo": Pagination,
  "results": [RecurringExecutiveReportConfiguration]
}
```

Types

ResponderAction

Allowed values for the responder action.

Enum Value	Description
DROP	
LOG	
REDIRECT_TO	
RESPOND_WITH	

Types

ResponderAnalyticsResponse

Field Name	Description
groups - [ResponderLogGroup!]	
logs - ResponderLogsWithPagination	
timeSeriesData - [ResponderLogTimeSeries!]	

Example

```
{
  "groups": [ResponderLogGroup],
  "logs": ResponderLogsWithPagination,
  "timeSeriesData": [ResponderLogTimeSeries]
}
```

Types

ResponderField

Allowed values for the responder match field.

Enum Value	Description
`CONTENT_TYPE`	
`COOKIE_SET_NAMES`	
`DESTINATION_PORT`	
`HEADER_SECTION`	
`HEADER_SECTION_SIZE`	
`HOSTNAME`	
`QUERY_STRING`	
`REFERER_URL`	
`REQUEST_SIZE`	
`SOURCE_IP`	
`URL_PATH`	
`X_FORWARDED_FOR`	

Types

ResponderLog

Represents a Responder Policy log.

Field Name	Description
`cookies` - `String`	The cookies in the original request.
`customer` - `String`	The customer account dname.
`destinationIP` - `IPAddress`	The destination IP the request was intended for.
`destinationPort` - `UnsignedInt16`	The destination port the request was intended for.
`domain` - `String`	The domain the request was intended for.
`host` - `String`	The hostname in the request.
`logType` - `ResponderLogType`	The responder log type
`method` - `String`	The HTTP method used.
`policyKey` - `String`	The policy key tied to this responder.

`responderAction` - `String`	The responder_action that caused this violation log.
`responderName` - `String`	The responder name in our DB. This will be null for log type network_control.
`sourceIP` - `IPAddress`	The source IP the request was intended for.
`timestamp` - `LogTime`	The timestamp of the violation log.
`uri` - `String`	The uri in the request.
`version` - `String`	The version.

Example

```
{
  "cookies": "abc123",
  "customer": "abc123",
  "destinationIP": IPAddress,
  "destinationPort": UnsignedInt16,
  "domain": "abc123",
  "host": "xyz789",
  "logType": ResponderLogType,
  "method": "xyz789",
  "policyKey": "xyz789",
  "responderAction": "xyz789",
  "responderName": "xyz789",
  "sourceIP": IPAddress,
  "timestamp": LogTime,
  "uri": "abc123",
  "version": "abc123"
}
```

Types

ResponderLogDimension

Enum Value	Description
`DESTINATION_IP`	
`RESPONDER_ACTION`	
`RESPONDER_NAME`	
`SOURCE_IP`	
`TIMESTAMP`	

`URI`

Types

`ResponderLogFilterInput`

Represents a Responder log filter input.

Input Field	Description
`all` - `String`	When set, the application looks in all the filters (destionationIP,sourceIP,uri,responderAction) for the input string.
`destinationIP` - `IPAddressInput`	The destination IP of the request.
`logType` - `ResponderLogType`	The responder log type
`responderAction` - `String`	The responder action triggering the logs.
`sourceIP` - `IPAddressInput`	The source IP of the request.
`uri` - `String`	The uri which cause the violation.

Example

```
{
  "all": "xyz789",
  "destinationIP": IPAddressInput,
  "logType": ResponderLogType,
  "responderAction": "xyz789",
  "sourceIP": IPAddressInput,
  "uri": "xyz789"
}
```

Types

`ResponderLogGroup`

A responder log group object.

Field Name	Description
`count` - `UnsignedInt32!`	The count of responder logs in this group.
`key` - `String!`	The group name.

Example

```
{"count": UnsignedInt32, "key": "abc123"}
```

Types

ResponderLogGroupByField

Enum Value	Description
DESTINATION_IP	
RESPONDER_ACTION	
RESPONDER_NAME	
SOURCE_IP	
URI	

Types

ResponderLogGroupByInput

Input Field	Description
direction - SortDirection! default = "DESCENDING"	The order of the groups listed (ascending or descending).
field - ResponderLogGroupByField!	
timeInterval - TimeInterval	

Example

```
{
  "direction": "DESCENDING",
  "field": ResponderLogGroupByField,
  "timeInterval": TimeInterval
}
```

Types

ResponderLogSortBy

Represents a responder log sort input.

Input Field	Description
`dimension` - `ResponderLogDimension!`	The dimension that will be used to sort the logs.
`direction` - `SortDirection!` default = `"DESCENDING"`	The order of the sort (ascending or descending).

Example

```
{
  "dimension": ResponderLogDimension,
  "direction": "DESCENDING"
}
```

Types

ResponderLogTimeSeries

Field Name	Description
`cnt` - `UnsignedInt64!`	
`key` - `String!`	
`ts` - `Time!`	

Example

```
{
  "cnt": UnsignedInt64,
  "key": "abc123",
  "ts": Time
}
```

Types

ResponderLogType

Enum Value	Description
`NETWORK_CONTROL`	
`RESPONDER`	

Types

ResponderLogsWithPagination

Field Name	Description
pageInfo - Pagination!	
results - [ResponderLog!]	

Example

```
{
  "pageInfo": Pagination,
  "results": [ResponderLog]
}
```

Types

ResponderMatch

A responder match in a given responder policy.

Field Name	Description
field - ResponderField!	The field name for the match.
operand - ResponderOperand!	The operand to be used for the match.
value - String!	The value to be used for the match.

Example

```
{
  "field": ResponderField,
  "operand": ResponderOperand,
  "value": "abc123"
}
```

Types

ResponderMatchInput

Create a responder match in a given responder policy.

Input Field	Description
`field` - `ResponderField!`	The field name for the match.
`operand` - `ResponderOperand!`	The operand to be used for the match.
`value` - `String!`	The value to be used for the match.

Example

```
{
  "field": ResponderField,
  "operand": ResponderOperand,
  "value": "abc123"
}
```

Types

ResponderOperand

Allowed values for the responder match operand.

Enum Value	Description
`CONTAINS`	
`DOES_NOT_CONTAIN`	
`DOES_NOT_EQUAL`	
`ENDS_WITH`	
`EQUALS`	
`GREATER_THAN`	
`IN_SUBNET`	
`LESS_THAN`	
`NOT_IN_SUBNET`	
`RATE_LIMIT`	
`STARTS_WITH`	

Types

ResponderPolicy

A responder policy for a given policy.

Field Name	Description
`action` - `ResponderAction!`	Action to be taken when the responder matches are found.
`name` - `String!`	The name of the responder policy.
`responderMatches` - `[ResponderMatch!]`	List of responder matches for this responder policy.
`response` - `String`	Response to be returned when the responder matches. NA when action is LOG OR DROP. Value is a URL when the action is REDIRECT_TO, value is a text found when action is when the action is RESPOND_WITH.

Example

```
{
  "action": ResponderAction,
  "name": "xyz789",
  "responderMatches": [ResponderMatch],
  "response": "abc123"
}
```

Types

`ResponderPolicyInput`

Create a responder policy for a given policy.

Input Field	Description
`action` - `ResponderAction!`	Action to be taken when the responder matches are found.
`name` - `String!`	The name of the responder policy.
`responderMatches` - `[ResponderMatchInput!]`	List of responder matches for this responder policy.
`response` - `String`	Response to be returned when the responder matches. NA when action is LOG OR DROP. Value is a URL when the action is REDIRECT_TO,

	value is a text found when action is when the action is RESPOND_WITH.

Example

```
{
  "action": ResponderAction,
  "name": "abc123",
  "responderMatches": [ResponderMatchInput],
  "response": "abc123"
}
```

Types

Router

Router Configuration

Field Name	Description
company - Company!	The company object.
flowConfig - FlowConfig	Flow configuration.
id - String!	Router identifier.
name - String!	
snmpConfig - SNMPConfig	SNMP configuration.

Example

```
{
  "company": Company,
  "flowConfig": FlowConfig,
  "id": "abc123",
  "name": "abc123",
  "snmpConfig": SNMPConfig
}
```

Types

SNMPConfig

SNMP Configuration

Field Name	Description
`community` - `String!`	SNMP community settings.
`ipAddress` - `IPAddress!`	SNMP server IP address.

Example

```
{"community": "abc123", "ipAddress": IPAddress}
```

Types

SQLInjectionType

Allowed list of injection types.

Enum Value	Description
`NONE`	
`SQL_KEYWORD`	
`SQL_SPECIAL_CHARACTER`	
`SQL_SPECIAL_CHARACTER_AND_KEYWORD`	
`SQL_SPECIAL_CHARACTER_OR_KEYWORD`	

Types

SemicolonFieldSeparator

A Semicolon field separator countermeasure.

Field Name	Description
`enabled` - `Boolean`	Whether the countermeasure is enabled.

Example

```
{"enabled": true}
```

Types

SendUserActivationEmailInput

Send user activation email.

Input Field	Description
`id` - `String!`	ID of the user to send activation email.

Example

```
{"id": "xyz789"}
```

Types

`SendUserActivationEmailOutput`

A send user activation email response.

Field Name	Description
`email` - `String!`	Email of the user.
`id` - `String!`	ID of the user.

Example

```
{"email": "xyz789", "id": "abc123"}
```

Types

`SendUserPasswordResetEmailInput`

Send user password reset email.

Input Field	Description
`id` - `String!`	ID of the user to send password reset email.

Example

```
{"id": "abc123"}
```

Types

`SendUserPasswordResetEmailOutput`

A send user password reset email response.

Field Name	Description
`email` - `String!`	Email of the user.
`id` - `String!`	ID of the user.

Example

```
{"email": "abc123", "id": "xyz789"}
```

Types

SessionlessFieldConsistency

Allowed values for SessionlessFieldConsistency. To use Sessionless Field Consistency on all web forms use ON. To use it only for forms submitted with the HTTP POST method, select POST_ONLY.

Enum Value	Description
`OFF`	
`ON`	
`POST_ONLY`	

Types

SignatureMatchFormat

Allowed values for a custom signature match format.

Enum Value	Description
`LITERAL`	
`PCRE`	

Types

SignatureRequestArea

Allowed values for a custom signature request area.

Enum Value	Description
`HTTP_COOKIE`	

`HTTP_FORM_FIELD`
`HTTP_HEADER`
`HTTP_METHOD`
`HTTP_ORIGIN_URL`
`HTTP_POST_BODY`
`HTTP_RAW_URL`
`HTTP_URL`

Types

SignatureRequestRule

A WAF custom signature request rule.

Field Name	Description
`area` - `SignatureRequestArea!`	Area where this rule would apply.
`cookieRule` - `CookieSignatureRule`	A cookie rule, if exists. For a given request rule, only one of cookie, header or form field can exist.
`formFieldSignatureRule` - `FormFieldSignatureRule`	A form field rule, if exists. For a given request rule, only one of cookie, header or form field can exist.
`headerRule` - `HeaderSignatureRule`	A header rule , if exists. For a given request rule, only one of cookie, header or form field can exist.
`match` - `String!`	A match string.
`matchFormat` - `SignatureMatchFormat!`	A format for matching from allowed list of formats.

Example

