# • **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1**

# Industrial Security Implementation Guide

First published: July 2021



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS DESCRIBED IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED "AS IS."

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, OR INCIDENTAL DAMAGES UNDER ANY THEORY OF LIABILITY, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF OR INABILITY TO USE THIS DOCUMENT, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

©2021 CISCO SYSTEMS, INC. ALL RIGHTS RESERVED

# · ı | ı . ı | ı . cısco .

# Contents

| Cisco Cyber Vision             |
|--------------------------------|
| Installation                   |
| Global Center and Center 1     |
| Sensors                        |
| Configuration                  |
| Licensing                      |
| Presets                        |
| Active Discovery               |
| Baseline                       |
| Upgrade                        |
| Global Center and Local Center |
| Knowledge Database             |
| Integrations                   |
| Analysis                       |
| Presets                        |
| Reports and Events             |
| Packet Capture                 |
| ISA 3000                       |
| Installation                   |
| Hardware Installation          |
| Software Installation          |
| Connecting to the Network 10   |
| Configuration                  |
| Connection to FMC              |
| Device Configuration in FMC    |
| Software Upgrade               |
| Firepower Management Center 14 |
| Installation                   |
| Configuration                  |
| Basic Configuration            |
| Licensing                      |
| Network Objects                |
| Access Control Policy 15       |
| Intrusion Policy               |

| File and Malware Policy   | 18   |
|---|------|
| Preprocessors   | 19   |
| Network Discovery   | 19   |
| Hardware Bypass   | 20   |
| Upgrade.  | 20   |
| Integrations  | 21   |
| Syslog  | 21   |
| Analysis  | 22   |
| Connection Events   | 22   |
| Intrusion Events  | 22   |
|   |      |
| Hosts   | 22   |
| File Events   | 23   |
| SecureX   | 24   |
| Troubleshooting   | 24   |
| Cyber Vision Network Sensor Placement in the Network                                    |      |
| FTD CLI   | 24   |
| FMC Access Control Logging and Hit Count  | 25   |
| FMC Health Monitor  | 25   |
| Appendix  |      |
| Cisco Catalyst IE 3400 and IE 3300 Configuration Preparation for the Cyber Vision Se 26 | nsor |
| ERSPAN  | 26   |
| IOx   | 26   |
| Port Configuration  | 27   |
| Cisco Catalyst 9300 Configuration Preparation for the Cyber Vision Sensor               | 27   |
| ERSPAN  | 27   |
| IOx   | 28   |
| Port Configuration  | 28   |
| 5   | -    |

# · I | I · I | I · I CISCO

# Industrial Security Implementation Guide

# **Cisco Cyber Vision**

# Installation

# Global Center and Center

The Cyber Vision Center can be deployed as a virtual machine (VM) or as a hardware appliance. In this design, the Global Center and Centers were deployed as VMs on a Cisco Unified Computing System (UCS). For more information on installation and resource recommendations, see

https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html. As recommended in the Industrial Security Design Guide

(https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial\_Automation/IA\_Horizontal/IA\_Security/IA\_Security\_DG.html), the local Centers were validated with dual interfaces for management and sensor communication, respectively.

# Sensors

There are two types of Cyber Vision Sensor: hardware and network. The hardware Sensor is the Cyber Vision IOx application installed on an Industrial Compute Gateway 3000 (IC3000) appliance. The network Sensor is the Cyber Vision IOx application installed on the supported switches. For information on installing a Sensor on the IC3000, see <a href="https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html">https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html</a>.

For network Sensors, there are three methods of installation: switch CLI, switch web interface, and Cyber Vision Center Extension. This guide will cover the network sensor installation using the Cyber Vision Center Extension feature. Refer to the Cyber Vision documentation for guidance on manual installations, if needed: https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html.

Prior to any installation, the following configurations must be done on the switch:

- SSH
- Data export using Encapsulated Remote Switched Port Analyzer (ERSPAN)
- IOx and storage formatting
- Port configuration

Refer to Appendix for details on these configurations.

Once the switch has all necessary configurations, the sensor can be deployed using the Cyber Vision Center extension. First, install the extension by doing the following:

- 1. Download the extension (.ext file) from cisco.com.
- 2. In Cyber Vision Center, navigate to Admin > Extensions.
- 3. Click the Import Extension File button and browse to the extension file.

After the extension has been installed, install a sensor by doing the following:

- 1. In Cyber Vision Center, navigate to Admin > Sensors > Sensors.
- 2. Click the Deploy Cisco Device button:
  - a. In the IP address field, enter the IP address of the switch.
  - b. In the Port field, enter 443 for a network sensor.
  - c. In the User field, enter the user name to use to log in to the switch.
  - d. In the **Password** field, enter the password associated with the user account on the switch.
  - e. In the **Center IP** field, you may enter the IP address of the Center that the sensors will use for communication. For dual interface Center deployments, it is recommended to enter the eth1 IP address here.
  - f. Under Capture mode, you may choose from the various options to change what data the sensor will process. In this validation, the Optimal (default) option was selected.
  - g. Click the Deploy button.
  - h. More configuration fields will show. In the Capture IP address field, enter the ERSPAN destination IP address for the sensor.
  - i. In the Capture prefix length field, enter the prefix associated with the ERSPAN IP address.
  - j. In the Capture VLAN number field, enter the monitoring session destination VLAN
  - k. In the Collection IP address field, enter the IP address of the eth0 interface of the sensor. This is the IP address that will be used for communication with the Center.
  - I. In the Collection prefix length field, enter the prefix associated with the sensor IP address.
  - **m.** In the **Collection gateway** field, enter the IP address of the gateway that the sensor will use for communicating through the network.
  - n. In the Collection VLAN number, enter the VLAN of the sensor IP address.
  - o. Under Application type, click the radio button of the type of sensor you wish to deploy. For the Passive and Active Discovery option, additional information is required:
    - i. In the **IP address** field, enter an IP address for the sensor to use in Active Discovery. Note that this IP address needs to be from the same subnet as the end devices you wish to discover. If active discovery is necessary on the same subnet as the sensor itself, you can click the **USE COLLECTION** button.
    - ii. In the **Prefix** length field, enter the prefix associated with the IP address.
    - iii. In the VLAN field, enter the VLAN for the subnet.
    - (Optional) Click the ADD ONE button to configure another Active Discovery interface. This secondary interface should be configured for doing active discovery on a different subnet than what was specified for the first interface.
  - p. Click the **Deploy** button.

# Configuration

# Licensing

Cyber Vision Center makes use of Cisco Smart Software Licensing, which can be installed via online or offline methods. For online licensing, the Center must be able to communicate externally to Cisco.com. To license Cyber Vison Center using the online method, do the following:

- 1. Ensure the Cisco Cyber Vision Advantage license is present in your Smart Software Account.
- 2. Copy the token associated with the Cyber Vision Advantage license from the Smart Software Licensing site.
- 3. In Cyber Vision Center, navigate to Admin > License.
- 4. Click the Register button.
- 5. In the Product Instance Registration Token field, paste the token.
- 6. Click the Register button.

### Presets

Presets allow the user to customize how components are displayed and grouped. In addition, the presets allow the user to quickly navigate to device activity, vulnerability, and event information. The Cisco Cyber Vision Center comes with default presets, such as Control Systems Management, but the user can create their own by doing the following:

- 1. In Cyber Vision Center, navigate to Explore.
- 2. At the top, click the New Preset button. Provide a name and an optional description.
- 3. The new preset will now show in the **My preset** list. Click the preset rectangle to display the preset dashboard and filter options.
- 4. From the left **Criteria** menu, select the necessary options to filter data included in the Preset. Click the **Save** icon at the top when finished.

## Active Discovery

The Active Discovery feature allows the sensor to send a broadcast message to a given subnet to retrieve device information. To initiate Active Discovery, do the following:

- 1. Create a Preset that is filtered for the Sensor with Active Discovery enabled.
- 2. Click the Save icon.
- 3. Click the Edit Active Discovery Settings icon.
- 4. Click the Active Discovery Status button to enable Active Discovery.
- 5. Click the button to the right of each protocol to enable.
- 6. Click the OK button.

| uluilu<br>cisco | CYBER VISION<br>Center | Edit active discovery settings         |                         |
|-----------------|------------------------|--|-------------------------|
| Ø               | Explore                | <u>.</u> මු ල් මි ඕ <u>ළ</u> ටු        | Mar 26, 2021 9:54:53 AN |
| Ē               | Reports                | 3400_active_discovery                  | Dashboard               |
| ŧ               | Events                 | Mypreset                               | Component               |
| C               | Monitor                | Active baseline: No active baseline    |                         |
| م               | Search                 | Active Discovery: Disabled             |                         |
| ¢               | Admin                  | Criteria Select all Reject all Default |                         |
|                 |                        | Search criteria Q                      | Credential              |
|                 |                        |  |                         |

# Figure 1 Enable Active Discovery

Figure 2 Active Discovery Settings

ACTIVE DISCOVERY SETTINGS

Х

Active discovery status: 1 Broadcasting sensors: FOC2316V092

| Protocol    | Enabled |      |
|-------------|---------|------|
| EtherNet/IP |         | ^    |
| S7Discovery |         |      |
| Profinet    |         | 1200 |

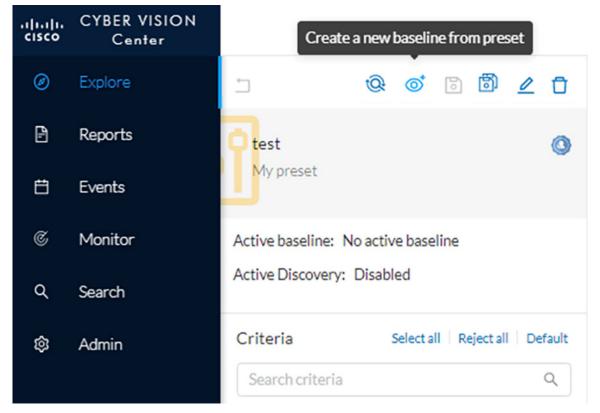
# Baseline

The Baseline feature helps to monitor given devices and/or communication for anomalous activity. To create a Baseline, do the following:

- 1. Create a Preset for the given devices and/or activity to be monitored.
- 2. Click the Save icon.

- 3. Click the Create a New Baseline from Preset icon.
  - a. In the Name field, enter a name for the Baseline.
  - b. Optionally, provide a Description.
  - c. Click the Create button.





# Upgrade

Upgrades can be done from the Center to upgrade both the Center and the Sensors. To upgrade the Center and Sensors, do the following:

- 1. Download the combined upgrade file (.dat) from Cisco.com
- 2. In Cyber Vision Center, navigate to Admin > System.
- 3. Click the System Update button and browse to the upgrade file.
- 4. The Center will verify if you want to run the update. Click the Yes, update button.

For information on individual device upgrades, refer to the Cyber Vision documentation: https://www.cisco.com/c/en/us/support/security/cyber-vision/series.html.

# Global Center and Local Center

The Global Center aggregates flows, devices, and events from local Centers. To connect a local Center to the Global Center, do the following:

- 1. In the local Center, navigate to Admin > System.
- 2. Scroll to the bottom and copy the string below Certificate fingerprint.
- 3. In Global Center, navigate to Admin > System > Management.
- 4. Click the Register a Center button.
  - a. In the Name field, enter a name for the local center.
  - b. In the Fingerprint field, paste the certificate fingerprint string from the local Center.
  - c. Click the OK button.
- 5. In Global Center, navigate to Admin > System.
- 6. Scroll to the bottom and copy the string below Certificate fingerprint.
- 7. In the local Center, navigate to Admin > System.
- 8. Scroll down and click the Enroll button under Enroll to a Global Center.
  - a. In the Global Center fingerprint field, paste the fingerprint copied from the Global Center.
  - **b.** In the **Global Center IP address** field, enter the IP address of the Global Center.
  - c. Click the Enroll button.

