SecTeer VulnDetect

Corporate API Guide

SecTeer VulnDetect

Patch Current - Stay Current

SecTeer VulnDetect 8.0.0 – Corporate API Guide

Table of Contents

SecTeer VulnDetect Corporate API

The SecTeer VulnDetect API allows corporate users to access their SecTeer VulnDetect data outside the web-based user-interface.

API Information

Character sets and timestamps

The character set used by SecTeer VulnDetect is UTF-8.

All date/time values returned by the API are in UTC.

The data format returned by the API is `Content-Type: application/json; charset=utf-8`

Identifiers

SecTeer VulnDetect uses uuids to identify most entities, such as agents/hosts and groups.

Authentication

The SecTeer VulnDetect API uses Bearer token authorization with the Authorization HTTP header. Tokens are uuids in the form 11111111-2222-3333-4444-555555555555.

Example:
Authorization: Bearer 11111111-2222-3333-4444-555555555555

API Tokens can be created and deleted in the SecTeer VulnDetect user interface, in the Configuration page, under the API Tokens tab. Each API Token is keyed to a specific site.

Additional useful headers

```
Accept-Encoding: gzip
```

Some of the API endpoints can return a significant amount of data and compressing it will significantly improve response times and reduce network transfer times.

If using PowerShell to interact with the API, then the data will be automatically decompressed upon reception.

Agent/Host

The terms 'host' and 'agent' have been used interchangeably in this manual.

Strictly speaking, a 'host' is a computer in the customer's network, and an 'agent' is the SecTeer VulnDetect agent, which is installed on a 'host', but this distinction is not always obvious.

Regardless, agents/hosts are uniquely identified by an **agentUuid**.

Days of week (DOW) of inspections

This value is a combination of bit-flags:

Sunday	64
Monday	32
Tuesday	16
Wednesday	8
Thursday	4
Friday	2
Saturday	1

Example: If the DOW value is 127, then the agent will run an inspection every day.

Hour of day (HOD) of inspections

The value is in seconds after midnight, interpreted in the local time zone on the host in question.
The window is the length of time, in seconds, after HOD during which the agent can run scheduled inspections.

Currently, the window is 6 hours, or 21600 seconds.

Manually requested inspections will still be performed outside the window.
Example: If the HOD value is 3600, and the window is 6 hours, then the agent will run its scheduled inspection as soon as possible after 01:00, but before 07:00, in its local time.

After performing an inspection, and the SecTeer VulnDetect backend servers have processed the inspection data, if there are available updates that have been approved the agent will attempt to perform those updates immediately.

This is also the case for manually requested inspections that fall outside the inspection window.

Enabled and disabled agents

Hosts/Agents that are shown in the Hosts page in the SecTeer VulnDetect interface are enabled (isEnabled=true).

Hosts/Agents shown in the Hidden Hosts tab in the Configuration page are disabled (isEnabled=false).

Hosts/Agents shown in the Dormant Hosts tab in the Configuration page are disabled (isEnabled=false), and dormant (isDormant=true).

Disabled agents cannot be in a group and have no application data. They can still check in and may perform inspections, but their inspections are not processed by the SecTeer VulnDetect backend servers.

Dormant agents are still members of their group, even though they are disabled.

API Details

Host name: `https://corporate.vulndetect.com`

Most endpoints return an object with a single property, which is either an array of objects or a single object.

Example:
When called without an agentUuid, the agent endpoint returns data with the following shape: `{"agents": [...]}`

Writeable endpoints typically return `{"success": true}`

Application Properties

channelTag	Uniquely identifies this application
title	Application title
vendor	Application vendor
icon	Application icon path (see notes)
countInsecure	Count of insecure installations of the application
countOk	Count of installations of the application with no known security issues
countEoL	Count of End-of-Life installations of the application
countZeroDay	Count of installations of the application which have a 0-Day
countVersions	Count of different versions of the application detected
countSolutions	Count of insecure installations of the application which have an upgrade that fixes the security issues
countTotal	Total count of installations of the application

Note that the counts are not independent, i.e., an *End-of-Life* installation will also be counted as either *Insecure* or *Ok*, as appropriate, and *0-Day* installations are also counted as *Insecure*.
Still, `countTotal` will equal the sum of `countInsecure` and `countOk`.
The application icon is available at the given path, with the url prefix:
`https://corporate.vulndetect.com/icons/`

Applications

`GET /api/corporate/v1/applications`

Query options:

status: *ok*, *insecure*, *eol* or *zeroday*. Filter applications by status.

groupUuid: <groupUuid>. Request the application list for hosts in a single group.
Fetches the list of detected applications in the `applications` array.