```
{
  "area": SignatureRequestArea,
  "cookieRule": CookieSignatureRule,
```

```
  "formFieldSignatureRule": FormFieldSignatureRule,
  "headerRule": HeaderSignatureRule,
  "match": "abc123",
  "matchFormat": SignatureMatchFormat
}
```

Types

SignatureRequestRuleInput

Create a WAF custom signature request rule.

Input Field	Description
`area` - `SignatureRequestArea!`	Area where this rule would apply.
`cookieRule` - `CookieSignatureRuleInput`	A cookie rule, if exists. For a given request rule, only one of cookie, header or form field can exist.
`formFieldSignatureRule` - `FormFieldSignatureRuleInput`	A form field rule, if exists. For a given request rule, only one of cookie, header or form field can exist.
`headerRule` - `HeaderSignatureRuleInput`	A header rule , if exists. For a given request rule, only one of cookie, header or form field can exist.
`match` - `String!`	A match string.
`matchFormat` - `SignatureMatchFormat!`	A format for matching from allowed list of formats.

Example

```
{
  "area": SignatureRequestArea,
  "cookieRule": CookieSignatureRuleInput,
  "formFieldSignatureRule": FormFieldSignatureRuleInput,
  "headerRule": HeaderSignatureRuleInput,
```

```
  "match": "xyz789",
  "matchFormat": SignatureMatchFormat
}
```

Types

SignatureResponseArea

Allowed values for a custom signature response area.

Enum Value	Description
HTTP_RESPONSE_BODY	
HTTP_RESPONSE_HEADER	
HTTP_SET_COOKIE	
HTTP_STATUS_CODE	
HTTP_STATUS_MESSAGE	

Types

SignatureResponseRule

A WAF custom signature response rule.

Field Name	Description
area - SignatureResponseArea!	Area where this rule would apply.
match - String!	A match string.
matchFormat - SignatureMatchFormat!	A format for matching from allowed list of formats.

Example

```
{
  "area": SignatureResponseArea,
  "match": "xyz789",
  "matchFormat": SignatureMatchFormat
}
```

Types

SignatureResponseRuleInput

Create a WAF custom signature response rule.

Input Field	Description
area - SignatureResponseArea!	Area where this rule would apply.
match - String!	A match string.
matchFormat - SignatureMatchFormat!	A format for matching from allowed list of formats.

Example

```
{
  "area": SignatureResponseArea,
  "match": "abc123",
  "matchFormat": SignatureMatchFormat
}
```

Types

SignatureRuleFormat

Allowed values for a custom signature rule format.

Enum Value	Description
ANY	
LITERAL	
PCRE	

Types

SortDirection

Allowed sort direction values.

Enum Value	Description
ASCENDING	
DESCENDING	

Types

String

The `String` scalar type represents textual data, represented as UTF-8 character sequences. The String type is most often used by GraphQL to represent free-form human-readable text.
Types

TLSCipher

Allowed list of TLS cipher suites.

Enum Value	Description
`TLS1_2_ECDHE_RSA_AES128_GCM_SHA256`	
`TLS1_2_ECDHE_RSA_AES256_GCM_SHA384`	
`TLS1_2_ECDHE_RSA_AES_128_SHA256`	
`TLS1_2_ECDHE_RSA_AES_256_SHA384`	
`TLS1_3_AES128_GCM_SHA256`	
`TLS1_3_AES256_GCM_SHA384`	
`TLS1_3_CHACHA20_POLY1305_SHA256`	
`TLS1_AES_128_CBC_SHA`	
`TLS1_AES_256_CBC_SHA`	
`TLS1_ECDHE_RSA_AES128_SHA`	
`TLS1_ECDHE_RSA_AES256_SHA`	

Types

TLSOptions

These are TLS settings for a virtual server that is using TLS/SSL.

Field Name	Description

`cipherSelection` - `CipherSelectionMode!`	Cipher Selection options viz. DEFAULT or CUSTOM.
`ciphers` - `[TLSCipher!]`	List of TLS ciphers.
`commonName` - `String`	Common name to be sent with request to back-end origin(s).
`forceBackendSNI` - `Boolean!`	Forces back-end SNI support between the proxy and the origin, sending the specified common name to initiate SNI to the back end.
`hstsEnabled` - `Boolean!`	Flag indicating whether or not to follow HTTP Strict Transport Security.
`hstsIncludeSubdomains` - `Boolean!`	Flag indicating whether to include subdomains parameter in HSTS.
`hstsMaxAge` - `UnsignedInt32!`	MaxAge parameter for HSTS in seconds.
`hstsPreload` - `Boolean!`	Flag indicating whether to include preload parameter in HSTS.
`minTLSVersion` - `MinTLSVersion!`	Minimum TLS versions to support. TLS 1.3 is support only for front end.

Example

```
{
  "cipherSelection": CipherSelectionMode,
  "ciphers": [TLSCipher],
  "commonName": "xyz789",
  "forceBackendSNI": true,
  "hstsEnabled": false,
  "hstsIncludeSubdomains": false,
  "hstsMaxAge": UnsignedInt32,
  "hstsPreload": true,
  "minTLSVersion": MinTLSVersion
}
```

Types

`TLSOptionsInput`

Define TLS options for a virtual server.

Input Field	Description

`cipherSelection` - `CipherSelectionMode!` default = `"DEFAULT"`	Cipher Selection options viz. DEFAULT or CUSTOM.
`ciphers` - `[TLSCipher!]`	List of TLS ciphers. At least one cipher should be selected for every version equal to and above the selected version. If not, default list of secure ciphers will be applied.
`commonName` - `String!`	Common name to be sent with request to back end origin(s).
`forceBackendSNI` - `Boolean!` default = `false`	Forces back-end SNI support between the proxy and the origin, sending the specified common name to initiate SNI to the back end.
`hstsEnabled` - `Boolean!` default = `false`	Flag indicating to follow HTTP Strict Transport Security.
`hstsIncludeSubdomains` - `Boolean!` default = `false`	Flag indicating whether to include subdomains parameter in HSTS.
`hstsMaxAge` - `UnsignedInt32!` default = `63072000`	MaxAge parameter for HSTS in seconds. Default is 2 years
`hstsPreload` - `Boolean!` default = `false`	Flag indicating whether to include preload parameter in HSTS.
`minTLSVersion` - `MinTLSVersion!`	Minimum TLS versions to support.

Example

```
{
  "cipherSelection": "DEFAULT",
  "ciphers": [TLSCipher],
  "commonName": "xyz789",
  "forceBackendSNI": false,
  "hstsEnabled": false,
  "hstsIncludeSubdomains": false,
  "hstsMaxAge": 63072000,
  "hstsPreload": false,
  "minTLSVersion": MinTLSVersion
}
```

Types

ThresholdInput

Create a WAF Application Security (AppSec) Threshold.

Input Field	Description
bucketDurationSeconds - UnsignedInt32! default = 60	Time period within which the minimum number of violations need to occur in order to generate alerts. (allowed values : 60).
count - UnsignedInt32!	Minimum number of violations for generating alerts.(allowed value range: 1-1000).

Example

```
{"bucketDurationSeconds": 60, "count": UnsignedInt32}
```

Types

Time

Time type

Example

```
object
```

Types

TimeInterval

A time interval.

Input Field	Description
interval - UnsignedInt16!	The interval value.
unit - TimeUnit!	The time units of the interval value.

Example

```
{
  "interval": UnsignedInt16,
  "unit": TimeUnit
}
```

Types

TimeUnit

Allowed values for time unit.

Enum Value	Description
DAY	
HOUR	
MINUTE	

Types

TrafficByKey

Values grouped by a non-timestammp key, with optional sub-grouping.

Field Name	Description
k - String!	The key associated with the value.
v - Float	The value for the given key. Null returned for NaN and Infinity.

Example

```
{"k": "abc123", "v": 123.45}
```

Types

TrafficByTime

Values grouped by a timestamp, with optional sub-grouping.

Field Name	Description
ts - Time!	The time associated with the value.
v - Float	The value at the given time. Null returned for NaN and Infinity.

Example

```
{"ts": Time, "v": 123.45}
```

Types

TrafficData

Field Name	Description
`field` - `TrafficField!`	The data type queried.
`groupedBy` - `[TrafficDimension!]`	How the results are aggregated.
`id` - `ID!`	A unique identifier per query or subscription.
`metric` - `TrafficMetric!`	The metric queried.
`value` - `Float`	If no `groupedBy` is present, or the top-level `groupedBy` has `includeRollup: true`, this will be the overall value. Null returned for NaN and Infinity.

Example

```
{
  "field": TrafficField,
  "groupedBy": [TrafficDimension],
  "id": ID,
  "metric": TrafficMetric,
  "value": 987.65
}
```

Types

TrafficDimension

Dimensions that results may be grouped by

Enum Value	Description
`COUNTRY`	
`DAY`	
`DESTINATION_IP`	

`DESTINATION_PORT`
`HOUR`
`IP_PROTOCOL`
`IP_VERSION`
`MINUTE`
`NODE`
`SOURCE_ASN`

Types

`TrafficField`

Field values that can be included in `TrafficData`

Enum Value	Description
`IN_BITS`	
`IN_BITS_PER_SECOND`	
`IN_PACKETS`	
`IN_PACKETS_PER_SECOND`	
`MITIGATED_BITS`	
`MITIGATED_BITS_PER_SECOND`	
`MITIGATED_PACKETS`	
`MITIGATED_PACKETS_PER_SECOND`	
`OUT_BITS`	
`OUT_BITS_PER_SECOND`	
`OUT_PACKETS`	
`OUT_PACKETS_PER_SECOND`	

Types

`TrafficMetric`

Metrics that can be reported for fields.

Enum Value	Description
`AVERAGE`	
`MAX`	
`MIN`	
`PERCENTILE_50`	
`PERCENTILE_95`	
`SUM`	

Types

`TrafficSortBy`

Sort criteria.

Either `field`/`metric` or `dimension` must be specified, and only one or the other. If `field`/`metric` is given, it must be a valid combination from the request `fields`/`metrics` lists. If `dimension` is given, it must be one of the `groupBy` dimensions.

Input Field	Description
`dimension` - `TrafficDimension`	A dimension to sort by.
`direction` - `SortDirection!` default = `"ASCENDING"`	The direction to sort in.
`field` - `TrafficField`	A field whose metric will be sorted on.
`metric` - `TrafficMetric`	The metric for the field to be sorted on.

Example