## Knowledge Database

The Knowledge Database (DB) includes vulnerability data for various hardware, firmware, and the like. The Knowledge DB is installed on the Global Center and pushed to the local Centers and must be updated separately from the Cyber Vision software itself. To install a Knowledge DB update, do the following:

- 1. Download the latest Cyber Vision Knowledge DB (.db) file from Cisco.com.
- 2. In Global Center, navigate to Admin > System.
- 3. Under Knowledge DB, click the Import a Knowledge DB button and browse to the update file.

# Integrations

#### **Cisco SecureX**

The Cyber Vision Center and Cisco SecureX integration allows the user to further investigate IP addresses detected by Cyber Vision in SecureX, which may provide more insight about the entity from the wealth of information collected in SecureX. To connect Cyber Vision Center to SecureX, do the following:

- 1. In Cyber Vision Center, navigate to Admin > Integrations > CTR.
- 2. Click the **Configure** button.
  - a. From the **Platform** drop-down list, choose the **Threat Response** that is geographically (and presumably logically) closest to the Cyber Vision Center.
  - b. Click the Save button.

# Analysis

## Presets

Presets provide different views to look at the data captured by the Cyber Vision Sensor, and can be tailored to highlight specific components or activity to speed analysis. Some tips for using Presets:

Components-These are the unique devices seen on the network, and each contains specific details about vendor, device type, protocol, and so on. From the **Components** button on the Preset Dashboard, you can see a list of each component and by clicking one, more details about the component will show in a **Component** pane on the right. From that pane, click the **Technical Sheet** icon to view full details about the component.

Figure 4 Component List

| cisco. | CYBER VISION<br>Center |  |           |                                |             |                          | 4                       | Diplore • / CE | ELLS • / Component | list +   |             |                 |  | × 0.               |
|--------|------------------------|--|-----------|--------------------------------|-------------|--------------------------|-------------------------|----------------|--------------------|--|-------------|-----------------|--|--------------------|
|        |                        |  | Mar 29, 2 | 021 2:30:03 PM - Mar 29, 2021  | 2:30:33 PM  | (XUN (cose 00)           |                         |                |                    |  |             | <               | Rack   | ×                  |
|        | Reports                | occus o  | 5 Co      | mponents                       |             |                          |                         |                |                    |  |             |                 | CLX, C   1756-L75/BLOG   | 2 0                |
|        | Events                 | Mypreset   | 1/5       | Components selected Select a   | Il Componen | ts Cear selection        |                         |                |                    |  |             | 0               | P 3037.50.52<br>   |                    |
|        | Monitor                | Description:<br>All components and activities are listed in this   | 1         | Component : v                  | Group       | Rotativity :             | Last activity           | P: 1           | MAC : Y            | Tags   | T Flows Web | X Dec 9, 2020 s | 121121964 E Mar 28,202   | 20243 PM           |
|        | Search                 | preset. This preset should not be used and other<br>more well defined presets would be preferred for   |           |                                | 0.00        | restativity ;            | catacovity .            |                | 1 1000 1 1         |  | T FIDES TO  |                 | O Module , Controller ,  |                    |
|        | Admin                  | more accurate findings.<br>Active baseline: No active baseline   | 0         | □ 1756-EN2TR/8                 |             | Dec 9, 2020 12:11:21 PM  | Mar 29, 2021 2:32:44 PM | 10.17.10.58    | 00.1d.9cbbicBie7   | <ul> <li>No Module, Controller, Web Server,</li> <li>Rodrivel Automation</li> </ul>                | 220326      |                 | Plackwell Automation<br>Program Download . # Start CP  |                    |
|        |                        | Active Discovery: Disabled   |           | ■ 1756-EN2TIA                  | CELL,2      | Dec 15, 2020 3:42:16 PM  | Mar 29, 2021 2:32:44 PM | 10.17.30.70    | 00:00:bc:3b:55:6f  | ID Mobile ,  | 197595      |                 | Chestablished, @ReadVar, @<br>SCADA Station, @Database,  | WriteVar.<br>Ping. |
|        |                        | Criteria Selectal Relectal Defait  | 0         | COGOSSISERMA                   | CELL,2      | Dec 15, 2020 3:58:57 PM  | Mar 29, 2021 2:32:44 PM | 10.17.10.65    | 00:00:bccd:f7:6a   | <ul> <li>IO Module ,               Controller ,               Rodowell Automation      </li> </ul> | 32750       |                 | Broadcart,      Low Volume,      ARP,      CIP-IO,      EthernetiP     Ovation protocol (Nide) |                    |
|        |                        | Search orberta Q   | 0         | B 176P-L36ERMA                 | CELL,1      | Nov 17, 2020 10:42:47 AM | Mar 29, 2021 2:32:43 PM | 10.17.10.68    | 00:00:bcoe:11:17   | <ul> <li>IO Module ,               Controller ,               Kadovell Automation      </li> </ul> | 33031       | Properties V    | CUCCI 1756-L75/BLOGOG  |                    |
|        |                        | A NETWOORS   |           | CUX,C  1756-L75/8<br>LOG035575 | CELL,2      | Dec 9, 2020 12:11:21 PM  | Mar 29, 2021 2:32:43 PM | 10.17.10.52    | 00:00:00:20:21:27  |  | 178201      |                 | inversion 26,012<br>rodelinef: 1754-075/8 000003<br>erisi-rumber: 008a6d2a                     | 175                |
|        |                        | Click here to set outform or bena based on<br>your network configuration (pladdress<br>and VLAN ID). These fitters will be applied<br>to this Preset only. | 1         |                                |             |                          |                         |                |                    |  |             |                 | where CLX_C   1756-L7578 L0<br>2139-137-19752<br>NDTo-To-To-To-To-To-To-To-To-To-To-To-To-T    | 62/5575            |
|        |                        | B CONFONENTINGS  |           |                                |             |                          |                         |                |                    |  |             |                 | Nidel  |                    |
|        |                        | Components without tags  |           |                                |             |                          |                         |                |                    |  |             |                 |  |                    |
|        |                        | O Device - Level 0-1   |           |                                |             |                          |                         |                |                    |  |             |                 |  |                    |
|        |                        | Oevice - Level 2   |           |                                |             |                          |                         |                |                    |  |             |                 |  |                    |
|        |                        | O Device - Level 3-4   |           |                                |             |                          |                         |                |                    |  |             |                 | (3)  |                    |
|        |                        | O Network analysis   |           |                                |             |                          |                         |                |                    |  |             |                 |  |                    |
|        |                        | • O Software     • O System  |           |                                |             |                          |                         |                |                    |  |             | S 178           |  |                    |
|        |                        | * ACTIVITY TAGS  |           |                                |             |                          |                         |                |                    |  |             | Flov            |  |                    |
|        |                        | o capues A   |           |                                |             |                          |                         |                |                    |  |             |                 |  |                    |
|        |                        | Components without groups  |           |                                |             |                          |                         |                |                    |  |             | La s            |  |                    |
|        |                        | <  |           |                                |             |                          |                         |                |                    |  |             | Varias          | N00  | /199               |

Activities-These are the communication flows between components. From the Activities button on the Preset Dashboard, you can view these communications based on the time reference selected.

| cisco | CYBER VISION<br>Center |  |                         |                            |                          | 00                      | plore • / SE • / Activity/list •   |         |           |          | ⊭ @∽            |
|-------|------------------------|--|-------------------------|----------------------------|--------------------------|-------------------------|--|---------|-----------|----------|-----------------|
|       |                        |  | Mar 29, 2021 2:37:48 PM | Mar 29, 2021 2:38:48 PM (1 | min) •LIVE               |                         |  |         |           |          |                 |
|       | Reports                | OSE O  | 7 Activities            |                            |                          |                         |  |         |           |          | Export to CSV   |
| 8     | Events                 | My preset  |                         |                            |                          |                         |  |         |           |          | < 1 > 20/page ~ |
|       |                        | -  | Component :             | T Component o              |                          | Last activity 🖕         | Tags $\forall$   | Flows o | Packets o | Volume : | Events o        |
|       | Monitor<br>Search      | Active baseline: No active baseline<br>Active Discovery: Disabled  |                         | Hodicon M580               | Jan 20, 2021 4:55:29 PM  | Mar 29, 2021 2:38:44 PM | <ul> <li>Crestablished,</li> <li>ConvVolume, <ul> <li>ASP,</li> <li>CIP+IO, <ul> <li>CthemetP</li> </ul> </li> </ul></li></ul> | 5120    | 561461069 | 43.368   | 0               |
| ٥     | Admin                  | Criteria Selectali Rejectali Default   | Modicon M580            | Broadcast ff.ff.ff         | Jan 19, 2021 11:44:06 AM | Mar 29, 2021 2:38:43 PM | € Broadcast, € ARP   | 17      | 66176776  | 1.85 GB  | 0               |
|       |                        | Search criteria Q  | Modicon M580            | 0 10.1.3.85                | Mar 15, 2021 10:13:50 AM | Mar 29, 2021 2:38:43 PM | @ Ping   | 1       | 327573    | 25.6 MB  | 0               |
|       |                        | # NETWORKS   |                         | R BMEPS840405              | Jan 20, 2021 3:38:31 PM  | Mar 29, 2021 2:38:27 PM | <ul> <li>♥ Unestablished,</li> <li>♥ Host Confg.</li> <li>♥ Low Volume,</li> <li>♥ ASP,</li> <li>♥ OP-IO,</li> </ul>           | 555     | 69300947  | 11.3 GB  | 0               |
|       |                        | +<br>Click here to set custom criteria based on  |                         |                            |                          |                         | EthernetiP   |         |           |          |                 |
|       |                        | your network configuration (biaddress<br>and VLANIO). These fibers will be applied<br>to this Preset only. | BMECRA31210             | Modicon M580               | Jan 21, 2021 9:41:54 AM  | Mar 29, 2021 2:38:27 PM | <ul> <li>Insecure,</li></ul>   | 48063   | 594007    | 64,4 MB  | 0               |
|       |                        | © COMPONENT TAGS   |                         |                            |                          |                         | e tetp   |         |           |          |                 |
|       |                        |  | EMECRA31210             | Broadcast #1911#           | Jan 19, 2021 10:14:19 AM | Mar 29, 2021 2:38:24 PM | 🕈 Broadcast , 🥜 ARP  | 21      | 13934544  | 390 MB   | 0               |
|       |                        | Components without tags  | EMENOC0301              | Broadcast ff.ff.ff         | Jan 13, 2021 2:56:38 PM  | Mar 29, 2021 2:37:54 PM | 🕈 Broadcast , 📌 ARP  | 14      | 6784918   | 190 MB   | ۰.              |
|       |                        | O Device - Level 0-1   | 4                       |                            |                          |                         |  |         |           |          |                 |
|       |                        | O Device - Level 2   |                         |                            |                          |                         |  |         |           |          | < 1 > 20/page ~ |
|       |                        | <ul> <li>O Device - Level 3-4</li> </ul>   |                         |                            |                          |                         |  |         |           |          |                 |

Vulnerabilities—The Knowledge DB identifies known vulnerabilities for devices based on their hardware, firmware, protocol, and so on. From the Vulnerabilities button on the Preset Dashboard, you can view all identified vulnerabilities for the components included in that preset. In the table, click the link in the Vulnerability title column for a given vulnerability to view more details, including the associated Common Vulnerabilities and Exposures (CVE) identifier and potential fixes. Each vulnerability can be acknowledged by the analyst to remove it from the list.

