Splunk OT Security Solution Technical Guide and Documentation

Version 2.0.1 - March 4, 2021

Table of Contents

Section 1: Introduction

Splunk for OT Security enables organizations that operate assets, networks, and facilities across both carpeted (IT) and concrete (OT) environments to better apply the globally proven SIEM, Splunk Enterprise Security, to improve threat detection, incident investigation, and response. The Splunk for OT Security add-on expands the capabilities of Splunk's platform to monitor for threats and attacks, compliance, incident investigation, forensics, and incident response across the broad spectrum of assets and topologies - from email servers to PLCs - that define modern manufacturing, energy, and public sector organizations.

The solution, comprised of an app and related documentation, provides the following features:

1. **Expanded Asset Framework and Asset Center:** Ability to capture, store and analyze additional asset attributes including logical location, asset criticality, asset types and classifications, exposure levels, safety indicators, asset status and operating zone data alongside traditional IT asset elements, including IP addresses, operating system versions, Media Access Control (MAC) addresses, protocols, patch-level information, and firmware versions.
2. **Integration with leading OT Asset Inventory systems:** Ingest asset inventory, vulnerabilities, and 3rd party generated notables from leading OT-ready systems including Armis, Langner OTBase, ForeScout SilentDefense, Tenable, Nozomi, Dragos, Claroty, IBM Maximo and ServiceNow.
3. **Integration to NIST National Vulnerability Database (NVD):** Ingest and map tens of thousands of documented vulnerabilities (CVEs) and associated platform enumerations (CPEs)
4. **Prioritized vulnerability matching:** Evaluate, filter, and score matching vulnerabilities using iteratively executing correlation queries and dynamically calculated Asset Risk scores.
5. **Integrated OT Asset Behavior Profiling**: Monitor asset behavior profiles to detect activity changes on critical assets that may represent increased threat risk.
6. **OT-ready Correlation Searches:** Extend the deep bench of existing Enterprise Security correlation searches that monitor identity, endpoint, network, access and other IT data in Splunk with OT-specific searches recommended by the ICS Mitre Attack framework cleanly integrated within the same platform to detect TTPs across the full breadth of a global enterprise.
7. **Support for key elements of NERC CIP 002, 005, 007 and 010):** Dashboards and associated reports reviewed by trusted practitioners and NERC CIP auditors to help clients focus on NERC CIP requirements where Splunk can be assistive in compliance monitoring and audit support.
8. **Integration with SOAR (Security Orchestration, Automation, and Response)**: Includes new models and supporting content for Splunk Phantom. Security organizations that hold responsibility for monitoring an OT environment are able to more rapidly implement automation and orchestration tactics that support MITRE ICS recommendations.

Section 2: System and other Requirements

This quick start guide assumes a configured, production installation of Splunk Enterprise and Splunk Enterprise Security. If the reader is starting from scratch, please refer to the following documentation before continuing with this guide:

Splunk Enterprise Overview
A technical overview of Splunk platform features and documentation

Splunk Enterprise Release Notes
Includes information about new features, known issues, and fixed problems

Splunk Enterprise Installation Manual
How to install, upgrade, or migrate Splunk Enterprise. Includes system migration requirements and licensing information

Search Tutorial
If you are new to Splunk search, start here. Guides you through adding data, searching data, and creating simple dashboards

Splunk Enterprise Admin Manual
The starting point for Splunk Enterprise administration. Includes information about managing licenses, configuring Splunk Enterprise, and using the command-line interface. Includes a complete reference to all Splunk Enterprise configuration files

Splunk Enterprise Getting Data In
How to get your machine data into your Splunk deployment and ensure that it is indexed efficiently and effectively

All pertinent information related to the installation, configuration, and deployment of Splunk Enterprise and related technology can be found at https://docs.splunk.com/documentation/Splunk

In addition to Splunk Enterprise Documentation, the reader should be familiar with the use of and concepts related to Splunk Enterprise Security:

Splunk Enterprise Security Release Notes
Information on the new features and functionality in this release of Splunk Enterprise Security

Splunk Enterprise Security Installation and Upgrade Manual
A guide to installing and upgrading Splunk Enterprise Security

Use Splunk Enterprise Security
A guide to the dashboards and security analyst workflows in Splunk Enterprise Security

Administer Splunk Enterprise Security
Configure, manage, customize, and audit Splunk Enterprise Security

All pertinent information related to the installation, configuration and deployment of Splunk Enterprise Security can be found at https://docs.splunk.com/documentation/ES

Section 3: Splunk for OT Security App (DA-ESS-OTSecurity) Installation

The Splunk for OT Security Solution is packaged as a Splunk App and is available on Splunkbase at no cost to our Enterprise Security customers. If you are not an Enterprise Security customer and would like to trial the OT Security Solution, please contact your Splunk sales representative or send an email to sales@splunk.com

Download and install the most recent release of the Splunk OT Security App from Splunkbase:

Single Instance Splunk Deployments:

1. If you have internet access from your Splunk server, download and install the app by clicking “Browse More Apps” from the Manage Apps page in the Splunk platform.
2. If your Splunk server is not connected to the internet, download the app from Splunkbase and install it using the Manage Apps page in the Splunk platform. Note: If you download the app as a .tgz file, Google Chrome could automatically decompress it as a tar file. If that happens to you, use a different browser to download the app file.

Distributed Splunk Deployments:

Install the app on the search head only. The app is safe to install in large size clusters and will not impact indexers as search and correlation rules are disabled by default. As correlation rules are enabled, this may impact indexer performance, especially if multiple correlation rules are enabled all at once. It is recommended that rules be enabled as needed and then incrementally to minimize any negative effects on indexer performance.

The app also contains templates for lookup tables. The lookup files related to assets and identities are essential for dashboards and reports to populate correctly.

Search Head Clusters:

Splunk for OT Security can be installed in an SHC by following the standard installation instructions for the app.

ES Specific Considerations:

The Splunk OT Security Solution is a companion app to Splunk Enterprise Security and can be installed alongside Enterprise Security in both ES Search Head and ES Search head clusters.

Note on Potential Performance and Other Impacts:

If you save and enable searches included with the app in your environment, you could see changes in the performance of your Splunk deployment.

As is true for all searches in Splunk, the amount of data that you search affects the search performance you see in your deployment. For example, if you search Windows logs for two HMIs or Process Historian Servers, even the most intensive searches in this app add no discernible load to your indexers. If you instead search domain controller logs with hundreds of thousands of users included, you would see an additional load.

The searches included with the app are scheduled to run regularly and leverage acceleration and efficient search techniques wherever possible. In addition, the searches have been vetted by performance experts at Splunk to ensure they are as performant as possible. If you are concerned about resource constraints, schedule any searches you save to run during off-peak times.

You can also configure these searches to run against cached or summary index data. If you have a large-scale deployment, use the lookup cache for “first time seen” searches and select the “High Scale / High Cardinality” option for time series analysis searches.

Getting Data In

Splunk Enterprise can index any kind of data. In particular, any and all IT streaming, machine, and historical data, such as Windows event logs, web server logs, live application logs, network feeds, metrics, change monitoring, message queues, archive files, etc.

To get data into your Splunk deployment, point it at a data source. Tell it a bit about the source. That source then becomes a data input. Splunk Enterprise indexes the data stream and transforms it into a series of events. You can view and search for those events right away. If the results aren't exactly what you want, you can tweak the indexing process until they are.

If you have Splunk Enterprise, the data can be on the same machine as an indexer (local data) or on another machine (remote data). If you have Splunk Cloud, the data resides in your corporate network, and you send it to your Splunk Cloud deployment. You can get remote data into your Splunk deployment using network feeds or by installing Splunk forwarders on the hosts where the data originates. For more information on local vs. remote data, see Where is my data?

Splunk offers apps and add-ons with pre-configured inputs for things like Windows- or Linux-specific data sources, Cisco security data, Symantec Blue Coat data, and so on. Look on Splunkbase for an app or add-on that fits your needs. Splunk Enterprise also comes with dozens of recipes for data sources like web server logs, Java 2 Platform, Enterprise Edition (J2EE) logs, or Windows performance metrics. You can get to these from the Add data page in Splunk Web. If the recipes and apps don't cover your needs, then you can use the general input configuration capabilities to specify your particular data source.

For more general information about indexing data in Splunk Enterprise, please refer to the following documentation: Getting Data In.

OT Security-Relevant Partner and Community Developed Add-ons

Splunkbase is home to over 2000 apps and add-ons from Splunk, our partners, and our community. You can find an app or add-on for almost any data source and use case.

Apps can be searched and filtered based on developer, applicability to Splunk products and solutions, type, technology, contents (visualization, alert action, data inputs), compatibility with supported Splunk product versions, versions of the Splunk Common Information Model (CIM), validations and certifications.

A subset of these Splunk apps have been identified by Splunk OT Security Subject Matter Experts (SMEs) as particularly relevant to the Splunk OT Security Solution, and several are partner-built to specification and compatibility with the Splunk OT Security App. This is not an exhaustive list but should provide some direction to optional add-ons which will speed the configuration and administration of the solution:

OT Security Product

Many OT asset tools today did not start out with a focus on OT asset discovery and monitoring. Existing solutions initially focused on anomaly detection across networks with passive monitoring; however, in response to customer feedback, these tools evolved to incorporate mechanisms for OT Asset discovery. These tools provide information on what devices and protocols are being used and, in some, can detect changes to these devices or provide threat intelligence. They often utilize appliances that are placed at critical segments of the network and monitor traffic across these segments. In most cases, monitoring is done passively, although several of them now offer active monitoring of assets by speaking native OT protocols to the devices.

The intelligence and information provided by these solutions can be critical in identifying OT assets and provide valuable context for assets. Splunk allows a customer to monitor the entirety of the OT environment, including critical IT infrastructure and networks, and extend visibility to IT and OT environments.

The following represent some of Splunk's current integrations with OT Asset Discovery tools:

Add-on	Description	Splunkbase Listing
Armis Add-on and Armis App for Splunk	The Armis add-on provides integration with the Armis data sources for notable events and assets. The App-on provides the pre-built dashboards to view data from the Armis platform. It also includes a mapping to the OT Asset Data Model.	Add-on: https://splunkbase.splunk.com/app/4872 App: https://splunkbase.splunk.com/app/4873
Claroty Add-on for Splunk	The Claroty Add-on for Splunk focused on integration with Splunk's Enterprise Security and OT Security Add-on, including direct integration with notables and asset information.	https://splunkbase.splunk.com/app/5450
CyberX ICS Threat Monitoring for Splunk	The CyberX App provides direct integration of notable events from the CyberX platform. It also provides dashboards to understand the data being sent by the CyberX solution.	https://splunkbase.splunk.com/app/4313/
Dragos ICS Threat Detection app for Splunk, Dragos Add-on for Splunk, Dragos Threat Intelligence App for Splunk	The Dragos ICS Threat Detection app integration Dragos data into the Splunk platform and provides high-level dashboards regarding the Dragos solutions. The Add-on allows data sources to be collected and normalized within Splunk. The Threat Intelligence app allows threat	ICS Threat Detection: https://splunkbase.splunk.com/app/4601/ Add-on for Splunk: https://splunkbase.splunk.com/app/5231 Threat Intelligence App: https://splunkbase.splunk.com/app/5232

	feed and intelligence to be integrated into Splunk from the Dragos platform.	
Indegy - Industrial Cybersecurity Suite for Splunk	The Indegy app provides integration of Indegy data into Splunk and dashboards to understand threats to the environment.	https://splunkbase.splunk.com/app/4417/
ForeScout Technology Add-on for Splunk	The Forescout Add-on allows data to be collected from the Forescout eyeInspect solution (formerly know as SilentDefence) to be ingested and normalized within Splunk. It also includes a mapping to the OT Asset Data Model.	https://splunkbase.splunk.com/app/3382/

Network and Infrastructure Monitoring

While some OT traffic continues on serial and other P2P networks, most of it eventually makes it to switched Ethernet and IP networks. The gateways, switches, routers, and other devices that handle this information often expose important data about this traffic through Syslog streams and APIs.

Security teams can mine this information for both operational and security insights - both critical to the uptime of critical assets and infrastructure. For example, if your organization uses Cisco for networking and endpoint protection, you can use a suite of free add-ons to gain better insight into your OT security posture by monitoring events from Cisco IPS devices for anomalous activity.

Add-on	Description	Splunkbase Listing
Cisco Security Suite	The Cisco Security Suite provides a single pane of glass interface into Cisco security data. It supports Cisco ASA and PIX firewall appliances, the FWSM firewall services module, Cisco IPS, Cisco Web Security Appliance (WSA), Cisco Email Security Appliance (ESA), Cisco	https://splunkbase.splunk.com/app/525/

	Identity Services Engine (ISE), pxGrid, and Cisco Advanced Malware Protection / Sourcefire.	
Cisco Networks Add-on for Splunk Enterprise	The Cisco Networks Add-on for Splunk Enterprise (TA-cisco_ios) sets the correct sourcetype and fields used for identifying data from Cisco IOS, IOS XE, IOS XR, NX-OS devices using Splunk® Enterprise.	https://splunkbase.splunk.com/app/1467/
Splunk Add-on for Cisco ASA	The Splunk Add-on for Cisco ASA allows a Splunk software administrator to map Cisco ASA events to the Splunk CIM. You can then use the data with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance.	https://splunkbase.splunk.com/app/1620/
Splunk Add-on for Cisco Identity Services	The Splunk Add-on for Cisco ISE allows a Splunk software administrator to collect Cisco Identity Service Engine (ISE) Syslog data. You can use the Splunk platform to analyze these logs directly or use them as a contextual data source to correlate with other communication and authentication data in the Splunk platform.	https://splunkbase.splunk.com/app/1915/
Palo Alto Networks Add-on for Splunk	The Palo Alto Networks Add-on for Splunk allows a Splunk® Enterprise administrator to collect data from every product in the Palo Alto Networks Next-generation Security Platform. The add-on collects and correlates data from Firewalls, Panorama, Traps Endpoints, Aperture SaaS	https://splunkbase.splunk.com/app/2757/

	Security, AutoFocus, MineMeld, and WildFire.	
Splunk Add-on for Symantec Endpoint Protection	The Splunk Add-on for Symantec Endpoint Protection allows a Splunk platform administrator to collect SEP server and client activity logs from Symantec Endpoint Protection Manager dump files.	https://splunkbase.splunk.com/app/2772/
Splunk Add-on for Juniper	The Splunk Add-on for Juniper allows a Splunk software administrator to pull system logs and traffic statistics from Juniper IDP, Juniper NetScreen Firewall, Juniper NSM, Juniper NSM IDP, Juniper SSLVPN, Junos OS, and Juniper SRX using Syslog.	https://splunkbase.splunk.com/app/2847/
Splunk Add-on for McAfee	The Splunk Add-on for McAfee allows a Splunk Enterprise administrator to collect anti-virus information and Network Security Platform (Intrushield) information.	https://splunkbase.splunk.com/app/1819/
Splunk Add-on for Zeek aka Bro	The Splunk Add-on for Zeek, aka Bro, allows a Splunk software administrator to analyze packet capture data directly or use it as a contextual data feed to correlate with other vulnerability-related data in the Splunk platform.	https://splunkbase.splunk.com/app/1617/
Fortinet FortiGate Add-On for Splunk	Fortinet FortiGate Add-On for Splunk is the technical add-on (TA) developed by Fortinet, Inc. The add-on enables Splunk Enterprise to ingest or map security and traffic data collected from FortiGate physical and virtual appliances across domains.	https://splunkbase.splunk.com/app/2846/

Splunk Add-on for RSA SecurID	The Splunk Add-on for RSA SecurID allows a Splunk software administrator to collect data from the RSA SecurID Authentication Manager (AM) server via Syslog.	https://splunkbase.splunk.com/app/2958/
Tenable Add-On for Splunk	The Tenable Add-On for Splunk provides a robust set of Adaptive Response actions and Inputs for operationalizing Tenable.io and Tenable.SC data in Splunk.	https://splunkbase.splunk.com/app/4060/

Even when there is no pre-built app or add-on to accelerate integration with your existing networking gear, you can usually integrate directly with Syslog, TCP, UDP, HTTP, or other built-in data endpoints on your network. Splunk Partners and Professional Services are also available to help you onboard any of your OT security-relevant data sources.

Windows and Linux Servers and Workstations

Most of your servers and workstations on OT networks are likely running some version of the Microsoft Windows Operating System. You can install the Splunk-built “Splunk Add-on for Microsoft Windows” within a Splunk Universal Forwarder on each of these machines to capture critical security-relevant information from the operating system, Active Directory, DNS Server, Security, Performance, DHCP and File Server services, and key application logs and events from Windows Event Logs.

The forwarders can be configured to send this data, as it is generated, to a Splunk instance in your data center or the cloud, and you will have near-immediate access to volumes of valuable information.

For example, you may want to search your Windows Event Logs for a specific error throw from your Wonderware System or from your OSIsoft Pi Historian. This error could appear on one or many of your Windows instances, and Splunk will let you know exactly where and when it occurs. Splunk’s real-time monitoring and alerting system also allows you to send emails or take other action any time these or other known issues occur in the future.

Another example would be monitoring your Windows Authentication logs in real-time for unauthorized or failed login attempts, and knowing who is trying to access your system when and from where is a critical first step in increasing your security posture.

In situations where vendor restrictions or other requirements do not allow the installation of third-party applications like the Splunk Universal Forwarder, you may decide to dedicate a single windows machine, either physical or virtual, for centralized data collection and installation of the Universal Forwarder. It is up to the end-user to decide how to migrate logs and events to this central repository. Options include FTP, scripted transfer, and Windows Event Forwarding. Once centralized, the information will be handled by the Universal Forwarder as if it was installed locally.

For OT environments where Linux servers and workstations are installed, a similar "Splunk Add-on for Unix and Linux" is available.

App and Add-on Licensing, Compatibility, and Support

Splunk's ecosystem is open, and community-developed apps and add-ons available on Splunkbase and elsewhere should be reviewed before installation. Partner and Community-developed apps are not supported by Splunk, Inc. and should be installed and configured at your own risk. In all situations, we would encourage you to closely review the license, codebase, and credibility of any apps not built and supported by Splunk.

Splunk provides all developers access to Splunk AppInspect, a set of resources for evaluating an app against a set of Splunk-defined criteria related to structure, features, security, and adherence to specific Splunk app guidelines. Effective August 2018, all apps posted to Splunkbase are processed by AppInspect before being published. We caution users not to deploy apps unless directly downloaded from Splunkbase.

Section 4: Splunk for OT Security App (DA-ESS-OTSecurity) Configuration

Once the Splunk OT Security Solution app has been installed in your Splunk environment alongside your Splunk Enterprise Security app, you will need to take the following steps to configure the application for production use:

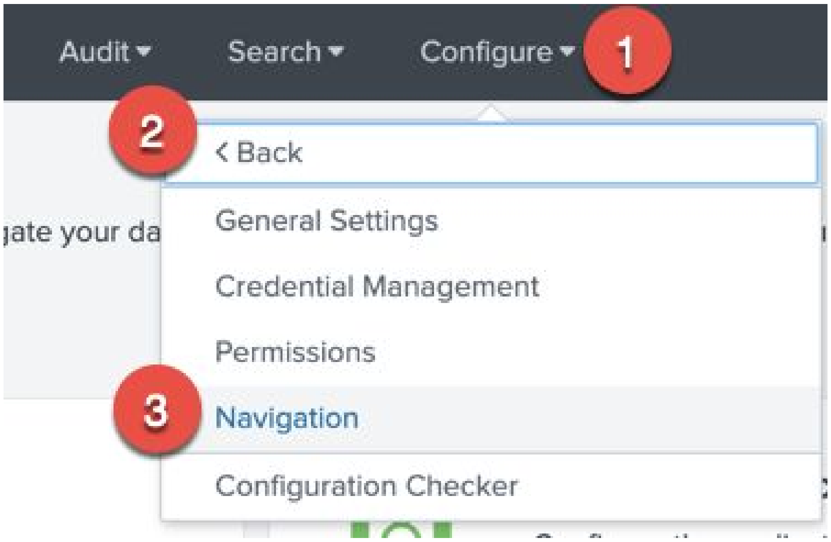
Configuration Step 1: Update Navigation Menus

Splunk for OT Security comes with navigation menus that can be edited to suit your Enterprise Security deployment. These navigation menus include links to dashboards and reports that are included in the Splunk for OT Security solution.

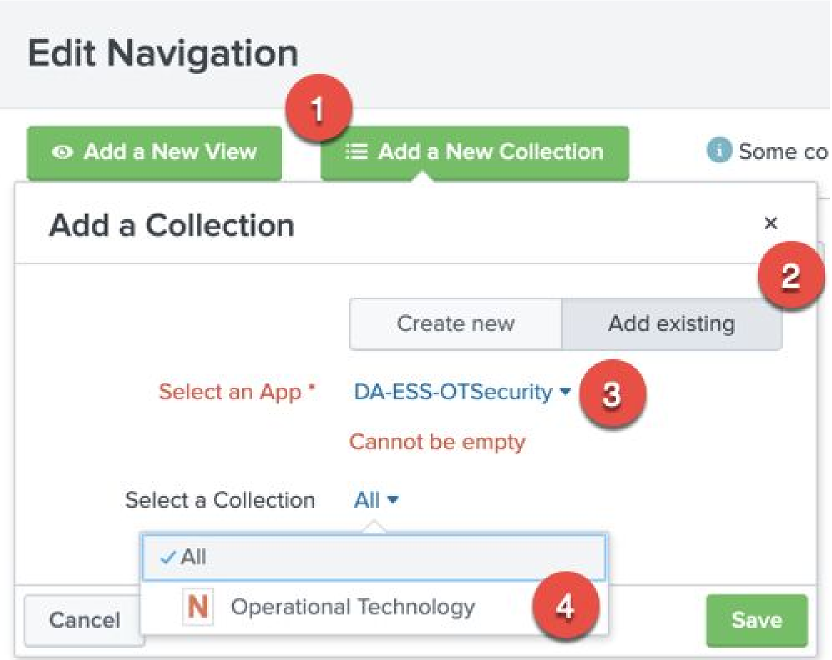
Managing Navigation Menus

1. Open the Enterprise Security app in your Splunk instance
2. Go to the Enterprise Security app in Splunk

3. In the app navigation bar, navigate to the following location: *Configure→General→Navigation*



4. On the *Edit Navigation* screen, add existing menus by selecting: *Add a New Collection→ Add Existing→ App: DA-ESS-OTSecurity→ Select a Collection*



Select an App * DA-ESS-OTSecurity

Select a Collection All

5. The menu containing all the Operation Technology dashboards and reports will now appear. These can be dragged to the desired location in the menu hierarchy or can be modified to fit your organizations needs. For example, the Compliance menu containing

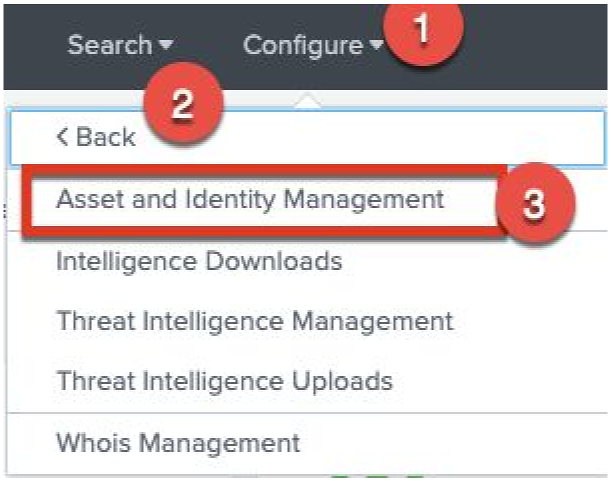
NERC CIP dashboards may be removed if your organization is not under NERC CIP regulations.

Configuration Step 2: Configure the Asset Framework

The Splunk for OT Security Solution extends the ES Asset Framework to provide additional context and information about OT assets.

To update the asset framework follow these steps:

1. Go the Enterprise Security app in Splunk
2. In the app navigation bar go to the following location: *Configure→ Data Enrichment→ Asset and Identity Management*


Search
Configure
1
2
< Back
Asset and Identity Management
3
Intelligence Downloads
Threat Intelligence Management
Threat Intelligence Uploads
Whois Management

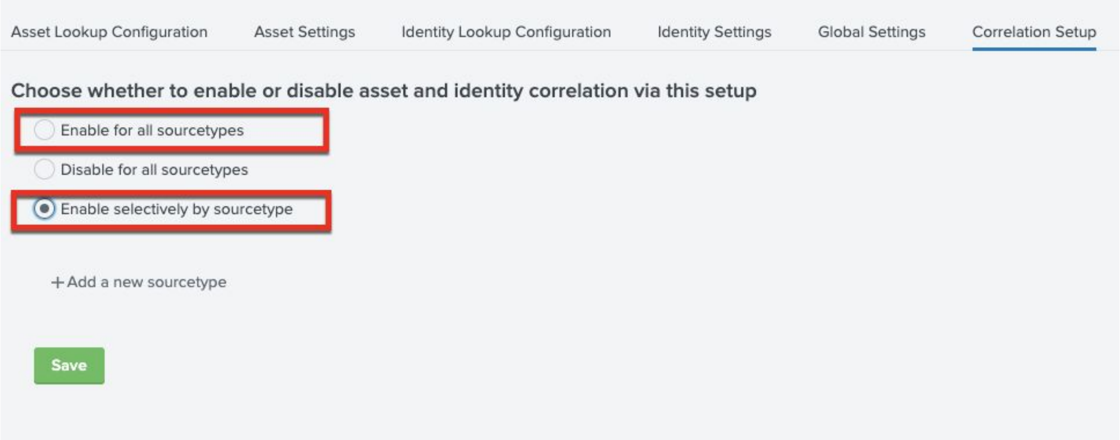
3. Go the *Asset Settings* table
   a. Update the Asset Framework by Adding New Fields (**important**: field names are case sensitive) as shown here:

Field Name	Tag	Multivalue
asset_id	Yes	No
asset_model	Yes	No
asset_status	Yes	No
asset_system	Yes	No
asset_type	Yes	No
asset_vendor	Yes	No

asset_version	Yes	No
classification	Yes	Yes
description	No	No
exposure	Yes	No
location	No	Yes
site_id	Yes	No
vlan	Yes	Yes
zone	Yes	Yes

b. Enable the new asset framework by navigating to the *Correlation Setup* tab

i. Enable *asset and identity correlation* via the setup to either *Enable for all sourcetypes* or *Enable selectively by sourcetype* and supply the required sourcetypes. In most cases, *Enable selectively by sourcetype* is preferred as it results in less load on the Splunk infrastructure since it only searches for specific data sources and not across all data.



Choose whether to enable or disable asset and identity correlation via this setup

○ Enable for all sourcetypes

○ Disable for all sourcetypes

● Enable selectively by sourcetype

Configuration Step 3: Upload Asset Information

Now that you have updated the Asset Framework, asset and identity lookup files can be uploaded into ES. By default, the Splunk for OT Security app contains three important lookup files that are leveraged throughout the app for saved searches, reports, and dashboards. Each is explained here:

All use cases:

- ot_asset_lookup.csv: This file contains a list of OT assets such as PLC's, RTU's, Historians, SCADA servers, etc.