```
{
  "dimension": TrafficDimension,
  "direction": "ASCENDING",
  "field": TrafficField,
  "metric": TrafficMetric
}
```

Types

TrafficValue

Various types of grouped field/metric values.

Union Types
TrafficByKey
TrafficByTime

Types

TrustedSource

A trusted IP source.

Field Name	Description
cidr - CIDR!	CIDR of the trusted source.
description - String	Description of the trusted source.
enabled - Boolean!	Whether the trusted source is enabled.

Example

```
{"cidr": CIDR, "description": "abc123", "enabled": false}
```

Types

TrustedSourceInput

A trusted IP source.

Input Field	Description
cidr - CIDR!	CIDR of the trusted source.
description - String	Description of the trusted source.
enabled - Boolean! default = true	Whether the trusted source is enabled.

Example

```
{"cidr": CIDR, "description": "abc123", "enabled": true}
```

Types

TrustedSourcesWithPagination

A paginated list of trusted IP sources. Traffic at these sources are used by the learning feature to generate recommendations.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[TrustedSource!]`	The trusted sources.

Example

```
{
  "pageInfo": Pagination,
  "results": [TrustedSource]
}
```

Types

Tunnel

Network tunnel to send clean traffic through.

Field Name	Description
`addressV4` - `[IPv4Address!]`	IPv4 address of the tunnel, network-side.
`addressV6` - `[IPv6Address!]`	IPv6 address of the tunnel, network-side.
`customerAddressV4` - `[IPv4Address!]`	IPv4 address of the tunnel, customer-side.
`customerAddressV6` - `[IPv6Address!]`	IPv6 address of the tunnel, customer-side.
`customerDescription` - `String`	Human-readable description.
`description` - `String!`	Brief description generated by the system.
`destinationIPs` - `[CIDR!]`	Destination IPs sent through this tunnel.
`devices` - `[String!]`	Internal descriptors for network devices implementing the tunnel.
`id` - `String!`	The unique identifier to distinguish tunnels. This identifier is same as the qualified device interface path.
`interfacePath` - `String`	Qualified Device Interface Path.

`networkNodes` - `[NetworkNode!]`	Physical interconnect points.
`tunnelDestination` - `String`	Tunnel destination description.
`tunnelSource` - `String`	Tunnel source description.
`type` - `TunnelType!`	Tunnel type.

Example


```
{
  "addressV4": [IPv4Address],
  "addressV6": [IPv6Address],
  "customerAddressV4": [IPv4Address],
  "customerAddressV6": [IPv6Address],
  "customerDescription": "abc123",
  "description": "xyz789",
  "destinationIPs": [CIDR],
  "devices": ["abc123"],
  "id": "abc123",
  "interfacePath": "xyz789",
  "networkNodes": [NetworkNode],
  "tunnelDestination": "abc123",
  "tunnelSource": "abc123",
  "type": TunnelType
}
```


Types

`TunnelType`

Tunnel type.

Enum Value	Description
`DIRECT_CONNECT`	
`DIRECT_CONNECT_TE`	
`GRE`	
`GRE_TE`	

Types

`UnsignedInt16`

Example

```
object
```

Types

UnsignedInt32

Unsigned int 32 type

Example

```
object
```

Types

UnsignedInt64

Unsigned int 64 type

Example

```
object
```

Types

UpdateBotBlackListInput

Modify a black list countermeasure.

Input Field	Description
`enabled` - `Boolean`	Whether the black list countermeasure is enabled.
`types` - `[BotBlackListBindingInput!]`	List of black list bindings.

Example

```
{"enabled": true, "types": [BotBlackListBindingInput]}
```

Types

UpdateBotCAPTCHAInput

Modify a CAPTCHA countermeasure.

Input Field	Description
`resources` - `[BotCAPTCHABindingInput!]`	List of CAPTCHA bindings.

Example

```
{"resources": [BotCAPTCHABindingInput]}
```

Types

UpdateBotDeviceFingerprintInput

Modify a device fingerprint countermeasure.

Input Field	Description
`action` - `BotDeviceFingerprintAction`	Action to be taken. Can only be set if response is ACTION_AND_LOG.
`enabled` - `Boolean`	Whether the device fingerprint countermeasure is enabled.
`response` - `BotResponse`	Response to be taken.

Example

```
{
  "action": BotDeviceFingerprintAction,
  "enabled": false,
  "response": BotResponse
}
```

Types

UpdateBotIPReputationInput

Modify an IP reputation countermeasure.

Input Field	Description
`categories` - `[BotIPReputationBindingInput!]`	List of IP reputation bindings.

`enabled` - `Boolean`	Whether the IP reputation countermeasure is enabled.

Example

```
{
  "categories": [BotIPReputationBindingInput],
  "enabled": true
}
```

Types

`UpdateBotProfileInput`

Modify a bot profile.

Input Field	Description
`blackList` - `UpdateBotBlackListInput`	The black list countermeasure settings.
`botTrap` - `UpdateBotTrapInput`	The bot trap countermeasure settings.
`captcha` - `UpdateBotCAPTCHAInput`	The CAPTCHA countermeasure settings.
`deviceFingerprint` - `UpdateBotDeviceFingerprintInput`	The device fingerprint countermeasure settings.
`enabled` - `Boolean`	Whether the bot profile is enabled.
`ipReputation` - `UpdateBotIPReputationInput`	The IP reputation countermeasure settings.
`rateLimit` - `UpdateBotRateLimitInput`	The rate limit countermeasure settings.
`signatures` - `UpdateBotSignaturesInput`	The bot signatures settings.
`tps` - `UpdateBotTPSInput`	The TPS countermeasure settings.
`whiteList` - `UpdateBotWhiteListInput`	The white list countermeasure settings.

Example

```
{
  "blackList": UpdateBotBlackListInput,
  "botTrap": UpdateBotTrapInput,
  "captcha": UpdateBotCAPTCHAInput,
  "deviceFingerprint": UpdateBotDeviceFingerprintInput,
  "enabled": false,
  "ipReputation": UpdateBotIPReputationInput,
  "rateLimit": UpdateBotRateLimitInput,
  "signatures": UpdateBotSignaturesInput,
  "tps": UpdateBotTPSInput,
  "whiteList": UpdateBotWhiteListInput
}
```

Types

`UpdateBotRateLimitInput`

Modify a rate limit countermeasure.

Input Field	Description
`enabled` - `Boolean`	Whether the rate limit countermeasure is enabled.
`resources` - `[BotRateLimitBindingInput!]`	List of rate limit bindings.

Example

```
{
  "enabled": false,
  "resources": [BotRateLimitBindingInput]
}
```

Types

`UpdateBotSignaturesInput`

Modify bot signatures.

Input Field	Description
`configuredBaseSignatures` - `[ConfiguredBaseBotSignatureInput!]`	List of bot signatures.
`enabled` - `Boolean`	Whether bot signatures are enabled.

Example

```
{
  "configuredBaseSignatures": [
    ConfiguredBaseBotSignatureInput
  ],
  "enabled": true
}
```

Types

UpdateBotTPSInput

Modify a TPS countermeasure.

Input Field	Description
`enabled` - `Boolean`	Whether the TPS countermeasure is enabled.
`resources` - `[BotTPSBindingInput!]`	List of TPS bindings.

Example

```
{"enabled": true, "resources": [BotTPSBindingInput]}
```

Types

UpdateBotTrapInput

Modify a bot trap countermeasure.

Input Field	Description
`action` - `BotTrapAction`	Action to be taken. Can only be set if response is ACTION_AND_LOG.
`enabled` - `Boolean`	Whether the bot trap countermeasure is enabled.
`insertionURLs` - `[BotTrapBindingInput!]`	List of bot trap bindings.
`response` - `BotResponse`	Response to be taken.

Example

```
{
  "action": BotTrapAction,
  "enabled": false,
```

```
  "insertionURLs": [BotTrapBindingInput],
  "response": BotResponse
}
```

Types

UpdateBotWhiteListInput

Modify a white list countermeasure.

Input Field	Description
`enabled` - `Boolean`	Whether the white list countermeasure is enabled.
`types` - `[BotWhiteListBindingInput!]`	List of white list bindings.

Example

```
{"enabled": true, "types": [BotWhiteListBindingInput]}
```

Types

UpdateBufferOverflowInput

Modify a buffer overflow countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`maxCookieLength` - `UnsignedInt16`	Maximum cookie length (in character) in requests to the protected web sites. Requests with longer cookie lengths will be blocked.
`maxHeaderLength` - `UnsignedInt16`	Maximum HTTP header length (in characters) in requests to the protected web sites. Requests with longer headers will be blocked.
`maxURLLength` - `UnsignedInt16`	Maximum URL length (in characters) of the protected web sites. Requests with longer URLs will be blocked.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for buffer overflow violations.

Example

```
{
  "action": WAFAction,
  "maxCookieLength": UnsignedInt16,
  "maxHeaderLength": UnsignedInt16,
  "maxURLLength": UnsignedInt16,
  "threshold": ThresholdInput
}
```

Types

UpdateCSRFSettingsInput

Modify a cross-site request forgery countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`learn` - `Boolean`	A flag to enable or disable learning.
`relaxationRules` - `[CSRFRelaxationRuleInput!]`	A list of CSRF relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for CSRF violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "relaxationRules": [CSRFRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

UpdateCommandInjectionInput

Modify a command injection countermeasure.

Input Field	Description
`action` - `WAFAction!`	Action to be taken.
`commandInjectionType` - `CommandInjectionType!`	A command injection type.

`relaxationRules` - `[CommandInjectionRelaxationRuleInput!]`	A list of command injection relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for command injection violations.

Example

```
{
  "action": WAFAction,
  "commandInjectionType": CommandInjectionType,
  "relaxationRules": [
    CommandInjectionRelaxationRuleInput
  ],
  "threshold": ThresholdInput
}
```

Types

`UpdateContentTypeInput`

Modify a content type countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`learn` - `Boolean`	A flag to enable or disable learning.
`relaxationRules` - `[ContentTypeRelaxationRuleInput!]`	A list of content type relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for content type violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "relaxationRules": [ContentTypeRelaxationRuleInput],
  "threshold": ThresholdInput
```

```
}
```