E O

|   | CYBER VISION<br>Center |  | ⊘ Epplore ▼ / All data ▼ / W   | Inerabilities =  |  |  | F   |
|---|------------------------|--|--|--|--|--|---|
|   |                        | ⊐ ©0020  | Mar 29, 2021 2:40:39 FM - Mar 29, 2021 2:41:39 FM (1 min)  |  |  |  | <b>O</b> (1) S  |
| Ð | Reports                | All data*  | © 55 Vulnerabilities   |  |  |  |   |
| 3 | Events                 | Basics   | 10 most matched vulnerabilities  |  |  |  |   |
|   | Monitor                | Description<br>All components and activities are listed in this  | CVE-2019-12262 • VMMorks TCP1IP Stack(IPNET) Ungent/11 Vulnerabilities - Handling of<br>unsolicited Reverse ARP recting (Ladical Flaw)   | CVE-2019-12263 • VolWorks TCP1P Stack (IPNET)<br>State Confusion due to Race Condition                         | Urgent/11 Vulnerabilities  | s - TCP Urgent Point   |   |
|   | Search                 | preset. This preset should not be used and other<br>more well defined presets would be preferred for   | 8 affected components<br>CVE-2019-12261 • WWWorks TCP1P Stack (IPNET) Urgent/11 Wilnerabilities - TCP Urgent Pointer   | 8 affected components<br>CVE-2019-12257 • VWWorks TCP1P Stack (IPNET)  | Urgent/11 Vulnerabilities  | s - Heap Overflow in   |   |
|   | Admin                  | more accurate findings.<br>Active baseline: No active baseline   | State Confusion during connect() to remote host<br>8 affected components   | DHCP Offet IACK parsing inside lpdhcpc<br>8 affected components  |  |  | 13  |
|   |                        | Active Discovery: Disabled   | CVE-2019-12255 • VMVorks TCP1P Stack (IPNET) Utgent/11 VLinerabilities - TCP Utgent Pointer -<br>Olisada to Integer underflow<br>8 affected components   | CVE-2019-12258 • VWWorks TCP1IP Stack (IPNET)<br>connection via malformed TCP options<br>8 affected components | Urgent/11 Vulnerabilities  | - DoS of TCP   | Total vulnera<br>components   |
|   |                        | Criteria selecul Adecal Deale  | s unrected components<br>CVE-2017-4034 • Schneider Electric Modicon Modous Protocol - Multiple Authentication Bypess<br>Winerabilities   | CVE-2019-12265 • WWorks TCP11P Stack (IPNET)<br>Leak via IGMPv3 specific membership report                     | Urgent/11 Vulnerabilities  | s - IGMP Information   |   |
|   |                        | Search orberla Q.  | 6 affected components<br>CVE-2019-12264 • VMVorks TCP1IP Stack (IPNET) Urgent/11 Vulnerabilities - Logical Flaw in IPv4  | 7 affected components<br>CVE-2017-6032 • Schweider Electric Modicon Mod  | bus Protocol Multiple Aut  | theretication Bypass   |   |
|   |                        | 8 NETWORKS   | assignment by the lpdhop DHCP client<br>6 affected components  | Winerabilities<br>6 affected components  |  |  |   |
|   |                        | to this Preset only.   |  |  |  |  | 1 2 3 > 20/pap  |
|   |                        | A 114414 B 8144  | Vulnerability title 0  |  | T CVE :  | T CVSS score :   | Affected components   |
|   |                        | e contonentracs  | Vulnerability title :<br>WWorks TCP1P Stack (PNET) Urgent/11 Vulnerabilities - DoS of TCP connection via mailformed TCP options  |  | T CVE :<br>CVE-2019-12258  | τ CVSS score :<br>7.5 stat   | Affected components   |
|   |                        | Components without tags  |  |  |  |  |   |
|   |                        | Components without tags  O Device - Level 0-1  | WWorks TCP1P Study (PNET) Urgent/11 Winerabilities - DoS of TCP connection via mailformed TCP options  |  | CVE-2019-12258   | 7.5 s-m  | 🖻 8 components  |
|   |                        | Components without taps<br>• O Device - Level 0-1<br>• O Device - Level 2  | WWWs/is TCRIP Stack (PNET) Urgent/11 WinnedBillisis - DuS of TCP connection via malformed TCP options<br>WWWs/is TCRIP Stack (PNET) Urgent/11 WinnedBillisis - Heap Overflow in CHCP Offer/RCC paining inside lipehopc   |  | CVE-2019-12258<br>CVE-2019-12257   | 7.5 sm<br>8.8 sm   | B components     B components   |
|   |                        | Components without tags     O Device - Level 0-1     O Device - Level 2     O Device - Level 3-4   | WWWwis TCHP Stack (IPACT) UpperUTI WinerABINe - Out of TCP connection via mathemed TCP cotons<br>WWWwis TCHP Stack (IPACT) UpperUTI WinerABINes - Haup Overflow in CHCP Other ACC gaming initial polytop:<br>WWWwis TCHP Stack (IPACT) UpperUTI WinerABINes - Logical Flaws In IPA and generate by the bohop CHCP direct   |  | CVE-2019-12258<br>CVE-2019-12257<br>CVE-2019-12264   | 7.5 sm<br>8.8 sm<br>7.1 sm   | E Scomponents<br>E Scomponents<br>E Scomponents   |
|   |                        | Components without taps<br>Components without taps<br>Convice - Level 0-1<br>Convice - Level 0-1<br>Convice - Level 0-4<br>Convice - Level 0-4<br>Convice - Level 0-4  | WWorks TOTP Seads (INRT) Urgent 31 Winnvällites - Did at TCP connection via mattermed TOP aptions<br>WWorks TOTP Seads (INRT) Urgent 31 Winnvällites - Hand Conflict win SEX/C Direct AC gareign Initial Behavior<br>WWorks TOTP Seads (INRT) Urgent 21 Winnvällites - TCP Urgent Painter State Conflict Multiple Conflict Conflict<br>WWorks TCPP Seads (INRT) Urgent 31 Winnvällites - TCP Urgent Painter State Conflict Aufrig connect (11 minute had   |  | CVE-2019-12258<br>CVE-2019-12257<br>CVE-2019-12264<br>CVE-2019-12261   | 7.5 sm<br>8.8 sm<br>7.1 sm<br>9.8 sm   | Scomponents     Scomponents     Scomponents     Scomponents     Scomponents   |
|   |                        | Components without taps<br>Components without taps<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Comp | WWorks TCHP Seak (INRT) Upen: 11 Warvabilities - Uod at TCP connection via malformed TCP options<br>WWorks TCHP Seak (INRT) Upen: 11 Warvabilities - Hang Cherline via Cherl Cherlar Copanity Initial behave<br>WWorks TCHP Seak (INRT) Upen: 11 Warvabilities - TCP panel Thirde antigement by the bodyce Cherl Cherl<br>WWorks TCHP Seak (INRT) Upen: 11 Warvabilities - TCP upen Thirde antigement by the bodyce Cherl Cherl<br>WWorks TCHP Seak (INRT) Upen: 11 Warvabilities - TCP upen Thirde antigement by the topic Cherl<br>WWorks TCHP Seak (INRT) Upen: 11 Warvabilities - TCP Upen Thirde and the Internet Netter<br>WWorks TCHP Seak (INRT) Upen: 11 Warvabilities - TCP Upen Thirder - O leads to Integer underflow  |  | CVE-2019-12258<br>CVE-2019-12257<br>CVE-2019-12264<br>CVE-2019-12261<br>CVE-2019-12265   | 7.5 sm<br>8.8 sm<br>7.1 sm<br>9.8 sm<br>9.8 sm                                       | Bcomponents     Bcomponents     Bcomponents     Bcomponents     Bcomponents     Bcomponents   |
|   |                        | Components without taps<br>Components without taps<br>Convice - Level 0-1<br>Convice - Level 0-1<br>Convice - Level 0-4<br>Convice - Level 0-4<br>Convice - Level 0-4  | Websits TOTP Sock (PNT) Upger(11) WarnelBites - Dod of TCP convention via nationnel TCP loadine<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - India Annue Durffens (SOLP) Of the ACX particle fails before<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - India Tale India Annue PNT behaviore State Dubble CONV-Orient<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner Sock Orientia Ange on year behaviore State<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Websits TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Methods to lenger underface<br>Methods TOTP Sock (PNT) Upger(11) WarnelBites - TOT Upger Phiner - O loads to lenger underface<br>Methods to lenger underface<br>Methods TOTP Sock (PNT) Upger Phiner - D loads to lenger underface<br>Methods to lenger underface<br>Methods TOTP Sock (PNT) Upger Phiner - D loads to lenger underface<br>Methods to lenger und |  | CVE-2019-12258<br>CVE-2019-12257<br>CVE-2019-12264<br>CVE-2019-12261<br>CVE-2019-12265<br>CVE-2019-12255   | 75 sa<br>88 sa<br>7,1 sa<br>9,8 sa<br>9,8 sa<br>8,8 sa<br>8,1 sa                     | Components |
|   |                        | Components without tags<br>Components without tags<br>Components without tags<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Components<br>Com   | WWorks TOTP Seads (INRT) Urgent 31 Warnabilities - Did at TCP connection via mathemed TOP aptions<br>WWorks TOTP Seads (INRT) Urgent 31 Warnabilities - Hand Conflict win SEX/C Direct 20 Careling India behapic<br>WWorks TOTP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of CONFC Unit<br>WWorks TOTP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Conflict<br>WWorks TOTP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Conflict<br>WWorks TOTP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Conflict<br>WWorks TOTP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Conflict<br>WWorks TCPP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Sear Conflict<br>WWorks TCPP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Sear Conflict<br>WWorks TCPP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Sear Conflict<br>WWorks TCPP Seads (INRT) Urgent 31 Warnabilities - TCP Urgent Patient Sear Conflict Out of Searce ADP regists 2 Applied Taxe)   |  | CVE-2019-12250<br>CVE-2019-12257<br>CVE-2019-12257<br>CVE-2019-12261<br>CVE-2019-12255<br>CVE-2019-12263<br>CVE-2019-12263   | 75 sm<br>88 sm<br>7,1 sm<br>9,8 sm<br>9,8 sm<br>8,1 sm<br>9,8 sm                     | Bitomponents  |
|   |                        | Components without taps     Operior-sheet 05  | Websis CRIP Seak (INRT) Upen:11 Wervahlitis- Edd of TCP connection via mathemed TCP options Websis CRIP Seak (INRT) Upen:11 Wervahlitis- Haup Cweffer win CNRCP CRIP Seaf (InRt) Behavior Websis CRIP Seak (INRT) Upen:11 Wervahlitis- Logical Faise In He Analyment by the bohav CRIP Crient Websis CRIP Seak (INRT) Upen:11 Wervahlitis- TCP Upen Fahrer – O seak to Integre random beit Websis CRIP Seak (INRT) Upen:11 Wervahlitis- TCP Upen Fahrer – O seak to Integre random beit Websis CRIP Seak (INRT) Upen:11 Wervahlitis- TCP Upen Fahrer – O seak to Integre random beit Websis CRIP Seak (INRT) Upen:11 Wervahlitis- TCP Upen Fahrer – O seak to Integre random beit Websis CRIP Seak (INRT) Upen:11 Wervahlitis- TCP Upen Fahrer – O seak to Integre underfahre Websis CRIP Seak (INRT) Upen:11 Wervahlitis- TCP Upen Fahrer – O seak to Integre Fahrer – O seak to Integre TCP (Integre Fahrer – O seak to Integre Upen Fahrer – O seak to Integre TCP (Integre Fahrer – O seak to Integre Fahrer – O seak to Integre TCP (Integre Fahrer – O seak to Integre TCP (Integre Fahrer – O seak to Integre Fahr   |  | CVE-2019-12250<br>CVE-2019-12257<br>CVE-2019-12264<br>CVE-2019-12261<br>CVE-2019-12263<br>CVE-2019-12263<br>CVE-2019-12262   | 755a<br>885a<br>7,15a<br>985a<br>985a<br>8,15a<br>985a<br>535a                       | Bit components     Components     Components     Components   |
|   |                        | Components without tags<br>Components without tags<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>Constructions<br>C   | Websits TOTP Sock (INRT) (Symp121 Warrabilities - Dod of TCP convection via mathemed TOP aptives<br>Websits TOTP Sock (INRT) (Symp121 Warrabilities - Totp and the Sock Of the SOC gaving inside before<br>Websits TOTP Sock (INRT) (Symp121 Warrabilities - Totp and Toth A subjects the Totp Sock (INRT) (Symp121 Warrabilities - TotP Sock (INRT) (Symp211 Warrabilities - TotP   |  | CVE-2019-12256<br>CVE-2019-12257<br>CVE-2019-12257<br>CVE-2019-12261<br>CVE-2019-12261<br>CVE-2019-12263<br>CVE-2019-12262<br>CVE-2019-12265<br>CVE-2019-12265<br>CVE-2019-12265                   | 7550<br>8850<br>7150<br>9850<br>9850<br>8150<br>9850<br>5350<br>5350                 | Bit components     Bit components     Bit components     Bit components     Bit components     Bit components     Components     Components     Git components     Git components     Git components     Git components   |
|   |                        | Components without typ<br>Components without typ<br>Obvio: Low/2<br>Obvio: Low   | Websits TOTP Seads (INRT) Urgent 31 Warrabilities - Dod at TCP connection via mathemed TCP aptions Websits TOTP Seads (INRT) Urgent 31 Warrabilities - Hand Conflict win SEXPC DRELACC gaming helds before: Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Ange connect) to see more held Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Ange connect) to see more held Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Ange connect) to see more held Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Ange connect) to see more held Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Balance and the Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Balance and the Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Balance and the Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Urgent Printer Searc Conflict on Balance AUXP regists 34(p)AT Fault Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Dispet Printer Searc Conflict on Balance AUXP regists 34(p)AT Fault Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Dispet Printer Searc Conflict on Balance AUXP regists 34(p)AT Fault Websits TOTP Seads (INRT) Urgent 31 Warrabilities - TCP Dispet Printer Searc Conflict on Balance AUXP regists 34(p)AT Fault 30 Printer   |  | CVE-2019-12256<br>CVE-2019-12267<br>CVE-2019-12264<br>CVE-2019-12265<br>CVE-2019-12265<br>CVE-2019-12265<br>CVE-2019-12265<br>CVE-2019-12265<br>CVE-2019-12265<br>CVE-2019-12265<br>CVE-2019-12265 | 7550<br>8850<br>7160<br>9850<br>9850<br>8150<br>9850<br>5350<br>5350<br>5350<br>9850 | Boomponents     Boomponents     Boomponents     Boomponents     Boomponents     Boomponents     Components     Components     Components     Components     Somponents     Somponents     Somponents     Somponents   |
|   |                        | Components without tags<br>Components without tags<br>Obvio: Level 34<br>Obvio:  | Websits TOTP Sock (PNT) Upger(11) Wareholdes - Dod at TCP assession via matheme TCP basins<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - Hand Darfield in SOciO TOTAL/Capacity Initial Bohac<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - Spatial Parks<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Or Analish and region web to the CAPA<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Or Analish and region web to the<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Or Analish and the Sock Ordelion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Soc Ordelion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Soc Ordelion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Soc Ordelion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Soc Ordelion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Sock Ordenion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Sock Ordenion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Sock Ordenion<br>Websits TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Sock Ordenion<br>Sock TOTP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Sock Ordenion<br>Sock TotP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion<br>Sock TotP Sock (PNT) Upger(11) Wareholdes - TCP Upger Printer Sock Ordenion Anal to Sock Ordenion<br>Sock TotP Sock (PNT) Upger TOTP Upger Printer Sock Ordenion Anal to Sock Ordenion<br>Sock TotP Sock (PNT) Upger TOTP Upger Printer Sock Ordenion Anal TotP Sock                            |  | CVE-2019-12259<br>CVE-2019-12257<br>CVE-2019-12267<br>CVE-2019-12261<br>CVE-2019-12263<br>CVE-2019-12263<br>CVE-2019-12263<br>CVE-2019-12263<br>CVE-2019-12602<br>CVE-2017-6024<br>CVE-2017-6024   | 7550<br>8850<br>7150<br>9850<br>9850<br>8150<br>9850<br>5350<br>5350<br>9850<br>7550 | C Components C C Components C C Components C C C C C C C C C C C C C C C C C C C  |