For NERC CIP use cases:

- *cip_asset_lookup.csv:* This file contains a list of OT assets that are included in NERC CIP compliance reporting. This may be a distinct set of OT assets or be a subset of the assets in the OT_asset_lookup.csv file. Since NERC CIP compliance requires that assets be classified, sites, and ESP zones defined, the following fields must be populated for each asset:

Field	Format	Example
classification	cip:<low,medium, or high>|cip<BCA,PCA,TSA,EACM,EAP>	cip:high|cip:EAP|cip:EACM
category	nerc	nerc
site_id	<site name>	Pleasanton Plant
zone	eap:<zone name>	eap:PPLT

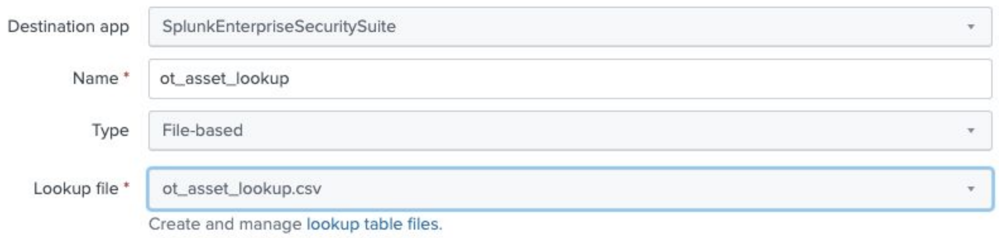
- *cip_identities.csv* names must be used since many of the NERC CIP dashboards leverage these lookups.

Important: In order to leverage lookup files from apps outside of Enterprise Security, *Lookup Definitions* **must be created within the Splunk Enterprise Security Suite app context.** For more information on managing lookups and knowledge objects within Splunk Enterprise, please refer to the documentation linked at the beginning of this document.

To create the lookup files and link them to the asset framework follow these steps:

1. Go to *Settings → Lookups*
2. Click on *Lookup Definitions*
3. Click on *New Lookup Definition*
    a. For all: Add ot_asset_lookup lookup definition
        i. Destination App: SplunkEnterpriseSecuritySuite
        ii. Name: ot_asset_lookup
        iii. Type: File-based

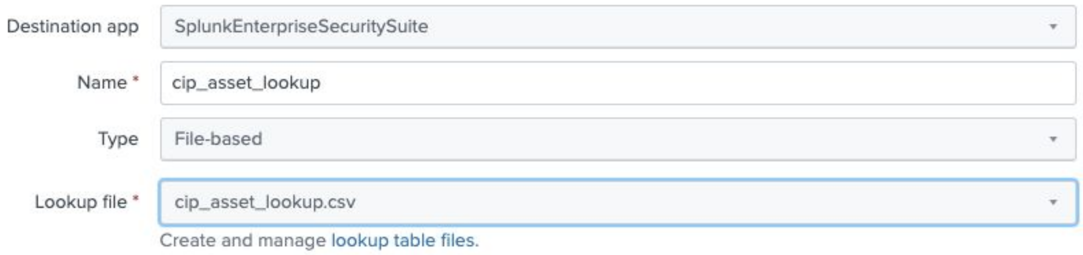
iv. Lookup file: ot_asset_lookup.csv



Destination app	SplunkEnterpriseSecuritySuite
Name *	ot_asset_lookup
Type	File-based
Lookup file *	ot_asset_lookup.csv

Create and manage lookup table files.

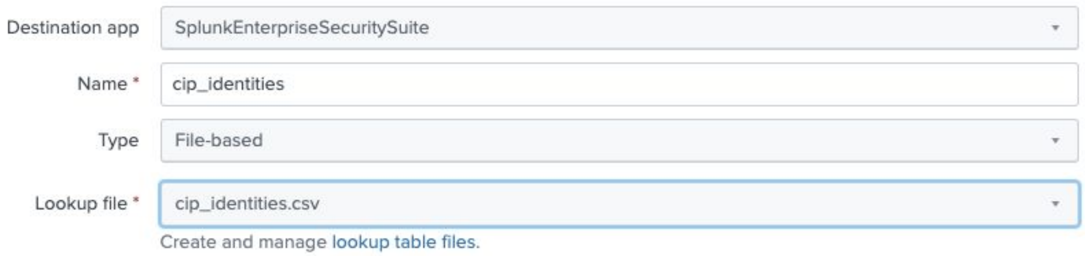
b. For NERC CIP: Add the cip_asset_lookup lookup definition
   i. Destination App: SplunkEnterpriseSecuritySuite
   ii. Name: cip_asset_lookup
   iii. Type: File-based
   iv. Lookup file: cip_asset_lookup.csv lookup definition



Destination app	SplunkEnterpriseSecuritySuite
Name *	cip_asset_lookup
Type	File-based
Lookup file *	cip_asset_lookup.csv

Create and manage lookup table files.

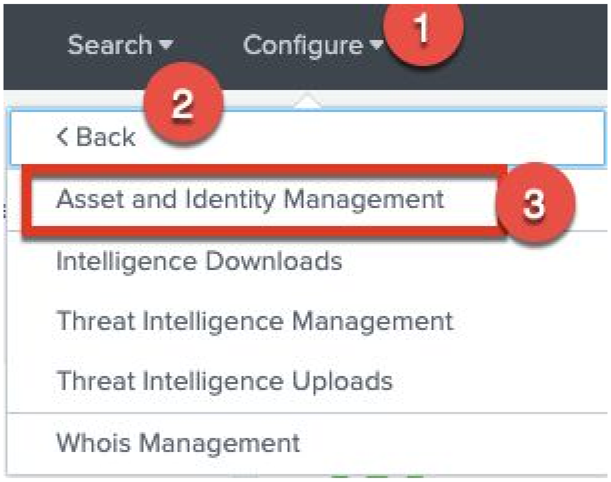
c. For NERC CIP: Add the cip_identities
   i. Destination App: SplunkEnterpriseSecuritySuite
   ii. Name: cip_identities
   iii. Type: File-based
   iv. Lookup file: cip_identities.csv



Destination app	SplunkEnterpriseSecuritySuite
Name *	cip_identities
Type	File-based
Lookup file *	cip_identities.csv

Create and manage lookup table files.

4. Open the Enterprise Security App
5. In the app navigation bar go to the following location: *Configure→ Data Enrichment→ Asset and Identity Management*


Search
Configure
1
2
< Back
Asset and Identity Management
3
Intelligence Downloads
Threat Intelligence Management
Threat Intelligence Uploads
Whois Management

6. Go to the *Asset Lookup Configuration* Tab
7. Click on + *New* button and configure your new asset lookup to match the name of your Lookup Definition for Assets created in step 3 above.
8. Repeat steps 6 and 7 until you have created new asset configurations for each of your asset lookup definitions
9. Go to the *Identity Lookup Configuration* Tab
10. Click on the + New button and configure you new asset lookup to the match of your Lookup Definition for Identities in step 3 above
11. Repeat steps 9 and 10 until you have created new identity configurations for each of your identity lookup definitions.

OT Data Models: Integrating Splunk Add-ons with Asset and Identity Frameworks

Splunk for OT Security includes several data models that can be leveraged to automatically generate asset lookups. In addition, OT partners of Splunk should populate any hardware and software data captured or created by their add-ons to these data models.

Two data models have been created to facilitate populating assets into Splunk for Enterprise Security. The **most critical model** for asset information in the Splunk OT Security Solution is the ***OT Asset*** data model contained in the Splunk for OT Security app. This data model is designed to be used with hardware assets such as servers, PLC's, workstations, etc. and contains all fields in the OT Asset Framework. An additional data model also exists called ***OT Software Asset*** which is used to populate additional information regarding firmware, operating system, and software present on each OT asset. Together data from each can be combined to provide additional context around an asset as well as components installed on each asset.

OT Data Models: Example Implementation

Ilium Energy, Inc. (see Section 7) has installed and configured the Splunk for OT Security App into their Enterprise Security installation. They would now like to leverage their data to gather information about their OT assets where they have traditionally had little if any information. They have several data sources from their endpoint protection solution which includes fields like host name, ip, domain, hardware information, and operating system. After reviewing the documentation, Ilium Energy realizes that some data will need to go in the OT Asset data model and other information will need to go into the OT Software Asset. They build a search that runs weekly (since this information is unlikely to update) and populates the OT Asset data model so their asset list is up to date:

nt_host: Ilium01
IP: 172.9.5.5:
DNS: Ilium01.opsdomain.local
asset_vendor: HP,
asset_model: Proliant G8

Ilium Energy also needs to publish some information into the OT Software Asset data model that runs daily with the following information:

nt_host: Ilium01
IP: 172.9.5.5:
DNS: Ilium01.opsdomain.local
vendor: Microsoft
version: Windows Server 2008 R2

Using this endpoint solution, once a day they schedule a search to move this data into the ot_asset_lookup.csv, updating any existing entries and appending any new ones.

OT Data Models: Example Integration

A Partner has released a Splunk app that integrates OT asset information generated by their application using it’s REST API interface. This partner also wants to make sure their customers can use Splunk’s OT Security Solution to get more value from that data. In their Splunk app, the partner executes REST API queries against their own application, and maps the json response to the OT Asset data model. When new assets are discovered by the OT Security Plus application, they automatically show up in the relevant Splunk data models and a scheduled Splunk search can be configured to automatically update the assets in the Splunk OT Security solution.

Configuration Step 4: Update Macros

Macros are leveraged in the Splunk OT Security solution for re-use of searches and so pre-configured indexes, sources, and sourcetypes can be automatically adjusted to represent a specific customer environment.
Note: Macros are designed for efficiency and should only include data sources relevant to the query being performed. Using default or otherwise overly-broad macro definitions may result in slow and process-intensive searches.

To update macros for the Splunk for OT Security app perform the following steps:

1. Go to *Settings → Advanced Search → Search macros*
2. Update the following macros to reflect the indexes, sources, and sourcetypes present in your environment. If a data source is not present in your environment it can be modified to a non-existing index and sourcetype to reduce query time.
   a. **Example:** For NERC CIP reporting:

      i. **get_2fa_indexes:** should point to data sources relevant to multi-factor authentication (e.g. OKTA, RSA, etc. logs.)
      ii. **get_app_datamodel**: should point to the data source that contains information on updates and applications being installed (e.g. windows update events)
      iii. **get_firewall_datasources:** should point to firewall configuration data sources (e.g. enabled and disabled port, system configuration files, etc.)
      iv. **get_installedapps_datasources:** should point to the data source which includes all the installed applications about hosts
      v. **get_os_datasources:** should point to the data source which contains OS information about hosts
      vi. **get_usb_datasources:** should point to the data source that logs external media devices being connected to a host (e.g. endpoint monitoring, windows registry, etc.)
      vii. **get_backup_indexes:** should point to the data source that contains client backup logs.
      viii. **get_physicalaccess_records:** should point to the data source that contains physical access logs such as badge scan records.
      ix. **exclude_internal_ips:** should contain a subnets which are considered internal to the company
      x. **get_ot_device_asset_types:** should contain a list of asset types which are considered OT devices and not devices in the OT environment (e.g. PLC's). This macro is pre-populated but should be adjusted to the customer's environment.
      xi. **get_ot_security_alerts:** should contain the index and/or sources types associated with OT Security solution. This macro is pre-populated with some common sourcetypes but should be adjusted based on the customer's OT security solution.

xii. **get_visitoraccess_records:** should contain the index and/or sourcetype where visitor access logs are stored

Section 5: Troubleshooting Installation and Configuration

While this guide is designed to be as comprehensive as possible, you may run into issues during installation and configuration. The larger body of Splunk Enterprise and Splunk Enterprise Security documentation at the top of this document will help you troubleshoot some of the more common issues encountered during this process. In addition, there are several gotchas that have been encountered during early adoption of the OT Security solution, you can resolve these quickly by double checking the following:

Issue 1: Cannot add lookups to asset or identity framework.

If you cannot add lookups to the Asset and Identity Framework, perform the following checks:

a. Verify the permissions of the DA-ESS-OTSecurity folders and files. These should match other apps installed. Often when a file is manually extracted into the SPLUNK_HOME/etc/apps directory their permissions will be those of the person who manually installed the app. Typically installing via the web gui can avoid these problems. Also check the permissions of the transforms.conf file in the SPLUNK_HOME/etc/apps/EnterpriseSecurity/local directory since lookup definitions are written to this file.
b. Verify that the Lookup Definition has been created in the Enterprise Security App and permissions are set to share objects globally via the Lookup Definitions menu

Issue 2: NERC CIP dashboards and reports are not populating automatically.

This problem most often occurs when one of two errors occur:

a. Verify that the asset lookup has been created and the following fields exist and are populated:

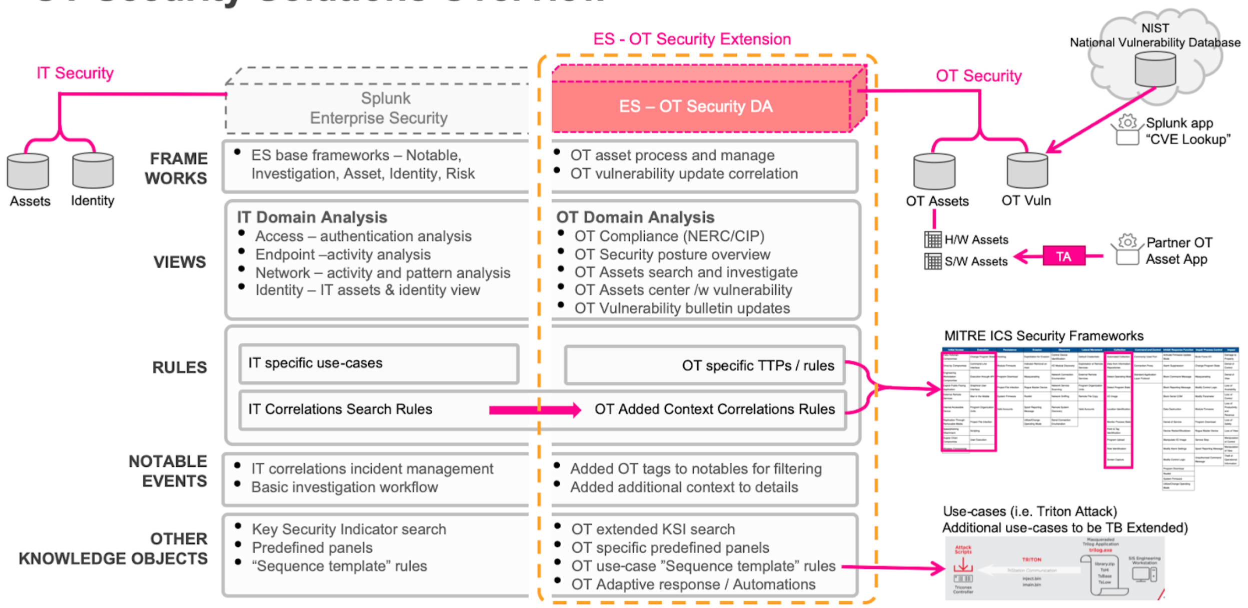
Field	Format	Example
classification	cip:<low,medium, or high>|cip<BCA,PCA,TSA,EACM,EAP>	cip:high|cip:EAP|cip:EACM
category	nerc	nerc

site_id	<site name>	Pleasanton Plant
zone	eap:<zone name>	eap:PPLT

b. Data is not present in the data models or disabled. The following data models should be enabled and contain data:

i. Authentication
ii. Intrusion Detection
iii. Inventory
iv. Malware
v. Network Sessions
vi. Network Traffic
vii. Updates

OT Security Solutions Overview



IT Security

Assets

Identity

Splunk Enterprise Security

ES - OT Security Extension

ES – OT Security DA

NIST National Vulnerability Database

OT Security

Splunk app "CVE Lookup"

OT Assets

OT Vuln

H/W Assets

S/W Assets

TA

Partner OT Asset App

FRAME WORKS

- ES base frameworks – Notable, Investigation, Asset, Identity, Risk

- OT asset process and manage
- OT vulnerability update correlation

VIEWS

IT Domain Analysis
- Access – authentication analysis
- Endpoint –activity analysis
- Network – activity and pattern analysis
- Identity – IT assets & identity view

OT Domain Analysis
- OT Compliance (NERC/CIP)
- OT Security posture overview
- OT Assets search and investigate
- OT Assets center /w vulnerability
- OT Vulnerability bulletin updates

RULES

IT specific use-cases

IT Correlations Search Rules

OT specific TTPs / rules

OT Added Context Correlations Rules

MITRE ICS Security Frameworks

NOTABLE EVENTS

- IT correlations incident management
- Basic investigation workflow

- Added OT tags to notables for filtering
- Added additional context to details

OTHER KNOWLEDGE OBJECTS

- Key Security Indicator search
- Predefined panels
- "Sequence template" rules

- OT extended KSI search
- OT specific predefined panels
- OT use-case "Sequence template" rules
- OT Adaptive response / Automations

Use-cases (i.e. Triton Attack)
Additional use-cases to be TB Extended)

Section 6: Using Splunk for OT Security

Overview:

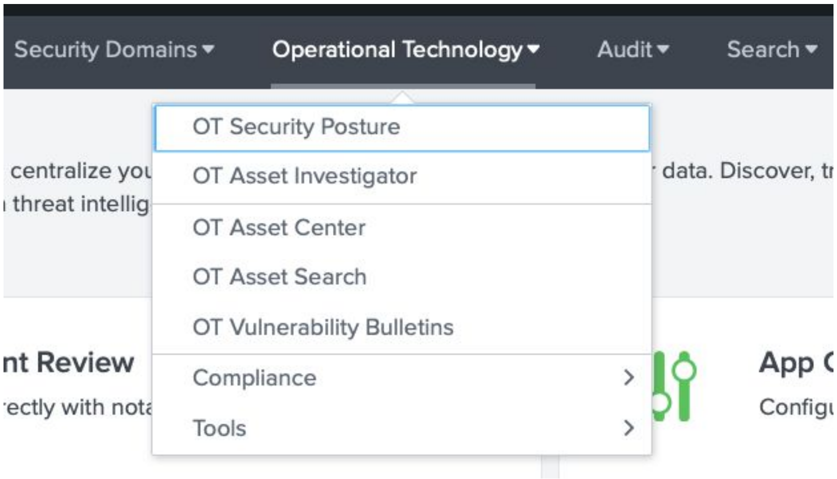
Splunk for OT Security is designed to work to help Splunk Enterprise Security customers understand more about their OT environments and create end-to-end security visibility across both OT and IT systems. In addition, customers under NERC CIP regulations will be able to leverage Splunk's platform to ensure compliance and auditing requirements. Splunk for OT

Security focuses around extending the current capabilities of Splunk Enterprise Security in two primary areas explained below.

Providing Asset Context:

While Splunk Enterprise Security provides existing dashboards and capabilities around understanding Assets, OT systems often require additional context and investigation before action is possible. Splunk for OT Security extends Splunk Enterprise Security's Asset & Identity Framework to include additional important fields such as site, role of machines, and location within ISA 99 models.

Dashboards that cover these areas can be found via the Operational Technology navigation menu item as shown here:

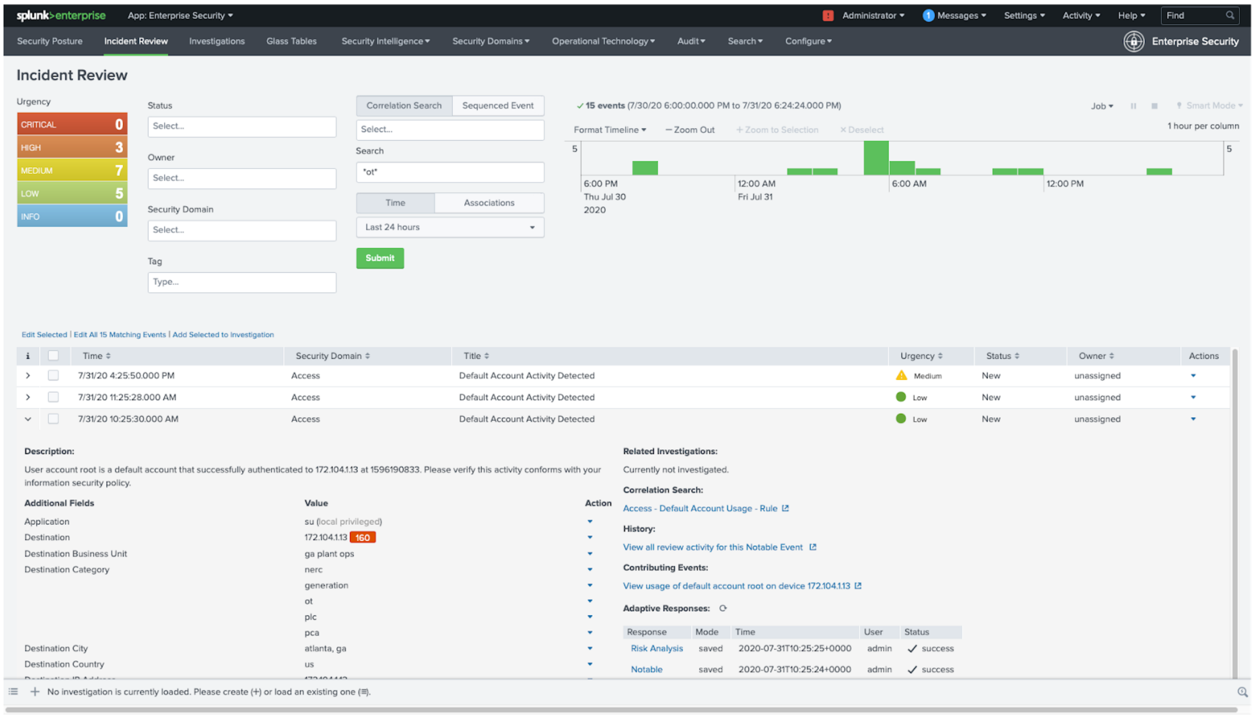


Extended Dashboards and Investigative Capabilities:

While in most cases Splunk for OT Security will be integrated in a combined Security Operations Center for both IT and OT, specific views into the OT environment can help an analyst understand current security posture. This includes specific views around security posture, OT assets, as well as vulnerabilities in OT Environments. In addition, OT assets are now integrated directly with Splunk Enterprise Security existing dashboards, reports, and incident management capabilities.

For example, OT assets can be tagged in the Asset and Identity Framework directly to produce a list of incidents related to OT Assets and Identities. This is shown here by simply putting in the word *ot* into the search criteria to produce a list of OT incidents which can be reviewed.

Incident Review Example:



Incident Review

Urgency	
CRITICAL	0
HIGH	3
MEDIUM	7
LOW	5
INFO	0

Status: Select...

Owner: Select...

Security Domain: Select...

Tag: Type...

Correlation Search | Sequenced Event: Select...

Search: *ot*

Time | Associations: Last 24 hours

✓ **15 events** (7/30/20 6:00:00.000 PM to 7/31/20 6:24:24.000 PM)

Edit Selected | Edit All 15 Matching Events | Add Selected to Investigation

i	□	Time ⇕	Security Domain ⇕	Title ⇕	Urgency ⇕	Status ⇕	Owner ⇕	Actions
>	□	7/31/20 4:25:50.000 PM	Access	Default Account Activity Detected	⚠ Medium	New	unassigned	▾
>	□	7/31/20 11:25:28.000 AM	Access	Default Account Activity Detected	● Low	New	unassigned	▾
⌄	□	7/31/20 10:25:30.000 AM	Access	Default Account Activity Detected	● Low	New	unassigned	▾

Description:

User account root is a default account that successfully authenticated to 172.104.1.13 at 1596190833. Please verify this activity conforms with your information security policy.

Additional Fields	Value	Action
Application	su (local privileged)	▾
Destination	172.104.1.13 160	▾
Destination Business Unit	ga plant ops	▾
Destination Category	nerc	▾
	generation	▾
	ot	▾
	plc	▾
	pca	▾
Destination City	atlanta, ga	▾
Destination Country	us	▾

Related Investigations:

Currently not investigated.

Correlation Search:

Access - Default Account Usage - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View usage of default account root on device 172.104.1.13

Adaptive Responses:

Response	Mode	Time	User	Status
Risk Analysis	saved	2020-07-31T10:25:25+0000	admin	✓ success
Notable	saved	2020-07-31T10:25:24+0000	admin	✓ success

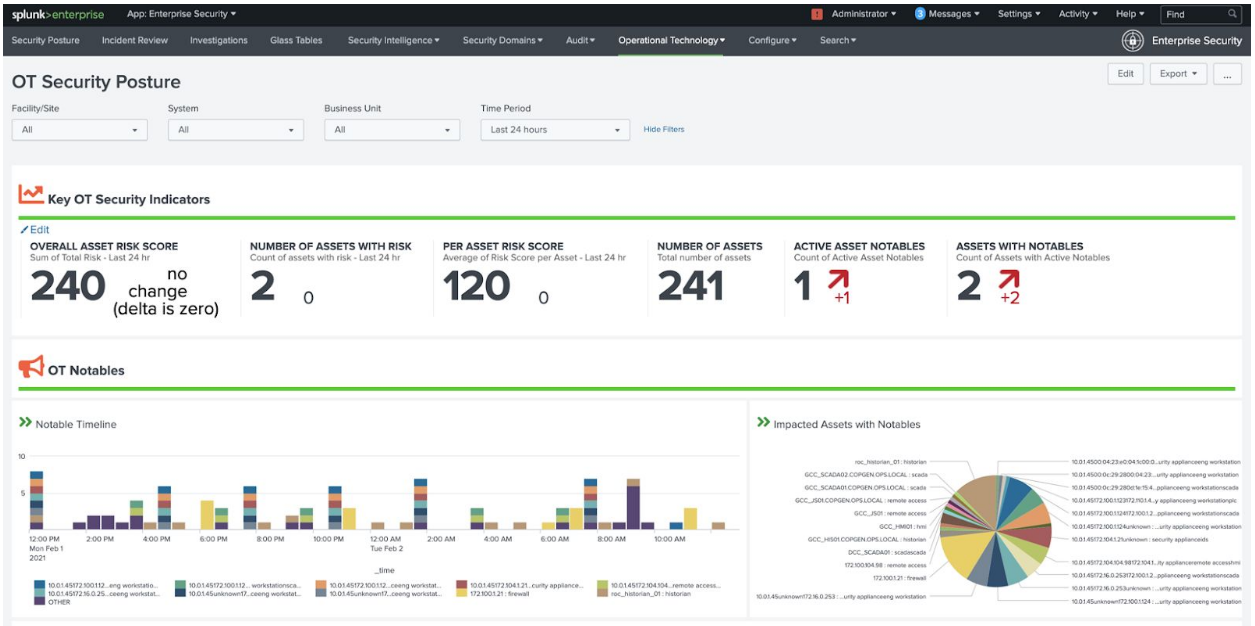
No investigation is currently loaded. Please create (+) or load an existing one (≡).

As a result of extending the Asset and Identity Framework being extended, any field such as site, environment, or classification can now be used as a filter by specifying a tag in the filter criteria.

OT Security Posture: At a glance visibility of OT security environment

The OT Security Posture dashboard is designed to provide a high level overview of an organization's security posture for their OT environment. New Key Performance Indicators (KPI’s) have been created that focus around the health and risk of OT security operations. Notable security events are also pre-filtered and include both existing correlation rules as well as new MITRE ICS ATT&CK correlation rules. Drilling down on a notable allows the security analysis to start an investigation within ES easily.