Application Version Properties

channelTag	Uniquely identifies this application
title	Application title
vendor	Application vendor
icon	Application icon path (see notes for *Application Properties* above)
version	Application version
countTotal	Total count of installations of this version the the application
vulnStatus	Vulnerability status of this version of the application. *Ok* or *Insecure*
updateStatus	Update type of this version of the application. *Plain* or *Security*
isUntracked	True if this version is not tracked. This means that the vendor does not provide useful vulnerability information for the application
isPrerelease	True if this version is a pre-release version of the application
isEoL	True if this version is End-of-Life
isZeroDay	True if this version has a 0-Day
statusFlags	Not used
isRecommendedVersion	True if this version is the recommended version for this application. If this is true, then the *recommendedVersion* property will not have any useful information, because it would be redundant.
hasRecommendedVersion	True if this application has a recommended version. Note that even if this is true, if isRecommendedVersinis also true, then the *recommendedVersion* property will not have any useful information, because it would be redundant
recommendedVersion	This property is an object that contains information about the recommended version of the application, including most of the same properties as described above. Some of those properties are contained in a child object named *display*, which is *null* if there is no recommended version of the application, or if this version of the application is the recommended version. In particular, the property *recommendedVersion.display.version*, if present, contains the version string of the recommended version of the application.

Application Versions

`GET /api/corporate/v1/application-versions`

Query options:

channelTag: <channelTag>. Identifies the application. This option is required.
status: *ok*, *insecure*, *eol* or *zeroday*. Filter application versions by status.

groupUuid: <groupUuid>. Request the application version list for hosts in a single group.
Fetches the list of detected versions of the application, identified by the **channelTag**, in the `versions` array.

Application Host Properties

channelTag	Uniquely identifies this application
title	Application title
vendor	Application vendor
icon	Application icon path (see notes for *Application Properties* above)
product	Not used
productFamily	Not used
version	Application version
icon	Application icon (see notes for *Application Properties* above)
appUuid	Not used
hostname	The host’s name
hostDomain	The host’s domain
agentUuid	The host’s agentUuid, uniquely identifies this host/agent
groupName	The name of the host’s group
groupUuid	The groupUuid of the host’s group
vulnStatus	Vulnerability status of this version of the application. *Ok* or *Insecure*
updateStatus	Update type of this version of the application. *Plain* or *Security*
isUntracked	True if this version is not tracked. This means that the vendor does not provide useful vulnerability information for the application
isPrerelease	True if this version is a pre-release version of the application
isEoL	True if this version is End-of-Life
isZeroDay	True if this version has a 0-Day
statusFlags	Not used
display	This property is an object that contains display information about the application. Some of the properties are duplicated, e.g., title, vendor, version. The display object contains the path and filename of the file that identifies the application. The display object also contains the *isRecommendedVersion* and *hasrecommendedVersion* properties that are described in the Application Version section, above.
recommendedVersion	This property is an object that contains information about the recommended version of the application, including some of the same properties as described above. Some of those properties are contained in a child object named *display*, which is *null* if there is no recommended version of the application, or if this version of the application is the recommended version. In particular, the property *recommendedVersion.display.version*, if present, contains the version string of the recommended version of the application.

Application Hosts

```
GET /api/corporate/v1/application-hosts
```

Query options:

channelTag: <channelTag>. Identifies the application. This option is required.
status: *ok*, *insecure*, *eol* or *zeroday*. Filter application by status.
version: <application version>. Filter by application version.

groupUuid: <groupUuid>. Request the list for hosts in a single group.
Fetches the list of hosts that have the application, identified by the **channelTag**, in the `hosts` array.