#### Figure 6 Vulnerabilities

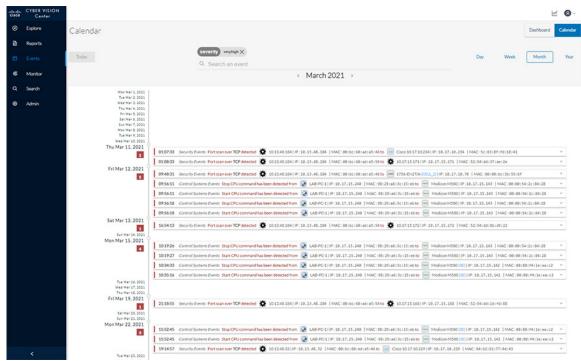
Baseline–If a baseline has been created for a Preset, it can highlight changes in activity or components beyond what is expected from the baseline. Click the link next to Active Baseline from the Preset side menu to view baseline updates. The baseline will show a map of the devices and their communications, highlighting new flows with a solid red line and any changed flows with a dashed line. From this view you can also click the New Activity or the Changed Activities button on the left to see details and acknowledge or report the activities. You can also see all baselines from the Monitor option on the main left menu.

#### Figure 7 Baseline Monitoring

| Explore | V L 0   | 7 Activi | ities                            | New Activity         |   |                          |                          |   |
|---------|---|----------|----------------------------------|----------------------|---|--------------------------|--------------------------|---|
| Reports | 10.20.8.10 Ø see on @ Explore                       | - 2 new  |                                  |                      |   |                          |                          | 10.1.3.85   |
| Events  | PLCBaseline   | STATUS   | Component 0                      | T Component 0        | Ψ | First activity 0         | Last activity 🖕          | IP 10.1.3.85<br>MAC 00:00:007ac01                                     |
|         | 2 new activities                                    | NEW      | 10.1.3.85                        | Siemens 10.20.8.10   |   | Oct 27, 2020 12:48:23 PM | Oct 27, 2020 12:48:27 PM | * Siemens 10.20.8.10  |
|         | Created with data seen between:                     | NEW      | 0 10.1.3.85                      | Siemens 10.20.8.10   |   | Oct 27, 2020 12:48:23 PM | Oct 27, 2020 12:48:27 PM | → SIEMENS IP. 10.20.8.10<br>MAC 28:63:36:04:45:92                     |
| Search  | Oct 27, 2020 12:43:00 PM - Oct 27, 2020 12:43:30 PM |          | Gisco 10.20.25.10                | Siemens 10.20.8.10   |   | Oct 27, 2020 10:45:10 AM | Oct 27, 2020 12:47:28 PM |   |
| Admin   | Last check: Oct 27, 2020 12:53:58 PM                | •        | Gisco 10.20.25.10                | - Siemens 10.20.8.10 |   | Oct 27, 2020 10:45:10 AM | Oct 27, 2020 12:47:28 PM | E Cast activity<br>Oct 27, 2020 12:48:23 PM C Cot 27, 2020 12:49:02 P |
| Admin   | Active criteria                                     |          | Cisco d2:1c:41                   | Siemens 10.20.8.10   |   | Oct 27, 2020 10:45:10 AM | Oct 27, 2020 12:47:28 PM | Taggi Si Investigate with flo   |
|         | No criteria   |          | Siemens 10.20.8.10               | Siemens a7:4c:cc     |   | Oct 27, 2020 10:45:10 AM | Oct 27, 2020 12:47:28 PM |   |
|         |   |          | Profinet DCP Multicast     0:0:0 | Siemens 10.20.8.10   |   | Oct 27, 2020 10:45:13 AM | Oct 27, 2020 12:47:26 PM | ✓ Acknowledge activity X Report activity                              |
|         |   | <        |                                  |                      |   |                          |                          | Show details  |

# **Reports and Events**

Cyber Vision Center provides various reports for the user to download in a Microsoft Excel or HTML format for offline analysis. Such reports can be useful for further investigation and remediation. Events in Cyber Vision Center highlight new activity, changes in the environment, and so on, and classify each by severity. Note that if activity from a baseline is reported, it will also show in the **Events** list.



#### Figure 8 Cisco Cyber Vision Events

## Packet Capture

Cyber Vision Center provides the capability to run a packet capture directly on a Cyber Vision Sensor for further analysis and troubleshooting. The data collected will be the raw traffic seen by the Sensor and is useful for understanding traffic flows and specific industrial traits and activities on devices. To run a packet capture on a sensor, do the following:

- 1. In Cyber Vision Center, navigate to Admin > Sensors > Capture.
- 2. In the Capture Actions column, click the Start Recording link for a given sensor.
- 3. When finished, click the Stop Recording link for the sensor.
- 4. Click the Download link to download the packet capture file.

# ISA 3000

# Installation

# Hardware Installation

For physical installation guidance, refer to https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/series.html#~tab-documents.

## Software Installation

Firepower Threat Defense (FTD) provides robust security, combining traditional access control with proprietary intrusion detection. To install FTD on the ISA 3000, refer to:

https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/series.html#~tab-documents.

# Connecting to the Network

The ISA 3000 has a dedicated management interface used for communications with the Firepower Management Center (FMC). This port should be connected to a switch that will be able to transmit the traffic through the network to the FMC. In addition, there are four data ports that can be used for all of the firewall transactions on network traffic; these interfaces are connected to the respective switches for which traffic inspection is required. For this design, two ISA 3000 ports were configured as a transparent inline set with the adjacent switch ports configured as trunk ports. This configuration allows multiple VLANs to traverse the firewall as a "bump in the wire". One interface is connected to the upstream or "outside" switch, and the other is connected to the downstream or "inside" switch. Note that inline sets require specific port pairings: port 1 and 2 or port 3 and 4.

On the adjacent switches to the ISA 3000, the ports should be configured like the following example:

```
interface GigabitEthernet1/0/1
switchport trunk allowed vlan 10,15,20,201
switchport mode trunk
```

# Configuration

## Connection to FMC

After FTD has been installed, run the following command to connect to the FMC:

>configure manager add FMC\_IP\_ADDRESS reg\_key

The registration key is a unique string that will be used on the FMC to add the FTD device. If the FTD device is behind a NAT boundary, do the following when configuring the manager:

>configure manager add FMC\_IP\_ADDRESS reg\_key NAT\_ID

In addition, NTP needs to be synced to the same time as FMC. To update the time on the FTD device, do the following from the CLI:

```
> expert
```

```
admin@FTD:~$ sudo ntpdate -u IP_address_of_timesource
admin@FTD:~$ sudo pmtool restartbyid ntpd
```

To make the ISA 3000 run in transparent mode, do the following:

>configure firewall transparent

## Device Configuration in FMC

To add the FTD device to the FMC, do the following:

- 1. In the FMC web UI, navigate to Devices > Device Management.
- 2. Click the Add button and choose Device.
  - a. In the Host field, enter the IP address of the FTD device.
  - b. In the Display Name field, enter a name for the FTD device.