OT Security Posture Example (OT Security Posture):


splunk>enterprise
App: Enterprise Security ▾
Administrator ▾
3 Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Security Posture
Incident Review
Investigations
Glass Tables
Security Intelligence ▾
Security Domains ▾
Audit ▾
Operational Technology ▾
Configure ▾
Search ▾
Enterprise Security
Edit
Export ▾
...
Hide Filters
Edit
10
5
12:00 PM Mon Feb 1 2021
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM Tue Feb 2
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
_time
10.0.1.45172.100.1.12...eng workstatio...
10.0.1.45172.16.0.25...ceeng workstat...
OTHER
10.0.1.45172.100.1.12... workstationsca...
10.0.1.45unknown17...ceeng workstat...
10.0.1.45172.100.1.12...ceeng workstat...
10.0.1.45unknown17...ceeng workstat...
10.0.1.45172.104.1.21...curity appliance...
172.100.1.21 : firewall
10.0.1.45172.104.104...remote access...
roc_historian_01 : historian
roc_historian_01 : historian
GCC_SCADA02.COPGEN.OPS.LOCAL : scada
GCC_SCADA01.COPGEN.OPS.LOCAL : scada
GCC_JS01.COPGEN.OPS.LOCAL : remote access
GCC_JS01 : remote access
GCC_HMI01 : hmi
GCC_HIS01.COPGEN.OPS.LOCAL : historian
DCC_SCADA01 : scadascada
172.100.104.98 : remote access
172.100.1.21 : firewall
10.0.1.45unknown172.16.0.253 : ...urity applianceeng workstation
10.0.1.4500:04:23:e0:04:1c00:0...urity applianceeng workstation
10.0.1.4500:0c:29:2800:04:23:...urity applianceeng workstation
10.0.1.4500:0c:29:280d:1e:15:4...pplianceeng workstationscada
10.0.1.45172.100.1.123172.110.1.4...y applianceeng workstationplc
10.0.1.45172.100.1.124172.100.1.2...pplianceeng workstationscada
10.0.1.45172.100.1.124unknown : ...urity applianceeng workstation
10.0.1.45172.104.1.21unknown : security applianceids
10.0.1.45172.104.104.98172.104.1...ity applianceremote accesshmi
10.0.1.45172.16.0.253172.100.1.2...pplianceeng workstationscada
10.0.1.45172.16.0.253unknown : ...urity applianceeng workstation
10.0.1.45unknown172.100.1.124 : ...urity applianceeng workstation

OT Security Posture

Facility/Site	System	Business Unit	Time Period
All	All	All	Last 24 hours

Key OT Security Indicators

OVERALL ASSET RISK SCORE
Sum of Total Risk - Last 24 hr
240 no change (delta is zero)

NUMBER OF ASSETS WITH RISK
Count of assets with risk - Last 24 hr
2 0

PER ASSET RISK SCORE
Average of Risk Score per Asset - Last 24 hr
120 0

NUMBER OF ASSETS
Total number of assets
241

ACTIVE ASSET NOTABLES
Count of Active Asset Notables
1 ↗ +1

ASSETS WITH NOTABLES
Count of Assets with Active Notables
2 ↗ +2

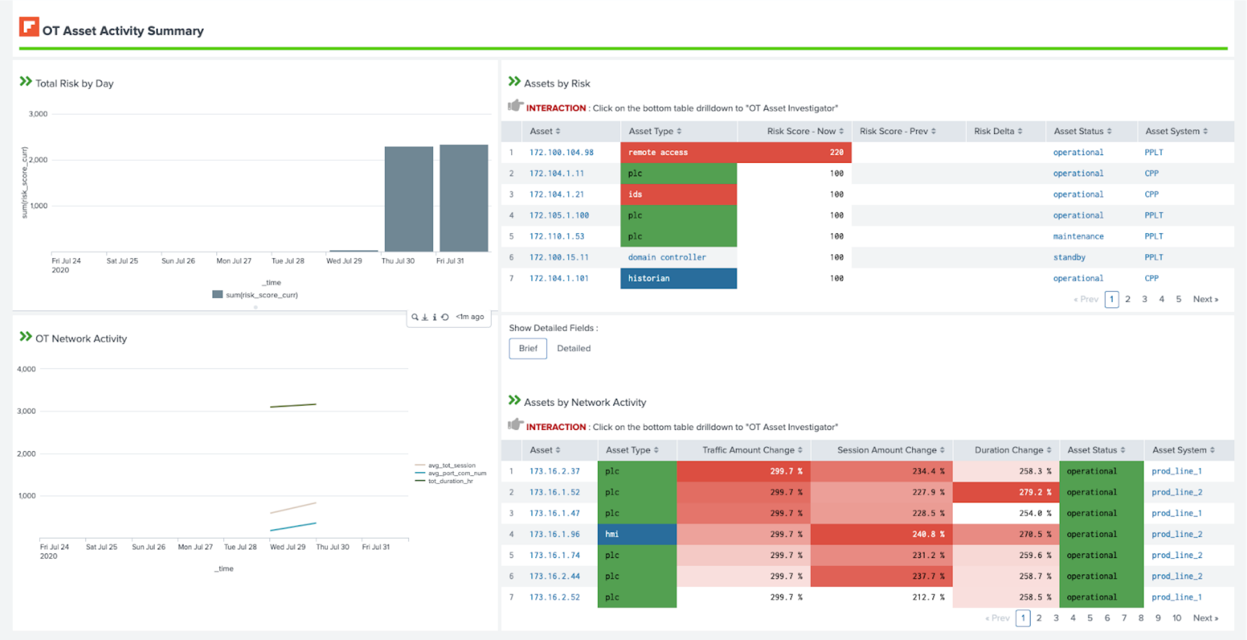
OT Notables

» Notable Timeline

» Impacted Assets with Notables

In addition, OT Asset Activity is summarized below so that the security analyst can understand how assets are network behavior might be changing or how their risk is changing over time. Additional filters at the top of the dashboard allow panels below to view details for specific sites, systems, or business units.

OT Asset Activity Example (OT Security Posture):



Assets by Risk

INTERACTION : Click on the bottom table drilldown to "OT Asset Investigator"

	Asset	Asset Type	Risk Score - Now	Risk Score - Prev	Risk Delta	Asset Status	Asset System
1	172.100.104.98	remote access	220			operational	PPLT
2	172.104.1.11	plc	100			operational	CPP
3	172.104.1.21	ids	100			operational	CPP
4	172.105.1.100	plc	100			operational	PPLT
5	172.110.1.53	plc	100			maintenance	PPLT
6	172.100.15.11	domain controller	100			standby	PPLT
7	172.104.1.101	historian	100			operational	CPP

« Prev 1 2 3 4 5 Next »

Show Detailed Fields :

Brief Detailed

Assets by Network Activity

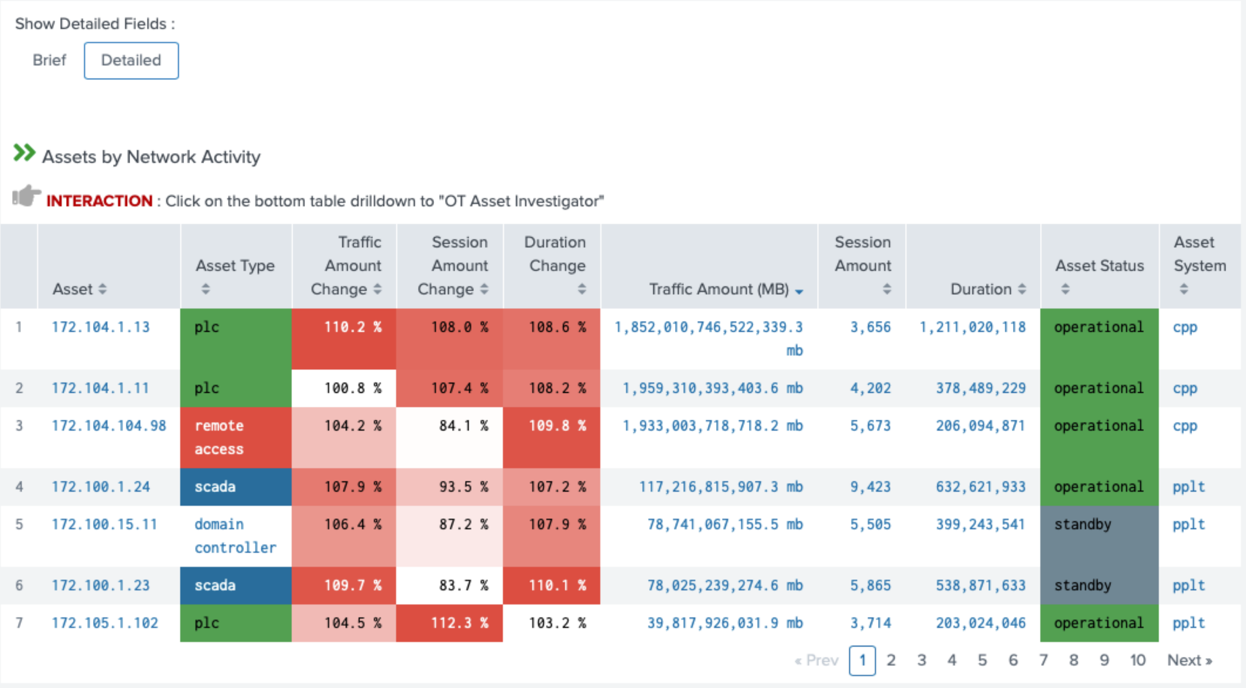
INTERACTION : Click on the bottom table drilldown to "OT Asset Investigator"

	Asset	Asset Type	Traffic Amount Change	Session Amount Change	Duration Change	Asset Status	Asset System
1	173.16.2.37	plc	299.7 %	234.4 %	258.3 %	operational	prod_line_1
2	173.16.1.52	plc	299.7 %	227.9 %	279.2 %	operational	prod_line_2
3	173.16.1.47	plc	299.7 %	228.5 %	254.0 %	operational	prod_line_1
4	173.16.1.96	hmi	299.7 %	240.8 %	270.5 %	operational	prod_line_2
5	173.16.1.74	plc	299.7 %	231.2 %	259.6 %	operational	prod_line_2
6	173.16.2.44	plc	299.7 %	237.7 %	258.7 %	operational	prod_line_2
7	173.16.2.52	plc	299.7 %	212.7 %	258.5 %	operational	prod_line_1

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Network dashboard panels provide both high level and detailed views including the ability to show basic information or more detailed statistical information about the asset. Furthermore, drilling down on an asset allows the security analyst to quickly understand more about the asset in the OT Asset Investigator dashboard.

Assets by Network Activity Detailed Example (OT Security Posture):



Show Detailed Fields :

Assets by Network Activity

INTERACTION : Click on the bottom table drilldown to "OT Asset Investigator"

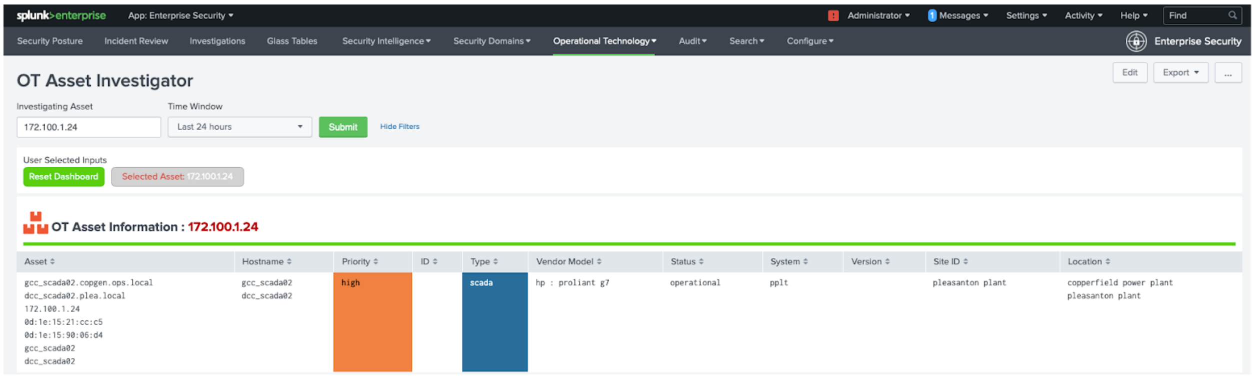
	Asset ⇕	Asset Type ⇕	Traffic Amount Change ⇕	Session Amount Change ⇕	Duration Change ⇕	Traffic Amount (MB) ▾	Session Amount ⇕	Duration ⇕	Asset Status ⇕	Asset System ⇕
1	172.104.1.13	plc	110.2 %	108.0 %	108.6 %	1,852,010,746,522,339.3 mb	3,656	1,211,020,118	operational	cpp
2	172.104.1.11	plc	100.8 %	107.4 %	108.2 %	1,959,310,393,403.6 mb	4,202	378,489,229	operational	cpp
3	172.104.104.98	remote access	104.2 %	84.1 %	109.8 %	1,933,003,718,718.2 mb	5,673	206,094,871	operational	cpp
4	172.100.1.24	scada	107.9 %	93.5 %	107.2 %	117,216,815,907.3 mb	9,423	632,621,933	operational	pplt
5	172.100.15.11	domain controller	106.4 %	87.2 %	107.9 %	78,741,067,155.5 mb	5,505	399,243,541	standby	pplt
6	172.100.1.23	scada	109.7 %	83.7 %	110.1 %	78,025,239,274.6 mb	5,865	538,871,633	standby	pplt
7	172.105.1.102	plc	104.5 %	112.3 %	103.2 %	39,817,926,031.9 mb	3,714	203,024,046	operational	pplt

OT Asset Investigator

The OT Asset Investigator dashboard is designed to provide OT security practitioners with additional context to and understanding of OT asset behavior over time. In addition, the dashboard provides an investigative workflow by presenting meaningful metrics and information that a security practitioner might be able to use for ad-hoc analysis, either for a specific asset or data source.

The dashboard upper section presents information about the asset itself, such as location, operational role, and critical information to determine the priority of the asset relating to a security incident.

OT Asset Details Example (OT Asset Investigator):



OT Asset Investigator

Investigating Asset: 172.100.1.24

Time Window: Last 24 hours

User Selected Inputs

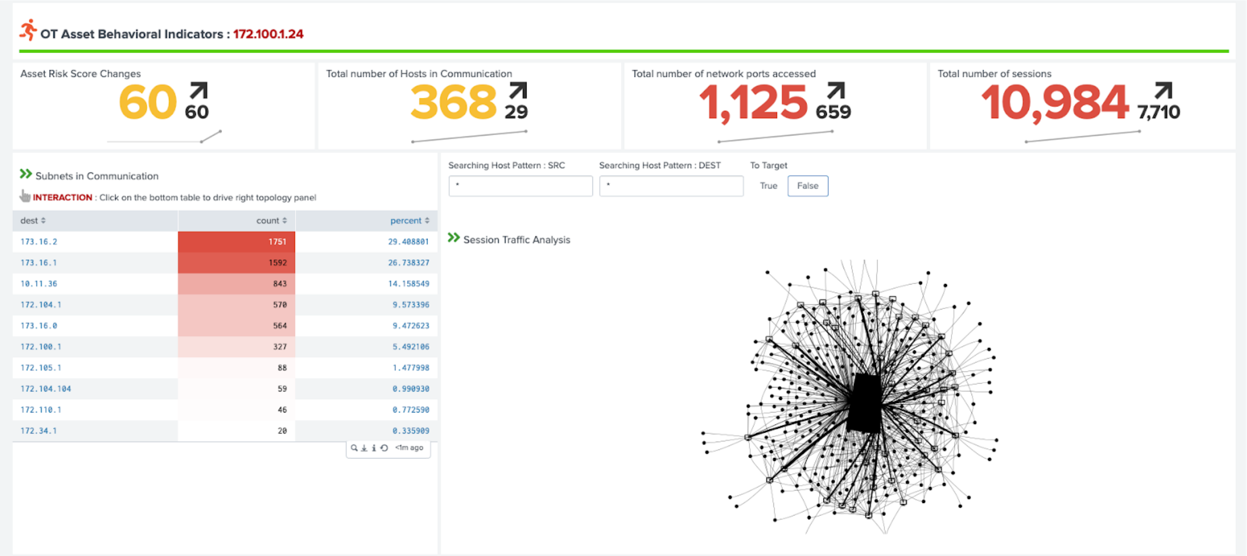
Selected Asset: 172.100.1.24

OT Asset Information : 172.100.1.24

Asset	Hostname	Priority	ID	Type	Vendor Model	Status	System	Version	Site ID	Location
gcc_scada02.copgen.ops.local dcc_scada02.plea.local 172.100.1.24 0d:1e:15:21:cc:c5 0d:1e:15:90:06:d4 gcc_scada02 dcc_scada02	gcc_scada02 dcc_scada02	high		scada	hp : proliant g7	operational	pplt		pleasanton plant	copperfield power plant pleasanton plant

The OT Asset Behavior Indicators provide base metrics on the networking behavior of the selected asset and also visualizes the types of communication with others hosts in the environment. This can prove important when trying to identify for example communication that should not be permitted between subnets. Subnets listed on the left can be clicked on to filter the network communication graph on the right hand side.

OT Asset Behavioral Indicators Example (OT Asset Investigator):



OT Asset Behavioral Indicators : 172.100.1.24

Asset Risk Score Changes	Total number of Hosts in Communication	Total number of network ports accessed	Total number of sessions
60 ↗ 60	368 ↗ 29	1,125 ↗ 659	10,984 ↗ 7,710

Subnets in Communication

INTERACTION : Click on the bottom table to drive right topology panel

dest	count	percent
173.16.2	1751	29.408801
173.16.1	1592	26.738327
10.11.36	843	14.158549
172.104.1	570	9.573396
173.16.0	564	9.472623
172.100.1	327	5.492106
172.105.1	88	1.477998
172.104.104	59	0.990930
172.110.1	46	0.772590
172.34.1	20	0.335909

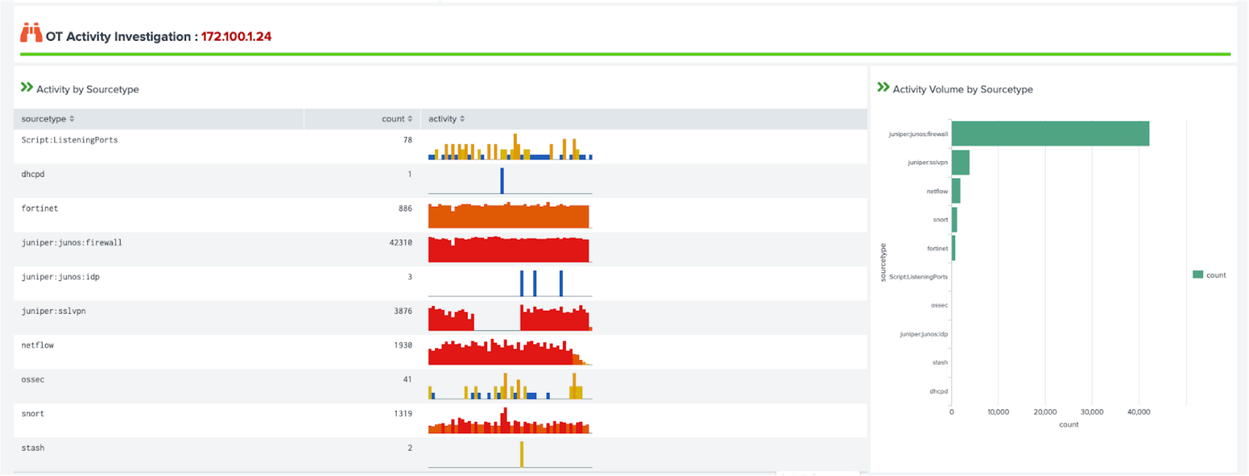
Searching Host Pattern : SRC: *

Searching Host Pattern : DEST: *

To Target: True [✓ False]

The last sections of the dashboards provide information around data sources which contain the selected asset and can help guide analysis to different data sources within Splunk to investigate. By selecting a data source in the bottom panel, analysts can quickly drill down into a Splunk search showing that data source and the asset selected for ad hoc analysis.

OT Datasource Investigation Example (OT Asset Investigator):



OT Activity Investigation : 172.100.1.24

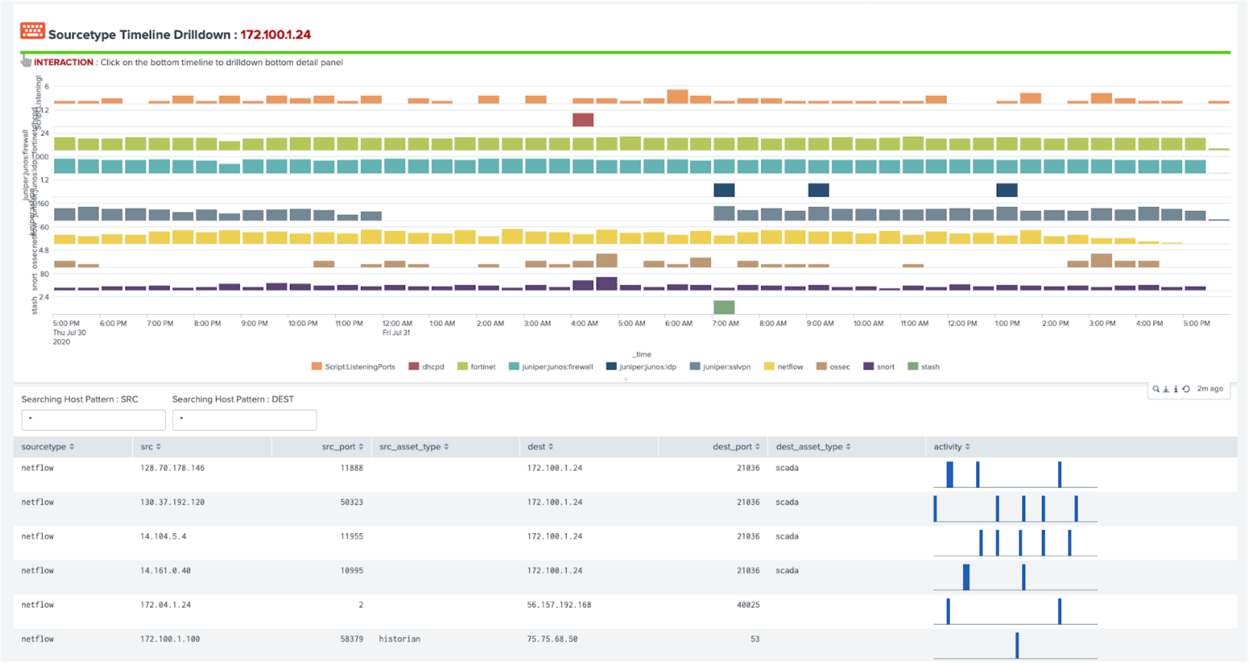
Activity by Sourcetype

sourcetype ⇕	count ⇕	activity ⇕
Script:ListeningPorts	78	
dhcpd	1	
fortinet	886	
juniper:junos:firewall	42310	
juniper:junos:idp	3	
juniper:sslvpn	3876	
netflow	1930	
ossec	41	
snort	1319	
stash	2	

Activity Volume by Sourcetype

The Sourcetype Drilldown allows an analyst to drilldown on specific data sources over time and understand their related fields and without having to rely on raw data. In addition, it shows a more granular timeline of how many events occur for that given data source and the selected asset. For example, using firewall data it becomes possible to understand what hosts are attempting to connect to the asset and whether they are being denied. Similarly it could be used to identify any public subnets the asset may be attempting to connect to and whether the firewall is blocking the suspicious traffic.

Sourcetype Timeline Drilldown Example (OT Asset Investigator):



Sourcetype Timeline Drilldown : 172.100.1.24

INTERACTION : Click on the bottom timeline to drilldown bottom detail panel

Searching Host Pattern : SRC: *

Searching Host Pattern : DEST: *

sourcetype	src	src_port	src_asset_type	dest	dest_port	dest_asset_type	activity
netflow	128.70.178.146	11888		172.100.1.24	21036	scada	
netflow	130.37.192.120	50323		172.100.1.24	21036	scada	
netflow	14.104.5.4	11955		172.100.1.24	21036	scada	
netflow	14.161.0.40	10995		172.100.1.24	21036	scada	
netflow	172.04.1.24	2		56.157.192.168	40025		
netflow	172.100.1.100	58379	historian	75.75.68.50	53		

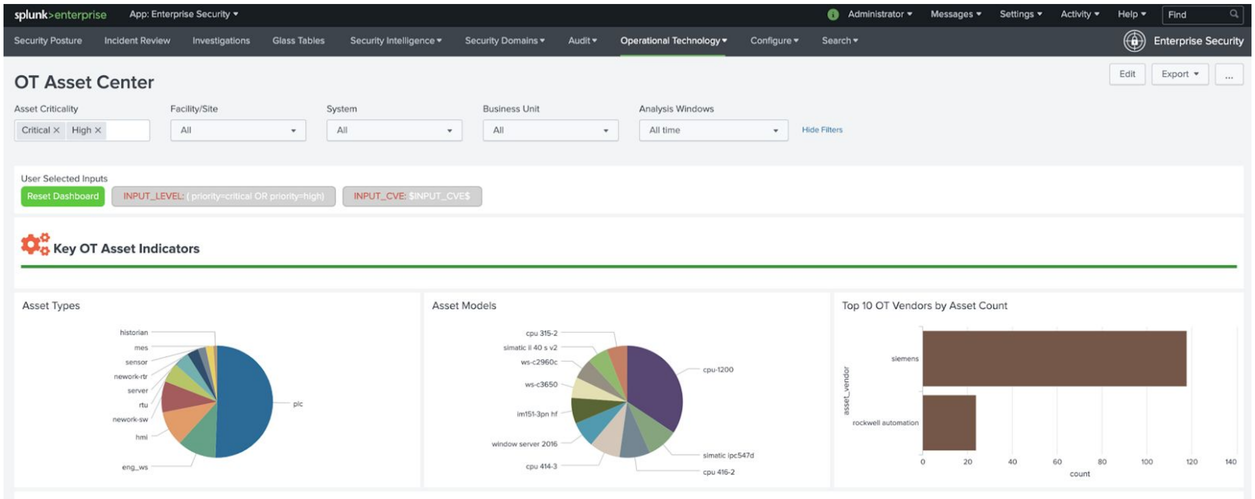
OT Asset Center

The OT Asset Center is designed to provide visibility into OT systems and provide meaningful metrics related to vendors, models, and asset types. Unlike the OT Asset Investigator, this dashboard focuses on the entire environment and not specific assets.

The *Key OT Asset Indicators* section includes key asset metrics and breakdowns by vendor, asset type, and asset model in the environment. This information helps security analysts understand how pervasive a vulnerability might be in their environment and help them to drive efforts to remediate those vulnerabilities.

Additional filters at the top of the dashboard allow panels below to view details for specific sites, systems, or business units.

