将WSA与CTR集成

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 注册设备 验证

简介

本文档介绍将网络安全设备(WSA)与思科威胁响应(CTR)门户集成的步骤。

供稿:Shikha Grover,编辑者:Yeraldin Sanchez Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题:

- WSA访问
- CTR门户访问
- 思科安全帐户

使用的组件

本文档中的信息基于以下软件和硬件版本:

•异步操作系统版本12.x或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

警告:如果您使用亚太地区、日本和中国地区URL(https://visibility.apjc.amp.cisco.com/)访<u>问</u> <u>CTR,则目前不</u>支持与您的设备集成。

步骤1.在CLI中的REPORTINGCONFIG下启用POSERVABLE并提交更改,如图所示。

| WSA-12-0-1-1/3.COM> reportingconing |
|---|
| hoose the operation you want to perform: COUNTERS - Limit counters recorded by the reporting system. WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries. AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings alculation |
| WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing. CTROBSERVABLE - Enable or Disable CTR observable based indexing. CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.]> ctrobservable |
| TR observable indexing currently Enabled. re you sure you want to change the setting? [N]> y |
| hoose the operation you want to perform: COUNTERS - Limit counters recorded by the reporting system. WEBTRACKINGQUERYTIMEOUT - Timeout value for Webtracking Queries. AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation. WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing. CTROBSERVABLE - Enable or Disable CTR observable based indexing. CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance. |

步骤2.配置安全服务交换(SSE)云门户,导航至**网络>云服务设置>编辑设置**,单击**启用**并提交**,如** 图所示。

Cloud Services Settings

| Settings | |
|------------------|---------------|
| Threat Response: | Enabled |
| | Edit Settings |

根据您的位置选择云,如图所示。

| Cloud Services Settings | |
|---|------------------------------|
| Success — Your changes have been commit | ted. |
| Settings | |
| Threat Response: | Enabled |
| | Edit Settings |
| Registration | |
| Cloud Services Status: | Not Registered |
| Threat Response Server: | AMERICAS (api-sse.cisco.com) |
| Registration Token: 🕐 | Register |
| | |
| | |

步骤3.如果您没有思科安全帐户,则可以在具有管理员访问权限的思科威胁响应门户中创建用户帐 户。

要创建新用户帐户,请导航至思科威胁响应门户登录页。

步骤4.在SSE门户上的云服务下启用思科威胁响应,如图所示。



第五步: 确保WSA在端口443上具有到SSE门户的可达性:

- api.eu.sse.itd.cisco.com(欧洲)
- api-sse.cisco.com (美国)

注册设备

步骤1.从安全服务交换(SSE)门户获取注册令牌,以在安全服务交换门户注册设备。

SSE门户链接为<u>https://admin.sse.itd.cisco.com/app/devices</u>。

注意:使用CTR帐户凭证登录SSE门户。

| \leftarrow \rightarrow C \triangle $(admin.sse.itd.cisco.com/app/devices)$ | 1 | | | | * < | . 🖬 🥥 🎯 | 0 🖷 🗍 : |
|--|---------------|-----------------|----------------|---------|-------------|---------|-----------------|
| CISCO Security Services Exchange | Devices Cloud | Services Events | Audits | | | 0 * 🔺 | Shikha Grover 🗸 |
| Devices for Cisco Systems | | | | | | | |
| Q Device Name / ID O Rows Selected | | | | | | | + 0 🖸 |
| □ 1/4 # Name ∧ | | Туре | Version | Status | Description | Actions | |
| | | | No Devices Con | figured | | | |
| Page Size: 25 🔻 Total Entries: 0 | | | | | | I< | < 1 > > |
| | | | | | | | |

| Add Devices and Genera | ate Tokens (| • | \times |
|--|--------------|--------|----------|
| Number of devices 1 Up to 100 Token expiration time 1 hour | ¥ | | |
| | | Cancel | Continue |

| Add Devices and Generate Tokens () | × |
|---|-----|
| The following tokens have been generated and will be valid for 1 hour(s): | |
| Tokens | |
| ef1324a199c106371542ee4d2d1bf1e7 | |
| | |
| Close Copy to Clipboard Save To F | ile |
| | _ |