- c. In the Registration Key field, enter the unique registration key used on the FTD device to connect to the FMC.
- d. Optionally, in the Group drop-down list choose a group for the FTD device.
- e. In the Access Control Policy drop-down list, choose the appropriate policy to apply to the device.
- f. Under Smart Licensing, check the appropriate license checkboxes for your needs.
- g. Optionally, in the Unique NAT ID field enter the NAT ID used on the FTD device.
- h. Click the Register button.

The FTD device will now show on the **Device Management** page. Click the **pencil** icon on the right to further configure the device:

- 1. Choose Interfaces from the top menu
- 2. Click the **pencil** icon to the right of each interface and do the following:
  - a. In the Name field, enter a name for the interface.
  - b. Check the Enabled check box.
  - c. Check the Propagate Security Group Tag check box.
  - d. Click the OK button.
- 3. Repeat Step 2 for each interface being used.
- 4. Choose Inline Sets from the top menu.
- 5. Click the Add Inline Set button.
  - a. In the Name field, enter a name for the Inline Set.
  - b. The Available Interfaces Pairs list will show the pair options to use in the Inline Set. Choose the necessary pair(s) and click the Add button to move it to the Selected Interface Pair list.
  - c. Choose the Advanced option on the top menu of the Add Inline Set dialog box.
  - d. Check the Propagate Link State check box.
  - e. Click the OK button.
- 6. Choose Interfaces from the top menu.
- 7. Click the pencil icon to the right of an interface used in an Inline Set.
  - a. From the Security Zone drop-down list, choose either inline\_inside or inline\_outside (depending on the interface being modified).
  - **b.** Click the **OK** button.
- 8. Repeat Step 7 for other interfaces being used in an Inline Set.
- 9. Click the Save button at the top right.

The configuration must be deployed to the FTD device by doing the following:

- 1. In FMC, navigate to Deploy > Deployment.
- 2. Check the check box for the FTD device.

3. Click the **Deploy** button.

#### **High Availability**

For a High Availability (HA) FTD deployment, do the following:

- 1. Register, configure, and deploy each FTD device in FMC as described above.
- 2. Connect the two devices using the same interface on each FTD device.
- 3. In FMC, navigate to Devices > Device Management.
- 4. Click the Add button and choose High Availability.
  - a. In the Name field, enter a name for the HA pair.
  - b. From the Device Type drop-down list, choose Firepower Threat Defense.
  - c. From the **Primary Peer** drop-down list, choose the FTD device that will be the primary member of the HA pair (typically the active node).
  - d. From the Secondary Peer drop-down list, choose the FTD device that will be the secondary member of the HA pair (typically the standby node).
  - e. Click the Continue button.
  - f. Under High Availability Link:
    - i. From the Interface drop-down list, choose the interface being used to connect the two FTD devices.
    - ii. In the Logical Name field, enter a name.
    - iii. In the **Primary IP** field, enter an IP address. This IP address must be in a unique subnet not being used elsewhere in the architecture.
    - iv. In the Secondary IP field, enter an IP address in the same subnet as the Primary IP address.
    - v. In the Subnet Mask field, enter a subnet mask for the two IP addresses.
  - g. Under State Link:, from the Interface drop-down list, choose Same as LAN Failover Link.
- 5. Click the Add button.

| Figure 9 | Hiah | Availability | / Pair | Configuration |
|----------|------|--------------|--------|---------------|
|          |      |              |        |               |

| High Availabi   | ility Link  | State Link     |                    |   |
|-----------------|---|----------------|--------------------|---|
| Interface:*     | GigabitEthernet1/4  | Interface:*    | GigabitEthernet1/4 | • |
| ogical Name:*   | HAlink  | Logical Name:* |                    |   |
| Primary IP:*    | 10.99.99.2  | Primary IP:*   |                    |   |
|                 | Use IPv6 Address  |                | Use IPv6 Address   |   |
| Secondary IP:*  | 10.99.99.3  | Secondary IP:* |                    |   |
| Subnet Mask:*   | 255.255.255.0   | Subnet Mask:*  |                    |   |
| Psec Encryp     | tion  |                |                    |   |
| Enabled         |   |                |                    |   |
| Key Generation: | Auto 👻  |                |                    |   |
| -               | ink is used to sync configuration, stat<br>Selected interface links and encryptio |                |                    |   |

The HA pair will be grouped together on the **Device Management** page, and configuration can be viewed or edited only for the active member. To change the roles of the FTD devices, click the **vertical ellipses** icon to the right of the HA pair and choose **Switch Active Peer**.

Figure 10 FMC Device List with High Availability Pair

|                    | irepower Management Center Ow                          | erview Analysis Policies           | Devices Ob | jects AMP   | Intelligence          | ٩                         | Deploy    | ¢ 🗘    | admin •      |
|--------------------|--|------------------------------------|------------|-------------|-----------------------|---------------------------|-----------|--------|--------------|
| View By :<br>Group |  |                                    |            |             |                       |                           |           | Deploy | ment History |
| All (3)            | Error (1)     Warning (0)     Offline (0)              | Normal (2)     Deployment P        | ending (1) | Upgrade (0) |                       |                           | Q, Search | Device | Add 🔻        |
| Collapse All       |  |                                    |            |             |                       |                           |           |        |              |
|                    | Name   | Model                              | Version    | Chassis     | Licenses              | Access Control Policy     |           |        |              |
|                    | ✓ Ungrouped (2)  |                                    |            |             |                       |                           |           |        |              |
|                    | ✓ HA<br>High Availability                              |                                    |            |             |                       |                           |           | /:     |              |
|                    | ISA3K-3(Primary, Standby)<br>10.17.99.6 - Transparent  | Cisco ISA-3000-4C-X Threat Defense | 6.7.0      | N/A         | Base, Threat (2 more) | cell_to_dist segment ISAs |           | :      |              |
|                    | ISA3k-4(Secondary, Active)<br>10.17.99.4 - Transparent | Cisco ISA-3000-4C-X Threat Defense | 6.7.0      | N/A         | Base, Threat (2 more) | cell_to_dist segment ISAs |           | :      |              |

# Software Upgrade

The FTD software can be upgraded through the FMC. For details on pushing an upgrade, see https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html.

# Firepower Management Center

# Installation

This design was validated with a virtual FMC. For details on installing the virtual FMC, see https://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/series.html.

# Configuration

# **Basic Configuration**

After deploying the virtual FMC, the IP address, administrator password, and the End User License Agreement (EULA), and so on need to be configured through the CLI to enable web interface connectivity. The initial log in to the FMC web interface will guide you through updating DNS as well as NTP. For details, refer to https://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/products-installation-guides-list.h tml.

Additional configurations can be adjusted in FMC by doing the following:

- 1. In FMC, navigate to System > Configuration.
- 2. Navigate to necessary options on the left menu bar to view specific settings.

# Licensing

The FMC is licensed through Cisco Smart Software Licensing and requires connectivity to communicate externally to Cisco.com. In addition, the FMC maintains licenses for the subsequent FTD devices it manages. To view or update licenses, do the following:

- 1. In FMC, navigate to System > Licenses > Smart Licenses.
- 2. The FMC will automatically synchronize to Cisco.com. Ensure your licenses are present in your Cisco Smart Software account. Click the **Synchronize** icon to refresh the license status.

## Network Objects

Network objects are IP addresses or groups of IP addresses to be used in other configurations such as access control rules. To add or update Network Objects, do the following:

- 1. In FMC, navigate to Objects > Object Management.
- 2. The Network page will be displayed. From the Add Network drop-down list, choose the Add Object option.
  - a. In the Name field, enter a name for the entity.
  - **b.** Optionally, provide a note in the **Description** field describing the object.
  - c. Under Network, click the radio button for your preferred input method. For example, click the Host radio button and enter the IP address of the entity in the field box.
  - d. Click the Save button.

If two or more IP addresses need to be grouped for use elsewhere in FMC, do the following:

1. From the Objects > Object Management > Network page, choose the Add Group option from the Add Network drop-down list.

- a. In the Name field, enter a name for the group.
- b. Optionally, provide a note in the **Description** field describing the group.
- c. From the Available Networks list, choose one or more options and click the Add button to move them to the Selected Networks list.
- d. Click the Save button.

#### Access Control Policy

An Access Control Policy consists of access control rules and other settings to determine the inspection behavior of the FTD device. For each FTD device, only one Access Control Policy can be applied at any given time. To create an Access Control Policy, do the following:

- 1. In FMC, navigate to **Policies > Access Control > Access Control**.
- 2. The Rules page will be displayed. Click the New Policy button.
  - a. In the Name field, enter a name for the policy.
  - **b.** In the **Description** field, enter a description for the policy.
  - c. From the Select Base Policy drop-down list, choose None.
  - **d.** Under **Default Action**, click the radio button of the desired option. This will be the action taken if traffic does not match any of the user-created rules.
  - Block all traffic-This option will drop traffic.
  - Intrusion Prevention—This option will pass traffic to be analyzed against the default Balanced Security and Connectivity Intrusion Policy.
  - Network Discovery

     This option will allow traffic to pass and populate the Host database for the IP addresses seen communicating.
  - e. Under Available Devices, choose the FTD device for which this policy will apply. Click the Add to Policy button.
  - f. Click the Save button.

To add Access Control Rules to the newly created Policy, do the following:

- 1. From the Access Control Policy page, click the pencil icon to the right of the Access Control Policy.
- 2. Click the Add Rule button.
  - a. In the Name field, enter a name for the rule.
  - b. Check the Enabled check box.
  - c. From the Action drop-down list, choose the desired segmentation action:
  - Allow-This option will pass the matched traffic for any further inspection (if any).
  - Trust-This option will pass the matched traffic without further inspection.
  - Monitor—This option will pass the traffic and automatically enable logging of the matched traffic.
  - **Block** This option will drop the traffic.
  - Block with reset This option will drop the traffic and reset the connection.

- Interactive Block-This option will allow the user to proceed or stop the connection.
- Interactive Block with reset—This option will block all non-web traffic and allow the user to proceed or stop the web connection.
- d. Optionally, enter a placement for the rule with the Insert drop-down list.
- e. Optionally, choose a time from the **Time Range** drop-down list or click the **plus** (+) icon to create a new time range.
- f. Choose the tabs needed to specify the rule criteria. Note that these are optional and are used to narrow the matching criteria and provide additional inspection. If nothing is selected, all traffic will match the rule and be subject to the Action specified:
- Zones-These are the "inside" or "outside" zones specified on the FTD device interfaces.
- Networks

   These are traditional IP addresses and subnets. Note that Network Objects or Groups can be used here.
- VLAN Tags-These are VLAN tag objects created by the user. Note these can only be used for inline sets.
- **Users**-If AD and FMC have been integrated, specific users can be added to the rule.
- Applications Applications, such as Microsoft PowerPoint, Common Industrial Protocol (CIP), Firefox, and so
  on can be specified.
- Ports-These are the Layer 4 ports used in the transaction.
- URLs-These are website addresses in the system or created by the user.
- SGT/ISE Attributes—If Cisco Identity Services Engine (ISE) and FMC have been integrated, specific security
  group tags (SGTs) can be added to the rule.
- Inspection

**1. Intrusion Policy**–An intrusion policy can be applied here. If the traffic matches the access control rule, it will then analyze the traffic against the specified intrusion policy and take action based on the intrusion policy settings.

**2. File Policy**–A file policy can be applied here. If the traffic matches the access control rule and there is a file included in the transaction, it will be inspected against the file policy and take action based on the file policy settings.