Types

UpdateCookieConsistencyInput

Modify a cookie consistency countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`learn` - `Boolean`	A flag to enable or disable learning.
`relaxationRules` - `[CookieConsistencyRelaxationRuleInput!]`	A list of relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for cookie consistency violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "relaxationRules": [
    CookieConsistencyRelaxationRuleInput
  ],
  "threshold": ThresholdInput
}
```

Types

UpdateDenyURLInput

Modify a deny URL countermeasures configuration.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`regexRules` - `[DenyURLRuleInput!]`	A list of deny URL regex rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for deny URL violations.

Example

```
{
  "action": WAFAction,
  "regexRules": [DenyURLRuleInput],
  "threshold": ThresholdInput
}
```

Types

UpdateFieldFormatInput

Modify a field format countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`enforcementRules` - `[FieldFormatEnforcementRuleInput!]`	A list of enforcement rules. These are tightening rules, in order to relax some rules you need to remove them from this list.
`learn` - `Boolean`	A flag to enable or disable learning.
`maxLength` - `UnsignedInt16`	Maximum length of the field (in characters, allowed range 0-65535). Please note that distinguishing an integer from an alpha character requires at least one character.
`minLength` - `UnsignedInt16`	Minimum length of the field (in characters, allowed range 0-65535). Please note that distinguishing an integer from an alpha character requires at least one character.

`threshold` - `ThresholdInput`	Appsec Threshold configuration for field format violations.
`type` - `FieldFormatType`	Allowed types for this field.

Example

```
{
  "action": WAFAction,
  "enforcementRules": [FieldFormatEnforcementRuleInput],
  "learn": false,
  "maxLength": UnsignedInt16,
  "minLength": UnsignedInt16,
  "threshold": ThresholdInput,
  "type": FieldFormatType
}
```

Types

`UpdateFormFieldConsistencyInput`

Modify a form field consistency countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`fieldConsistencyExemptions` - `[FormFieldConsistencyRuleInput!]`	A list of exemption rules.
`learn` - `Boolean`	A flag to enable or disable learning.
`sessionlessFieldConsistency` - `SessionlessFieldConsistency`	When turned on, it checks only the web form structure.
`threshold` - `ThresholdInput`	Appsec Threshold configuration

	for form field consistency violations.

Example

```
{
  "action": WAFAction,
  "fieldConsistencyExemptions": [
    FormFieldConsistencyRuleInput
  ],
  "learn": true,
  "sessionlessFieldConsistency": SessionlessFieldConsistency,
  "threshold": ThresholdInput
}
```

Types

`UpdateHTMLSQLInjectionInput`

Modify an HTML SQL injection countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`checkSQLWildChars` - `Boolean`	Whether to check for form fields that contain SQL wild chars.
`exemptCommentsWith` - `CommentExemption`	Exempts all comments of the given type.
`learn` - `Boolean`	A flag to enable or disable learning.
`relaxationRules` - `[HTMLSQLInjectionRelaxationRuleInput!]`	A list of XML SQL injection relaxation rules.
`sqlInjectionType` - `SQLInjectionType`	A SQL injection type.
`sqliGrammar` - `Boolean`	Enable SQL Injection grammar

`threshold` - `ThresholdInput`	Appsec Threshold configuration for HTML SQL injection violations.

Example

```
{
  "action": WAFAction,
  "checkSQLWildChars": true,
  "exemptCommentsWith": CommentExemption,
  "learn": true,
  "relaxationRules": [
    HTMLSQLInjectionRelaxationRuleInput
  ],
  "sqlInjectionType": SQLInjectionType,
  "sqliGrammar": false,
  "threshold": ThresholdInput
}
```

Types

`UpdateHTMLXSSInput`

Modify an HTML cross-site scripting countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`checkCompleteURLs` - `Boolean`	A flag to enforce checks for complete URLs for cross-site scripts, instead of just the query portions of URLs.
`learn` - `Boolean`	A flag to enable or disable learning.
`relaxationRules` - `[HTMLXSSRelaxationRuleInput!]`	A list of HTML cross-site scripting relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for HTML cross-site scripting violations.

Example

```
{
  "action": WAFAction,
  "checkCompleteURLs": false,
  "learn": true,
  "relaxationRules": [HTMLXSSRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

`UpdateHTTPRFCProfileInput`

Modify an HTTP RFC Profile countermeasure.

Input Field	Description
`action` - `HTTPRFCProfileAction`	Action to be taken when there is a non compliant request.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for HTTP RFC violations.

Example

```
{
  "action": HTTPRFCProfileAction,
  "threshold": ThresholdInput
}
```

Types

`UpdateJSONCommandInjectionSettingsInput`

Modufy a JSON command injection Settings Input.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`commandInjectionType` - `CommandInjectionType`	A Command injection type.
`relaxationRules` - `[JSONCommandInjectionRelaxationRuleInput!]`	A list of command injection rules.

`threshold` - `ThresholdInput`	Appsec Threshold configuration for json command injection violations.

Example

```
{
  "action": WAFAction,
  "commandInjectionType": CommandInjectionType,
  "relaxationRules": [
    JSONCommandInjectionRelaxationRuleInput
  ],
  "threshold": ThresholdInput
}
```

Types

`UpdateJSONCrossSiteScriptingSettingsInput`

Modify a JSON cross-site scripting settings input to protect applications from XSS Attacks through JSON requests

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`relaxationRules` - `[JSONXSSRelaxationRuleInput!]`	A list of JSON XSS rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for JSON XSS violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": [JSONXSSRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

UpdateJSONDenialOfServiceSettingsInput

Modify a JSON Denial of Service Settings input to protect applications from Denial of Service Attacks through JSON requests

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`enforcementRule` - `JSONDoSEnforcementRuleInput`	A paginated list of enforcement rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for JSON DOS violations.

Example

```
{
  "action": WAFAction,
  "enforcementRule": JSONDoSEnforcementRuleInput,
  "threshold": ThresholdInput
}
```

Types

UpdateJSONSQLInjectionSettingsInput

Modify a JSON SQL Injection Settings input to protect applications from SQL Injection attacks through JSON requests

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`relaxationRules` - `[JSONSQLInjectionRelaxationRuleInput!]`	A paginated list of SQL Injection rules.
`sqlInjectionType` - `SQLInjectionType`	A SQL injection type.
`sqliGrammar` - `Boolean`	Enable SQL Injection grammar
`threshold` - `ThresholdInput`	Appsec Threshold configuration for JSON SQL injection violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": [
    JSONSQLInjectionRelaxationRuleInput
  ],
  "sqlInjectionType": SQLInjectionType,
  "sqliGrammar": false,
  "threshold": ThresholdInput
}
```

Types

UpdateJSONSettingsInput

Modify a JSON Security Settings input to protect JSON Applications

Input Field	Description
`jsonCommandInjectionSettings` - `UpdateJSONCommandInjectionSettingsInput`	JSON Command Injection Settings.
`jsonCrossSiteScriptingSettings` - `UpdateJSONCrossSiteScriptingSettingsInput`	JSON Cross Site Scripting Settings.
`jsonDenialOfServiceSettings` - `UpdateJSONDenialOfServiceSettingsInput`	JSON Denial Of Service Settings.
`jsonSQLInjectionSettings` - `UpdateJSONSQLInjectionSettingsInput`	JSON SQL Injection Settings.

Example

```
{
  "jsonCommandInjectionSettings": UpdateJSONCommandInjectionSettingsInput,
  "jsonCrossSiteScriptingSettings": UpdateJSONCrossSiteScriptingSettingsInput,
  "jsonDenialOfServiceSettings": UpdateJSONDenialOfServiceSettingsInput,
  "jsonSQLInjectionSettings": UpdateJSONSQLInjectionSettingsInput
}
```

Types

UpdateNetworkControlsInput

Modify network controls.

Input Field	Description
blockedCountries - [CountryCode!]	A list of blocked countries.
ipFilterList - [IPFilterInput!]	A list of ip filters.

Example

```
{
  "blockedCountries": [CountryCode],
  "ipFilterList": [IPFilterInput]
}
```

Types

UpdatePOSTBodyInput

Modify a POST BODY limit countermeasure.

Input Field	Description
limit - UnsignedInt32	A post body size limit value.
threshold - ThresholdInput	Appsec Threshold configuration for post body limit violations.

Example

```
{
  "limit": UnsignedInt32,
  "threshold": ThresholdInput
}
```

Types

UpdatePolicyInput

Modify a policy.

Input Field	Description
`appSecThresholds` - `[AppSecThresholdInput!]`	The appsec thresholds associated to this policy.
`botProfile` - `UpdateBotProfileInput`	The bot profile associated to this policy.
`id` - `String!`	ID of the policy to be updated.
`name` - `String`	The name of the policy.
`networkControls` - `UpdateNetworkControlsInput`	The network controls associated to this policy.
`responderPolicies` - `[ResponderPolicyInput!]`	The responder polices associated to this policy.
`trustedSources` - `[TrustedSourceInput!]`	The trusted IP sources associated to this policy. Traffic at these sources are used by the learning feature to generate recommendations.
`wafProfile` - `UpdateWAFProfileInput`	The WAF profile associated to this policy.

Example

```
{
  "appSecThresholds": [AppSecThresholdInput],
  "botProfile": UpdateBotProfileInput,
  "id": "xyz789",
  "name": "xyz789",
  "networkControls": UpdateNetworkControlsInput,
  "responderPolicies": [ResponderPolicyInput],
  "trustedSources": [TrustedSourceInput],
  "wafProfile": UpdateWAFProfileInput
}
```

Types

`UpdatePolicyOutput`

Returned when updating a policy.

Field Name	Description
`policy` - `Policy!`	The updated policy.

Example

```
{"policy": Policy}
```

Types

UpdateProxyInput

Modify a proxy.

Input Field	Description
`id` - `String!`	ID of the proxy to be updated.
`name` - `String`	Company the proxy configuration belongs to.
`policyIDs` - `[String!]`	A list of policies associated with this proxy.
`vServers` - `[VServerInput!]`	The back-end origin servers, ports and protocols that bind it to the front-end port.

Example

```
{
  "id": "xyz789",
  "name": "abc123",
  "policyIDs": ["xyz789"],
  "vServers": [VServerInput]
}
```

Types

UpdateProxyOutput

Output from updating a proxy.

Field Name	Description
`proxy` - `Proxy!`	The updated proxy.

Example

