Home

API Reference SaaS (V3)

Introduction

API Call Format

Authentication

CYNET API

Authentication

Cynet 360 Settings

Alerts

Hosts

Host Information

Host Actions

Remediation Actions

ESPM

Post Misconfigurations POST

Get Misconfiguration Filter Fi... GET

Get Misconfiguration Endpoi... GET

Post Vulnerabilities (CVEs) POST

Get Vulnerabilities (CVE) Filt... GET

Get Vulnerabilities (CVE) End... GET

Schemas

Users on Hosts

Files

Domains

Network

IT Hygiene

Settings

SSPM

System Monitoring

Custom Remediations

Post Misconfigurations

POST https://YOUR_DOMAIN.api.cynet.com/api/v2/hosts/{siteGuid}/espm/misconfigurati…

Creates a paginated list of misconfigurations (ESPM risks) for a specific site (v4.31 and above).

Request

Security: Bearer Auth

Path Parameters

siteGuid string required

The unique identifier of the site as found in the URL when using the Cynet Console.

Body

application/json

limit number required

Number of items to return (max: 500)

`<= 500`

offset number required

Number of items to skip for pagination

`>= 0`

search string

Search query to filter results

selectedInternalId string

Optionally enter an `internalId` taken from the initial response to the POST Misconfigurations API. Provides a focused view on the selected risk.

sortBy object

Sort configuration

- **by** string

  Field to sort by

  Allowed values: `severity` `unprotectedEndpoints` `platform` `subject` `category` `products` `status`

- **direction** string

  Sort direction

  Allowed values: `ASC` `DESC`

filter object

Filter configuration

- **severity** object

  Severity filter

- **category** object

  Category filter

- **products** object

  Products filter

- **component** object

  Component filter

- **host_names** object

  Host names filter

- **groups** object

  Groups filter

Responses

200

Success - Request completed successfully

Body

application/json

- **data** array[object]
  - **riskId** string
    Risk identifier
  - **severity** string
    Severity: 'Critical', 'High', 'Medium', 'Low'
  - **category** string
    Risk category
  - **relatedEndpoints** object
  - **subject** string
    Risk subject/title
  - **products** array[string]
    Affected products
  - **component** string
    Component name
  - **industryReferences** array[string]
    Industry reference identifiers
  - **MITRETactics** array[object]
    MITRE ATT&CK tactics (renamed from tactics)
  - **MITRETechniques** array[object]
    MITRE ATT&CK techniques (renamed from techniques)
  - **description** string
    Risk description
- **count** integer
  Total count of items matching the query

Request Sample: Shell / cURL

```
curl --request POST \
  --url https://your_domain.api.cynet.com/api/v2/hosts/{siteGuid}/espm/misconfigurations \
  --header 'Accept: application/json' \
  --header 'Authorization: Bearer 123' \
  --header 'Content-Type: application/json' \
  --data '{
  "limit": 0,
  "offset": 0,
  "search": "string",
  "selectedInternalId": "string",
  "sortBy": {
    "by": "severity",
    "direction": "ASC"
  },
  "filter": {
    "severity": {
      "value": []
    },
    "category": {
      "value": "string"
    },
    "products": {
      "value": []
    },
    "component": {
      "value": "string"
    },
    "host_names": {
      "value": []
    },
    "groups": {
      "value": []
    }
  }
}'
```

Response Example


```
{
  "data": [
    {
      "riskId": "string",
      "severity": "string",
      "category": "string",
      "relatedEndpoints": {
        "protectedEndpoints": 0,
        "unprotectedEndpoints": 0,
        "ignoredEndpoints": 0
      },
      "subject": "string",
      "products": [
        "string"
      ],
      "component": "string",
      "industryReferences": [
        "string"
      ],
      "MITRETactics": [
        {
          "linkName": "string",
          "link": "string"
        }
      ],
      "MITRETechniques": [
        {
          "linkName": "string",
          "link": "string"
        }
      ],
      "description": "string"
    }
  ],
  "count": 0
}
```