- Logging–This will ensure the connection event is logged for the matched traffic, which can provide useful
  information for analysis and troubleshooting. It is recommended to at least check the Log at Beginning of
  Connection check box if logging is desired.
- Comments-Provide notes about the rule.
- g. Click the Add button.
- **3.** Repeat Step 2 for any additional rules, being mindful of rule order which can impact action taken as well as processing. Refer to the Industrial Security Design Guide for best practices.
- 4. Click the Save button.

To apply the Access Control Policy, do the following:

- 1. In FMC, navigate to **Deploy > Deployment**.
- 2. Check the check box for the FTD device.
- 3. Click the **Deploy** button.

# Intrusion Policy

Intrusion policies make use of Cisco Talos intelligence and research to find abnormal or malicious activity in network traffic. There are thousands of Snort signatures to use for detection, many of which are grouped into categories for ease of configuration, such as OS-Windows or Protocol-SCADA. If an access rule has an intrusion policy applied, the traffic will first be matched against the traditional access control and if allowed, it will then be matched against the intrusion rules contained within the intrusion policy. To create an intrusion policy, do the following:

- 1. In FMC, navigate to Policies > Access Control > Intrusion.
- 2. Click the Create Policy button.
  - a. In the Name field, enter a name for the policy.
  - b. Optionally, in the Description field, provide detail about the policy.
  - c. Optionally, check the **Drop when Inline** check box. This means when the FTD device is deployed with an Inline set, the traffic can be dropped if successfully matched against an intrusion rule (with additional configuration).
  - d. In the **Base Policy** drop-down list, choose an option for the initial policy configuration:
  - **Balanced Security and Connectivity**-This option does not favor threat detection or speed, but rather has an average amount of intrusion rules applied so as to not overload processing.
  - Connectivity Over Security—Throughput and traffic connections are prioritized over inspection, therefore there
    are less intrusion rules applied.
  - Maximum Detection—This contains the most enabled intrusion rules of the default policies, making security the highest priority.
  - No Rules Active—This does not enable any intrusion rules and allows for the user to create a truly custom rule set.
  - Security Over Connectivity-Intrusion detection takes precedence over throughput and traffic connections.
  - e. Click the Create Policy button.

If any customizations to the policy are necessary, click the **pencil** icon to the right of the policy. To add additional rules to the policy, do the following:

- 1. On the Policy Information page, click the Manage Rules button.
- 2. Browse through the categories on the left menu to see available rules. In addition, rules can be searched for using the **Filter** field. For example, to find all CIP related rules, do the following:
  - a. In the **Rules** menu, navigate to **Category > protocol-scada**. The **Filter** field will now show: Category:"protocol-scada".
  - b. Add the following to the Filter field: CIP. The Filter field will now show: Category:"protocol-scada:"CIP. Press Enter.
- 3. Click the GID check box next to any desired rules and from the Rule State drop-down list, choose the necessary action:
  - Generate Events—If the traffic matches the intrusion rule, an event will show in the Intrusion Events. The traffic will not be dropped.
  - Drop and Generate Events—If the traffic matches the intrusion rule, an event will be created and the traffic will be dropped.
  - Disable-This is for any rule you do not wish the traffic to be inspected against.

- 4. After all rules have been added, click the Back link at the top of the Rules page.
- 5. From the **Policy Information** menu, click **Policy Layers**. The details of the default rules and any customizations are shown. When finished reviewing, click the **Back** link at the top of the **Policy Layers** page.
- 6. Click the Commit Changes button to save the policy.

The Intrusion Policy can now be added to an Access Control Policy and then deployed to the FTD device.

# File and Malware Policy

FTD can further inspect files if needed to prevent unwanted traversal through the network. If licensed for malware inspection, the Cisco Advanced Malware Protection (AMP) cloud is used to analyze files for malware. To create a File Policy, do the following:

- 1. In FMC, navigate to **Policies > Access Control > Malware & File**.
- 2. Click the New File Policy button.
  - a. In the Name field, enter a name for the policy.
  - b. Optionally, in the Description field, enter details about the policy.
  - c. Click the Save button.
  - d. Click the Add Rule link on the right.
    - i. From the **Application Protocol** drop-down list, choose the necessary protocol for file inspection. **Any** includes all protocols from the list.
    - ii. From the **Direction of Transfer** drop-down list, choose the file transfer direction to be inspected. **Any** includes both directions.
    - iii. From the **Action** drop-down list, choose the action to be taken by the FTD device upon a successful file match:
      - 1. Detect Files-This will allow the file to continue to transfer, and will generate an event for analysis.
      - 2. Block Files-This will stop the file from being transferred, and will generate an event for analysis.
      - 3. Malware Cloud Lookup-This will use AMP cloud for analysis and will allow the file to continue to transfer.
      - 4. **Block Malware**—The file will be analyzed against AMP cloud intelligence and blocked if matched. Options are displayed for tools to be used for the inspection. Please review FMC documentation for more information on these tools.
    - iv. From the File Type Categories and File Types lists, choose the necessary file types and click the Add button.
    - v. Click the Save button.
  - e. Repeat Step d for any additional rules.
  - f. Click the Save button.

The File Policy can now be added to an Access Control Policy and then deployed to the FTD device.

#### Preprocessors

FMC uses preprocessors to decode traffic before undergoing intrusion inspection, as some traffic may not be decipherable by the Snort engine. These preprocessors are configured as a Network Analysis Policy, and can be tailored to monitor specific traffic types, such as SCADA protocols. To create a custom Network Analysis Policy, do the following:

- 1. In FMC, navigate to **Policies > Access Control > Access Control**.
- 2. Click the Network Analysis Policy link.
- 3. Click the Create Policy button.
  - a. In the Name field, enter a name for the policy.
  - b. Optionally, in the Description field, enter details about the policy.
  - c. Check the Inline Mode check box if using an Inline Set on your FTD device.
  - d. From the Base Policy drop-down list, choose the necessary option:
  - Balanced Security and Connectivity—This option does not favor threat detection or speed, but maintains an average decoding process to not impact connectivity.
  - Connectivity Over Security
     Throughput and traffic connections are prioritized over traffic decoding.
  - Maximum Detection-All preprocessing resources are dedicated to traffic decoding.
  - Security Over Connectivity–Traffic decoding is prioritized over connectivity.
  - e. Click the Create and Edit Policy button.
  - f. From the Policy Information menu, choose Settings.
  - **g.** Click the **Enabled** radio button for each protocol to be included in preprocessing. In this validation, the SCADA Preprocessors were enabled in addition to the default Balanced Security and Connectivity base policy.
  - h. Click the Back link on the Settings page.
  - i. From the Policy Information menu, choose Settings > TCP Stream configuration.
    - i. In the **Perform Stream Reassembly on Both Ports** field, append the following ports for SCADA protocols: **502**, **20000**, **44818**.
  - j. Optionally, choose from the other various protocols in the **Policy Information** menu to review the preprocessor configurations. Click the **Back** link when finished.
  - k. Click the Commit Changes button.

## Network Discovery

Network Discovery allows you to specify which hosts on your network FMC should keep track of in the Network Map. To configure Network Discovery, do the following:

- 1. In FMC, navigate to **Policies > Access Control > Network Discovery**.
- 2. Click the Add Rule button.
  - a. Leave the Discover option selected in the drop-down list, as well as the Hosts check box checked.
  - **b.** Under the **Networks** tab, choose pertinent hosts or groups from the **Available Networks** list. Click the **Add** button to move them to the **Networks** list.

c. Click the Save button.

To view the hosts learned by FMC, navigate to Analysis > Hosts > Hosts.

## Hardware Bypass

The hardware bypass feature allows traffic to continue to flow in the event of a power interruption or reload of the ISA 3000. To configure hardware bypass, do the following:

1. In FMC, navigate to **Devices > FlexConfig**.

- 2. Click the New Policy button.
  - a. In the Name field, enter a name for the policy.
  - b. Optionally, in the **Description** field, enter details about the policy.
  - c. From the Available Devices list, choose the necessary FTD device(s) and click the Add to Policy button.
  - d. Click the Save button.
  - e. On the FlexConfig Policy Editor page, click the FlexConfig Object button.
    - i. In the Name field, enter a name for the object.
    - ii. In the **Description** field, enter details about the object.
    - iii. From the Deployment drop-down list, choose Everytime.
    - iv. From the Type drop-down list, choose Append.
    - v. In the blank text box, enter the command(s) to enable hardware bypass on the necessary ports:

hardware-bypass GigabitEthernet 1/1-1/2 hardware-bypass GigabitEthernet 1/3-1/4

- vi. Click the Save button.
- f. On the FlexConfig Policy Editor page, click the Save button.

Apply the hardware bypass configuration to the FTD device by doing the following:

- 1. In FMC, navigate to **Deploy > Deployment**.
- 2. Check the check box for the FTD device.
- 3. Click the **Deploy** button.

## Upgrade

For details on upgrading the FMC, see https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html.

## Integrations

#### SecureX and AMP

Cisco SecureX integrates many Cisco security products to provide a holistic view of network activity with a focus on threats. FTD sends connection, intrusion, and file event information to SecureX where it can be analyzed against other intelligence sources. To create a SecureX account, refer to

https://www.cisco.com/c/en/us/td/docs/security/securex/sign-on/securex-sign-on-guide.html. To connect FMC to SecureX, do the following:

- 1. In FMC, navigate to **System > Integration**.
- 2. Under the Cloud Services tab, in the Cisco Cloud Region pane, choose the closest cloud destination from the Region drop-down list. Click the Save button.
- 3. In the **Cisco Cloud Event Configuration** pane, click the slider to enable FMC to send events to the cloud. Click the individual event sliders to enable or disable those events in the export. Click the **Save** button.

Cisco Advanced Malware Protection (AMP) provides extensive malware analysis and blocking across multiple systems, including FTD. FMC connects to the AMP cloud to check network traffic against up-to-date threat intelligence. To connect FMC to the AMP cloud, do the following:

- 1. In FMC, navigate to AMP > AMP Management.
- 2. Click the **pencil** icon to update the existing cloud connection.
  - a. From the Cloud Name drop-down list, choose the option that is geographically closest to the FMC.
  - b. Click the Save button.

## Syslog

FMC can export FTD syslog messages for further analysis and troubleshooting. The syslog messages are configurable based on severity, and specific syslog messages can be customized. To enable a basic syslog export to an external server, do the following:

- 1. In FMC, navigate to Devices > Platform Settings.
- 2. Click the New Policy button.
  - a. In the Name field, enter a name for the policy
  - b. Optionally, in the **Description** field, enter details about the policy.
  - c. In the Available Devices list, choose one or more FTD devices and click the Add to Policy button.
  - d. Click the Save button.
  - e. On the Platform Settings Editor page, choose Syslog from the left menu.
    - i. On the Logging Setup tab, under Basic Logging Settings, check the Enable Logging check box.
    - ii. On the Logging Destinations tab, click the Add button.
      - 1. From the Logging Destination drop-down list, choose Syslog Servers.
      - 2. From the **Event Class** drop-down lists, choose **Filter on Severity** and **Alerts**, respectively. Note the severity order:
      - a. Emergencies (syslog messages cannot be generated for this severity on FTD)

- b. Alert
- c. Critical
- d. Error
- e. Warning
- f. Notification
- g. Informational
- h. Debugging
- 3. Click the **OK** button.
- iii. On the **Syslog Settings** tab, leave the defaults selected in the drop-down lists and check the **Enable Timestamp on Syslog Messages** and **Enable Syslog Device ID** check boxes.
- iv. On the Syslog Servers tab, click the Add button.
  - 1. In the **IP Address** drop-down list, choose a syslog destination from the list of Network Objects. Alternatively, click the **plus** (+) icon to add a Network Object if needed.
- 2. For **Protocol**, click the **UDP** radio button.
- 3. In the Port field, enter 514.
- 4. Under Reachable By, click the Device Management Interface radio button.
- 5. Click the **OK** button.
- f. On the Platform Settings Editor page, click the Save button.