Note that if multiple instances of the application were found on a host, then that host will occur multiple times in the results.

Dashboard Data Properties

The dashboard data is returned in a `dashboard` object that has two properties: `counts` and `updates`.

The `updates` property is an array of 7 objects, one for each day of the past week. Each object has a `date` property and a `countVerified` property, which indicates how many updates were successfully completed on that day.

The `counts` object has various properties that are listed in the table below:

countAgents	Host count
countChannelTagVersions	Count of distinct application versions
countChannelTags	Count of distinct applications
countEoL	Count of End-of-Life applications
countEoLNotZeroDayNotInsecure	Count of End-of-Life applications with no known security issues
countGroups	Group count
countInsecure	Count of applications with known security issues
countInsecureNotZeroDay	Count of applications with known security issues but not affected by a 0-day
countOk	Count of applications with no known security issues
countOkNotZeroDayNotEoL	Count of applications with no known security issues that are not End-of-Life
countOutOfDateApprovals	Count of out-of-date group-approvals
countSolutions	Count of applications with known security issues that can be updated
countTotal	Total count of all applications found
countUnknown	Count of applications with an unknown security status. This value should always be 0
countZeroDay	Count of applications that are affected by a 0-day

Dashboard

`GET /api/corporate/v1/dashboard`

Fetches the dashboard data, in the `dashboard` object.

Group Properties

groupUuid	Uniquely identifies this group
groupName	The group's name
comment	A descriptive comment
countHosts	Number of hosts in this group
countInsecure	Count of insecure applications installed on the hosts in this group
countOk	Count of applications with no known security issues installed on the hosts in this group
countTotal	Count of all applications installed on the hosts in this group
createdAt	Creation time of the group
updatedAt	Last update time of the group

Groups

`GET /api/corporate/v1/group`

Returns the list of groups in the `groups` array.

Single Group

`GET /api/corporate/v1/group/${groupUuid}`

Returns a single group, by **groupUuid**, in the `group` property.
To find the groupUuid, see the non-parameterized group endpoint above.

Agent Properties

agentUuid	Uniquely identifies this host/agent
hostName	The host's name
hostDomain	The host's domain name
canonicalName	The AD canonical name of the host
timezoneOffset	The timezone offset of the host, in seconds
lastInspectionAt	UTC time of the last inspection of the agent
lastCheckinAt	UTC time of the last check-in of the agent
lastKnownBootTime	UTC time of the last known startup of the host. Note that only agents version >= 3.2.0.0 report the host startup time
lastIp	The last seen IP address of the host, as observed by the SecTeer servers
isEnabled	Indicates whether the agent is enabled or disabled. Disabled agents are those that are in the Hidden Hosts tab, or Dormant Hosts tab.
version	The version of the SecTeer VulnDetect agent installed on the host
countOk	Number of applications with no known vulnerabilities found on the host
countInsecure	Number of insecure applications found on the host
countUnknown	Number of applications found on the host, where no reliable security information is available from the vendor
countEoL	Number of End-of-Life applications found on the host
countZeroDay	Number of insecure applications found on the host that are affected by a 0-Day vulnerability
countInsecureNotZeroDay	Number of insecure applications found on the host that are not affected by a 0-Day vulnerability
countEoLNotZeroDayNotInsecure	Number of applications found on the host that are not insecure (and not affected by a 0-Day vulnerability)
countOkNotZeroDayNotEoL	Number of applications with no known vulnerabilities and not End-of-Life, that are found on the host
countTotal	Total number of applications found on the host
havePendingInspection	Indicates whether the agent has a pending non-scheduled inspection, i.e. if an inspection has been manually requested
haveInProgressInspection	Indicates whether the agent is currently running an inspection
checkInInterval	The agent check-in interval in seconds
inspectionScheduleDow	The days of the week in which this agent runs inspections
inspectionScheduleHod	The hour of day that this agent runs inspections. The value is in seconds after midnight
inspectionScheduleWindow	The window in which to run inspections, in seconds
groupUuid	Uniquely identifies the agent's group
groupName	The name of the agent's group
nextInspectionTime	UTC time of the next scheduled inspection

The list shows properties that are present on all agents. Additional properties may be present on some agents.