OT Asset Indicators Example (OT Asset Center):



OT Asset Center

Asset Criticality: Critical × High ×
Facility/Site: All
System: All
Business Unit: All
Analysis Windows: All time

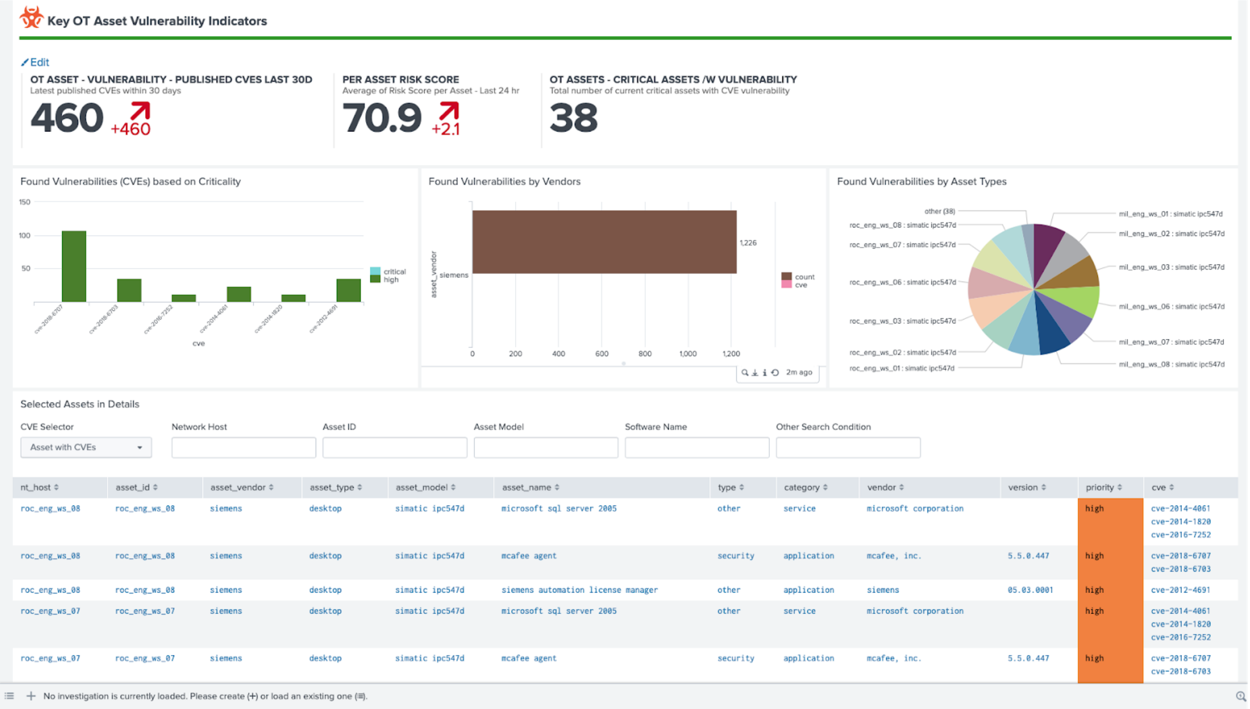
User Selected Inputs

INPUT_LEVEL: (priority=critical OR priority=high)
INPUT_CVE: $INPUT_CVE$

Key OT Asset Indicators

The OT Asset Vulnerability Indicators panels provide metrics on vulnerabilities associated with the assets in the OT environment. It provides what assets have outstanding vulnerabilities and their asset criticality based on user inputs about assets. Additional filters at the top of the dashboard allow panels below to view details for criticalities, specific sites, systems, or business units.

OT Asset Vulnerability Example (OT Asset Center):


Edit
Found Vulnerabilities (CVEs) based on Criticality
150
100
50
cve-2018-6707
cve-2018-6703
cve-2016-7252
cve-2014-4061
cve-2014-1820
cve-2012-4691
cve
critical
high
Found Vulnerabilities by Vendors
asset_vendor
siemens
1,226
count
cve
0
200
400
600
800
1,000
1,200
2m ago
Found Vulnerabilities by Asset Types
other (38)
roc_eng_ws_08 : simatic ipc547d
roc_eng_ws_07 : simatic ipc547d
roc_eng_ws_06 : simatic ipc547d
roc_eng_ws_03 : simatic ipc547d
roc_eng_ws_02 : simatic ipc547d
roc_eng_ws_01 : simatic ipc547d
mil_eng_ws_01 : simatic ipc547d
mil_eng_ws_02 : simatic ipc547d
mil_eng_ws_03 : simatic ipc547d
mil_eng_ws_06 : simatic ipc547d
mil_eng_ws_07 : simatic ipc547d
mil_eng_ws_08 : simatic ipc547d

Key OT Asset Vulnerability Indicators

OT ASSET - VULNERABILITY - PUBLISHED CVES LAST 30D
Latest published CVEs within 30 days
460 ↗ +460

PER ASSET RISK SCORE
Average of Risk Score per Asset - Last 24 hr
70.9 ↗ +2.1

OT ASSETS - CRITICAL ASSETS /W VULNERABILITY
Total number of current critical assets with CVE vulnerability
38

Selected Assets in Details

CVE Selector: Asset with CVEs
Network Host:
Asset ID:
Asset Model:
Software Name:
Other Search Condition:

nt_host	asset_id	asset_vendor	asset_type	asset_model	asset_name	type	category	vendor	version	priority	cve
roc_eng_ws_08	roc_eng_ws_08	siemens	desktop	simatic ipc547d	microsoft sql server 2005	other	service	microsoft corporation		high	cve-2014-4061 cve-2014-1820 cve-2016-7252
roc_eng_ws_08	roc_eng_ws_08	siemens	desktop	simatic ipc547d	mcafee agent	security	application	mcafee, inc.	5.5.0.447	high	cve-2018-6707 cve-2018-6703
roc_eng_ws_08	roc_eng_ws_08	siemens	desktop	simatic ipc547d	siemens automation license manager	other	application	siemens	05.03.0001	high	cve-2012-4691
roc_eng_ws_07	roc_eng_ws_07	siemens	desktop	simatic ipc547d	microsoft sql server 2005	other	service	microsoft corporation		high	cve-2014-4061 cve-2014-1820 cve-2016-7252
roc_eng_ws_07	roc_eng_ws_07	siemens	desktop	simatic ipc547d	mcafee agent	security	application	mcafee, inc.	5.5.0.447	high	cve-2018-6707 cve-2018-6703

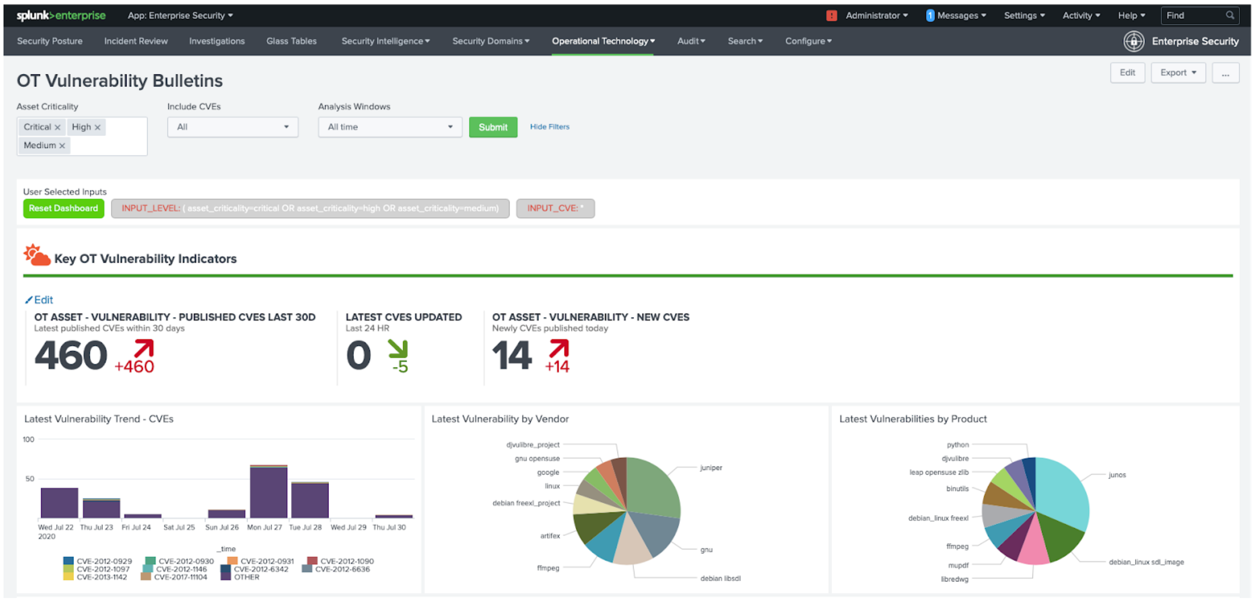
No investigation is currently loaded. Please create (+) or load an existing one (≡).

OT Vulnerability Bulletins

This dashboard is intended to provide a security analyst a method to review the latest vulnerabilities published to the National Vulnerability Database (NVD) for the type of assets in operation at their organization (e.g. Siemens, Rockwell, Schneider, etc). It provides the latest vulnerabilities as well as vulnerabilities published in the past for those same assets.

The *Key OT Vulnerability Indicators* present key asset metrics based on changes in the vulnerabilities published in the NVD.

Key OT Vulnerability Indicators Examples (OT Vulnerability Bulletins):



OT Vulnerability Bulletins

Asset Criticality: Critical × High × Medium ×

Include CVEs: All

Analysis Windows: All time

User Selected Inputs

INPUT_LEVEL: (asset_criticality=critical OR asset_criticality=high OR asset_criticality=medium)

INPUT_CVE: *

Key OT Vulnerability Indicators

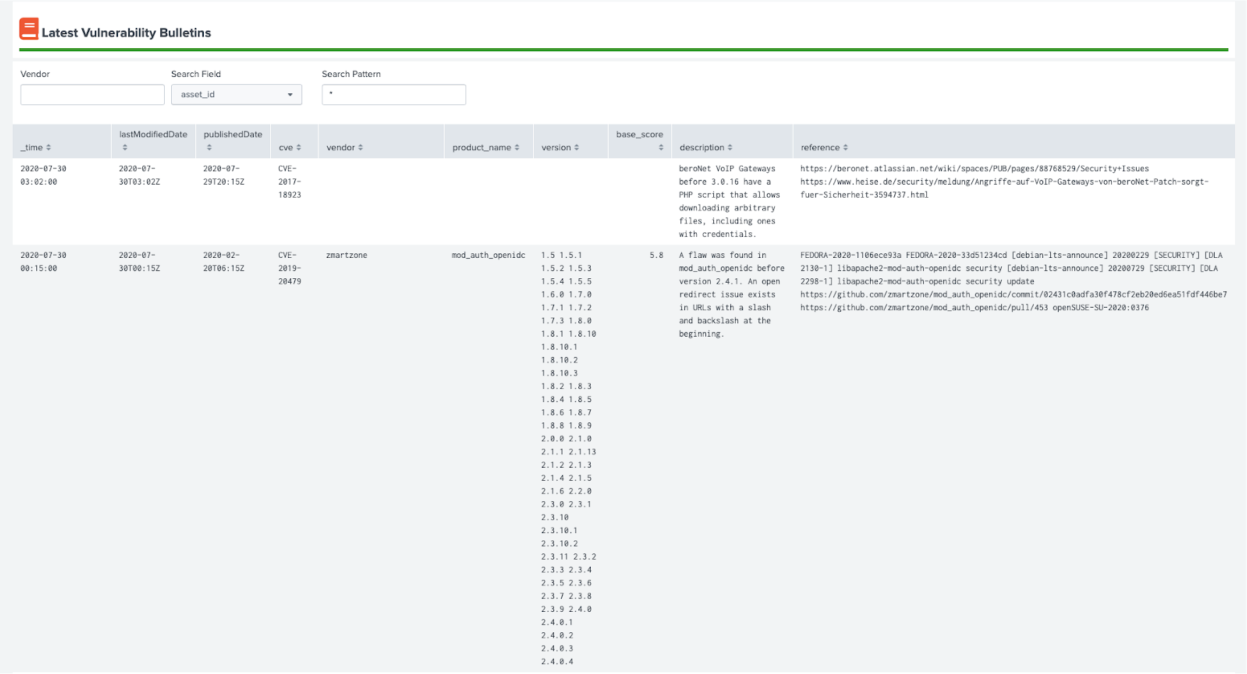
OT ASSET - VULNERABILITY - PUBLISHED CVES LAST 30D
Latest published CVEs within 30 days
460 ↗ +460

LATEST CVES UPDATED
Last 24 HR
0 ↘ -5

OT ASSET - VULNERABILITY - NEW CVES
Newly CVEs published today
14 ↗ +14

The Latest Vulnerability Bulletins section provides detailed descriptions of latest vulnerabilities published to the NVD.

Latest Vulnerability Bulletins Example (OT Vulnerability Bulletins):



Latest Vulnerability Bulletins

Vendor:

Search Field: asset_id

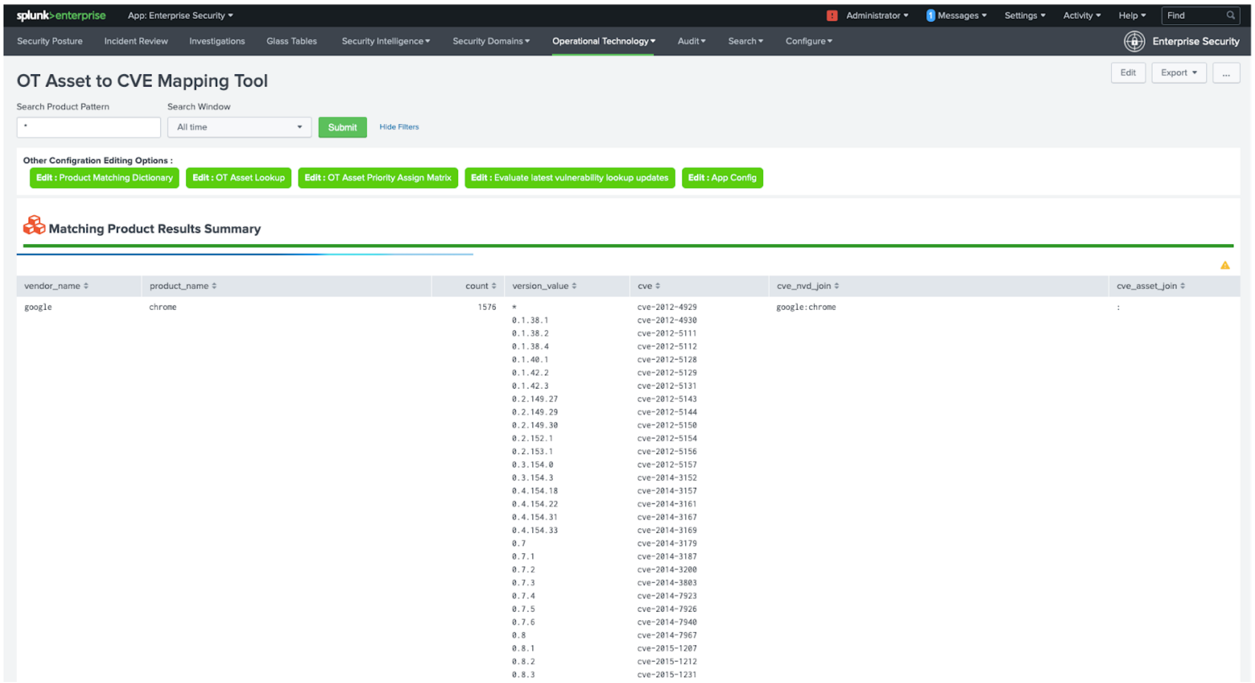
Search Pattern: *

_time	lastModifiedDate	publishedDate	cve	vendor	product_name	version	base_score	description	reference
2020-07-30 03:02:00	2020-07-30T03:02Z	2020-07-29T20:15Z	CVE-2017-18923					beroNet VoIP Gateways before 3.0.16 have a PHP script that allows downloading arbitrary files, including ones with credentials.	https://beronet.atlassian.net/wiki/spaces/PUB/pages/88768529/Security+Issues https://www.heise.de/security/meldung/Angriffe-auf-VoIP-Gateways-von-beroNet-Patch-sorgt-fuer-Sicherheit-3594737.html
2020-07-30 00:15:00	2020-07-30T00:15Z	2020-02-20T06:15Z	CVE-2019-20479	zmartzone	mod_auth_openidc	1.5 1.5.1 1.5.2 1.5.3 1.5.4 1.5.5 1.6.0 1.7.0 1.7.1 1.7.2 1.7.3 1.8.0 1.8.1 1.8.10 1.8.10.1 1.8.10.2 1.8.10.3 1.8.2 1.8.3 1.8.4 1.8.5 1.8.6 1.8.7 1.8.8 1.8.9 2.0.0 2.1.0 2.1.1 2.1.13 2.1.2 2.1.3 2.1.4 2.1.5 2.1.6 2.2.0 2.3.0 2.3.1 2.3.10 2.3.10.1 2.3.10.2 2.3.11 2.3.2 2.3.3 2.3.4 2.3.5 2.3.6 2.3.7 2.3.8 2.3.9 2.4.0 2.4.0.1 2.4.0.2 2.4.0.3 2.4.0.4	5.8	A flaw was found in mod_auth_openidc before version 2.4.1. An open redirect issue exists in URLs with a slash and backslash at the beginning.	FEDORA-2020-1106ece93a FEDORA-2020-33d51234cd [debian-lts-announce] 20200229 [SECURITY] [DLA 2130-1] libapache2-mod-auth-openidc security [debian-lts-announce] 20200729 [SECURITY] [DLA 2298-1] libapache2-mod-auth-openidc security update https://github.com/zmartzone/mod_auth_openidc/commit/02431c0adfa30f478cf2eb20ed6ea51fdf446be7 https://github.com/zmartzone/mod_auth_openidc/pull/453 openSUSE-SU-2020:0376

OT Asset to CVE Mapping Tool

One of the tools including the Splunk for OT Security app, the OT Asset to CVE Mapping Tool provides an easy method for OT security managers to create a dictionary to map internally operating assets to assets from the NVD database. This mapping is important due to various vendor product listings and spellings. For example when querying a device the vendor may be Rockwell, Rockwell Automation, or Rock Automation/Allen Bradley. This dictionary informsmany of the vulnerability dashboards and provides a method to validate existing dictionary mappings.

OT Asset to CVE Mapping Tool Example (OT Asset to CVE Mapping Tool):



OT Asset to CVE Mapping Tool

Search Product Pattern: *

Search Window: All time

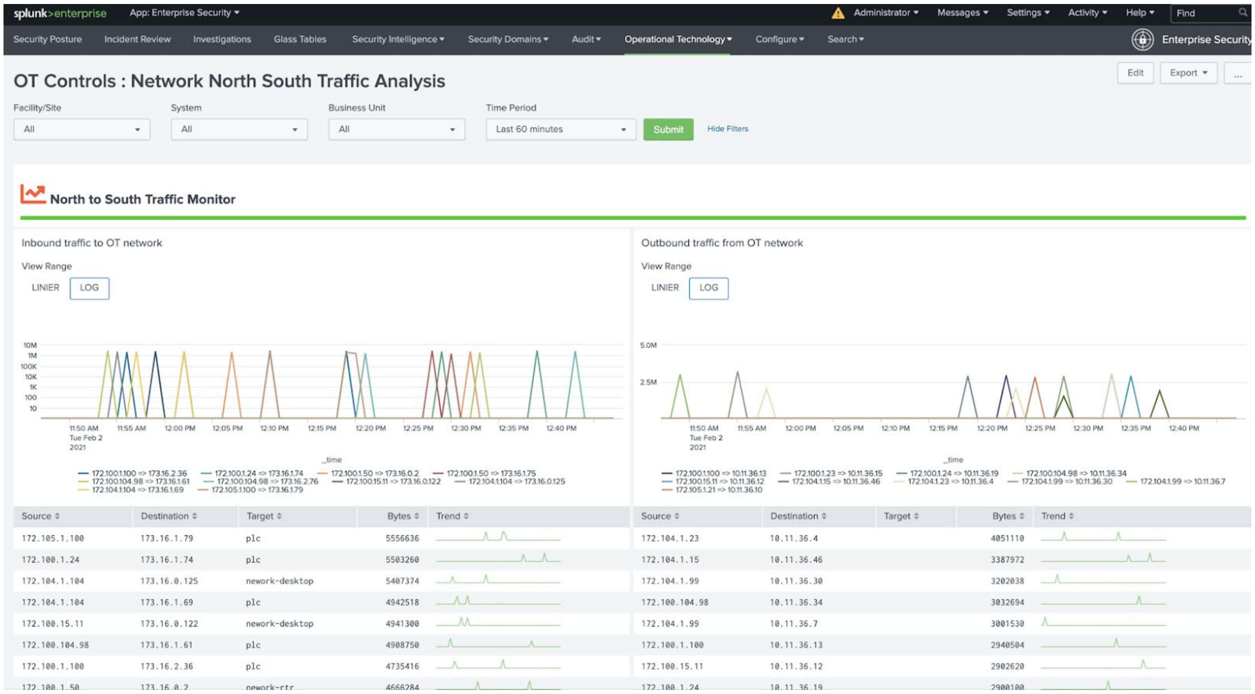
Other Configration Editing Options :

Matching Product Results Summary

vendor_name	product_name	count	version_value	cve	cve_nvd_join	cve_asset_join
google	chrome	1576	* 0.1.38.1 0.1.38.2 0.1.38.4 0.1.40.1 0.1.42.2 0.1.42.3 0.2.149.27 0.2.149.29 0.2.149.30 0.2.152.1 0.2.153.1 0.3.154.0 0.3.154.3 0.4.154.18 0.4.154.22 0.4.154.31 0.4.154.33 0.7 0.7.1 0.7.2 0.7.3 0.7.4 0.7.5 0.7.6 0.8 0.8.1 0.8.2 0.8.3	cve-2012-4929 cve-2012-4930 cve-2012-5111 cve-2012-5112 cve-2012-5128 cve-2012-5129 cve-2012-5131 cve-2012-5143 cve-2012-5144 cve-2012-5150 cve-2012-5154 cve-2012-5156 cve-2012-5157 cve-2014-3152 cve-2014-3157 cve-2014-3161 cve-2014-3167 cve-2014-3169 cve-2014-3179 cve-2014-3187 cve-2014-3200 cve-2014-3803 cve-2014-7923 cve-2014-7926 cve-2014-7940 cve-2014-7967 cve-2015-1207 cve-2015-1212 cve-2015-1231	google:chrome	:

OT Controls: Network North-to-South Traffic Analysis

This dashboard is intended to provide a security analyst a method to review traffic inbound and outbound from their OT environment (commonly called north to south). In most cases firewalls or data diodes represent a boundary into OT environments and traffic across these boundaries is normally restricted. Additional filters at the top of the dashboard allow panels below to view details for specific sites, systems, or business units.



OT Controls : Network North South Traffic Analysis

Facility/Site: All ▾
System: All ▾
Business Unit: All ▾
Time Period: Last 60 minutes ▾

North to South Traffic Monitor

Inbound traffic to OT network

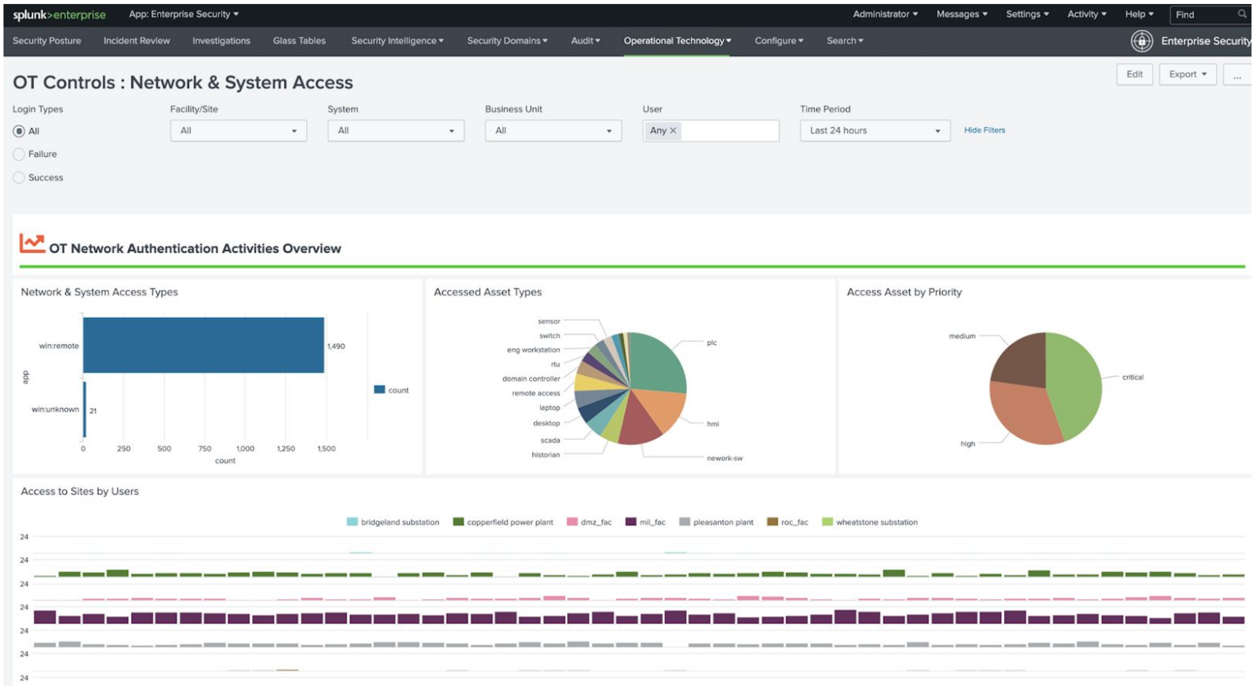
Source ⇕	Destination ⇕	Target ⇕	Bytes ⇕	Trend ⇕
172.105.1.100	173.16.1.79	plc	5556636	
172.100.1.24	173.16.1.74	plc	5503260	
172.104.1.104	173.16.0.125	nework-desktop	5407374	
172.104.1.104	173.16.1.69	plc	4942518	
172.100.15.11	173.16.0.122	nework-desktop	4941300	
172.100.104.98	173.16.1.61	plc	4908750	
172.100.1.100	173.16.2.36	plc	4735416	
172.100.1.50	173.16.0.2	nework-rtr	4666284	

Outbound traffic from OT network

Source ⇕	Destination ⇕	Target ⇕	Bytes ⇕	Trend ⇕
172.104.1.23	10.11.36.4		4051110	
172.104.1.15	10.11.36.46		3387972	
172.104.1.99	10.11.36.30		3202038	
172.100.104.98	10.11.36.34		3032694	
172.104.1.99	10.11.36.7		3001530	
172.100.1.100	10.11.36.13		2940504	
172.100.15.11	10.11.36.12		2902620	
172.100.1.24	10.11.36.19		2900100	

OT Controls: Network & System Access

This dashboard is useful for monitoring remote access to network devices and systems. It highlights common methods to access remote systems such as RDP, SSH, and VNC. It shows how accounts, such as generic accounts are leveraged across different sites (e.g. operator accounts). Additional filters at the top of the dashboard allow panels below to view details for specific sites, systems, or business units.