Deploy the configuration to the FTD device.

# Analysis

## Connection Events

Connection events contain all of the traditional firewall activity of allowed or blocked connections. In addition to providing typical source and destination IP addresses and ports, the Connection Events table shows the firewall action taken, application protocol, URL (if available), and other details for investigation. In FMC, navigate to **Analysis > Connections > Events** to view connection events and click the **Edit Search** link to filter the results shown in the table. In addition, the search timeframe can be adjusted by clicking the date and time link at the top of the **Connection Events** page.

## Intrusion Events

Intrusion events show the activity that has successfully matched the Snort signatures included in intrusion policies applied to the access control rules. For each intrusion event, the corresponding access control details are provided, such as source and destination IP address, ports, and the access control rule that handled the traffic flow. In FMC, navigate to **Analysis > Intrusions > Events** to view intrusion events, and click the **Edit Search** link to filter the results shown in the table. Click the **Table View of Events** tab at the top of the table for a detailed view of each event.

## Hosts

Each IP address detected by the FTD device is logged and FMC displays details about the entity, including any attributes sent from Cyber Vision and indicators of compromise (IoCs). In FMC, navigate to **Analysis > Hosts > Network Map** and choose an IP address from the **Hosts** menu on the left to view the details.

#### Figure 11 FMC Host Analysis

| Hosts Network Devices Mobile   | Devices Indicatio   | ons of Compromise  | Application Proto          | cols Vulnerabilities Host Attributes                |                     |                             |        |                             |           |
|--|---|--|----------------------------|---|---------------------|-----------------------------|--------|-----------------------------|-----------|
| Filter by IP and MAC addresses X   | Host Profile  |  |                            |   |                     |                             | Scan   | Host Generate White List    | t Profile |
| Unique hosts: 1720   | IP Addr   | esses 10.17.15.143   | 3                          |   |                     |                             |        |                             |           |
|  | NetBIOS   |  |                            |   |                     |                             |        |                             |           |
| sts [IPv4] (1700)  |   | Hops) ISA3k-1 (0)  |                            |   |                     |                             |        |                             |           |
| 0 (11)   |   | (TTL) 00:00:54:2C  | .84:28 (Schneider Ele      | ctric) (64)   |                     |                             |        |                             |           |
| 3 (37)   |   | Type Host<br>Seen 2021-03-30   | 10-20-05                   |   |                     |                             |        |                             |           |
| 8 (57)   | Curren  |  | 19.20.05                   |   |                     |                             |        |                             |           |
| 10 (128)   |   |  | storer   Connection        | Events   Intrusion Events   File Events   M         | Malware Events      |                             |        |                             |           |
| ▶ 10.1 (8)   |   |  |                            |   |                     |                             |        |                             |           |
| ▶ 10.2 (2)   | <ul> <li>Indication:</li> </ul>                                 | s of Compromise  | + (1)                      |   |                     |                             | /      | Edit Rule States 🗑 Mark All | l Reso    |
| • 10.5 (1)   |   |  |                            |   |                     |                             |        | -                           |           |
| 10.10 (2)  | Category  | Event Type   |                            | Description   | First Seen          | Last Seen                   |        |                             |           |
| • 10.13 (18)   | Impact 2 Attack   | Impact 2 Intrusion Ev  | vent - attempted-admi      | in The host was attacked and is potentially vulnera | ble • 2021-03-08 14 | 13:19 o 2021-03-15 10:18:21 | ŵ.     |                             |           |
| 10.17 (77)   | <ul> <li>Operating</li> </ul>                                   | System   |                            |   |                     |                             |        | / Edit Operatin             | na Sva    |
| ▶ 10.17.10 (16)  |   | -,   |                            |   |                     |                             |        |                             |           |
| ► 10.17.11 (3)   | Vendor  |  |                            | Product   | Versio              | in So                       | urce   |                             |           |
| 10.17.15 (34)  | unknown   |  |                            | unknown   | unknow              | wn Fire                     | epower |                             |           |
| 10.17.15.1   |   |  |                            |   |                     |                             |        |                             |           |
| 10.17.15.33  | Users (no us  | ser history availal  | ble)                       |   |                     |                             |        |                             |           |
| 10.17.15.34  |   |  |                            |   |                     |                             |        |                             |           |
| 10.17.15.35  | <ul> <li>Attributes</li> </ul>                                  |  |                            |   |                     |                             |        | / Edit                      | Attrib    |
|  |   |  |                            |   |                     |                             |        |                             |           |
| 10.17.15.44  |   | ticality None  |                            | 0-1-10  |                     |                             |        |                             |           |
|  |   |  |                            |   |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80   |   | issetid b67e3e42-b   |                            | 2000000   |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124   | a<br>assetipAd  | ddress 10.17.15.14   | 3                          | 23030030  |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124<br>10.17.15.128   | a<br>asset0pAr<br>assetMacAr                                    |  | 3<br>84:28                 | 23035030  |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124<br>10.17.15.128<br>10.17.15.129   | a<br>asset0pAd<br>assetMacAd<br>asset                           | ddress 10.17.15.14<br>ddress 00:00:54:2c   | 3<br>:84:28<br>0.17.15.143 | /20030600   |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124<br>10.17.15.128<br>10.17.15.129<br>10.17.15.137   | a<br>asset0pAd<br>assetMacAd<br>asset                           | ddress 10.17.15.14<br>ddress 00:00:54:2c<br>tName Schneider 10                         | 3<br>:84:28<br>0.17.15.143 | 20030030  |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124<br>10.17.15.128<br>10.17.15.129<br>10.17.15.137<br>10.17.15.143                                 | a<br>asset0pAd<br>assetMacAd<br>asset                           | ddress 10.17.15.14<br>ddress 00.00:54:2c;<br>tName Schneider 10<br>/endor Schneider Ei | 3<br>:84:28<br>0.17.15.143 | 20030040  |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124<br>10.17.15.128<br>10.17.15.129<br>10.17.15.137<br>10.17.15.143<br>10.17.15.149                 | a<br>assetlpAc<br>assetMacAc<br>asset<br>assetv<br>• Host Proto | ddress 10.17.15.14<br>ddress 00.00:54:2c;<br>tName Schneider 10<br>/endor Schneider Ei | 3<br>:84:28<br>0.17.15.143 | /20030640   |                     |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124<br>10.17.15.128<br>10.17.15.129<br>10.17.15.137<br>10.17.15.149<br>10.17.15.149<br>10.17.15.150 | a<br>assettpAc<br>asset<br>asset<br>asset<br>• Host Proto       | ddress 10.17.15.14<br>ddress 00.00:54:2c;<br>tName Schneider 10<br>/endor Schneider Ei | 3<br>:84:28<br>0.17.15.143 | 20030640  | Layer               |                             |        |                             |           |
| 10.17.15.44<br>10.17.15.80<br>10.17.15.124<br>10.17.15.128<br>10.17.15.129<br>10.17.15.137<br><b>10.17.15.149</b>                          | a<br>assetlpAc<br>assetMacAc<br>asset<br>assetv<br>• Host Proto | ddress 10.17.15.14<br>ddress 00.00:54:2c;<br>tName Schneider 10<br>/endor Schneider Ei | 3<br>:84:28<br>0.17.15.143 | 20030640  | Layer<br>Transport  |                             |        |                             | i         |

# File Events

Much like connection and intrusion events, if a malware and file policy has been created, FMC shows an events list for activity matching the policy. In FMC, navigate to **Analysis > Files > Malware Events** or **Analysis > Files > Fi** 

|  | ver Management Ce<br>Fles / Network File Trajectory                     | Nter Overview Anal  | ysis Policies Devices                        | Objects AMP Inte | ligence                          |  |   |                                  | 8   | Q. Deploy    | ¢ 0        | • •   |
|--|---|---|--|------------------|----------------------------------|--|---|----------------------------------|---|--------------|------------|-------|
| letwork File Traje   | ctory for 275a021bf65   | 1fdor   |  |                  |                                  |  |   |                                  |   |              |            |       |
| lle SHA256   | 275a021b_16511d0f + (   |   |  |                  | First Seen 2021                  | 1-02-10 10:52:21                         | on 🗱 10.20.8.171                                |                                  |   |              |            |       |
| le Names   | eicar.txt , eicarnew.rtf , eica   | mew.txt_eicamew1.rtf  |  |                  | Last Seen 2021                   | 1-03-09 12.49:09                         | on 10.13.48.172 by                              | Not Found                        |   |              |            |       |
| le Size (KB)   | 0   |   |  |                  | Event Count 96                   |  |   |                                  |   |              |            |       |
| le Type  | ECAR  |   |  |                  | Seen On 2 hor                    | osts                                     |   |                                  |   |              |            |       |
| le Category  | Executables   |   |  |                  | Seen On Breakdown 2 ser          | nders 0 receive                          | rs  |                                  |   |              |            |       |
| urrent Disposition   | O Malware /   |   |  |                  |                                  |  |   |                                  |   |              |            |       |
| hreat Score  | None  |   |  |                  |                                  |  |   |                                  |   |              |            |       |
| Antection Name   | EICAR   |   |  |                  |                                  |  |   |                                  |   |              |            |       |
| rajectory  | Feb 10<br>10:52   | Feb 11<br>1.23 10.09  | 10.10  |                  | 0.11 10.16                       |  |   |                                  | 10-27                                     |              |            | 10.28 |
| 0.20.8.171<br>0.13.48.172  | <u>Q</u> Q Q  | <u>0 0 0 0</u>  |  | <u> </u>         |                                  | <u>0</u> 0                               | 0 0 0 0   | 2 2 9                            |   | <u>0</u> 0   | <u>Q</u> Q | 0     |
| Events O Tran<br>Dispositions O Units  | nsfer <u></u> Block ③ Cr<br>nown 🔆 Malware 🔘 Cr                         | ate  Move Move Decute an Custom Custom                                  |  | Quarantine       |                                  |  |   |                                  |   |              |            |       |
| vents  |   |   |  |                  |                                  |  |   |                                  |   |              |            |       |
|  | Event Type  | Sending IP  | Receiving IP                                 | User             | File Name                        | Disposition                              | Action  | Protocol                         | Client                                    | Web Applicat | io De      |       |
| Time   |   | or and a  |  |                  |                                  | 0.00000000                               |   |                                  |   |              |            |       |
| Time<br>2021-02-10 10:52   |   | 10.20.8.171   | 10.13.48.172                                 |                  | eicar.txt                        | Malware                                  | Malware Block                                   | FTP Data                         | FTP Data cl                               |              |            |       |
|  | 21 Transfer   | 1   | 10.13.48.172                                 |                  | eicar.txt<br>eicar.txt           |  | Malware Block<br>Malware Block                  | FTP Data                         | FTP Data cl                               |              |            |       |
| 2021-02-10 10:52   | 21 Transfer<br>23 Transfer  | 10.20.8.171   |  |                  |                                  | Malware                                  |   |                                  |   |              |            |       |
| 2021-02-10 10.52<br>2021-02-10 10.52<br>2021-02-10 10.52                     | 21 Transfer<br>23 Transfer<br>24 Transfer                               | 10.20.8.171<br>10.20.8.171  | 10.13.48.172                                 |                  | eicar.txt                        | Malware<br>Malware                       | Malware Block                                   | FTP Data                         | FTP Data cl                               |              |            |       |
| 2021-02-10 10.52<br>2021-02-10 10.52<br>2021-02-10 10.52<br>2021-02-10 11.52 | 21 Transfer<br>23 Transfer<br>24 Transfer<br>54 Transfer                | 10.20.8.171<br>10.20.8.171<br>10.20.8.171                               | 10.13.48.172<br>10.13.48.172                 |                  | eicartut<br>eicartut             | Malware<br>Malware<br>Malware            | Malware Block<br>Malware Block                  | FTP Data                         | FTP Data cl                               |              |            |       |
| 2021-02-10 10.52   | 21 Transfer<br>23 Transfer<br>24 Transfer<br>54 Transfer<br>57 Transfer | 10.20.8.171<br>10.20.8.171<br>10.20.8.171<br>10.20.8.171<br>10.20.8.171 | 10.13.48.172<br>10.13.48.172<br>10.13.48.172 |                  | eicartot<br>eicartot<br>eicartot | Malware<br>Malware<br>Malware<br>Malware | Malware Block<br>Malware Block<br>Malware Block | FTP Data<br>FTP Data<br>FTP Data | FTP Data cl<br>FTP Data cl<br>FTP Data cl |              |            |       |

#### Figure 12 FMC File Trajectory Analysis

#### Troubleshooting

## SecureX

Cisco SecureX contains a wealth of information correlated for numerous sources to aid detection and analysis. After integrating FMC with SecureX, the SecureX dashboard will display events and metrics from FMC. Events can be reviewed and escalated as incidents.