```
{"proxy": Proxy}
```

Types

UpdateRecurringExecutiveReportConfigurationInput

Input to an update of a recurring report configuration.

Input Field	Description
dName - String!	The unique, primary identifier for the company.
description - String	Description of Report Configuration.
enabled - Boolean	If true, this report configuration generates reports.
from - Time	Timestamp when the first report is generated.
id - String!	ID of recurring executive report configuration.
includeBot - Boolean	If true, includes Bot mitigation summary in the report
includeDDOS - Boolean	If true, includes DDOS mitigation summary in the report
includeWAF - Boolean	If true, includes WAF violation summary in the report
notification - ExecutiveReportNotificationDetailsInput	List of email recepients of generated reports.
period - ExecutiveReportPeriod!	Metric summary interval of report.
to - Time	Timestamp when this report configuration will expire and won't be run after.

Example

```
{
  "dName": "abc123",
  "description": "xyz789",
  "enabled": false,
  "from": Time,
  "id": "xyz789",
  "includeBot": true,
  "includeDDOS": false,
  "includeWAF": false,
  "notification": ExecutiveReportNotificationDetailsInput,
  "period": ExecutiveReportPeriod,
  "to": Time
}
```

Types

`UpdateRecurringExecutiveReportConfigurationOutput`

Output of an update of a recurring report configuration operation.

Field Name	Description
`configuration` - `RecurringExecutiveReportConfiguration!`	Configuration of a recurring report job.

Example

```
{"configuration": RecurringExecutiveReportConfiguration}
```

Types

`UpdateSemicolonFieldSeparatorInput`

Modify a Semicolon field separator countermeasure.

Input Field	Description
`enabled` - `Boolean`	Whether the countermeasure is enabled.

Example

```
{"enabled": true}
```

Types

`UpdateUserInput`

Modify a user.

Input Field	Description
`enabled` - `Boolean`	Enabled status of this user.
`firstName` - `String`	First name of this user.
`id` - `String!`	ID of the user to be updated.
`jobTitle` - `String`	Job title of this user.
`lastName` - `String`	Last name of this user.
`mobile` - `String`	Mobile number of this user.
`phone` - `String`	Phone number of this user.
`roles` - `[UserRole!]`	Roles of this user

Example

```
{
  "enabled": true,
  "firstName": "abc123",
  "id": "abc123",
  "jobTitle": "abc123",
  "lastName": "abc123",
  "mobile": "xyz789",
  "phone": "abc123",
  "roles": [UserRole]
}
```

Types

`UpdateUserOutput`

Returned when updating a user.

Field Name	Description
`user` - `User!`	The updated user.

Example

```
{"user": User}
```

Types

UpdateWAFProfileInput

Modify a WAF profile.

Input Field	Description
`bufferOverflow` - `UpdateBufferOverflowInput`	The buffer overflow countermeasure settings.
`commandInjection` - `UpdateCommandInjectionInput`	The Command Injection countermeasure settings.
`contentType` - `UpdateContentTypeInput`	The content type countermeasure settings.
`cookieConsistency` - `UpdateCookieConsistencyInput`	The cookie consistency countermeasure settings.
`crossSiteScripting` - `UpdateHTMLXSSInput`	The HTML cross-site scripting countermeasure settings.
`csrfSettings` - `UpdateCSRFSettingsInput`	The CSRF countermeasure settings.
`denyURL` - `UpdateDenyURLInput`	The deny URL countermeasure settings.
`enabled` - `Boolean`	Whether the WAF profile is enabled.

`fieldConsistency` - `UpdateFormFieldConsistencyInput`	The form field consistency countermeasure settings.
`fieldFormat` - `UpdateFieldFormatInput`	The field format countermeasure settings.
`htmlSQLInjection` - `UpdateHTMLSQLInjectionInput`	The HTML SQL Injection countermeasure settings.
`httpRFCProfile` - `UpdateHTTPRFCProfileInput`	Check requests for HTTP RFC non compliance.
`jsonSettings` - `UpdateJSONSettingsInput`	The JSON related countermeasure settings.
`postBody` - `UpdatePOSTBodyInput`	Limits the request payload size.
`semicolonFieldSeparator` - `UpdateSemicolonFieldSeparatorInput`	Allow or disallow semicolon field separator between request fields.
`signatures` - `UpdateWAFSignaturesInput`	The WAF signatures settings.
`wsiSettings` - `UpdateWSISettingsInput`	The web service interoperability countermeasure settings.
`xmlCrossSiteScripting` - `UpdateXMLXSSInput`	The XML cross-site scripting

	countermeasure settings.
`xmlFormat` - `UpdateXMLFormatInput`	The XML format countermeasure settings.
`xmlSOAPFault` - `UpdateXMLSOAPFaultInput`	The XML SOAP fault countermeasure settings.
`xmlSQLInjection` - `UpdateXMLSQLInjectionInput`	The XML SQL Injection countermeasure settings.

Example

```
{
  "bufferOverflow": UpdateBufferOverflowInput,
  "commandInjection": UpdateCommandInjectionInput,
  "contentType": UpdateContentTypeInput,
  "cookieConsistency": UpdateCookieConsistencyInput,
  "crossSiteScripting": UpdateHTMLXSSInput,
  "csrfSettings": UpdateCSRFSettingsInput,
  "denyURL": UpdateDenyURLInput,
  "enabled": false,
  "fieldConsistency": UpdateFormFieldConsistencyInput,
  "fieldFormat": UpdateFieldFormatInput,
  "htmlSQLInjection": UpdateHTMLSQLInjectionInput,
  "httpRFCProfile": UpdateHTTPRFCProfileInput,
  "jsonSettings": UpdateJSONSettingsInput,
  "postBody": UpdatePOSTBodyInput,
  "semicolonFieldSeparator": UpdateSemicolonFieldSeparatorInput,
  "signatures": UpdateWAFSignaturesInput,
  "wsiSettings": UpdateWSISettingsInput,
  "xmlCrossSiteScripting": UpdateXMLXSSInput,
  "xmlFormat": UpdateXMLFormatInput,
  "xmlSOAPFault": UpdateXMLSOAPFaultInput,
  "xmlSQLInjection": UpdateXMLSQLInjectionInput
}
```

Types

UpdateWAFSignaturesInput

Modify WAF signatures.

Input Field	Description
`configuredBaseSignatures` - `[ConfiguredBaseWAFSignatureInput!]`	A list of signatures for a policy configured from a list of available base signatures.
`customSignatures` - `[CustomWAFSignatureInput!]`	A list of custom signatures created for a policy.

Example

```
{
  "configuredBaseSignatures": [
    ConfiguredBaseWAFSignatureInput
  ],
  "customSignatures": [CustomWAFSignatureInput]
}
```

Types

UpdateWSISettingsInput

Modify a web services interoperability countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`learn` - `Boolean`	A flag to enable or disable learning.
`standards` - `[WSIStandardInput!]`	A list of WSI standards.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for WSI violations.

Example

```
{
  "action": WAFAction,
  "learn": true,
  "standards": [WSIStandardInput],
  "threshold": ThresholdInput
}
```

Types

UpdateXMLFormatInput

Modify an XML format countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML format violations.

Example

```
{
  "action": WAFAction,
  "threshold": ThresholdInput
}
```

Types

UpdateXMLSOAPFaultInput

Modify an XML SOAP fault countermeasure.

Input Field	Description
`action` - `XMLSOAPFaultAction`	Action to be taken.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML format violations.

Example

```
{
  "action": XMLSOAPFaultAction,
  "threshold": ThresholdInput
```

```
}
```

Types

UpdateXMLSQLInjectionInput

Modify an HTML SQL injection countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`checkSQLWildChars` - `Boolean`	Whether to check for form fields that contain SQL wild chars.
`exemptCommentsWith` - `CommentExemption`	Exempts all comments of the given type.
`relaxationRules` - `[XMLSQLInjectionRelaxationRuleInput!]`	A list of XML SQL injection relaxation rules.
`sqlInjectionType` - `SQLInjectionType`	An XML SQL injection type.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML SQL injection violations.

Example

```
{
  "action": WAFAction,
  "checkSQLWildChars": true,
  "exemptCommentsWith": CommentExemption,
  "relaxationRules": [XMLSQLInjectionRelaxationRuleInput],
  "sqlInjectionType": SQLInjectionType,
  "threshold": ThresholdInput
}
```

Types

UpdateXMLXSSInput

Modify an XML cross-site scripting countermeasure.

Input Field	Description
`action` - `WAFAction`	Action to be taken.
`relaxationRules` - `[XMLXSSRelaxationRuleInput!]`	A list of XML cross-site scripting relaxation rules.
`threshold` - `ThresholdInput`	Appsec Threshold configuration for XML cross-site scripting violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": [XMLXSSRelaxationRuleInput],
  "threshold": ThresholdInput
}
```

Types

User

A user of the system.

Field Name	Description
`company` - `Company!`	Details of company.
`createdAt` - `Time!`	Timestamp of when user was created.
`email` - `String!`	User email.
`enabled` - `Boolean!`	Whether the user is able to access the system.
`firstName` - `String!`	First name.
`id` - `String!`	ID of company User.
`jobTitle` - `String`	Job title.
`lastLogin` - `Time`	Timestamp of last login of this user.
`lastName` - `String!`	Last name.
`mobile` - `String`	Mobile number.
`phone` - `String`	Phone number.
`roles` - `[UserRole!]`	Roles.

`updatedAt` - `Time!`	Timestamp of when user was last updated.
`userName` - `String!`	User name.

Example


```
{
  "company": Company,
  "createdAt": Time,
  "email": "xyz789",
  "enabled": true,
  "firstName": "abc123",
  "id": "xyz789",
  "jobTitle": "abc123",
  "lastLogin": Time,
  "lastName": "abc123",
  "mobile": "abc123",
  "phone": "xyz789",
  "roles": [UserRole],
  "updatedAt": Time,
  "userName": "xyz789"
}
```


Types

`UserFilterInput`

For reducing the returned list of users.

Input Field	Description
`email` - `String`	Specifies user email to filter query results on.
`id` - `String`	Specifies user ID to filter query results on.
`includeDisabled` - `Boolean`	Indicates whether users disabled in portal should be included in query results.

Example


```
{"email": "abc123", "id": "xyz789", "includeDisabled": false}
```


Types

`UserLog`

Auth0 event log for a user.

Field Name	Description
`date` - `Time!`	The date when the event occurred.
`description` - `String!`	The description of this event.
`ip` - `String!`	The IP address of the log event source.
`logID` - `String!`	The unique ID of the event.
`type` - `String!`	The type of event
`userID` - `String!`	The ID of the user.