Note that the counts of the number of applications found with various overlap in some cases. For example, *countInsecure* includes all applications in *countZeroDay*. Applications may also be End-of-Life independently of whether they are *Ok* or *Insecure* (or *Unknown*).

Agents

```
GET /api/corporate/v1/agent
```

Returns the list of enabled agents in the `agents` array.

Disabled Agents

```
GET /api/corporate/v1/agent/disable
```

Returns the list of disabled agents in the `agents` array.

Single Agent

`GET /api/corporate/v1/agent/${agentUuid}`

Returns a single agent, by **agentUuid**, in the `agent` property.

To find the agentUuid, see the non-parameterized agent endpoints above.

Disable Agent

`PATCH /api/corporate/v1/agent/${agentUuid}/disable`

Disables an agent, by **agentUuid**. The host/agent is moved to Hidden Hosts, it is removed from any group it is in, and its application information is deleted.

Returns `{"success": true}`

Enable Agent

`PATCH /api/corporate/v1/agent/${agentUuid}/enable`

Enables an agent, by **agentUuid**. The host/agent is moved from Hidden Hosts and is again visible in the Hosts page. The host/agent is not in any group. No application information will be available until the agent has performed either the next scheduled inspection, or a manually requested one.
Returns `{"success": true}`

Request an immediate inspection

`POST /api/corporate/v1/agent/${agentUuid}/inspect`

Requests that the agent with the specified **agentUuid** perform an inspection and update cycle as soon as possible.

Returns `{"success": true}`

Agent Applications

`GET /api/corporate/v1/agent/${agentUuid}/applications`

Query options:
status: *ok*, *insecure*, *eol* or *zeroday*. Filter application versions by status.

Returns the list of applications found by the agent specified by the **agentUuid**, in the applications property. The properties on an application shown in the Application Hosts table.

Agent Site Switching

`PATCH /api/corporate/v1/agent/${agentUuid}/site-switcher/${destSiteAccountUuid}`

This is an advanced feature that allows switching an agent to a different site.

The agent is identified by the **agentUuid**, and the destination site is identified by its **siteAccountUuid**. The **siteAccountUuid** for a site can be found by using the Site Settings endpoint, with an API Token for that site.

Note that using this feature requires two distinct API Tokens, one for the destination site, to find its **siteAccountUuid**, and one for the source site, to enable site-switching for the agent.
When site-switching is enabled for an agent, it is immediately disabled and will not be shown in Hidden

Hosts

On its next check-in, the agent will get a new **agentUuid**, and appear as a completely new agent in the destination site, with no relation to the host in its previous site.

Site Settings

`GET /api/corporate/v1/settings`

Returns the **siteAccountUuid** and the settings of the site for the API Token used.

Examples

PowerShell examples:

The examples use the following API authentication token:
11111111-2222-3333-4444-555555555555.

The examples assume that an agent exists with the following agentUuid:
12345678-90ab-cdef-0123-456789abcdef

Fetch list of applications

```
Invoke-RestMethod -Method GET -Uri
https://corporate.vulndetect.com/api/corporate/v1/applications -Headers
@{Authorization='Bearer 11111111-2222-3333-4444-555555555555'; 'Accept-
Encoding'='gzip'}|select -expand applications|ft -property
vendor,title,channelTag,countInsecure,countTotal
```

Fetch list of different versions of Google Chrome

```
Invoke-RestMethod -Method GET -Uri
https://corporate.vulndetect.com/api/corporate/v1/application-
versions?channelTag=google.chrome.default -Headers @{Authorization='Bearer 11111111-
2222-3333-4444-555555555555'; 'Accept-Encoding'='gzip'}|select -expand versions|ft -
property vendor,title,version,countInsecure,vulnStatus,countTotal
```

Fetch list of hosts that have an insecure version of Google Chrome

```
Invoke-RestMethod -Method GET -Uri
https://corporate.vulndetect.com/api/corporate/v1/application-
hosts?channelTag=google.chrome.default&status=insecure -Headers @{Authorization='Bearer
11111111-2222-3333-4444-555555555555'; 'Accept-Encoding'='gzip'}|select -expand
hosts|ft -property hostname,vendor,title,version
```