OT Controls : Network & System Access

Login Types
● All
○ Failure
○ Success

Facility/Site: All ▾
System: All ▾
Business Unit: All ▾
User: Any ×
Time Period: Last 24 hours ▾

OT Network Authentication Activities Overview

Network & System Access Types

Accessed Asset Types

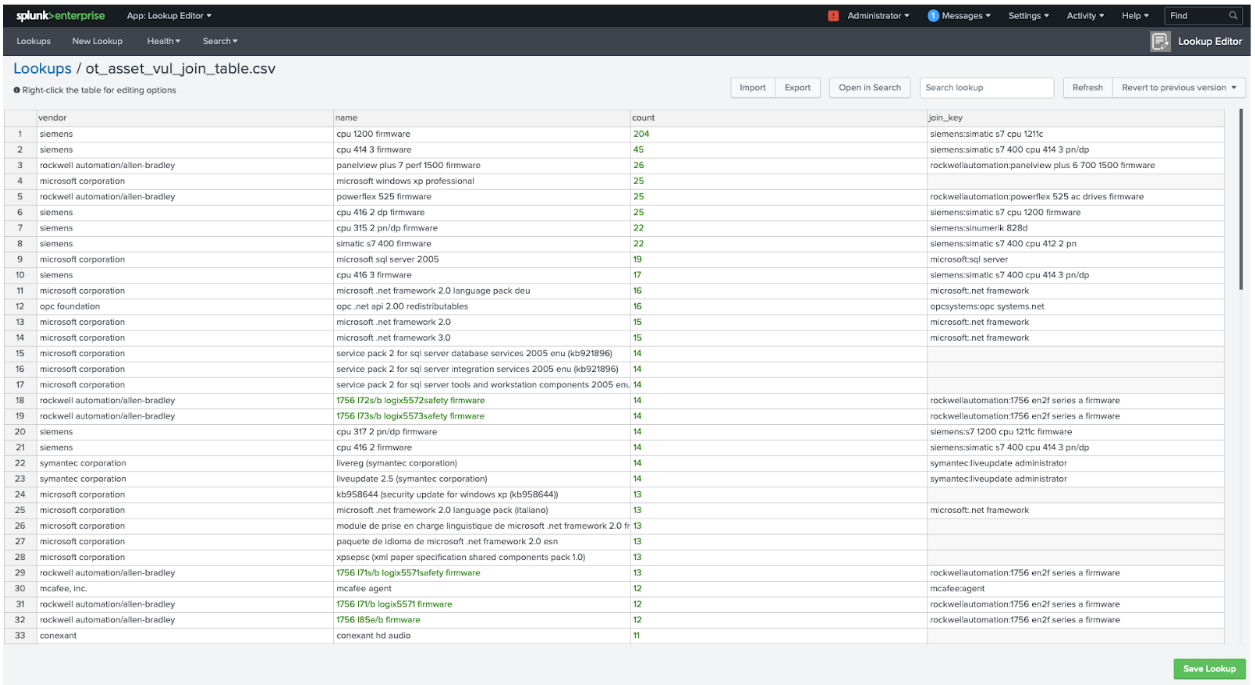
Access Asset by Priority

Access to Sites by Users

Splunk for OT Security Lookups

Various lookup tables are essential for populating dashboards with data. The following sections break down each lookup and its intended purpose.

Lookup name: ot_asset_vulnerability_join_table.csv
This lookup is used to map customer products to the NVD mapped dictionary.



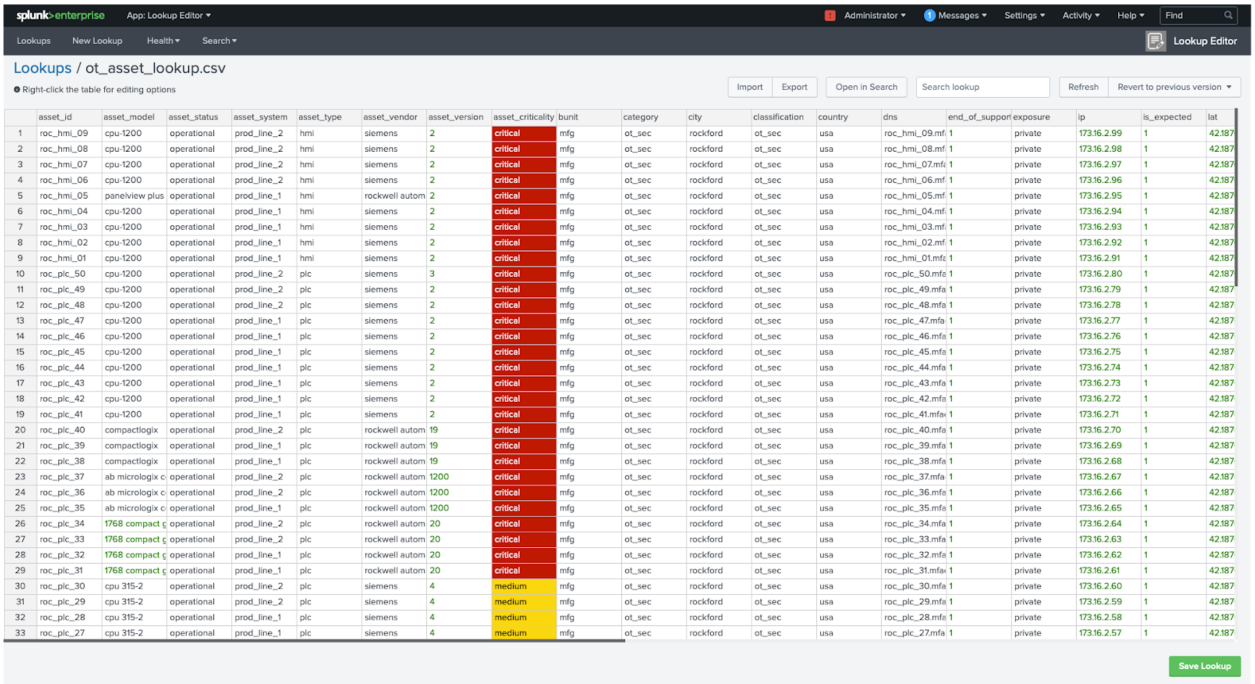
Lookups / ot_asset_vul_join_table.csv

❶ Right-click the table for editing options

	vendor	name	count	join_key
1	siemens	cpu 1200 firmware	204	siemens:simatic s7 cpu 1211c
2	siemens	cpu 414 3 firmware	45	siemens:simatic s7 400 cpu 414 3 pn/dp
3	rockwell automation/allen-bradley	panelview plus 7 perf 1500 firmware	26	rockwellautomation:panelview plus 6 700 1500 firmware
4	microsoft corporation	microsoft windows xp professional	25	
5	rockwell automation/allen-bradley	powerflex 525 firmware	25	rockwellautomation:powerflex 525 ac drives firmware
6	siemens	cpu 416 2 dp firmware	25	siemens:simatic s7 cpu 1200 firmware
7	siemens	cpu 315 2 pn/dp firmware	22	siemens:sinumerik 828d
8	siemens	simatic s7 400 firmware	22	siemens:simatic s7 400 cpu 412 2 pn
9	microsoft corporation	microsoft sql server 2005	19	microsoft:sql server
10	siemens	cpu 416 3 firmware	17	siemens:simatic s7 400 cpu 414 3 pn/dp
11	microsoft corporation	microsoft .net framework 2.0 language pack deu	16	microsoft:.net framework
12	opc foundation	opc .net api 2.00 redistributables	16	opcsystems:opc systems.net
13	microsoft corporation	microsoft .net framework 2.0	15	microsoft:.net framework
14	microsoft corporation	microsoft .net framework 3.0	15	microsoft:.net framework
15	microsoft corporation	service pack 2 for sql server database services 2005 enu (kb921896)	14	
16	microsoft corporation	service pack 2 for sql server integration services 2005 enu (kb921896)	14	
17	microsoft corporation	service pack 2 for sql server tools and workstation components 2005 enu	14	
18	rockwell automation/allen-bradley	1756 l72s/b logix5572safety firmware	14	rockwellautomation:1756 en2f series a firmware
19	rockwell automation/allen-bradley	1756 l73s/b logix5573safety firmware	14	rockwellautomation:1756 en2f series a firmware
20	siemens	cpu 317 2 pn/dp firmware	14	siemens:s7 1200 cpu 1211c firmware
21	siemens	cpu 416 2 firmware	14	siemens:simatic s7 400 cpu 414 3 pn/dp
22	symantec corporation	livereg (symantec corporation)	14	symantec:liveupdate administrator
23	symantec corporation	liveupdate 2.5 (symantec corporation)	14	symantec:liveupdate administrator
24	microsoft corporation	kb958644 (security update for windows xp (kb958644))	13	
25	microsoft corporation	microsoft .net framework 2.0 language pack (italiano)	13	microsoft:.net framework
26	microsoft corporation	module de prise en charge linguistique de microsoft .net framework 2.0 fr	13	
27	microsoft corporation	paquete de idioma de microsoft .net framework 2.0 esn	13	
28	microsoft corporation	xpsepsc (xml paper specification shared components pack 1.0)	13	
29	rockwell automation/allen-bradley	1756 l71s/b logix5571safety firmware	13	rockwellautomation:1756 en2f series a firmware
30	mcafee, inc.	mcafee agent	12	mcafee:agent
31	rockwell automation/allen-bradley	1756 l71/b logix5571 firmware	12	rockwellautomation:1756 en2f series a firmware
32	rockwell automation/allen-bradley	1756 l85e/b firmware	12	rockwellautomation:1756 en2f series a firmware
33	conexant	conexant hd audio	11	

Lookup name: ot_asset_lookup.csv

This lookup table to the main OT asset lookup table that contains all the data about each asset that is security relevant.

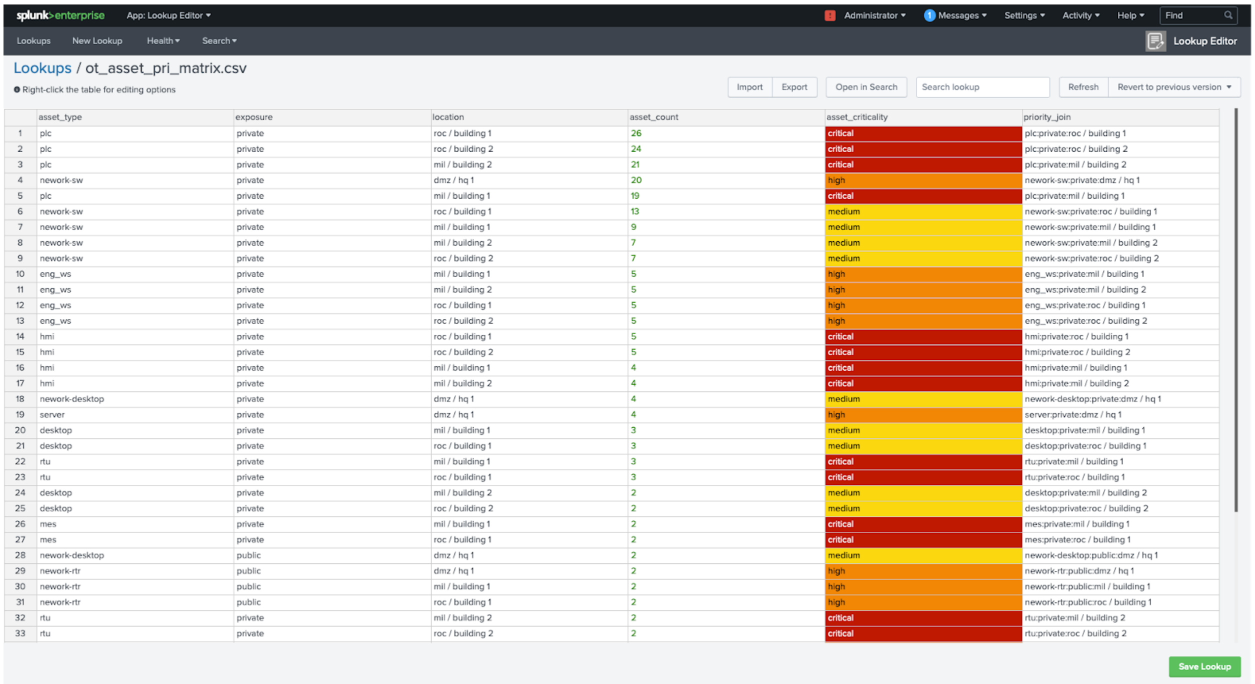


Lookups / ot_asset_lookup.csv

Right-click the table for editing options

	asset_id	asset_model	asset_status	asset_system	asset_type	asset_vendor	asset_version	asset_criticality	bunit	category	city	classification	country	dns	end_of_support	exposure	ip	is_expected	lat
1	roc_hmi_09	cpu-1200	operational	prod_line_2	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_09.mf	1	private	173.16.2.99	1	42.187
2	roc_hmi_08	cpu-1200	operational	prod_line_2	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_08.mf	1	private	173.16.2.98	1	42.187
3	roc_hmi_07	cpu-1200	operational	prod_line_2	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_07.mfa	1	private	173.16.2.97	1	42.187
4	roc_hmi_06	cpu-1200	operational	prod_line_2	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_06.mf	1	private	173.16.2.96	1	42.187
5	roc_hmi_05	panelview plus	operational	prod_line_1	hmi	rockwell autom	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_05.mf	1	private	173.16.2.95	1	42.187
6	roc_hmi_04	cpu-1200	operational	prod_line_1	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_04.mf	1	private	173.16.2.94	1	42.187
7	roc_hmi_03	cpu-1200	operational	prod_line_1	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_03.mf	1	private	173.16.2.93	1	42.187
8	roc_hmi_02	cpu-1200	operational	prod_line_1	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_02.mf	1	private	173.16.2.92	1	42.187
9	roc_hmi_01	cpu-1200	operational	prod_line_1	hmi	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_hmi_01.mfa	1	private	173.16.2.91	1	42.187
10	roc_plc_50	cpu-1200	operational	prod_line_2	plc	siemens	3	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_50.mfa	1	private	173.16.2.80	1	42.187
11	roc_plc_49	cpu-1200	operational	prod_line_2	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_49.mfa	1	private	173.16.2.79	1	42.187
12	roc_plc_48	cpu-1200	operational	prod_line_2	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_48.mfa	1	private	173.16.2.78	1	42.187
13	roc_plc_47	cpu-1200	operational	prod_line_1	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_47.mfa	1	private	173.16.2.77	1	42.187
14	roc_plc_46	cpu-1200	operational	prod_line_1	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_46.mfa	1	private	173.16.2.76	1	42.187
15	roc_plc_45	cpu-1200	operational	prod_line_1	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_45.mfa	1	private	173.16.2.75	1	42.187
16	roc_plc_44	cpu-1200	operational	prod_line_1	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_44.mfa	1	private	173.16.2.74	1	42.187
17	roc_plc_43	cpu-1200	operational	prod_line_1	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_43.mfa	1	private	173.16.2.73	1	42.187
18	roc_plc_42	cpu-1200	operational	prod_line_1	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_42.mfa	1	private	173.16.2.72	1	42.187
19	roc_plc_41	cpu-1200	operational	prod_line_1	plc	siemens	2	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_41.mfa	1	private	173.16.2.71	1	42.187
20	roc_plc_40	compactlogix	operational	prod_line_2	plc	rockwell autom	19	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_40.mfa	1	private	173.16.2.70	1	42.187
21	roc_plc_39	compactlogix	operational	prod_line_1	plc	rockwell autom	19	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_39.mfa	1	private	173.16.2.69	1	42.187
22	roc_plc_38	compactlogix	operational	prod_line_1	plc	rockwell autom	19	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_38.mfa	1	private	173.16.2.68	1	42.187
23	roc_plc_37	ab micrologix c	operational	prod_line_2	plc	rockwell autom	1200	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_37.mfa	1	private	173.16.2.67	1	42.187
24	roc_plc_36	ab micrologix c	operational	prod_line_2	plc	rockwell autom	1200	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_36.mfa	1	private	173.16.2.66	1	42.187
25	roc_plc_35	ab micrologix c	operational	prod_line_1	plc	rockwell autom	1200	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_35.mfa	1	private	173.16.2.65	1	42.187
26	roc_plc_34	1768 compact g	operational	prod_line_2	plc	rockwell autom	20	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_34.mfa	1	private	173.16.2.64	1	42.187
27	roc_plc_33	1768 compact g	operational	prod_line_2	plc	rockwell autom	20	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_33.mfa	1	private	173.16.2.63	1	42.187
28	roc_plc_32	1768 compact g	operational	prod_line_1	plc	rockwell autom	20	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_32.mfa	1	private	173.16.2.62	1	42.187
29	roc_plc_31	1768 compact g	operational	prod_line_1	plc	rockwell autom	20	critical	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_31.mfa	1	private	173.16.2.61	1	42.187
30	roc_plc_30	cpu 315-2	operational	prod_line_2	plc	siemens	4	medium	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_30.mfa	1	private	173.16.2.60	1	42.187
31	roc_plc_29	cpu 315-2	operational	prod_line_2	plc	siemens	4	medium	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_29.mfa	1	private	173.16.2.59	1	42.187
32	roc_plc_28	cpu 315-2	operational	prod_line_1	plc	siemens	4	medium	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_28.mfa	1	private	173.16.2.58	1	42.187
33	roc_plc_27	cpu 315-2	operational	prod_line_1	plc	siemens	4	medium	mfg	ot_sec	rockford	ot_sec	usa	roc_plc_27.mfa	1	private	173.16.2.57	1	42.187

Lookup name: ot_asset_pri_matrix.csv
Decision tree of default asset priority by use of selected attribute entity. The following example, the user chose asset_type, exposure, location as the decision criteria for the default asset priority assignment.



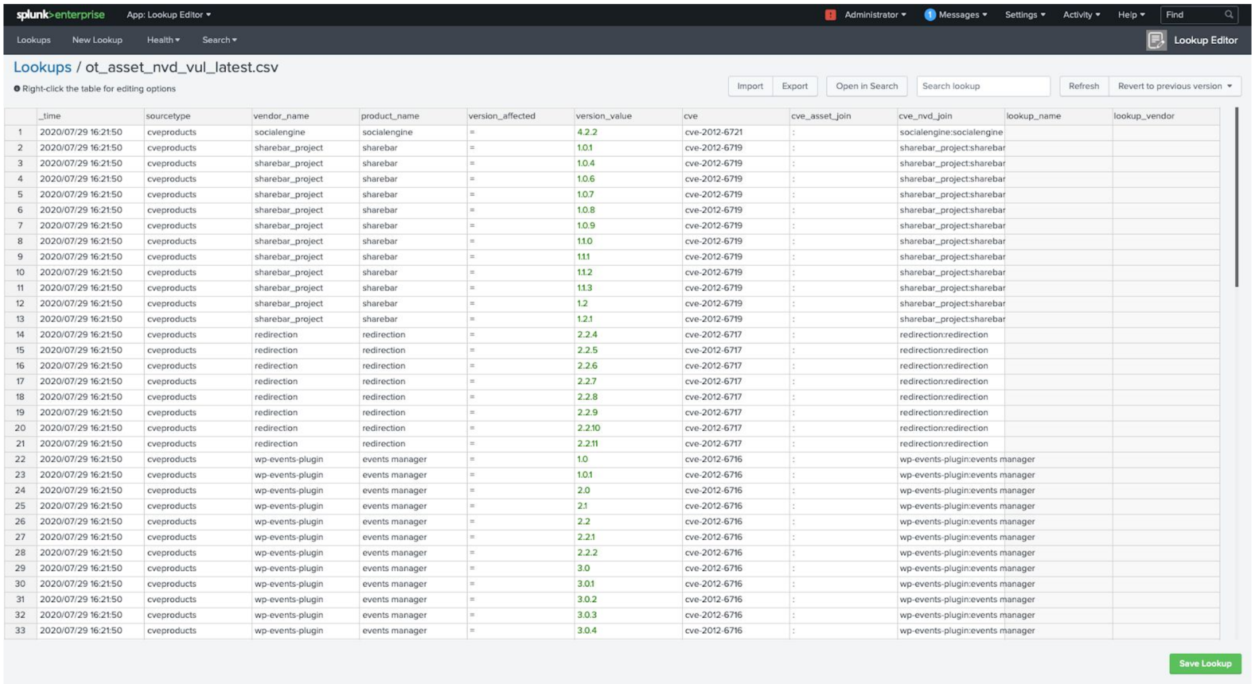
Lookups / ot_asset_pri_matrix.csv

Right-click the table for editing options

	asset_type	exposure	location	asset_count	asset_criticality	priority_join
1	plc	private	roc / building 1	26	critical	plc:private:roc / building 1
2	plc	private	roc / building 2	24	critical	plc:private:roc / building 2
3	plc	private	mil / building 2	21	critical	plc:private:mil / building 2
4	nework-sw	private	dmz / hq 1	20	high	nework-sw:private:dmz / hq 1
5	plc	private	mil / building 1	19	critical	plc:private:mil / building 1
6	nework-sw	private	roc / building 1	13	medium	nework-sw:private:roc / building 1
7	nework-sw	private	mil / building 1	9	medium	nework-sw:private:mil / building 1
8	nework-sw	private	mil / building 2	7	medium	nework-sw:private:mil / building 2
9	nework-sw	private	roc / building 2	7	medium	nework-sw:private:roc / building 2
10	eng_ws	private	mil / building 1	5	high	eng_ws:private:mil / building 1
11	eng_ws	private	mil / building 2	5	high	eng_ws:private:mil / building 2
12	eng_ws	private	roc / building 1	5	high	eng_ws:private:roc / building 1
13	eng_ws	private	roc / building 2	5	high	eng_ws:private:roc / building 2
14	hmi	private	roc / building 1	5	critical	hmi:private:roc / building 1
15	hmi	private	roc / building 2	5	critical	hmi:private:roc / building 2
16	hmi	private	mil / building 1	4	critical	hmi:private:mil / building 1
17	hmi	private	mil / building 2	4	critical	hmi:private:mil / building 2
18	nework-desktop	private	dmz / hq 1	4	medium	nework-desktop:private:dmz / hq 1
19	server	private	dmz / hq 1	4	high	server:private:dmz / hq 1
20	desktop	private	mil / building 1	3	medium	desktop:private:mil / building 1
21	desktop	private	roc / building 1	3	medium	desktop:private:roc / building 1
22	rtu	private	mil / building 1	3	critical	rtu:private:mil / building 1
23	rtu	private	roc / building 1	3	critical	rtu:private:roc / building 1
24	desktop	private	mil / building 2	2	medium	desktop:private:mil / building 2
25	desktop	private	roc / building 2	2	medium	desktop:private:roc / building 2
26	mes	private	mil / building 1	2	critical	mes:private:mil / building 1
27	mes	private	roc / building 1	2	critical	mes:private:roc / building 1
28	nework-desktop	public	dmz / hq 1	2	medium	nework-desktop:public:dmz / hq 1
29	nework-rtr	public	dmz / hq 1	2	high	nework-rtr:public:dmz / hq 1
30	nework-rtr	public	mil / building 1	2	high	nework-rtr:public:mil / building 1
31	nework-rtr	public	roc / building 1	2	high	nework-rtr:public:roc / building 1
32	rtu	private	mil / building 2	2	critical	rtu:private:mil / building 2
33	rtu	private	roc / building 2	2	critical	rtu:private:roc / building 2

Lookup name: ot_asset_nvd_vul_latest.csv

This lookup contains the results of processed vulnerability data processes with product match using the custom dictionary.



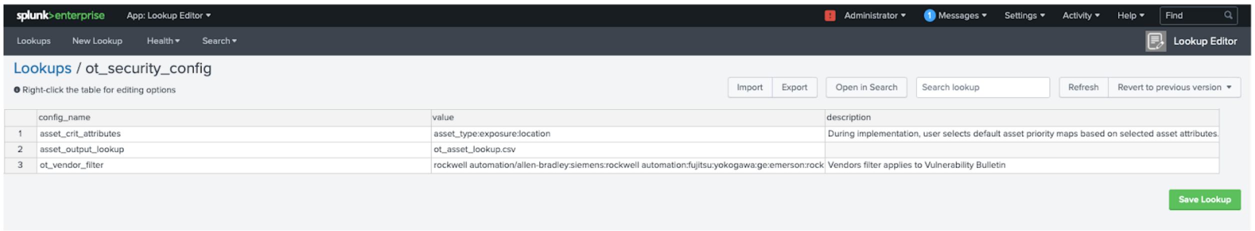
Lookups / ot_asset_nvd_vul_latest.csv

● Right-click the table for editing options

	_time	sourcetype	vendor_name	product_name	version_affected	version_value	cve	cve_asset_join	cve_nvd_join	lookup_name	lookup_vendor
1	2020/07/29 16:21:50	cveproducts	socialengine	socialengine	=	4.2.2	cve-2012-6721	:	socialengine:socialengine		
2	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.0.1	cve-2012-6719	:	sharebar_project:sharebar		
3	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.0.4	cve-2012-6719	:	sharebar_project:sharebar		
4	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.0.6	cve-2012-6719	:	sharebar_project:sharebar		
5	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.0.7	cve-2012-6719	:	sharebar_project:sharebar		
6	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.0.8	cve-2012-6719	:	sharebar_project:sharebar		
7	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.0.9	cve-2012-6719	:	sharebar_project:sharebar		
8	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.1.0	cve-2012-6719	:	sharebar_project:sharebar		
9	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.1.1	cve-2012-6719	:	sharebar_project:sharebar		
10	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.1.2	cve-2012-6719	:	sharebar_project:sharebar		
11	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.1.3	cve-2012-6719	:	sharebar_project:sharebar		
12	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.2	cve-2012-6719	:	sharebar_project:sharebar		
13	2020/07/29 16:21:50	cveproducts	sharebar_project	sharebar	=	1.2.1	cve-2012-6719	:	sharebar_project:sharebar		
14	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.4	cve-2012-6717	:	redirection:redirection		
15	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.5	cve-2012-6717	:	redirection:redirection		
16	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.6	cve-2012-6717	:	redirection:redirection		
17	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.7	cve-2012-6717	:	redirection:redirection		
18	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.8	cve-2012-6717	:	redirection:redirection		
19	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.9	cve-2012-6717	:	redirection:redirection		
20	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.10	cve-2012-6717	:	redirection:redirection		
21	2020/07/29 16:21:50	cveproducts	redirection	redirection	=	2.2.11	cve-2012-6717	:	redirection:redirection		
22	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	1.0	cve-2012-6716	:	wp-events-plugin:events manager		
23	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	1.0.1	cve-2012-6716	:	wp-events-plugin:events manager		
24	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	2.0	cve-2012-6716	:	wp-events-plugin:events manager		
25	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	2.1	cve-2012-6716	:	wp-events-plugin:events manager		
26	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	2.2	cve-2012-6716	:	wp-events-plugin:events manager		
27	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	2.2.1	cve-2012-6716	:	wp-events-plugin:events manager		
28	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	2.2.2	cve-2012-6716	:	wp-events-plugin:events manager		
29	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	3.0	cve-2012-6716	:	wp-events-plugin:events manager		
30	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	3.0.1	cve-2012-6716	:	wp-events-plugin:events manager		
31	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	3.0.2	cve-2012-6716	:	wp-events-plugin:events manager		
32	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	3.0.3	cve-2012-6716	:	wp-events-plugin:events manager		
33	2020/07/29 16:21:50	cveproducts	wp-events-plugin	events manager	=	3.0.4	cve-2012-6716	:	wp-events-plugin:events manager		

Lookup name: ot_security_config

Extensible app configuration file used through the app for specific components of the app.

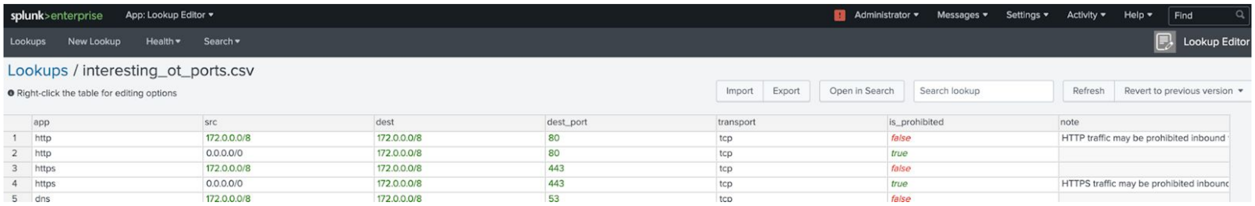


Lookups / ot_security_config

● Right-click the table for editing options

	config_name	value	description
1	asset_crit_attributes	asset_type:exposure:location	During implementation, user selects default asset priority maps based on selected asset attributes.
2	asset_output_lookup	ot_asset_lookup.csv	
3	ot_vendor_filter	rockwell automation/allen-bradley:siemens:rockwell automation:fujitsu:yokogawa:ge:emerson:rock	Vendors filter applies to Vulnerability Bulletin

Lookup name: interesting_ot_ports.csv
This lookup is used to label port activity that should and should not be permitted across security boundaries. For example, ports 80 and 443 are often prohibited between OT environments and public networks is typically prohibited, but may be permitted between specific IP's on a company's corporate network. CIDR ranges can be used to designate particular network segments for src and dest networks.