Example

```
{
  "date": Time,
  "description": "abc123",
  "ip": "abc123",
  "logID": "xyz789",
  "type": "xyz789",
  "userID": "abc123"
}
```

Types

`UserLogsFilterInput`

Filter for Auth0 event log for a user.

Input Field	Description
`endTime` - `Time`	Specifies end time to filter query results on.
`id` - `String!`	Specifies user ID to filter query results on.
`startTime` - `Time`	Specifies start time to filter query results on.
`types` - `String`	Specifies log event types to filter query results on.

Example

```
{
  "endTime": Time,
  "id": "xyz789",
  "startTime": Time,
  "types": "xyz789"
```

```
}
```

Types

UserRole

Allowed list of user roles.

Enum Value	Description
`PRIMARY_ADMIN`	Primary admin role.
`READ_ONLY`	Read-only role.
`TECHNICAL_USER`	Technical user role.

Types

UsersWithPagination

A paginated list of users.

Field Name	Description
`pageInfo` - `Pagination!`	Pagination settings for query results.
`results` - `[User!]`	Set of users returned by query.

Example

```
{
  "pageInfo": Pagination,
  "results": [User]
}
```

Types

VServer

A collection of properties that define a virtual server.

Field Name	Description
`applicationServices` - `[ApplicationService!]`	Application services that make up this virtual server's back end.

`certificateBindings` - `[CertificateBinding!]`	Certficate(s) for this virtual server.
`loadBalanceMethod` - `ProxyLoadBalanceMethod!`	Method used to load-balance connections.
`persistenceType` - `ProxyLoadBalancePersistenceType!`	A session persistence type to apply to requests.
`port` - `UnsignedInt16!`	The virtual server's front-end server port.
`protocol` - `ProxyProtocol!`	Protocol type used for the front and back ends.
`sp` - `Boolean!`	Ensure connections to the server occur at a rate that the server can handle.
`tcpb` - `Boolean!`	Use TCP Buffering for the service.
`tlsOptions` - `TLSOptions`	TLS/SSL protocol options.
`xffHeader` - `String!`	The name of the 'forwarded-for' header.

Example

```
{
  "applicationServices": [ApplicationService],
  "certificateBindings": [CertificateBinding],
  "loadBalanceMethod": ProxyLoadBalanceMethod,
  "persistenceType": ProxyLoadBalancePersistenceType,
  "port": UnsignedInt16,
  "protocol": ProxyProtocol,
  "sp": false,
  "tcpb": true,
  "tlsOptions": TLSOptions,
  "xffHeader": "xyz789"
}
```

Types

`VServerInput`

Add a VServer to a Proxy.

Input Field	Description
`applicationServices` - `[ApplicationServiceInput!]`	Application services that make up this virtual server's back end.
`certificateBindings` - `[CertificateBindingInput!]`	Certficate(s) for this virtual server.
`loadBalanceMethod` - `ProxyLoadBalanceMethod!`	Method used to load-balance connections.
`persistenceType` - `ProxyLoadBalancePersistenceType!` default = `"SOURCE_IP"`	A session persistence type to apply to requests.
`port` - `UnsignedInt16!`	Back end origin server port.
`protocol` - `ProxyProtocol!`	Protocol type of the front end.
`sp` - `Boolean`	Ensure connections to the server occur at a rate that the server can handle.
`tcpb` - `Boolean`	Use TCP Buffering for the service.
`tlsOptions` - `TLSOptionsInput`	TLS/SSL protocol options. Only required for TLS.
`xffHeader` - `String!` default = `"X-Forwarded-For"`	The name of the 'forwarded-for' header.

Example

```
{
  "applicationServices": [ApplicationServiceInput],
  "certificateBindings": [CertificateBindingInput],
  "loadBalanceMethod": ProxyLoadBalanceMethod,
  "persistenceType": "SOURCE_IP",
  "port": UnsignedInt16,
```

```
  "protocol": ProxyProtocol,
  "sp": false,
  "tcpb": true,
  "tlsOptions": TLSOptionsInput,
  "xffHeader": "X-Forwarded-For"
}
```

Types

VServerState

VServer state value.

Enum Value	Description
`DOWN`	Down or nonoperational.
`UNAVAILABLE`	Unavailable.
`UP`	Up or operational.

Types

VServerStatus

Represents the status of a vserver (VIP-protocol-port combination).

Field Name	Description
`currentState` - `VServerState!`	State of the vserver.
`port` - `UnsignedInt32!`	Port of the vserver.
`protocol` - `String!`	Protocol of the vserver.

Example

```
{
  "currentState": VServerState,
  "port": UnsignedInt32,
  "protocol": "xyz789"
}
```

Types

ValueType

Allowed list of values for value types.

Enum Value	Description
`KEYWORD`	
`SPECIAL_STRING`	
`WILDCHAR`	

Types

`ViolationLog`

A WAF violation log.

Field Name	Description
`action` - `String`	The action that caused this violation log.
`aggregatedURI` - `String`	The aggregated uri string which caused the violation
`cefVersion` - `String`	The engine's CEF version.
`cookies` - `String`	The cookies in the original request.
`customer` - `String`	The customer account dname.
`destinationIP` - `IPAddress`	The destination IP the request was intended for.
`devVersion` - `String`	The dev version.
`domain` - `String`	The domain the request was intended for.
`eventID` - `String`	The unique event ID for this event.
`host` - `String`	The hostname in the request.
`httptxID` - `String`	The HTTP transaction ID from the engine.
`method` - `String`	The HTTP method used.
`profile` - `String`	The policy key generating this violation.
`protocol` - `String`	The protocol used.
`rawHeaders` - `String`	The raw headers in the original request.
`reason` - `String`	The reason for the violation to occur.
`sessionID` - `String`	The session ID.
`severity` - `UnsignedInt32`	The severity code of the violation.

`severityString` - `String`	The severity string of the violation.
`signatureID` - `String`	The signature code prefix.
`signatureName` - `String`	The signature name which triggered the violation.
`site` - `String`	The processing site location.
`sourceIP` - `IPAddress`	The source IP of the request.
`sourceLocation` - `GeoLocation`	The source location where the request originated.
`sourcePort` - `UnsignedInt16`	The source port of the request.
`timestamp` - `LogTime`	The timestamp of the violation log.
`timestampEvent` - `LogTime`	The log timestamp event.
`type` - `String`	The type of the violation.
`uri` - `String`	The uri which cause the violation.
`userAgent` - `String`	The user agent in the original request header.
`version` - `String`	The version.
`wafVersion` - `String`	The WAF version.

Example


```
{
  "action": "xyz789",
  "aggregatedURI": "abc123",
  "cefVersion": "xyz789",
  "cookies": "xyz789",
  "customer": "xyz789",
  "destinationIP": IPAddress,
  "devVersion": "abc123",
  "domain": "xyz789",
  "eventID": "abc123",
  "host": "xyz789",
  "httptxID": "abc123",
  "method": "abc123",
  "profile": "abc123",
  "protocol": "xyz789",
  "rawHeaders": "xyz789",
  "reason": "abc123",
  "sessionID": "abc123",
  "severity": UnsignedInt32,
  "severityString": "xyz789",
```

```
  "signatureID": "abc123",
  "signatureName": "abc123",
  "site": "xyz789",
  "sourceIP": IPAddress,
  "sourceLocation": GeoLocation,
  "sourcePort": UnsignedInt16,
  "timestamp": LogTime,
  "timestampEvent": LogTime,
  "type": "xyz789",
  "uri": "xyz789",
  "userAgent": "abc123",
  "version": "xyz789",
  "wafVersion": "abc123"
}
```

Types

ViolationLogDimension

Violation log sort dimensions.

Enum Value	Description
DESTINATION_IP	
DOMAIN	
SIGNATURE_NAME	
SITE	
SOURCE_COUNTRY	
SOURCE_IP	
TIMESTAMP	
URI	

Types

ViolationLogFilterInput

A WAF violation log filter input.

Input Field	Description
action - String	The violation log action.

`aggregatedURI` - `String`	The aggregated uri string which caused the violation
`all` - `String`	The All filters looks at all the filters mentioned above, with the exception of profile.
`destinationIP` - `IPAddressInput`	The destination IP of the request.
`domain` - `String`	The domain the request was intended for.
`eventID` - `String`	The unique event ID for this event.
`host` - `String`	The host of the request.
`httptxID` - `String`	The HTTP transaction ID from the engine.
`profile` - `String`	The policy key generating this violation.
`reason` - `String`	The reason for the violation to occur.
`signatureName` - `String`	The signature name which triggered the violation.
`site` - `String`	The processing site location.
`sourceCity` - `String`	The source city name.
`sourceCountryName` - `String`	The source country name.
`sourceIP` - `IPAddressInput`	The source IP of the request.
`timestamp` - `String`	The timestamp of the violation log.
`uri` - `String`	The uri which cause the violation.
`userAgent` - `String`	The user agent in the original request header.

Example


```
{
  "action": "xyz789",
  "aggregatedURI": "abc123",
  "all": "abc123",
  "destinationIP": IPAddressInput,
  "domain": "abc123",
  "eventID": "abc123",
  "host": "xyz789",
  "httptxID": "abc123",
  "profile": "abc123",
  "reason": "xyz789",
  "signatureName": "abc123",
  "site": "abc123",
  "sourceCity": "abc123",
```

```
  "sourceCountryName": "xyz789",
  "sourceIP": IPAddressInput,
  "timestamp": "xyz789",
  "uri": "xyz789",
  "userAgent": "xyz789"
}
```

Types

ViolationLogGroup

A violation log group.

Field Name	Description
`count` - `UnsignedInt32!`	The count of violation logs in this group.
`key` - `String!`	The group name.

Example

```
{"count": UnsignedInt32, "key": "abc123"}
```

Types

ViolationLogGroupByField

Allowed list of violation log group by fields.

Enum Value	Description
`DESTINATION_IP`	
`DOMAIN`	
`PROFILE`	
`SIGNATURE_NAME`	
`SOURCE_CONTINENT`	
`SOURCE_COUNTRY`	
`SOURCE_IP`	
`URI`	

Types

ViolationLogGroupByInput

A WAF violation log group by input.

Input Field	Description
direction - SortDirection	The order of the groups listed (ascending or descending).
field - ViolationLogGroupByField!	The field that will be used to group the logs.
timeInterval - TimeInterval	The time interval when the group of logs occurred.