步骤2.输入从WSA中的安全服务交换门户获取的注册令牌,然后**单击**注册,如图所示。

Cloud Services Settings

| rungs | |
|-------------------------|------------------------------|
| Threat Response: | Enabled |
| | Edit Settings |
| | |
| Registration | |
| Cloud Services Status: | Not Registered |
| Threat Response Server: | AMERICAS (api-sse.cisco.com) |
| | |

步骤3.几秒钟后,您将看到注册成功。

警告:确保生成的令牌在到期之前已使用。

Cloud Services Settings

| Success — Your appliance is successfully reg | jistered with the Cisco Threat Response portal. |
|--|---|
| Settings | |
| Threat Response: | Enabled |
| | Edit Settings |
| | |
| Registration | |
| Cloud Services Status: | Registered |
| Threat Response Server: | AMERICAS (api-sse.cisco.com) |
| Deregister Appliance: | Deregister |

步骤4.在SSE门户上,您可以看到设备状态。

| $\leftrightarrow \rightarrow c$ | Ċ | 🗎 a | dmin.sse.itd. | cisco.com/app/devices | | | | Å | 🛆 🖪 🍳 🎯 | 0 🖷 💭 🗄 |
|---------------------------------|---------|-----------|---------------|-----------------------|----------------------|------------|--------------------------------|-------------|---------|-----------------|
| altalo cisco | Sec | curity \$ | Services | Exchange Devices | Cloud Services Event | s Audits | | | 0 * 🔺 | Shikha Grover 🗸 |
| Devic | ces fo | or Ciso | co Syste | ms | | | | | | |
| V 0 Ro | Q D | evice Na | ime / ID | | | | | | | + 0 🖸 |
| | | 1/4 | # | Name < | Туре | Version | Status | Description | Actions | |
| 0 | | > | 1 | vWSA-12-0-1-173.COM | WSA | 12.0.1-173 | Registered | \$300V | / 🖬 😘 | |
| Page | e Size: | 25 🔻 | Total En | tries: 1 | | | | | I< | < 1 > > |

步骤5.在CTR门户上显示注册的设备。

| \leftrightarrow \rightarrow C \triangle $$ visibility.amp | o.cisco.com/settings/devices | | | | *) 🛆 🖪 | o o o o = : 🔘 : |
|---|------------------------------|----------------------|------------|-------------|--------------------------------------|---------------------|
| Threat Response | vestigate Snapshots Incider | ts Beta Intelligence | Modules | | (| ? 🔅 Shikha Grover 🗸 |
| Settings > Devices | | | | | | |
| Settings | Devices | | | | | |
| Your Account Devices | | | | | | |
| API Clients | Manage Devices Rel | bad Devices | | | | |
| > Modules | Name | Туре | Version | Description | ID | IP Address |
| Users | vWSA-12-0-1-173.COM | WSA | 12.0.1-173 | S300V | 3af01d56-a93e-4edc-926e-de1a4588409d | 10.150.215.123 |
| | 25 per page 1-1 of 1 | | | | C Prev | vious Next > |
| | | | | | | |
| | | | | | | |

您可以将此设备关联到模块,导航至Modules > Add New Module > Web Security Appliance,如图 所示。

| cisco | Threat Response In | vestigate Snapshots Incidents Beta Intelligence Modules |
|--|-------------------------|--|
| Settings | > Modules > Available M | Iodules > Web Security Appliance > Add New Module |
| Setti | ngs | Add New Web Security Appliance Module |
| Your A Device API CI | Account es ients | Module Name* Web Security Appliance |
| Modul Ava | es ilable Modules | Registered Device* |
| Users | | Search registered devices by name Request Timeframe (days) Save Cancel |

设备现已集成。您可以通过WSA的流量并在CTR门户上调查威胁。

使用本部分可确认配置能否正常运行。

用于WSA模块的加密(查询WSA日志)及其支持的格式,用于从CTR门户运行查询:

• 域 — **域**:"<u>com</u>"

- URL url:"<u>http://www.neverssl.com</u>"
- SHA256 -

sha256:"8d3aa8badf6e5a38e1b6d59a254969b1e0274f8fa120254ba1f7e02991872379"

- IP ip:"172.217.26.164"
- 文**件名** file_name:"test.txt"

使用中的加密示例:

| Investigation Assign to Incident | | | | | | |
|--|-------------------------------|-----------------|--|---|--|--|
| ፼1 ×°1 | ÷▼ @ 0 | @ 0 | ₿ o | ≕ 0 | iiii 1 | Automatic Layout 👻 |
| Target v Observable v | Indicators | Domains | File Hashes | IP Addresses | URL 🗸 | Modules 🗸 |
| tigation 1 of 1 enrichments complete | | _ | Sightings Timeline | | | - Malicious |
| http://amazon.com/" | | h | 1 Sighting in My Environment First: Aug 28, 2019 Last: Aug 28, 2019 | 2 1 | 28, 2019 Aug 28, 2019 Aug 28, 20 | - Suspicious - Unknown - Clean • Targets |
| Istigate Clear Reset What can I search | for? | | Observables | | | List View 👻 - |
| Clean URL V | | - | http://amazon. _{Clean URL} | .com/ 🔍 | | |
| | Corrected In | | My Environment Global 1 Sighting in My Environment First: Aug 28, 2019 Last: Aug 28, 2019 | 2 1 0 Aug 20, 2019 Aug | 18, 2019 Aug 28, 2019 Aug 28, 2019 | Malicious Suspicious Unknown Clean Targets |
| Hosted By URL | target ende | IT EERVABLES | Judgement (1) Verdict (1) | Sighting (1) | | |
| 176.32.08166 🧹 | up: 10.10.513 USER: 10.10. | 99 | Module Obs Web Security Appliance 4 he | served ▲ Description Confi ours ago Transaction processed by Web Pro xy Services | dence Severity Details Resc Low Allow | alution Sensor \$ ved network.proxy v r £ |
| / Investigation Assign to Incident | Snapshots 🔻 | | | | | Automatic L |
| 0 Targets | V 🖗 0 Indicators | 1 Domai 1 | in ✓ 0 File Ha | shes 0 IP Add | resses 0 U | RLs 2 1 Mode |
| estigation 1 of 1 enrichments complete | with 5 Alerts | | — Sightings Tim | eline | | |
| ww.cisco.com | | | My Environme 0 Sightings in | nt Global 0- My Environment 1- | | – Mali – Sus – Unk – Clea |
| | | | | 1- | 2000 Jan 01, 20 | 000 Jan 02, 20 Targ |
| nvestigate Clear Reset Wh | at can I search for? | | | 101 | | |
| westigate Clear Roset What Management and the second secon | at can I search for? | | _ Observables | unon | | List View |
| westigate Clear Reset Wh ations Graph Showing 1 node Expand | hat can I search for? | | Observables | isco.com 🗹 🖌 | ? <u>~</u> | List Viev |
| westigate Clear Roset Wh ations Graph Showing 1 node Expand Domain www.cisco.com | at can I search for? | | Observables WWW.C Domain My Environm 0 Sightings in | isco.com V | 2 2 | List View – Malici – Suspi – Unkm – Clean 200 |
| tvestigate Clear Reset Wh ations Graph Showing 1 node Expand Domain ♥ www.cisco.com | hat can I search for? | | Observables WWW.Cl Domain My Environm 0 Sightings in Judgements | isco.com V | ? (2) - 1, 2000 Jan 01, 20 | – Malici – Suspi – Unkn – Clean 200 Jan 62, 201 Target |

如果我遗漏了应包含的内容,请随时通知我。 如果我遗漏了应包含的内容,请随时通知我。 如果我 遗漏了应包含的内容,请随时通知我。 如果我遗漏了应包含的内容,请随时通知我。