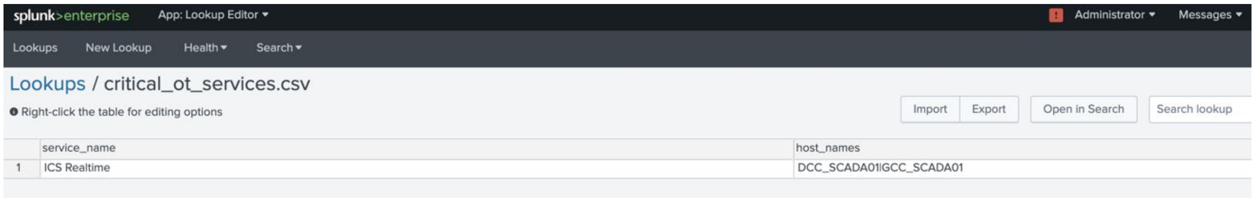


Lookups / interesting_ot_ports.csv

❶ Right-click the table for editing options

	app	src	dest	dest_port	transport	is_prohibited	note
1	http	172.0.0.0/8	172.0.0.0/8	80	tcp	false	HTTP traffic may be prohibited inbound
2	http	0.0.0.0/0	172.0.0.0/8	80	tcp	true	
3	https	172.0.0.0/8	172.0.0.0/8	443	tcp	false	
4	https	0.0.0.0/0	172.0.0.0/8	443	tcp	true	HTTPS traffic may be prohibited inbounc
5	dns	172.0.0.0/8	172.0.0.0/8	53	tcp	false	

Lookup name: critical_ot_services.csv
This lookup is used to identify critical services which require notification or may result in loss of operations. One of the MITRE ICS rules requires identifying when critical services have been stopped. The name of the service should match the service name by the operating system. Additional host names or wildcards can be used in the host_names column.



Lookups / critical_ot_services.csv

❶ Right-click the table for editing options

	service_name	host_names
1	ICS Realtime	DCC_SCADA01|GCC_SCADA01

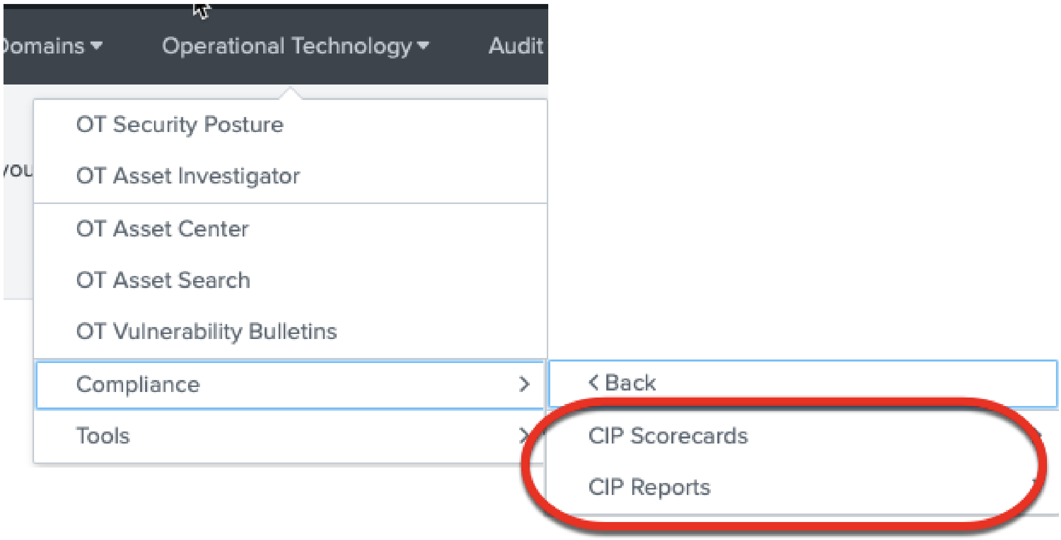
NERC CIP

Overview

The Splunk for OT Security CIP components are meant to help automate CIP investigations and reports that are mandated by NERC. This focus is reflected in how the Scorecards and Reports are organized and how they are populated. Whenever possible, they leverage Splunk's Common Information and Enterprise Security's Asset framework to make implementation easier and faster for organizations.

NERC CIP: Scorecards and Reports

The NERC CIP components of Splunk for OT Security are broken into two main categories: Scorecards and Reports. Navigation in the app is differentiate between the two as shown here:



All Scorecards and Reports are grouped together under CIP Numbers (e.g. CIP 002, 004, etc) to help organizations quickly navigate between the various requirements; however, there are differences between the two that are important to understand when using them for reporting purposes.

Scorecards are a collection of CIP Requirements (R2, R4, etc) for each area. They are **not** prefiltered for reporting purposes to auditors, but allow organizations to understand their overall posture and state and maximize flexibility when needing to investigate potential issues.

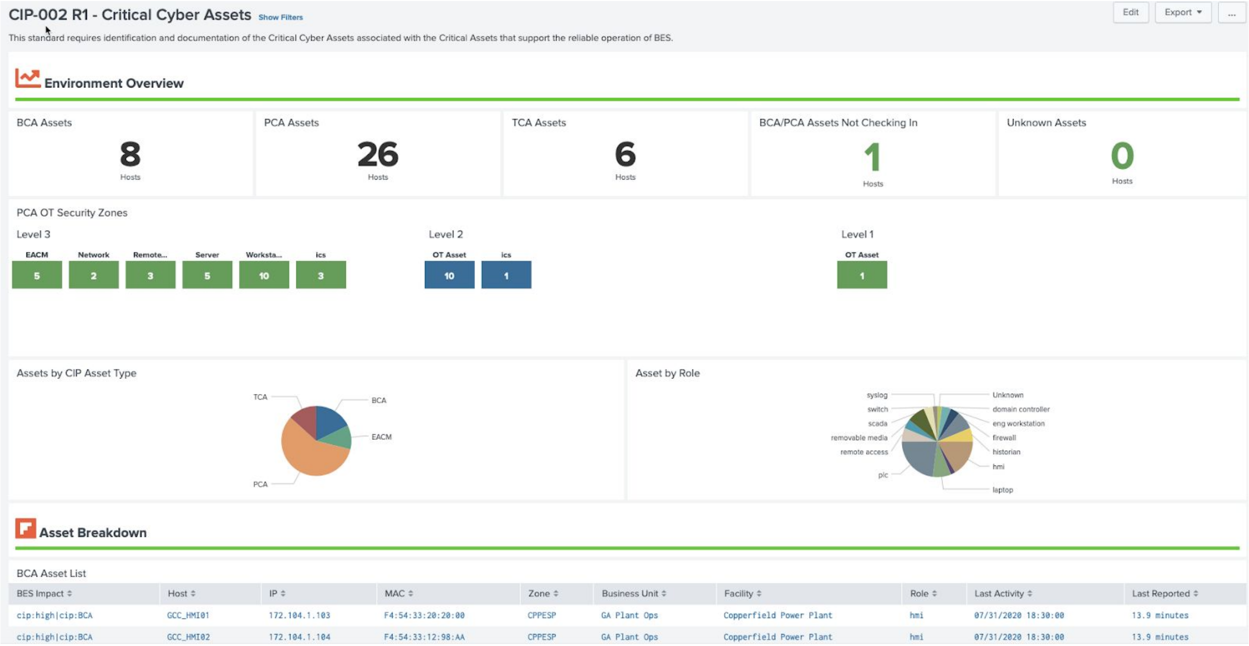
Reports are specific to CIP Requirements and thus more granular than reports. In addition, reports are **pre-filtered** based on the NERC CIP requirements and are designed to be used as input for an audit (although depending on an auditor's request may need additional filtering).

The following section breaks down the Scorecards and Reports by their major classifications:

NERC CIP 002: Critical Cyber Assets

NERC CIP requires assets to be classified and broken down by specific classifications and security zones. The classifications require an asset to be assigned a CIP criticality as well as CIP asset type. CIP specifically explicitly defines criticality as Low, Medium, or High and has numerous asset types (BCA, PCA, EAP are all examples). In addition, typically at a site level an asset will be assigned to a CIP asset zone, although Splunk does not explicitly make that mandatory. The Critical Cyber Asset Scorecard provides a customer to method to understand all the assets in their environment. As a result, assets should be tagged with these fields as explained in the Section 3. If these assets are tagged appropriately they will show up CIP 002 Scorecards and Reports automatically.

Critical Cyber Assets Example (CIP 002 R1):



CIP-002 R1 - Critical Cyber Assets

This standard requires identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of BES.

Environment Overview

BCA Assets	PCA Assets	TCA Assets	BCA/PCA Assets Not Checking In	Unknown Assets
8 Hosts	26 Hosts	6 Hosts	1 Hosts	0 Hosts

PCA OT Security Zones

Level 3

EACM	Network	Remote...	Server	Worksta...	ics
5	2	3	5	10	3

Level 2

OT Asset	ics
10	1

Level 1

OT Asset
1

Assets by CIP Asset Type

Asset by Role

Asset Breakdown

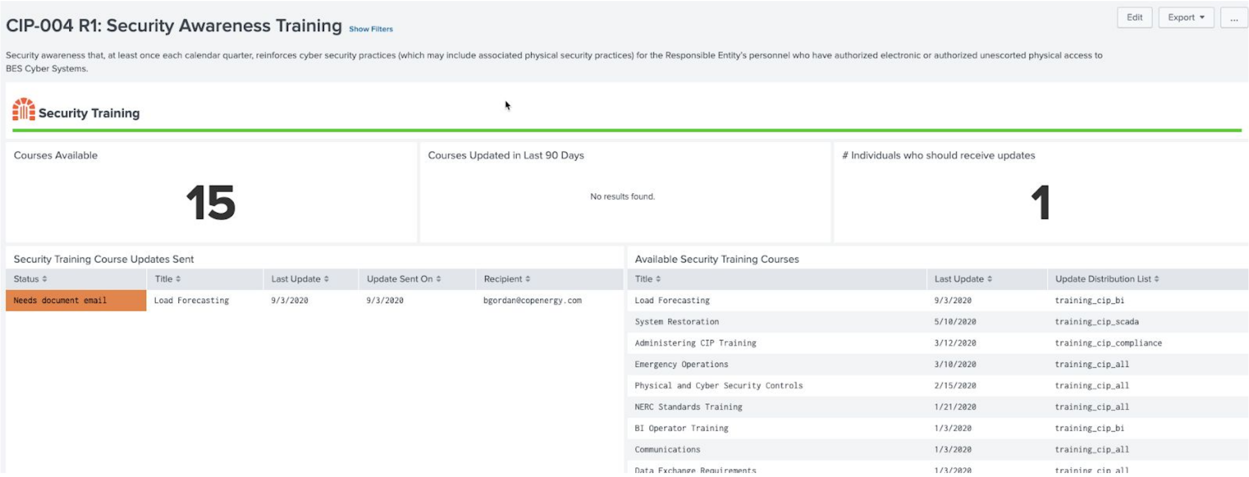
BCA Asset List

BES Impact ⇕	Host ⇕	IP ⇕	MAC ⇕	Zone ⇕	Business Unit ⇕	Facility ⇕	Role ⇕	Last Activity ⇕	Last Reported ⇕
cip:high|cip:BCA	GCC_HMI01	172.104.1.103	F4:54:33:20:20:00	CPPESP	GA Plant Ops	Copperfield Power Plant	hmi	07/31/2020 18:30:00	13.9 minutes
cip:high|cip:BCA	GCC_HMI02	172.104.1.104	F4:54:33:12:98:AA	CPPESP	GA Plant Ops	Copperfield Power Plant	hmi	07/31/2020 18:30:00	13.9 minutes

NERC CIP 004: Security Awareness Training

NERC CIP requires that users and operators in regulated environments complete specific training as part of the certification process. For users who require certification, they must be classified into groups which determine which training is required. In addition, updates to course materials should be communicated to individuals who have previously taken this training (normally via email). The email data model is used to identify whether notifications have been received.

Security Awareness Training Example (CIP 004 R1):



CIP-004 R1: Security Awareness Training

Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.

Security Training

Courses Available	Courses Updated in Last 90 Days	# Individuals who should receive updates
15	No results found.	1

Security Training Course Updates Sent

Status ⇕	Title ⇕	Last Update ⇕	Update Sent On ⇕	Recipient ⇕
Needs document email	Load Forecasting	9/3/2020	9/3/2020	bgordan@copenergy.com

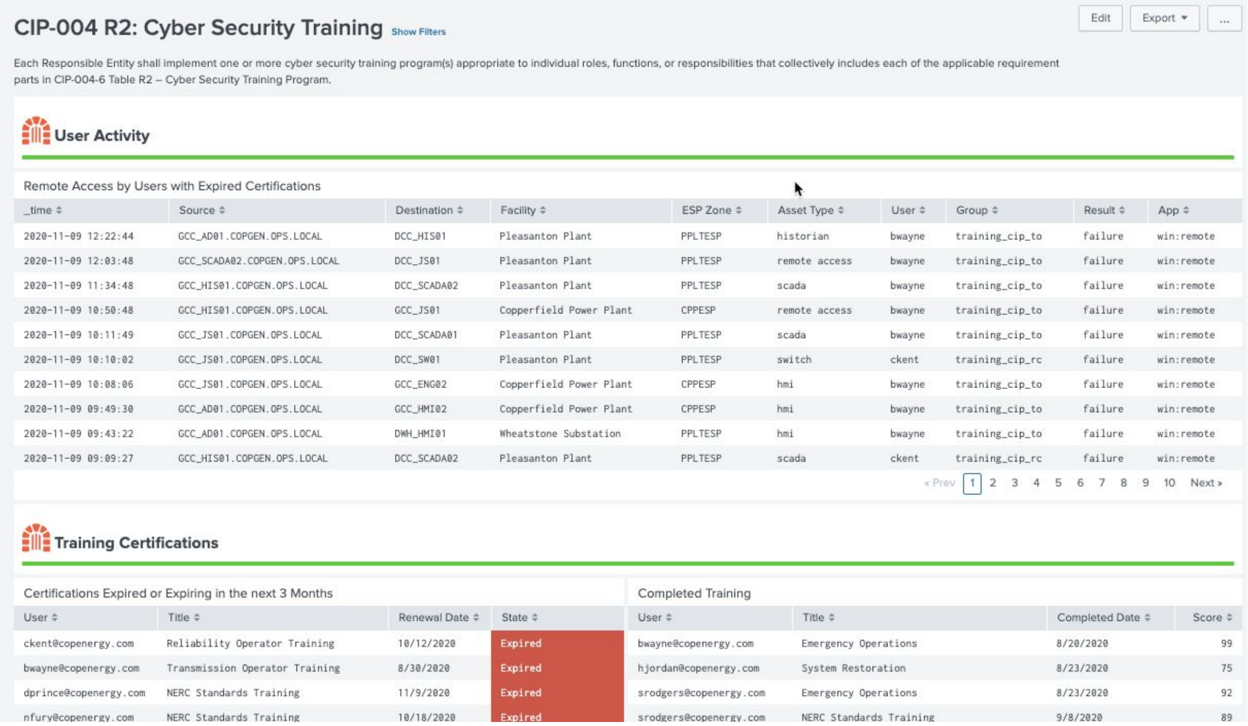
Available Security Training Courses

Title ⇕	Last Update ⇕	Update Distribution List ⇕
Load Forecasting	9/3/2020	training_cip_bi
System Restoration	5/10/2020	training_cip_scada
Administering CIP Training	3/12/2020	training_cip_compliance
Emergency Operations	3/10/2020	training_cip_all
Physical and Cyber Security Controls	2/15/2020	training_cip_all
NERC Standards Training	1/21/2020	training_cip_all
BI Operator Training	1/3/2020	training_cip_bi
Communications	1/3/2020	training_cip_all
Data Exchange Requirements	1/3/2020	training_cip_all

NERC CIP 004: Cyber Security Training

Individuals accessing NERC CIP environments must be trained and certified before accessing assets within NERC CIP environments, remotely, onsite, or physically. NERC CIP requires that training requirements be tracked and monitored for expired certifications and then correlated with access records. This dashboard makes use of the authentication data model to track to determine remote or local access to systems by individuals required to be NERC CIP certified.

Cyber Security Training Example (CIP 004 R2):



CIP-004 R2: Cyber Security Training Show Filters

Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program.

User Activity

Remote Access by Users with Expired Certifications

_time ⇕	Source ⇕	Destination ⇕	Facility ⇕	ESP Zone ⇕	Asset Type ⇕	User ⇕	Group ⇕	Result ⇕	App ⇕
2020-11-09 12:22:44	GCC_AD01.COPGEN.OPS.LOCAL	DCC_HIS01	Pleasanton Plant	PPLTESP	historian	bwayne	training_cip_to	failure	win:remote
2020-11-09 12:03:48	GCC_SCADA02.COPGEN.OPS.LOCAL	DCC_JS01	Pleasanton Plant	PPLTESP	remote access	bwayne	training_cip_to	failure	win:remote
2020-11-09 11:34:48	GCC_HIS01.COPGEN.OPS.LOCAL	DCC_SCADA02	Pleasanton Plant	PPLTESP	scada	bwayne	training_cip_to	failure	win:remote
2020-11-09 10:50:48	GCC_HIS01.COPGEN.OPS.LOCAL	GCC_JS01	Copperfield Power Plant	CPPESP	remote access	bwayne	training_cip_to	failure	win:remote
2020-11-09 10:11:49	GCC_JS01.COPGEN.OPS.LOCAL	DCC_SCADA01	Pleasanton Plant	PPLTESP	scada	bwayne	training_cip_to	failure	win:remote
2020-11-09 10:10:02	GCC_JS01.COPGEN.OPS.LOCAL	DCC_SW01	Pleasanton Plant	PPLTESP	switch	ckent	training_cip_rc	failure	win:remote
2020-11-09 10:08:06	GCC_JS01.COPGEN.OPS.LOCAL	GCC_ENG02	Copperfield Power Plant	CPPESP	hmi	bwayne	training_cip_to	failure	win:remote
2020-11-09 09:49:30	GCC_AD01.COPGEN.OPS.LOCAL	GCC_HMI02	Copperfield Power Plant	CPPESP	hmi	bwayne	training_cip_to	failure	win:remote
2020-11-09 09:43:22	GCC_AD01.COPGEN.OPS.LOCAL	DWH_HMI01	Wheatstone Substation	PPLTESP	hmi	bwayne	training_cip_to	failure	win:remote
2020-11-09 09:09:27	GCC_HIS01.COPGEN.OPS.LOCAL	DCC_SCADA02	Pleasanton Plant	PPLTESP	scada	ckent	training_cip_rc	failure	win:remote

Training Certifications

Certifications Expired or Expiring in the next 3 Months

User ⇕	Title ⇕	Renewal Date ⇕	State ⇕
ckent@copenergy.com	Reliability Operator Training	10/12/2020	Expired
bwayne@copenergy.com	Transmission Operator Training	8/30/2020	Expired
dprince@copenergy.com	NERC Standards Training	11/9/2020	Expired
nfury@copenergy.com	NERC Standards Training	10/18/2020	Expired

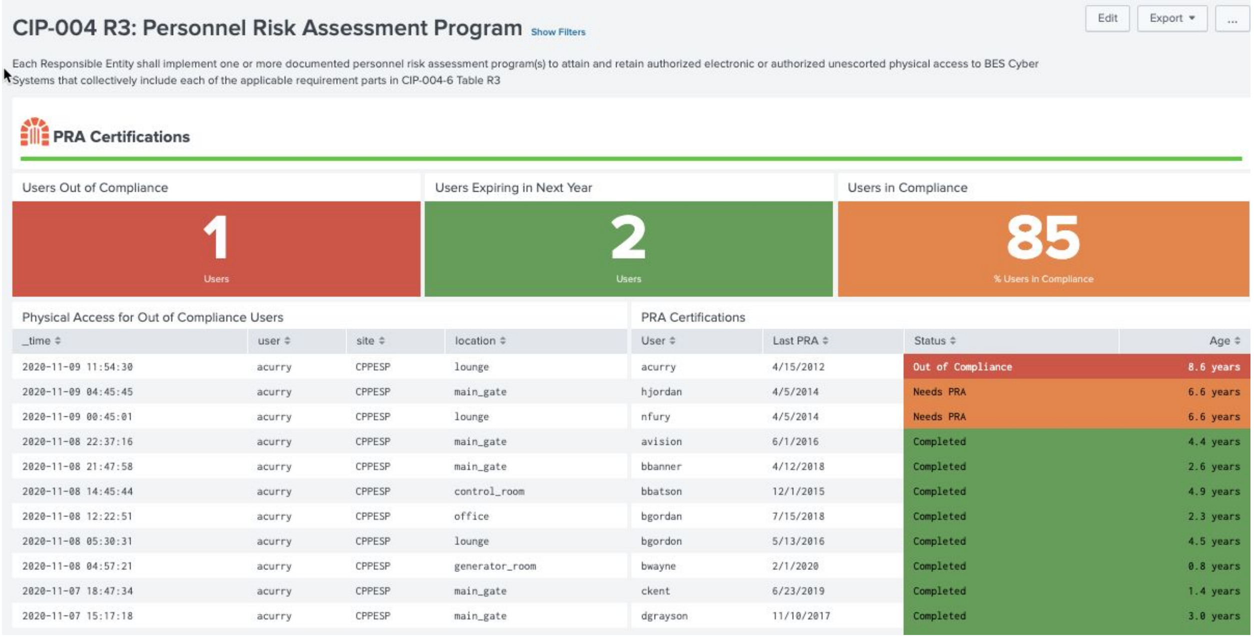
Completed Training

User ⇕	Title ⇕	Completed Date ⇕	Score ⇕
bwayne@copenergy.com	Emergency Operations	8/20/2020	99
hjordan@copenergy.com	System Restoration	8/23/2020	75
srodgers@copenergy.com	Emergency Operations	8/23/2020	92
srodgers@copenergy.com	NERC Standards Training	9/8/2020	89

NERC CIP 004: Personnel Risk Assessment (PRA) Program

Individuals accessing NERC CIP environments must periodically have personnel risk assessments (PRA) performed not to exceed every 15 months. This certification may be performed by outside entities, but should be tracked and recorded by operators of NERC CIP assets. In addition, access to NERC CIP environments should be monitored for individuals out of compliance.

Cyber Security Training Example (CIP 004 R3):



CIP-004 R3: Personnel Risk Assessment Program

Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3

PRA Certifications

Users Out of Compliance	Users Expiring in Next Year	Users in Compliance
1 Users	2 Users	85 % Users in Compliance

Physical Access for Out of Compliance Users

_time	user	site	location
2020-11-09 11:54:30	acurry	CPPESP	lounge
2020-11-09 04:45:45	acurry	CPPESP	main_gate
2020-11-09 00:45:01	acurry	CPPESP	lounge
2020-11-08 22:37:16	acurry	CPPESP	main_gate
2020-11-08 21:47:58	acurry	CPPESP	main_gate
2020-11-08 14:45:44	acurry	CPPESP	control_room
2020-11-08 12:22:51	acurry	CPPESP	office
2020-11-08 05:30:31	acurry	CPPESP	lounge
2020-11-08 04:57:21	acurry	CPPESP	generator_room
2020-11-07 18:47:34	acurry	CPPESP	main_gate
2020-11-07 15:17:18	acurry	CPPESP	main_gate

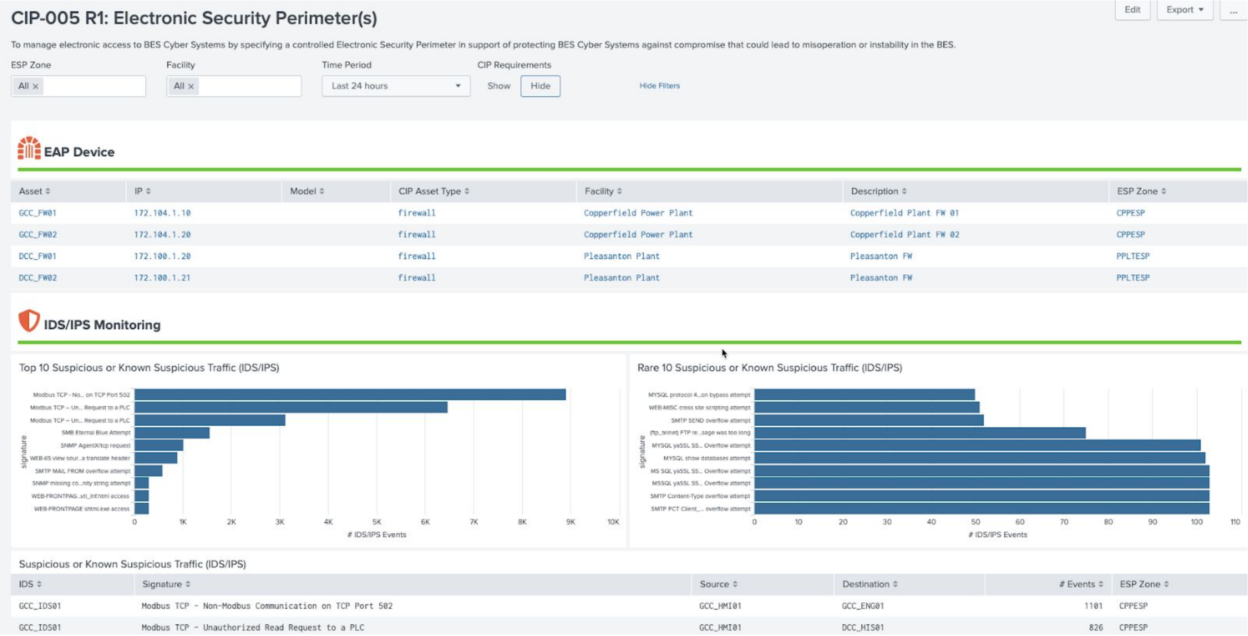
PRA Certifications

User	Last PRA	Status	Age
acurry	4/15/2012	Out of Compliance	8.6 years
hjordan	4/5/2014	Needs PRA	6.6 years
nfury	4/5/2014	Needs PRA	6.6 years
avision	6/1/2016	Completed	4.4 years
bbanner	4/12/2018	Completed	2.6 years
bbatson	12/1/2015	Completed	4.9 years
bgordan	7/15/2018	Completed	2.3 years
bgordon	5/13/2016	Completed	4.5 years
bwayne	2/1/2020	Completed	0.8 years
ckent	6/23/2019	Completed	1.4 years
dgrayson	11/10/2017	Completed	3.0 years

NERC CIP 005: Electronic Security Perimeter and Remote Access

NERC CIP 005 is focused on protecting the perimeter of the NERC CIP environment by monitoring the Electronic Security Perimeter (ESP) and Remote Access into the environment. For assets which are part of the ESP (normally firewalls and data diodes), the devices must be explicitly tagged with the classification of cip:EAP in the cip_asset_lookup.csv. For devices that are on the perimeter and are often responsible for monitoring ingress and egress traffic (e.g. IDS, IPS) they should be tagged with the classification of cip:EACM in the cip_asset_lookup.csv. Most ESP devices are also EACM devices and should be tagged with both classifications (pipe delimiter). Additional data sources from equipment such as networking equipment and multi-factor authentication systems help to determine if remote communications are properly secured. The macro get_2fa_indexes can be used to point to specific indexes, sources, and sourcetypes to capture multi-factor addition logs and improve search performance.