Fetch list of agents

```
Invoke-RestMethod -Method GET -Uri
https://corporate.vulndetect.com/api/corporate/v1/agent -Headers
@{Authorization='Bearer 11111111-2222-3333-4444-555555555555'; 'Accept-
Encoding'='gzip'}|select -expand agents|ft -property agentUuid,hostName,hostDomain
```

Request an inspection

If that agent has no results or the results are old, request an inspection:

```
Invoke-RestMethod -Method POST -Uri
https://corporate.vulndetect.com/api/corporate/v1/agent/12345678-90ab-cdef-0123-
456789abcdef/inspect -Headers @{Authorization='Bearer 11111111-2222-3333-4444-
555555555555'; 'Accept-Encoding'='gzip'}
```

Check when the agent finished its last inspection

```
Invoke-RestMethod -Method GET -Uri
https://corporate.vulndetect.com/api/corporate/v1/agent/12345678-90ab-cdef-0123-
456789abcdef -Headers @{Authorization='Bearer 11111111-2222-3333-4444-555555555555';
'Accept-Encoding'='gzip'}|select -expand agent|fl -property
hostname,lastCheckinAt,lastInspectionAt,havePendingInspection,haveInProgressInspection
```

Note that the times returned are in UTC. Periodically issue requests to this endpoint until the inspection has completed.

System Requirements

Supported Microsoft Operating Systems:

- Windows 11
- Windows 10
- Windows 8.1*
- Windows 7 SP2 or later*
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012*

* Due to limitations in the default PowerShell on these Operating Systems, not all packages are supported. Also, these versions are in extended support from Microsoft or will reach End-of-Life soon.

** PowerShell 5.1 is installed by default on all modern Windows and Windows Server systems.

Supported Browsers (Latest Version for Viewing Results):

Although most modern browsers will work with VulnDetect, the following are officially supported:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge (Chromium Based)
- Vivaldi
- Opera

Agent-based Scanning, Deployment and Patching:

- Network/Internet connection (TLSv1.2/TLSv1.3 to VulnDetect.com)
- Local administrative privileges for Agent deployment to Network
- 25 MB of free disk space
- 1GB of free disk space for upgrading software

(To ensure that there is space for the downloaded installers and the unpacked temporary files). Some software may require more space.

For Certificate Verification, Access to the Following Addresses is Required:

- r3.o.lencr.org
- r3.i.lencr.org

The Addresses of SecTeer Services Are:

- https://*.vulndetect.com/ (port 443/tcp)

The above should be whitelisted in the Firewall/Proxy configuration.

The addresses for Amazon trust services:
ocsp.sca1b.amazontrust.com
crt.sca1b.amazontrust.com
and to SecTeer:
https://*.vulndetect.com/
should be white listed in the Firewall/Proxy configuration.

Support and Maintenance

Our support team will assist with the actual setup.

All support questions should be addressed to the SecTeer Customer Support Center:

support@secteer.com

- **User Forums**
  https://www.vulndetect.org/
  Interact with other users by posting questions or submitting tips.

- **Additional Product Details**
  Review product specifications, getting started guides are available through your user account. If you currently do not have a user account, please contact;
  contact@secteer.com

- **Configuration**
  If you already have an account, you can contact us at support@secteer.com to set up an onboarding call. Our support team is available to assist.

PLEASE NOTE: You should always refer to the website for up-to-date technical requirements:

https://secteer.com/system-requirements/

About SecTeer

Founded by veterans within the Cyber Security industry. We help organizations better protect themselves against vulnerabilities and threats that compromise the integrity of any network. Our mission is to help IT Security professionals and IT operations personnel across industries uphold and maintain a more secure system through effective and affordable Security Patch Management solutions and ultimately repel the rising threats from a multitude of cybercriminals.

Contact:

For further information about our competencies:

Please contact contact@secteer.com

Try out SecTeer VulnDetect today**:**

REQUEST A DEMO

Visit us at: SecTeer.com

Patch Current - Stay Current