# Troubleshooting

# Cyber Vision Network Sensor Placement in the Network

Providing the correct ERSPAN source and choosing an appropriate point in the traffic path for data ingestion is key for the Cyber Vision Sensor to provide needed visibility. For example, in ring topologies with several switches and end devices distributed around the ring, there is potential for missed traffic if the end device data does not flow through the switch with the Cyber Vision Sensor. Further, resiliency mechanisms such as the REP alternate port can change the traffic path and potentially bypass the switch with the Cyber Vision Sensor. Keeping these things in mind can help if expected device communications are not ingested by the Cyber Vision Sensor.

# FTD CLI

The FTD CLI has many useful commands for checking statistics and other real-time configurations and metrics. The following commands can help in troubleshooting performance as well as Snort processing.

The **show snort statistics** command gives real-time counts of the Snort engine performance, such as packets that are passed or packets that are dropped because Snort is busy or down.

#### > show snort statistics

| Packet Counters:                      |          |
|---------------------------------------|----------|
| Passed Packets                        | 16336627 |
| Blocked Packets                       | 0        |
| Injected Packets                      | 0        |
| Packets bypassed (Snort Down)         | 0        |
| Packets bypassed (Snort Busy)         | 0        |
| Flow Counters:                        |          |
| Fast-Forwarded Flows                  | 188      |
| Blacklisted Flows                     | 0        |
| Miscellaneous Counters:               |          |
| Start-of-Flow events                  | 0        |
| End-of-Flow events                    | 225      |
| Denied flow events                    | 0        |
| Frames forwarded to Snort before drop | 0        |
| Inject packets dropped                | 0        |

The **system support trace** command allows the user to specify traffic for debugging that is output to the CLI as Snort engine processes the traffic.

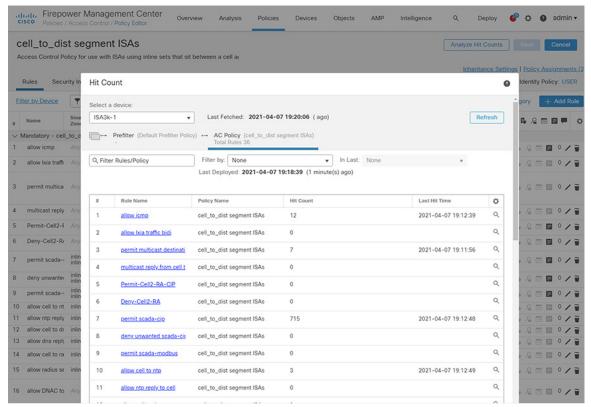
#### > system support trace

Enable firewall-engine-debug too? [n]: **y** Please specify an IP protocol: **tcp** Please specify a client IP address: Please specify a client port: Please specify a server IP address: Please specify a server port: Monitoring packet tracer and firewall debug messages Troubleshooting

# FMC Access Control Logging and Hit Count

Enabling logging for each access control rule provides a record of each allowed or blocked communication that the FTD devices processes and is useful for tuning access control rules. See Access Control Policy for details on configuring logging. In addition, the **Analyze Hit Counts** button on the access control **Policy Editor** page can help determine the efficacy of access control rules.





# **FMC Health Monitor**

The FMC has system monitoring capabilities for itself as well as the FTD devices it manages. Resources such as CPU, memory, and disk are monitored for utilization over time and FMC will alarm when usage has exceeded a healthy threshold. In FMC, navigate to **System > Health > Monitor** and choose the necessary device to view the health statistics.

#### Appendix

|             | Health: ISA3k-1 O Critical  | Last 1 hour   |
|-------------|---|---|
| ගි Home     | Overview Alerts: 1 A 0 0 25 Interfaces Connections Snort                | <u></u>   |
| • FMC       | CPU for 5 Alerts  |   |
| Devices (2) | Data Diany © Snort Identity Memory Usage System Apr 17.3 %              | Memory Data Plane Avg 45.4 % Snort Avg 31.7 % System Avg 59.6 %         |
| ~ HA        | 1 core<br>0 Local Malware Analysis                                      | 3.0508 45.4% - 45.5% 3.8108 31.7% - 31.7% 7.7608 58.7% - 61.5%          |
| ISA3K-3     | 100 Cluster/Failover Status Critical                                    | 100   |
| ISA3k-4     | 80 Click to view more details Warning                                   | 80  |
|             | 60  | 60  |
| ISA3k-1     |   | 40  |
|             |   | ~   |
|             | » ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~                                  | 20  |
|             | 0.0   | 0.0   |
|             | 14.20 14.25 14.30 14.35 14.40 14.45 14.50 14.55 15.00 15.05 15.10 15.15 | 14/20 14/25 14/30 14/35 14/40 14/45 14/50 14/55 15/00 15/05 15/10 15/15 |
|             | Throughput Avg - All Interfaces V                                       | Connection Statistics   |
|             | Input Date Avg 2.03Mops Output Date Avg 2.03Mops                        | Connections Avg 258<br>249 - 264 NAT Translations Avg 0<br>0 - 0        |
|             | 2.01Vbps - 2.08Vbps   | 300   |
|             | 8<br>2.3M   | ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~                                 |
|             | and the   | 200   |
|             | 1.5M  |   |
|             |   | 100   |
|             | 761.3X  |   |
|             |   | 0.0   |
|             |   | 14.20 14.25 14.30 14.35 14.40 14.45 14.50 14.55 15.00 15.05 15.10 15.15 |
|             | 1420 1425 1430 1435 1440 1445 1450 1455 1500 1505 1510 1515             | 1440 1440 1400 1400 1400 1400 1400 1400                                 |
|             | Disk Usage  | Critical Processes  |
|             | Entire Disk Critical Partitions   | AMP Java Data Plane SF Data Strunnel Snort01 SSE                        |
|             |   |   |

#### Figure 14 Health Monitoring

# Appendix

# Cisco Catalyst IE 3400 and IE 3300 Configuration Preparation for the Cyber Vision Sensor

# **ERSPAN**

The Encapsulated Remote Switched Port Analyzer (ERSPAN) feature in Cisco IOS sends data to the Cisco Cyber Vision Sensor application within the switch. ERSPAN creates copy of specified source traffic from a port or VLAN and sends it to an IP address, making use of generic routing encapsulation (GRE) allowing it to traverse to a remote destination across the Layer 3 network. The Cisco Cyber Vision Sensor interface that captures traffic is given an IP address in order to receive the data sent from the ERSPAN instance on the switch. To configure the ERSPAN on the switch, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#vlan destination_vlan_#
Switch(config-vlan)#remote-span
Switch(config-vlan)#exit
Switch(config)#monitor session 1 source {vlan vlan_# | interface int_#}
Switch(config)#monitor session 1 destination remote vlan destination_vlan_#
Switch(config)#monitor session 1 destination format-erspan IP_address
Switch(config)#end
```

#### **IOx**

The IE 3400 and IE 3300 switches require a 4GB SD card to be used for IOx applications. To format the SD card, enter the following command in enable mode:

#### Appendix

#### Switch#format sdflash: ext4

To enable IOx, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#iox
Switch(config)#ip http server
Switch(config)#ip http secure-server
Switch(config)#end
```

# Port Configuration

The Cisco Cyber Vision Sensor application communicates over IP to the Cisco Cyber Vision Center, therefore at least one interface (SVI or physical) must be configured with an IP address that is able to communicate through the network to the Cisco Cyber Vision Center. A VLAN interface was used in this implementation:

```
IE3400-3#sho run int vlan 15
!
interface Vlan15
ip address 10.17.15.157 255.255.255.0
```

In addition, the AppGigabitEthernet interface must be configured as a trunk to transfer data to and from the Cisco Cyber Vision Sensor application:

```
Switch#conf t
Switch(config)#interface AppGigabitEthernet 1/1
Switch(config)#switchport mode trunk
Switch(config)#end
```

The Cisco IOS XE image for the IE 3400 can also run on the SD card alongside the Cyber Vision IOx application. For this configuration, do the following:

```
Switch# format sdflash: ext4
Switch# partition sdflash: iox 72
```

The argument 72 in the **partition** command is the storage percentage allocated to the IOx partition, and can be adjusted to suit your needs, however the Cyber Vision Sensor requires at least 2048 MB. The switch will automatically reload after running the **partition** command. After the switch has reloaded, the boot variable can be set to the image stored in SDFLASH and IOx can be activated for the Cyber Vision Sensor installation.

# Cisco Catalyst 9300 Configuration Preparation for the Cyber Vision Sensor

# **ERSPAN**

As with the IE 3400 and IE3000 switches, the Cisco Catalyst 9300 switch uses ERSPAN to copy traffic to the Cisco Cyber Vision Sensor application. To configure the ERSPAN on the switch, enter the following commands in enable mode:

```
Switch#conf t
Switch(config)#monitor session 1 type erspan-source
Switch(config-mon-erspan-src)#source {interface int_#_or_list | vlan vlan_#_or_list}
Switch(config-mon-erspan-src-dst)#erspan-id 2
Switch(config-mon-erspan-src-dst)#mtu 9000
Switch(config-mon-erspan-src-dst)#ip address IP_address
Switch(config-mon-erspan-src-dst)#origin ip address IP_address
Switch(config-mon-erspan-src-dst)#end
```

#### Appendix

# **IOx**

The Cisco Catalyst 9300 switch requires a Solid State Drive (SSD) for IOx applications. For more information about installing the SSD, see:

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/hardware/install/b\_c9300\_hig/b\_c9300\_hig\_chap ter\_01010.html.

If the Cisco Catalyst 9300 is in a StackWise-480 configuration, the switch with the SSD must be in the active role. To format the SSD, enter the following command in enable mode:

Switch#format usbflash1: ext4

To enable IOx, enter the following commands in enable mode:

Switch#conf t
Switch(config)#iox
Switch(config)#ip http server
Switch(config)#ip http secure-server
Switch(config)#end

# Port Configuration

The Cisco Cyber Vision Sensor application communicates over IP to the Cisco Cyber Vision Center, therefore at least one interface (SVI or physical) must be configured with an IP address that is able to communicate through the network to the Cisco Cyber Vision Center. A VLAN interface was used in this implementation:

```
Cat9300#sho run int vlan 15
!
interface Vlan15
ip address 10.17.15.1 255.255.255.0
```