Electronic Security Perimeter Example (CIP 005 R1):



CIP-005 R1: Electronic Security Perimeter(s)

To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

ESP Zone: All ×

Facility: All ×

Time Period: Last 24 hours

CIP Requirements

EAP Device

Asset	IP	Model	CIP Asset Type	Facility	Description	ESP Zone
GCC_FW01	172.104.1.10		firewall	Copperfield Power Plant	Copperfield Plant FW 01	CPPESP
GCC_FW02	172.104.1.20		firewall	Copperfield Power Plant	Copperfield Plant FW 02	CPPESP
DCC_FW01	172.100.1.20		firewall	Pleasanton Plant	Pleasanton FW	PPLTESP
DCC_FW02	172.100.1.21		firewall	Pleasanton Plant	Pleasanton FW	PPLTESP

IDS/IPS Monitoring

Top 10 Suspicious or Known Suspicious Traffic (IDS/IPS)

signature
Modbus TCP - No... on TCP Port 502
Modbus TCP – Un... Request to a PLC
Modbus TCP – Un... Request to a PLC
SMB Eternal Blue Attempt
SNMP AgentX/tcp request
WEB-IIS view sour...a translate header
SMTP MAIL FROM overflow attempt
SNMP missing co...nity string attempt
WEB-FRONTPAG...vti_inf.html access
WEB-FRONTPAGE shtml.exe access
0
1K
2K
3K
4K
5K
6K
7K
8K
9K
10K
# IDS/IPS Events

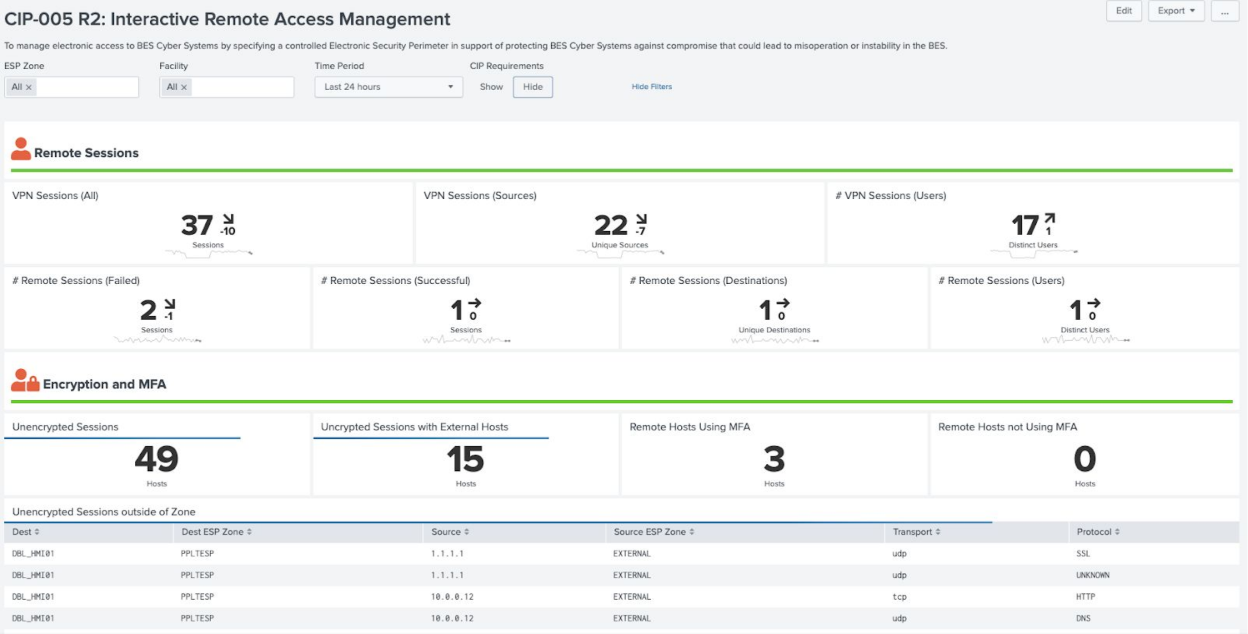
Rare 10 Suspicious or Known Suspicious Traffic (IDS/IPS)

signature
MYSQL protocol 4...on bypass attempt
WEB-MISC cross site scripting attempt
SMTP SEND overflow attempt
(ftp_telnet) FTP re...sage was too long
MYSQL yaSSL SS... Overflow attempt
MYSQL show databases attempt
MS SQL yaSSL SS... Overflow attempt
MSSQL yaSSL SS... Overflow attempt
SMTP Content-Type overflow attempt
SMTP PCT Client_... overflow attempt
0
10
20
30
40
50
60
70
80
90
100
110
# IDS/IPS Events

Suspicious or Known Suspicious Traffic (IDS/IPS)

IDS	Signature	Source	Destination	# Events	ESP Zone
GCC_IDS01	Modbus TCP - Non-Modbus Communication on TCP Port 502	GCC_HMI01	GCC_ENG01	1101	CPPESP
GCC_IDS01	Modbus TCP - Unauthorized Read Request to a PLC	GCC_HMI01	DCC_HIS01	826	CPPESP

Interactive Remote Access Management Example (CIP 005 R2):



CIP-005 R2: Interactive Remote Access Management

To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

ESP Zone: All ×

Facility: All ×

Time Period: Last 24 hours

CIP Requirements

Remote Sessions

VPN Sessions (All): 37 ↘ -10 Sessions

VPN Sessions (Sources): 22 ↘ -7 Unique Sources

VPN Sessions (Users): 17 ↗ 1 Distinct Users

Remote Sessions (Failed): 2 ↘ -1 Sessions

Remote Sessions (Successful): 1 → 0 Sessions

Remote Sessions (Destinations): 1 → 0 Unique Destinations

Remote Sessions (Users): 1 → 0 Distinct Users

Encryption and MFA

Unencrypted Sessions: 49 Hosts

Uncrypted Sessions with External Hosts: 15 Hosts

Remote Hosts Using MFA: 3 Hosts

Remote Hosts not Using MFA: 0 Hosts

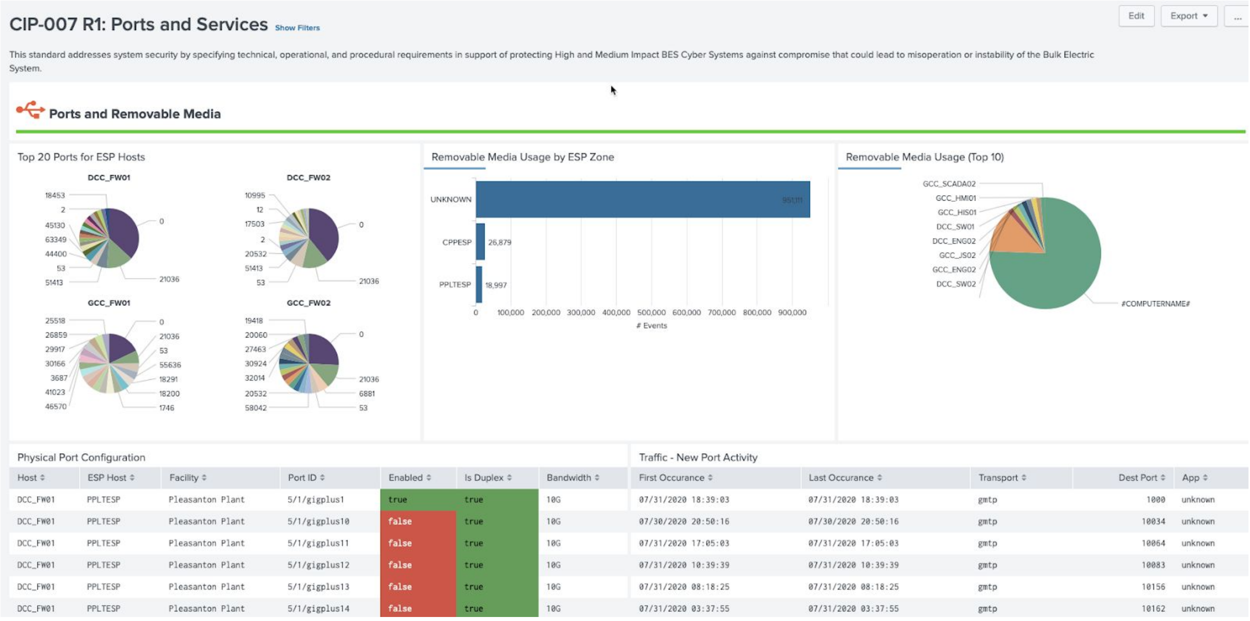
Unencrypted Sessions outside of Zone

Dest	Dest ESP Zone	Source	Source ESP Zone	Transport	Protocol
DBL_HMI01	PPLTESP	1.1.1.1	EXTERNAL	udp	SSL
DBL_HMI01	PPLTESP	1.1.1.1	EXTERNAL	udp	UNKNOWN
DBL_HMI01	PPLTESP	10.0.0.12	EXTERNAL	tcp	HTTP
DBL_HMI01	PPLTESP	10.0.0.12	EXTERNAL	udp	DNS

NERC CIP 007: Ports and Services

Ports and services being used and present on machines is mandated by NERC CIP and involves a wide plethora of data sources relevant to these requirements. Firewall, routers, switches can provide information on ports being used, as well as logs from machines themselves or data can be collected via Splunk Stream. In addition, events from endpoint protection logs that monitor USB usage, or directly from Windows Events (current OS) as well as windows registry (older OS's) play a role in determining when remote media is being used. Since the source of remote media usage can vary, the macro get_removable_media_indexes can be used to point to specific indexes, sources, and sourcetypes that contain this information.

Ports and Services Example (CIP 007 R1):



CIP-007 R1: Ports and Services

This standard addresses system security by specifying technical, operational, and procedural requirements in support of protecting High and Medium Impact BES Cyber Systems against compromise that could lead to misoperation or instability of the Bulk Electric System.

Ports and Removable Media

Physical Port Configuration

Host ⇕	ESP Host ⇕	Facility ⇕	Port ID ⇕	Enabled ⇕	Is Duplex ⇕	Bandwidth ⇕
DCC_FW01	PPLTESP	Pleasanton Plant	5/1/gigplus1	true	true	10G
DCC_FW01	PPLTESP	Pleasanton Plant	5/1/gigplus10	false	true	10G
DCC_FW01	PPLTESP	Pleasanton Plant	5/1/gigplus11	false	true	10G
DCC_FW01	PPLTESP	Pleasanton Plant	5/1/gigplus12	false	true	10G
DCC_FW01	PPLTESP	Pleasanton Plant	5/1/gigplus13	false	true	10G
DCC_FW01	PPLTESP	Pleasanton Plant	5/1/gigplus14	false	true	10G

Traffic - New Port Activity

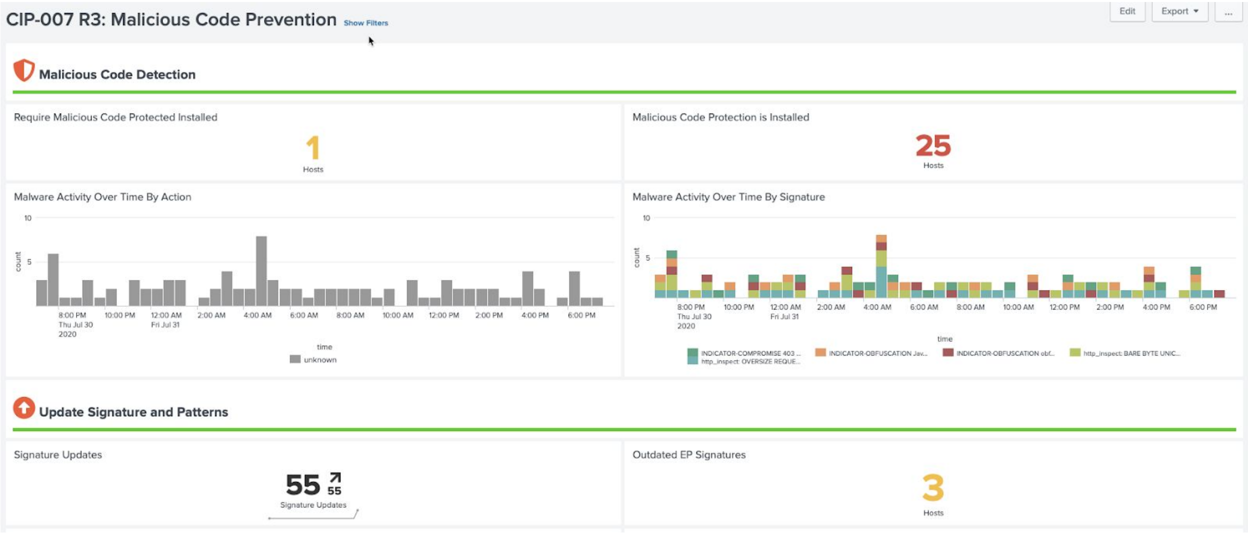
First Occurance ⇕	Last Occurance ⇕	Transport ⇕	Dest Port ⇕	App ⇕
07/31/2020 18:39:03	07/31/2020 18:39:03	gmtp	1000	unknown
07/30/2020 20:50:16	07/30/2020 20:50:16	gmtp	10034	unknown
07/31/2020 17:05:03	07/31/2020 17:05:03	gmtp	10064	unknown
07/31/2020 10:39:39	07/31/2020 10:39:39	gmtp	10083	unknown
07/31/2020 08:18:25	07/31/2020 08:18:25	gmtp	10156	unknown
07/31/2020 03:37:55	07/31/2020 03:37:55	gmtp	10162	unknown

NERC CIP 007: Security Events, Malware Alerts, and Monitoring

The monitoring of the NERC CIP environment is essential to understand threats to the environment. Monitoring of those alerts requires NERC environments to collect security logs and endpoint protection logs such as antivirus. In addition, NERC regulations require that logs be kept for at least 90 days and be periodically reviewed. The 5 dashboards in this section depend completely on Splunk's Common Information Models for malware, network sessions, and authentication. Since several of the requirements specify there should be a method to trigger and investigate incidents, Splunk's Enterprise Security notable and investigations features are essential to meeting several of these requirements.

Dashboards involving malware require endpoint protection to be installed, updated with signatures, and malware alerts be sent to Splunk. Those involving security logs are primarily focused on logon events, triggering security events for suspicious activity, and review of those logs.

Malicious Code Prevention Example (CIP 007 R3):



CIP-007 R3: Malicious Code Prevention

Malicious Code Detection

Require Malicious Code Protected Installed: 1 Hosts

Malicious Code Protection is Installed: 25 Hosts

Malware Activity Over Time By Action

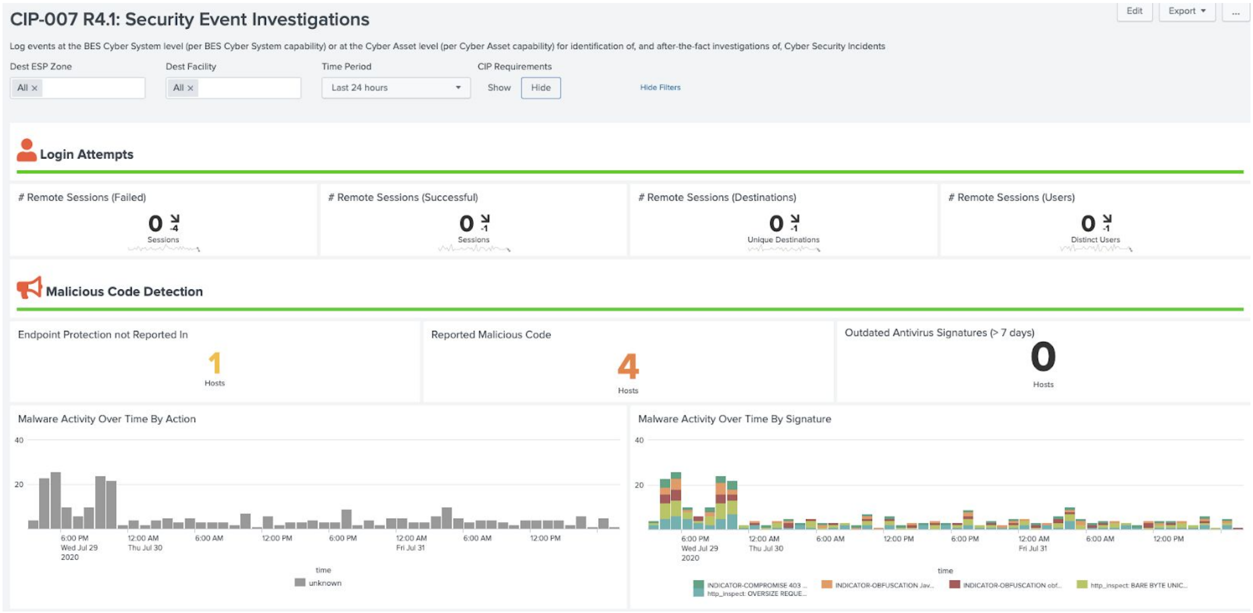
Malware Activity Over Time By Signature

Update Signature and Patterns

Signature Updates: 55 ↗ 55 Signature Updates

Outdated EP Signatures: 3 Hosts

Security Event Investigations Example (CIP 004 R4.1):



CIP-007 R4.1: Security Event Investigations

Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents

Dest ESP Zone: All ×

Dest Facility: All ×

Time Period: Last 24 hours ▾

CIP Requirements: Show | Hide

Login Attempts

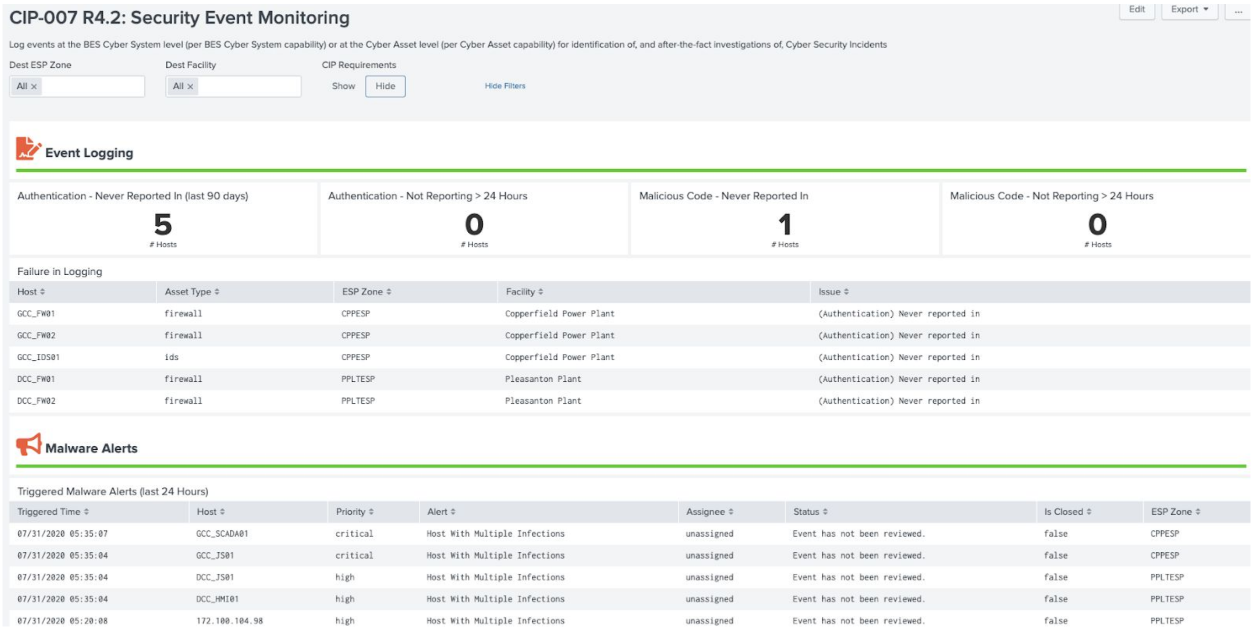
# Remote Sessions (Failed)	# Remote Sessions (Successful)	# Remote Sessions (Destinations)	# Remote Sessions (Users)
0 ↘ -4 Sessions	0 ↘ -1 Sessions	0 ↘ -1 Unique Destinations	0 ↘ -1 Distinct Users

Malicious Code Detection

Endpoint Protection not Reported In	Reported Malicious Code	Outdated Antivirus Signatures (> 7 days)
1 Hosts	4 Hosts	0 Hosts

Malware Activity Over Time By Action
40
20
6:00 PM
Wed Jul 29
2020
12:00 AM
Thu Jul 30
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Fri Jul 31
6:00 AM
12:00 PM
time
unknown
Malware Activity Over Time By Signature
40
20
6:00 PM
Wed Jul 29
2020
12:00 AM
Thu Jul 30
6:00 AM
12:00 PM
6:00 PM
12:00 AM
Fri Jul 31
6:00 AM
12:00 PM
time
INDICATOR-COMPROMISE 403 ...
http_inspect: OVERSIZE REQUE...
INDICATOR-OBFUSCATION Jav...
INDICATOR-OBFUSCATION obf...
http_inspect: BARE BYTE UNIC...

Security Event Monitoring Example (CIP 007 R4.2):



CIP-007 R4.2: Security Event Monitoring

Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents

Dest ESP Zone: All ×

Dest Facility: All ×

CIP Requirements: Show | Hide

Event Logging

Authentication - Never Reported In (last 90 days)	Authentication - Not Reporting > 24 Hours	Malicious Code - Never Reported In	Malicious Code - Not Reporting > 24 Hours
5 # Hosts	0 # Hosts	1 # Hosts	0 # Hosts

Failure in Logging

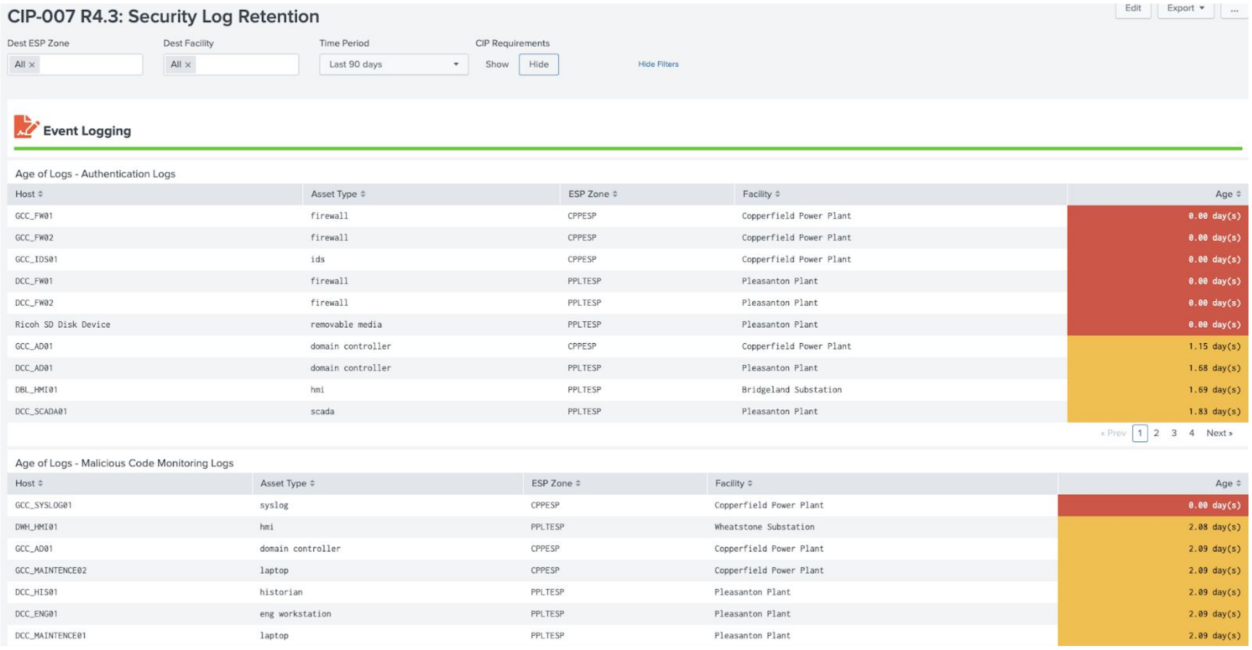
Host ⇕	Asset Type ⇕	ESP Zone ⇕	Facility ⇕	Issue ⇕
GCC_FW01	firewall	CPPESP	Copperfield Power Plant	(Authentication) Never reported in
GCC_FW02	firewall	CPPESP	Copperfield Power Plant	(Authentication) Never reported in
GCC_IDS01	ids	CPPESP	Copperfield Power Plant	(Authentication) Never reported in
DCC_FW01	firewall	PPLTESP	Pleasanton Plant	(Authentication) Never reported in
DCC_FW02	firewall	PPLTESP	Pleasanton Plant	(Authentication) Never reported in

Malware Alerts

Triggered Malware Alerts (last 24 Hours)

Triggered Time ⇕	Host ⇕	Priority ⇕	Alert ⇕	Assignee ⇕	Status ⇕	Is Closed ⇕	ESP Zone ⇕
07/31/2020 05:35:07	GCC_SCADA01	critical	Host With Multiple Infections	unassigned	Event has not been reviewed.	false	CPPESP
07/31/2020 05:35:04	GCC_JS01	critical	Host With Multiple Infections	unassigned	Event has not been reviewed.	false	CPPESP
07/31/2020 05:35:04	DCC_JS01	high	Host With Multiple Infections	unassigned	Event has not been reviewed.	false	PPLTESP
07/31/2020 05:35:04	DCC_HMI01	high	Host With Multiple Infections	unassigned	Event has not been reviewed.	false	PPLTESP
07/31/2020 05:20:08	172.100.104.98	high	Host With Multiple Infections	unassigned	Event has not been reviewed.	false	PPLTESP

Security Log Retention Example (CIP 007 R4.3):



CIP-007 R4.3: Security Log Retention

Edit | Export ▾ | ...