Example

```
{
  "direction": SortDirection,
  "field": ViolationLogGroupByField,
  "timeInterval": TimeInterval
}
```

Types

ViolationLogSortBy

A WAF violation log sort input.

Input Field	Description
dimension - ViolationLogDimension!	The dimension that will be used to sort the logs.
direction - SortDirection! default = "DESCENDING"	The order of the sort (ascending or descending).

Example

```
{
  "dimension": ViolationLogDimension,
  "direction": "DESCENDING"
}
```

Types

ViolationLogTimeSeries

A violation log time series group.

Field Name	Description
`cnt` - `UnsignedInt64!`	The count of violation logs in this timeframe.
`key` - `String!`	The key name.
`ts` - `Time!`	The timestamp of these occurrences.

Example

```
{
  "cnt": UnsignedInt64,
  "key": "xyz789",
  "ts": Time
}
```

Types

ViolationLogsWithPagination

A paginated list of WAF violation logs.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[ViolationLog!]`	Violation log data

Example

```
{
  "pageInfo": Pagination,
  "results": [ViolationLog]
}
```

Types

WAFAction

Allowed list of actions for a given WAF countermeasure.

Enum Value	Description
`BLOCK_AND_LOG`	
`LOG`	
`NONE`	

Types

`WAFAnalyticsResponse`

A WAF analytics response.

Field Name	Description
`groups` - `[ViolationLogGroup!]`	The list of aggregated group results satisfying the group by criteria.
`logs` - `ViolationLogsWithPagination`	A paginated list of violation logs satisfying the filter criteria.
`timeSeriesData` - `[ViolationLogTimeSeries!]`	The time series information of the violation logs occurrences.

Example

```
{
  "groups": [ViolationLogGroup],
  "logs": ViolationLogsWithPagination,
  "timeSeriesData": [ViolationLogTimeSeries]
}
```

Types

`WAFMitigation`

Web Application Firewall(WAF) violation.

Field Name	Description
`company` - `Company!`	
`countermeasures` - `[WAFViolation!]`	The countermeasures associated with the mitigation.
`destinationIPs` - `[CIDR!]`	The destination IPs.

`end` - `Time`	The end time of the mitigation. A non-zero value of end time means that the mitigation has ended.
`id` - `String!`	The identifier of the mitigation.
`policy` - `Policy`	The Policy that triggered this mitigation.
`start` - `Time!`	The start time of the mitigation.

Example

```
{
  "company": Company,
  "countermeasures": [WAFViolation],
  "destinationIPs": [CIDR],
  "end": Time,
  "id": "xyz789",
  "policy": Policy,
  "start": Time
}
```

Types

WAFProfile

A WAF profile for a given policy.

Field Name	Description
`bufferOverflow` - `BufferOverflow`	The buffer overflow countermeasure settings.
`commandInjection` - `CommandInjection`	The Command Injection countermeasure settings.
`contentType` - `ContentType`	The content type countermeasure settings.
`cookieConsistency` - `CookieConsistency`	The cookie consistency countermeasure settings.
`crossSiteScripting` - `HTMLXSS`	The HTML cross-site scripting countermeasure settings.
`csrfSettings` - `CSRFSettings`	The CSRF countermeasure settings.

`denyURL` - `DenyURL`	The deny URL countermeasure settings.
`enabled` - `Boolean!`	Whether the WAF profile is enabled.
`fieldConsistency` - `FormFieldConsistency`	The form field consistency countermeasure settings.
`fieldFormat` - `FieldFormat`	The field format countermeasure settings.
`htmlSQLInjection` - `HTMLSQLInjection`	The HTML SQL Injection countermeasure settings.
`httpRFCProfile` - `HTTPRFCProfile`	Check requests for HTTP RFC non compliance.
`jsonSettings` - `JSONSettings`	The JSON related countermeasure settings.
`postBody` - `POSTBody`	Limits the request payload size.
`semicolonFieldSeparator` - `SemicolonFieldSeparator`	Allow or disallow semicolon field separator between request fields.
`signatures` - `WAFSignatures`	The WAF signatures settings.
`wsiSettings` - `WSISettings`	The web service interoperability countermeasure settings.
`xmlCrossSiteScripting` - `XMLXSS`	The XML cross-site scripting countermeasure settings.
`xmlFormat` - `XMLFormat`	The XML format countermeasure settings.
`xmlSOAPFault` - `XMLSOAPFault`	The XML SOAP fault countermeasure settings.
`xmlSQLInjection` - `XMLSQLInjection`	The XML SQL Injection countermeasure settings.

Example

```
{
  "bufferOverflow": BufferOverflow,
```

```
  "commandInjection": CommandInjection,
  "contentType": ContentType,
  "cookieConsistency": CookieConsistency,
  "crossSiteScripting": HTMLXSS,
  "csrfSettings": CSRFSettings,
  "denyURL": DenyURL,
  "enabled": false,
  "fieldConsistency": FormFieldConsistency,
  "fieldFormat": FieldFormat,
  "htmlSQLInjection": HTMLSQLInjection,
  "httpRFCProfile": HTTPRFCProfile,
  "jsonSettings": JSONSettings,
  "postBody": POSTBody,
  "semicolonFieldSeparator": SemicolonFieldSeparator,
  "signatures": WAFSignatures,
  "wsiSettings": WSISettings,
  "xmlCrossSiteScripting": XMLXSS,
  "xmlFormat": XMLFormat,
  "xmlSOAPFault": XMLSOAPFault,
  "xmlSQLInjection": XMLSQLInjection
}
```

Types

WAFSignatureDimension

Allowed values for sorting the Signature list.

Enum Value	Description
CATEGORY	
DESCRIPTION	

Types

WAFSignatureFilterInput

Filter a list of WAF signatures.

Input Field	Description
category - String	Category to filter the signatures by.
search - String	Substring to search in description and other text, etc.

Example

```
{"category": "xyz789", "search": "xyz789"}
```

Types

WAFSignatureSortBy

Signature sorting input.

Input Field	Description
`dimension` - `WAFSignatureDimension!`	The dimension to sort by.
`direction` - `SortDirection!`	The direction to sort in.

Example

```
{
  "dimension": WAFSignatureDimension,
  "direction": SortDirection
}
```

Types

WAFSignatures

A WAF signature.

Field Name	Description
`configuredBaseSignatures` - `ConfiguredBaseWAFSignaturesWithPagination`	A paginated list of signatures for a policy configured from a list of available base signatures.

Arguments

`filter` - `WAFSignatureFilterInput`

Reduce the returned list to specific items.

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`sortBy` - `[WAFSignatureSortBy!]`

Sort the results.

`customSignatures` - `CustomWAFSignaturesWithPagination`

A paginated list of custom WAF signatures created for a policy.

Arguments

`filter` - `CustomWAFSignatureFilterInput`

Reduce the returned list to specific items.

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`sortBy` - `[WAFSignatureSortBy!]`

Sort the results.

Example

```
{
  "configuredBaseSignatures": ConfiguredBaseWAFSignaturesWithPagination,
  "customSignatures": CustomWAFSignaturesWithPagination
}
```

Types

WAFViolation

Represents WAF violations for a company.

Field Name	Description
company - Company!	The company object.
id - String!	The identifier of a violation.
name - String!	The signature name.
violationsDetails - [AppViolationData!]	The details of the violations.

Arguments

metrics - [AppViolationMetric!]

Example

```
{
  "company": Company,
  "id": "abc123",
  "name": "xyz789",
  "violationsDetails": [AppViolationData]
}
```

Types

WSISettings

A web services interoperability countermeasure.

Field Name	Description
action - WAFAction!	Action to be taken.
learn - Boolean!	A flag to enable or disable learning.
standards - WSIStandardsWithPagination	A paginated list of WSI standards.

Arguments

page - UnsignedInt32! default = 1

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`threshold` - `AppSecThreshold` — Appsec Threshold configuration for WSI violations.

Example

```
{
  "action": WAFAction,
  "learn": false,
  "standards": WSIStandardsWithPagination,
  "threshold": AppSecThreshold
}
```

Types

`WSISettingsRuleCount`

WSI settings rule count.

Field Name	Description
`count` - `UnsignedInt32!`	
`rule` - `LearnedWSISettingsRule!`	

Example

```
{
  "count": UnsignedInt32,
  "rule": LearnedWSISettingsRule
}
```

Types

`WSISettingsRuleCountsWithPagination`

WSI settings learning rules.

Field Name	Description
`pageInfo` - `Pagination!`	
`results` - `[WSISettingsRuleCount!]`	

Example

```
{
  "pageInfo": Pagination,
  "results": [WSISettingsRuleCount]
}
```

Types

WSIStandard

A web service interoperability standard.

Field Name	Description
`enabled` - `Boolean!`	Whether the standard is enabled.
`rule` - `WSIStandardRule!`	A WSI rule.
`ruleID` - `WSIStandardRuleID!`	A unique rule ID for the standard.

Example

```
{
  "enabled": false,
  "rule": WSIStandardRule,
  "ruleID": WSIStandardRuleID
}
```

Types

WSIStandardInput

A web service interoperability standard.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the standard is enabled.
`ruleID` - `WSIStandardRuleID!`	The unique rule ID for the standard.

Example

```
{"enabled": true, "ruleID": WSIStandardRuleID}
```

Types

WSIStandardRule

A web service interoperability standard rule.

Field Name	Description
code - String!	A code for the standard.
description - String!	A decsription of the standard.
id - WSIStandardRuleID!	A unique rule ID for the standard.

Example

```
{
  "code": "xyz789",
  "description": "abc123",
  "id": WSIStandardRuleID
}
```

Types

WSIStandardRuleID

Allowed list of WSI standard rule IDs.

Enum Value	Description
ALL_SOAPBIND_FAULTS_DESCRIBED	A wsdl:binding in a DESCRIPTION SHO a soapbind:fault describing each known fa
ALL_SOAPBIND_HEADERS_INCLUDED	An ENVELOPE MUST include all soapbi specified on a wsdl:input or wsdl:output of wsdl:operation of a wsdl:binding that desc
BODY_CHILDREN_NAMESPACED	The children of the soap:Body element in a ENVELOPE MUST be namespace qualifie
FAULTCODE_VALID_CONTENT	When an ENVELOPE contains a faultcode content of that element SHOULD be either fault codes defined in SOAP 1.1 (supplyin information if necessary in the detail eleme Qname whose namespace is controlled by specifying authority (in that order of prefer

`FAULT_IF_INVALID_ENVELOPE`	A RECEIVER MUST generate a fault if th an envelope whose document element is no soap:Envelope
`HTTP_REQUEST_INCLUDES_VALID_SOAPACTION_HEADER`	A HTTP request MESSAGE MUST conta SOAPAction HTTP header field with a qu equal to the value of the soapAction attribu soapbind:operation, if present in the corres WSDL description.
`MESSAGE_SERIALIZATION`	A MESSAGE MUST be serialized as eithe UTF-16
`MUST_ACCEPT_FAULT_MESSAGES`	A RECEIVER MUST accept fault messag any number of qualified or unqualified attr including zero, appearing on the detail elem namespace of qualified attributes can be an than the namespace of the qualified docum 'Envelope'
`MUST_UNDERSTAND_ATTR_VALID`	An ENVELOPE containing a soap:mustUn attribute MUST only use the lexical forms
`MUST_USE_HTTP_1_1_OR_1_0`	A MESSAGE MUST be sent using either H HTTP/1.0.
`MUST_USE_HTTP_POST`	A HTTP request MESSAGE MUST use th POST method
`NO_ARRAYTYPE_ENCODING_ATTR`	An ENVELOPE MUST NOT include the soapenc:arrayType attribute.
`NO_DOT_NOTATION_FAULTCODE`	When an ENVELOPE contains a faultcode content of that element SHOULD NOT use 1.1 'dot' notation to refine the meaning of t
`NO_ENVELOPE_FOLLOWING_BODY`	An ENVELOPE MUST NOT have any ele of soap:Envelope following the soap:Body
`ONE_WAY_RESPONSE_MUST_BE_EMPTY`	For one-way operations, an INSTANCE M return a HTTP response that contains an em Specifically, the HTTP response entity-bod empty.
`RPC_LITERAL_NO_ENCODING_STYLE_ATTRS_ON_BODY_GRANDCHILD`	An ENVELOPE described in an rpc-literal MUST NOT contain soap:encodingStyle a any element that is a grandchild of soap:Bo
`RPC_LITERAL_NO_INVALID_NIL_ATTR`	An ENVELOPE described with an rpc-lite MUST NOT have the xsi:nil attribute with or 'true' on the part accessors.

`RPC_LITERAL_PART_ACCESSORS_NO_NAMESPACE`	An ENVELOPE described with an rpc-lite MUST place the part accessor elements fo and return value in no namespace.
`RPC_LITERAL_VALID_RESPONSE`	An ENVELOPE described with an rpc-lite that is a response MUST have a wrapper el name is the corresponding wsdl:operation with the string 'Response'.
`SHOULD_USE_HTTP_1_1`	A MESSAGE SHOULD be sent using HT
`SOAP_ACTION_HTTP_HEADER_VALID`	The value of the SOAPAction HTTP head HTTP request MESSAGE MUST be a quo
`SOAP_ENCODING_STYLE_ATTRS_NOT_ON_BODY_CHILD`	An ENVELOPE MUST NOT contain soap:encodingStyle attributes on any eleme child of soap:Body.
`SOAP_ENCODING_STYLE_VALID_ATTRS`	An ENVELOPE MUST NOT contain soap:encodingStyle attribute on any of the whose namespace is the same as the names qualified document element 'Envelope'
`SOAP_FAULT_CHILDREN_NOT_UNQUALIFIED`	When an ENVELOPE is a Fault, the eleme the soap:Fault element MUST be unqualifi
`SOAP_FAULT_VALID_CHILDREN`	When an ENVELOPE is a Fault, the soap: MUST NOT have element children other t faultstring, faultactor and detail.
`VALID_ENVELOPE_HEADER_BODY_ATTRS`	The soap:Envelope, soap:Header, and soap elements in an ENVELOPE MUST NOT h in the same namespace as that of the qualif element 'Envelope'
`VALID_ENVELOPE_NAMESPACE`	An ENVELOPE SHOULD NOT contain t declaration xmlns:xml=' http://www.w3.org/XML/199
`VALID_HTTP_RESPONSE_IF_FAULT`	An INSTANCE MUST return a '500 Intern Error' HTTP status code if the response en Fault.
`VALID_HTTP_RESPONSE_IF_NO_FAULT`	An INSTANCE SHOULD use a '200 OK' code on a response message that contains a that is not a fault.

Types

WSIStandardsWithPagination

A paginated list of WSI standards.

Field Name	Description
pageInfo - Pagination!	The returned page information.
results - [WSIStandard!]	A list of WSI standards.

Example

```
{
  "pageInfo": Pagination,
  "results": [WSIStandard]
}
```

Types

WhiteLabel

Specifications for elements that can be modified for white-labelled customers.

Field Name	Description
bottomLeftLabel - String!	Bottom left label to be rendered for company.
bottomRightLabel - String!	Bottom right label to be rendered for company.
domain - String!	Company domain.
email - EMail!	Company contact email ID.
enabled - Boolean!	Whether white-labelling is enabled for the Company.
favicon - Map	Specifies a map of fav icons for this company's pages.
footerLinks - [Link!]	List of all URLs and Labels associated with this company.
headerLogo - String!	Header logo for this company.
loginMarqueeItems - [String!]	Marquee elements to be displayed on login for this company.
productName - String!	Product Name as displayed by/for this company.
supportURL - String!	Support URL to be displayed for this company.

`supportUser` - `String!`	Company support username.
`theme` - `String!`	Theme for company.

Example

```
{
  "bottomLeftLabel": "abc123",
  "bottomRightLabel": "abc123",
  "domain": "xyz789",
  "email": EMail,
  "enabled": false,
  "favicon": Map,
  "footerLinks": [Link],
  "headerLogo": "abc123",
  "loginMarqueeItems": ["xyz789"],
  "productName": "abc123",
  "supportURL": "xyz789",
  "supportUser": "xyz789",
  "theme": "abc123"
}
```

Types

`XMLFormat`

An XML format countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for XML format violations.

Example

```
{
  "action": WAFAction,
  "threshold": AppSecThreshold
}
```

Types

`XMLLocation`

Allowed list of values for an XML location.

Enum Value	Description
`ATTRIBUTE`	
`ELEMENT`	

Types

XMLSOAPFault

An XML SOAP fault countermeasure.

Field Name	Description
`action` - `XMLSOAPFaultAction!`	Action to be taken.
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for XML format violations.

Example

```
{
  "action": XMLSOAPFaultAction,
  "threshold": AppSecThreshold
}
```

Types

XMLSOAPFaultAction

Allowed list of actions for XML SOAP Fault countermeasure.

Enum Value	Description
`BLOCK_AND_LOG`	
`LOG`	
`NONE`	
`REMOVE`	

Types

XMLSQLInjection

An XML SQL injection countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`checkSQLWildChars` - `Boolean!`	Whether to check for form fields that contain SQL wild chars.
`exemptCommentsWith` - `CommentExemption!`	Exempts all comments of the given type.
`relaxationRules` - `XMLSQLInjectionRelaxationRulesWithPagination`	A list of XML SQL injection relaxation rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`sqlInjectionType` - `SQLInjectionType!`	An XML SQL injection type.
`threshold` - `AppSecThreshold`	Appsec Threshold configuration for XML SQL injection violations.

Example

```
{
  "action": WAFAction,
  "checkSQLWildChars": true,
  "exemptCommentsWith": CommentExemption,
  "relaxationRules": XMLSQLInjectionRelaxationRulesWithPagination,
  "sqlInjectionType": SQLInjectionType,
  "threshold": AppSecThreshold
}
```

Types

XMLSQLInjectionRelaxationRule

An XML SQL injection relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!`	Whether the name is in regex format.
`location` - `XMLLocation`	The location of the attachment.
`name` - `String!`	The name of the rule.

Example

```
{
  "enabled": true,
  "isNameRegex": false,
  "location": XMLLocation,
  "name": "xyz789"
}
```

Types

XMLSQLInjectionRelaxationRuleInput

An XML SQL injection relaxation rule.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!` default = `false`	Whether the name is in regex format.

`location` - `XMLLocation`	The location that should be examined by the rule.
`name` - `String!`	The name of the rule.

Example

```
{
  "enabled": true,
  "isNameRegex": false,
  "location": XMLLocation,
  "name": "xyz789"
}
```

Types

XMLSQLInjectionRelaxationRulesWithPagination

A paginated list SQL injection relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[XMLSQLInjectionRelaxationRule!]`	A list of relaxation rules.

Example

```
{
  "pageInfo": Pagination,
  "results": [XMLSQLInjectionRelaxationRule]
}
```

Types

XMLXSS

An XML cross-site scripting countermeasure.

Field Name	Description
`action` - `WAFAction!`	Action to be taken.
`relaxationRules` - `XMLXSSRelaxationRulesWithPagination`	A paginated list of XML cross-site

	scripting relaxation rules.

Arguments

`page` - `UnsignedInt32!` default = `1`

The page number to fetch results for.

`perPage` - `UnsignedInt32!` default = `1000`

The maximum number of results to show per page.

`threshold` - `AppSecThreshold`	Appsec Threshold configuration for XML cross-site scripting violations.

Example

```
{
  "action": WAFAction,
  "relaxationRules": XMLXSSRelaxationRulesWithPagination,
  "threshold": AppSecThreshold
}
```

Types

`XMLXSSRelaxationRule`

An XML XSS relaxation rule.

Field Name	Description
`enabled` - `Boolean!`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!`	Whether the name is in regex format.
`location` - `XMLLocation`	The location of the attachment.
`name` - `String!`	The name of the rule.

Example

```
{
  "enabled": false,
  "isNameRegex": false,
```

```
  "location": XMLLocation,
  "name": "xyz789"
}
```

Types

XMLXSSRelaxationRuleInput

An XML XSS relaxation rule.

Input Field	Description
`enabled` - `Boolean!` default = `true`	Whether the relaxation rule is enabled.
`isNameRegex` - `Boolean!` default = `false`	Whether the name is in regex format.
`location` - `XMLLocation`	The location of the attachment.
`name` - `String!`	The name of the rule.

Example

```
{
  "enabled": true,
  "isNameRegex": false,
  "location": XMLLocation,
  "name": "abc123"
}
```

Types

XMLXSSRelaxationRulesWithPagination

A paginated list of XML cross-site scripting (XSS) relaxation rules.

Field Name	Description
`pageInfo` - `Pagination!`	The returned page information.
`results` - `[XMLXSSRelaxationRule!]`	A list of XML XSS relaxation rules

Example

```
{
  "pageInfo": Pagination,
  "results": [XMLXSSRelaxationRule]
}
```

Types

XSSValueType

Allowed list of values for value types in XSS.

Enum Value	Description
ATTRIBUTE	
PATTERN	
TAG	