Dest ESP Zone: All × | Dest Facility: All × | Time Period: Last 90 days ▾ | CIP Requirements: Show [✓ Hide] | Hide Filters

Event Logging

Age of Logs - Authentication Logs

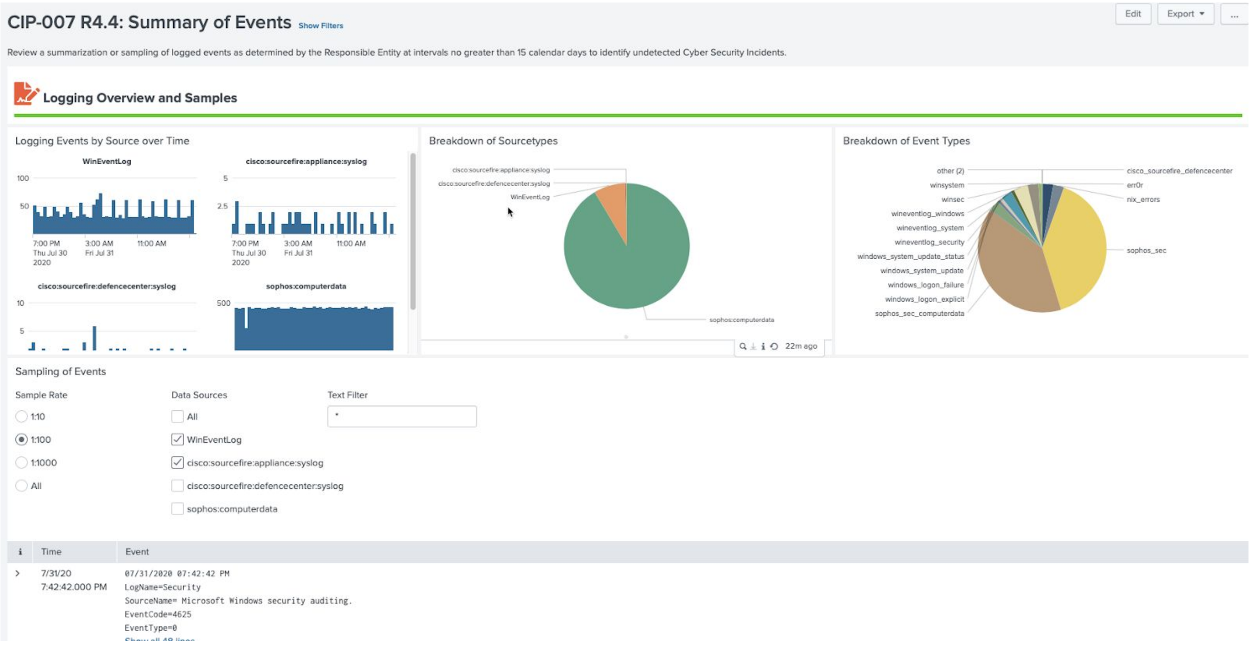
Host	Asset Type	ESP Zone	Facility	Age
GCC_FW01	firewall	CPPESP	Copperfield Power Plant	0.00 day(s)
GCC_FW02	firewall	CPPESP	Copperfield Power Plant	0.00 day(s)
GCC_IDS01	ids	CPPESP	Copperfield Power Plant	0.00 day(s)
DCC_FW01	firewall	PPLTESP	Pleasanton Plant	0.00 day(s)
DCC_FW02	firewall	PPLTESP	Pleasanton Plant	0.00 day(s)
Ricoh SD Disk Device	removable media	PPLTESP	Pleasanton Plant	0.00 day(s)
GCC_AD01	domain controller	CPPESP	Copperfield Power Plant	1.15 day(s)
DCC_AD01	domain controller	PPLTESP	Pleasanton Plant	1.68 day(s)
DBL_HMI01	hmi	PPLTESP	Bridgeland Substation	1.69 day(s)
DCC_SCADA01	scada	PPLTESP	Pleasanton Plant	1.83 day(s)

« Prev 1 2 3 4 Next »

Age of Logs - Malicious Code Monitoring Logs

Host	Asset Type	ESP Zone	Facility	Age
GCC_SYSLOG01	syslog	CPPESP	Copperfield Power Plant	0.00 day(s)
DWH_HMI01	hmi	PPLTESP	Wheatstone Substation	2.08 day(s)
GCC_AD01	domain controller	CPPESP	Copperfield Power Plant	2.09 day(s)
GCC_MAINTENCE02	laptop	CPPESP	Copperfield Power Plant	2.09 day(s)
DCC_HIS01	historian	PPLTESP	Pleasanton Plant	2.09 day(s)
DCC_ENG01	eng workstation	PPLTESP	Pleasanton Plant	2.09 day(s)
DCC_MAINTENCE01	laptop	PPLTESP	Pleasanton Plant	2.09 day(s)

Summary of Events Review Example (CIP 007 R4.4):



CIP-007 R4.4: Summary of Events

Show Filters

Edit | Export ▾ | ...

Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.

Logging Overview and Samples

Sampling of Events

Sample Rate
○ 1:10
● 1:100
○ 1:1000
○ All

Data Sources
□ All
☑ WinEventLog
☑ cisco:sourcefire:appliance:syslog
□ cisco:sourcefire:defencecenter:syslog
□ sophos:computerdata

Text Filter: *

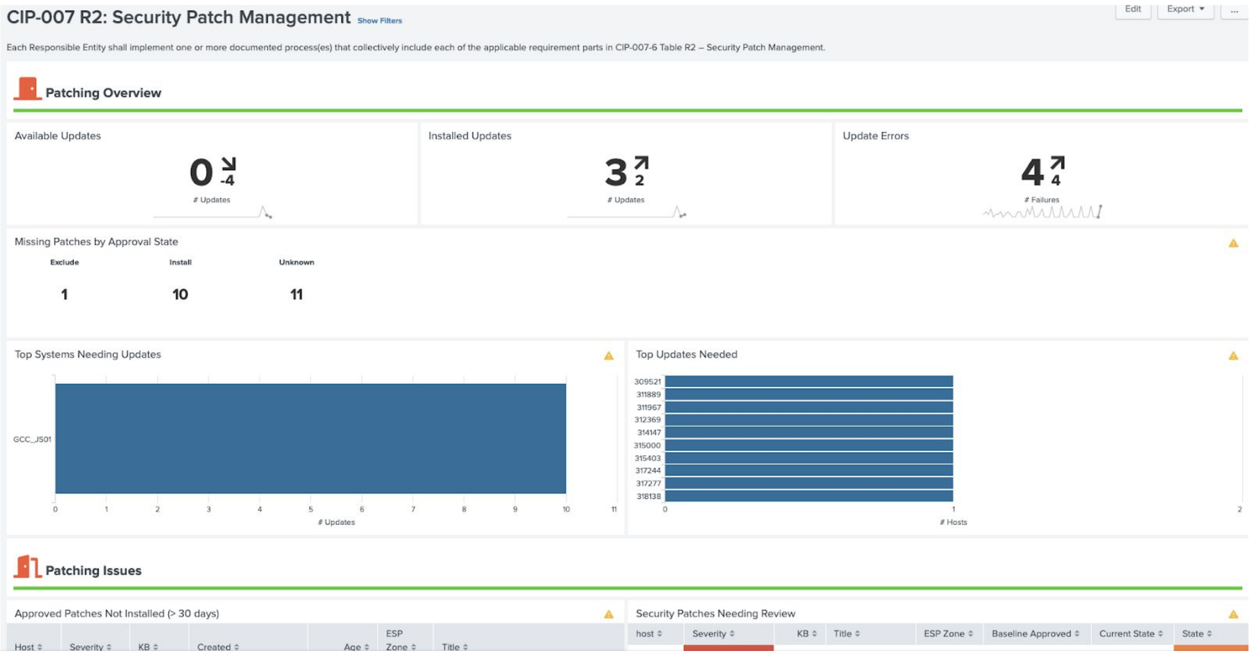
i	Time	Event

>	7/31/20
	7:42:42.000 PM
		07/31/2020 07:42:42 PM
		LogName=Security
		SourceName= Microsoft Windows security auditing.
		EventCode=4625
		EventType=0
		Show all 48 lines

NERC CIP 007: Patching

NERC CIP requires that NERC environments be updated and monitored for missing patches. In many cases, NERC environments already utilize patching solutions to help manage and approve patches (such as WSUS). In order to prevent duplication of effort, if it recommended that most of the approved patches come from existing solutions and be periodically updated. These scorecards rely on the patch baselines outlined in CIP 010 to determine when patches should be installed, as well as logs indicating patches back been installed either from the endpoint or the patching solution.

Security Patch Management Example (CIP 007 R2):



CIP-007 R2: Security Patch Management

Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.

Patching Overview

Available Updates: 0 ↘ -4 # Updates

Installed Updates: 3 ↗ 2 # Updates

Update Errors: 4 ↗ 4 # Failures

Missing Patches by Approval State

Exclude	Install	Unknown
1	10	11

Top Systems Needing Updates

Top Updates Needed

Patching Issues

Approved Patches Not Installed (> 30 days)

Host ≑	Severity ≑	KB ≑	Created ≑	Age ≑	ESP Zone ≑	Title ≑

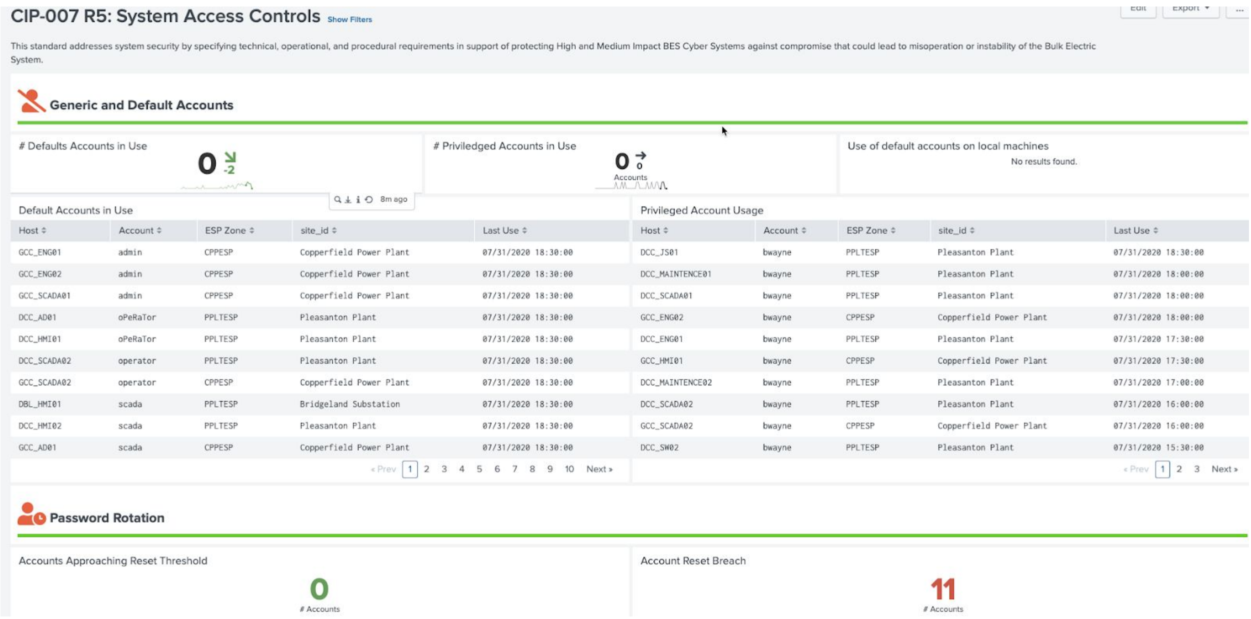
Security Patches Needing Review

host ≑	Severity ≑	KB ≑	Title ≑	ESP Zone ≑	Baseline Approved ≑	Current State ≑	State ≑

NERC CIP 007: Identities

The behavior of identities and user accounts is a critical part of CIP 007, especially the use of default and privileged accounts. Since this section primarily deals with identities and heavily leverages content from the cip_identities.csv. As a result this lookup should be part of the asset framework as detailed in Section 3. Identities utilized the category field in the cip_identities lookup to designate when an account is default, generic, or privileged. This field can also be used to designate certain accounts as nerc, operations, or other classifications as needed. In addition, data regarding password changes should be included as essential for reporting purposes.

System Access Controls Example (CIP 007 R5):



CIP-007 R5: System Access Controls

This standard addresses system security by specifying technical, operational, and procedural requirements in support of protecting High and Medium Impact BES Cyber Systems against compromise that could lead to misoperation or instability of the Bulk Electric System.

Generic and Default Accounts

Defaults Accounts in Use: 0 ↘ -2

Priviledged Accounts in Use: 0 → 0 Accounts

Use of default accounts on local machines: No results found.

Default Accounts in Use

Host	Account	ESP Zone	site_id	Last Use
GCC_ENG01	admin	CPPESP	Copperfield Power Plant	07/31/2020 18:30:00
GCC_ENG02	admin	CPPESP	Copperfield Power Plant	07/31/2020 18:30:00
GCC_SCADA01	admin	CPPESP	Copperfield Power Plant	07/31/2020 18:30:00
DCC_AD01	oPeRaTor	PPLTESP	Pleasanton Plant	07/31/2020 18:30:00
DCC_HMI01	oPeRaTor	PPLTESP	Pleasanton Plant	07/31/2020 18:30:00
DCC_SCADA02	operator	PPLTESP	Pleasanton Plant	07/31/2020 18:30:00
GCC_SCADA02	operator	CPPESP	Copperfield Power Plant	07/31/2020 18:30:00
DBL_HMI01	scada	PPLTESP	Bridgeland Substation	07/31/2020 18:30:00
DCC_HMI02	scada	PPLTESP	Pleasanton Plant	07/31/2020 18:30:00
GCC_AD01	scada	CPPESP	Copperfield Power Plant	07/31/2020 18:30:00

Privileged Account Usage

Host	Account	ESP Zone	site_id	Last Use
DCC_JS01	bwayne	PPLTESP	Pleasanton Plant	07/31/2020 18:30:00
DCC_MAINTENCE01	bwayne	PPLTESP	Pleasanton Plant	07/31/2020 18:00:00
DCC_SCADA01	bwayne	PPLTESP	Pleasanton Plant	07/31/2020 18:00:00
GCC_ENG02	bwayne	CPPESP	Copperfield Power Plant	07/31/2020 18:00:00
DCC_ENG01	bwayne	PPLTESP	Pleasanton Plant	07/31/2020 17:30:00
GCC_HMI01	bwayne	CPPESP	Copperfield Power Plant	07/31/2020 17:30:00
DCC_MAINTENCE02	bwayne	PPLTESP	Pleasanton Plant	07/31/2020 17:00:00
DCC_SCADA02	bwayne	PPLTESP	Pleasanton Plant	07/31/2020 16:00:00
GCC_SCADA02	bwayne	CPPESP	Copperfield Power Plant	07/31/2020 16:00:00
DCC_SW02	bwayne	PPLTESP	Pleasanton Plant	07/31/2020 15:30:00

Password Rotation

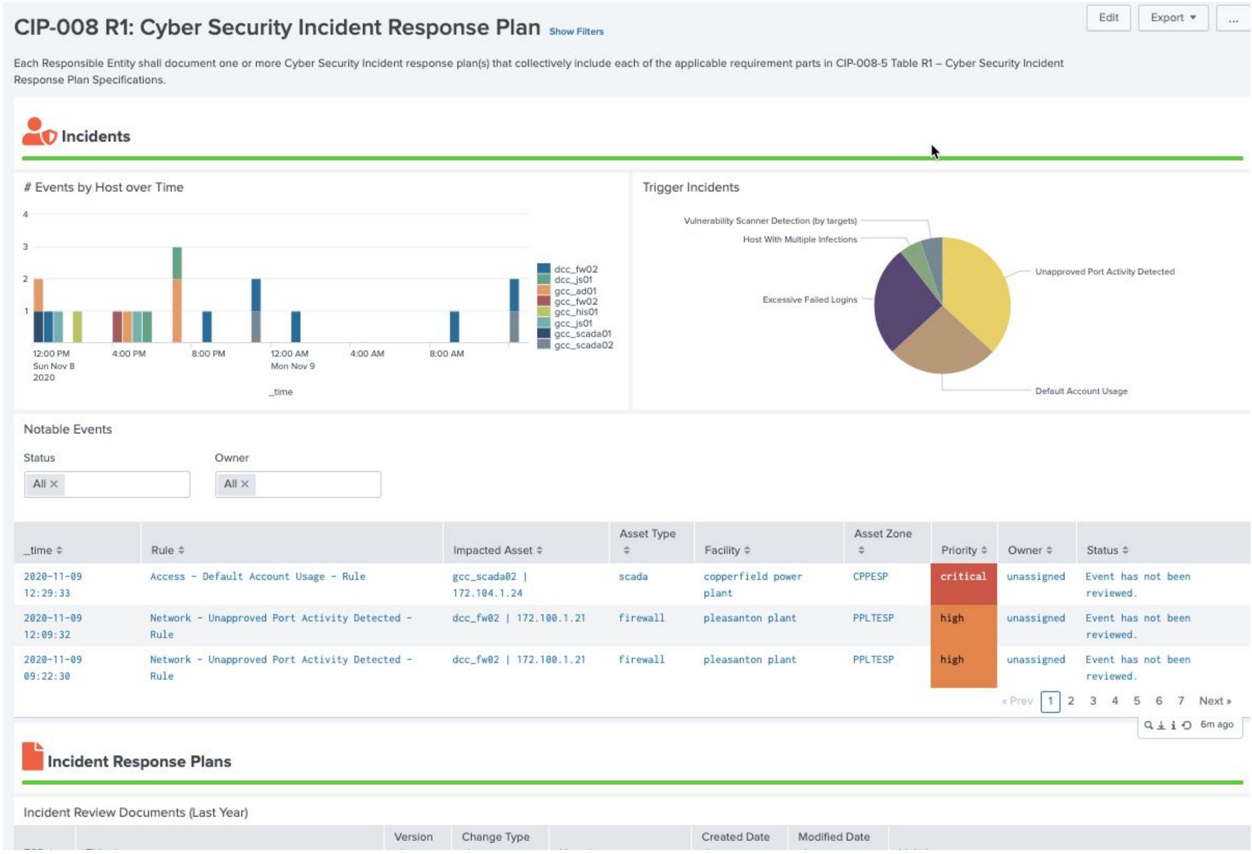
Accounts Approaching Reset Threshold: 0 # Accounts

Account Reset Breach: 11 # Accounts

NERC CIP 008 R1: Cyber Security Incident Response Plan

NERC CIP operators are required to have defined cyber security incident response plans (IRP) that identify how to respond to cyber incidents or violations of NERC CIP regulations. Part of this regulation requires a method to show notable or cyber incidents. This dashboard provides an overview of all the notable alerts that have been generated for NERC CIP regulated assets and is dependent on existing correlation rules built into Enterprise Security. The status and incident owner of each notable is reported to ensure incidents have been assigned and/or resolved. IRP plans should be reviewed at least yearly and updated and this dashboard provides a method to report on changes to IRP plans.

System Access Controls Example (CIP 008 R1):



CIP-008 R1: Cyber Security Incident Response Plan

Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications.

Notable Events

Status: All ×

Owner: All ×

_time ⇕	Rule ⇕	Impacted Asset ⇕	Asset Type ⇕	Facility ⇕	Asset Zone ⇕	Priority ⇕	Owner ⇕	Status ⇕
2020-11-09 12:29:33	Access - Default Account Usage - Rule	gcc_scada02 | 172.104.1.24	scada	copperfield power plant	CPPESP	critical	unassigned	Event has not been reviewed.
2020-11-09 12:09:32	Network - Unapproved Port Activity Detected - Rule	dcc_fw02 | 172.100.1.21	firewall	pleasanton plant	PPLTESP	high	unassigned	Event has not been reviewed.
2020-11-09 09:22:30	Network - Unapproved Port Activity Detected - Rule	dcc_fw02 | 172.100.1.21	firewall	pleasanton plant	PPLTESP	high	unassigned	Event has not been reviewed.

Incident Response Plans

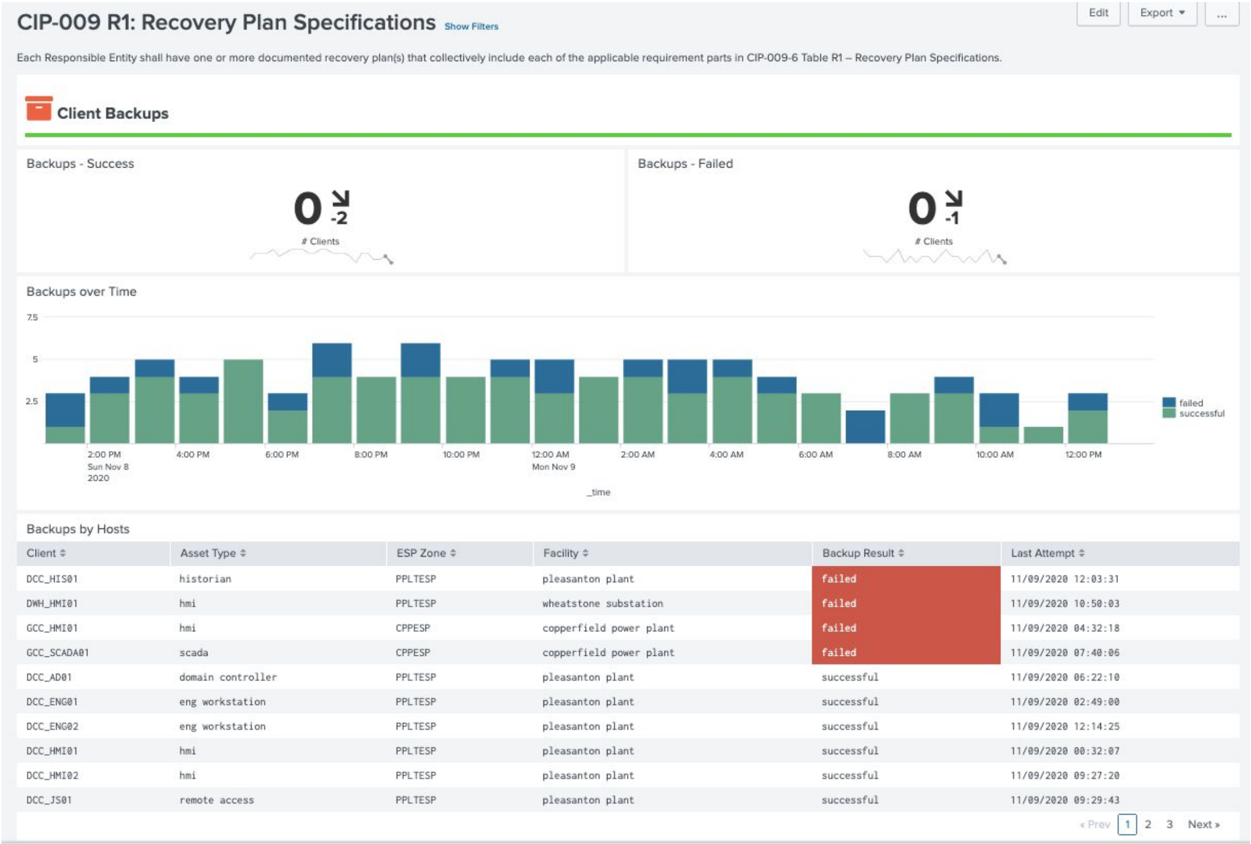
Incident Review Documents (Last Year)

		Version	Change Type		Created Date	Modified Date	

NERC CIP 009 R1: Recovery Plan Specifications

NERC CIP Operators are required to ensure their BES Cyber Systems can be restored quickly in case of failure or cyber attack. This includes monitoring not only the BES Cyber System but also any CIP assets which require backup. This dashboard provides information about the Splunk environment, including index retention, clustering, and Splunk features tied to High Availability and Disaster Recovery. This dashboard also brings in data from backup logs to ensure CIP assets are being backed up. The macro get_backup_indexes is used to specify data sources that contain records around client backups.

Recovery Plan Specifications Example (CIP 009 R1):



CIP-009 R1: Recovery Plan Specifications

Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.

Client Backups

Backups - Success

0 -2

# Clients

Backups - Failed

0 -1

# Clients

Backups over Time

Backups by Hosts

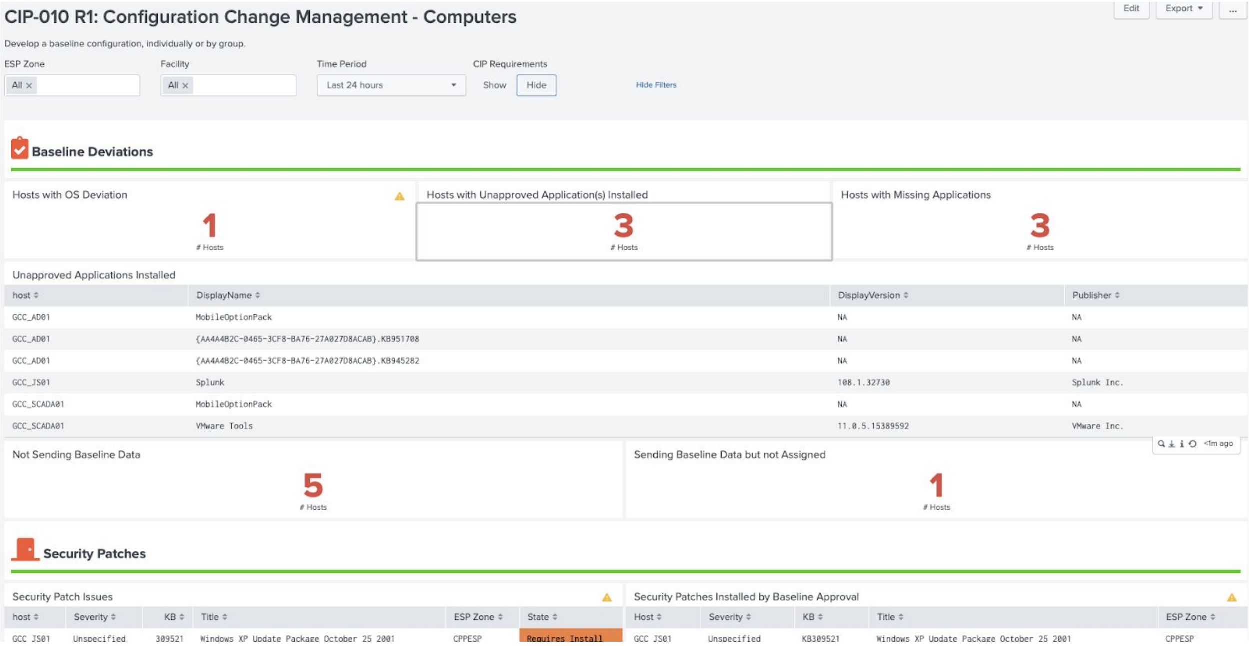
Client ⇕	Asset Type ⇕	ESP Zone ⇕	Facility ⇕	Backup Result ⇕	Last Attempt ⇕
DCC_HIS01	historian	PPLTESP	pleasanton plant	failed	11/09/2020 12:03:31
DWH_HMI01	hmi	PPLTESP	wheatstone substation	failed	11/09/2020 10:50:03
GCC_HMI01	hmi	CPPESP	copperfield power plant	failed	11/09/2020 04:32:18
GCC_SCADA01	scada	CPPESP	copperfield power plant	failed	11/09/2020 07:40:06
DCC_AD01	domain controller	PPLTESP	pleasanton plant	successful	11/09/2020 06:22:10
DCC_ENG01	eng workstation	PPLTESP	pleasanton plant	successful	11/09/2020 02:49:00
DCC_ENG02	eng workstation	PPLTESP	pleasanton plant	successful	11/09/2020 12:14:25
DCC_HMI01	hmi	PPLTESP	pleasanton plant	successful	11/09/2020 00:32:07
DCC_HMI02	hmi	PPLTESP	pleasanton plant	successful	11/09/2020 09:27:20
DCC_JS01	remote access	PPLTESP	pleasanton plant	successful	11/09/2020 09:29:43

NERC CIP 010: Baselining of Assets

Baselining of computers and network devices is required for CIP 010 compliance. Baselines can be the result of static configurations (e.g. a list of approved patches) but ideally are generated from data sources. Some good examples of data sources to consider when generating baselines are patching approval systems (such as WSUS), asset information (endpoint protection, Splunk forwarders, etc), installed software inventories, as well networking management systems. The baseline features implemented in Splunk are designed to keep track of baselines so that assets can be reviewed against specific baselines. Keeping these baselines is also required by regulation.

Assets can be grouped together so that assets within a group should match a particular configuration. Currently computer and network baselines are the only requirement kinds of baselines and each has specific elements which must be baselined. In the case of each Scorecards are designed to identify deviations from the baseline and provide information of how the item deviates from the baseline (for example, software that is installed but not approved) including hosts.

Computer Baselines Example (CIP 010 R1 - Computers):



CIP-010 R1: Configuration Change Management - Computers

Develop a baseline configuration, individually or by group.

Baseline Deviations

Hosts with OS Deviation: 1 # Hosts

Hosts with Unapproved Application(s) Installed: 3 # Hosts

Hosts with Missing Applications: 3 # Hosts

Unapproved Applications Installed

host	DisplayName	DisplayVersion	Publisher
GCC_AD01	MobileOptionPack	NA	NA
GCC_AD01	{AA4A4B2C-0465-3CF8-BA76-27A027D8ACAB}.KB951708	NA	NA
GCC_AD01	{AA4A4B2C-0465-3CF8-BA76-27A027D8ACAB}.KB945282	NA	NA
GCC_JS01	Splunk	108.1.32730	Splunk Inc.
GCC_SCADA01	MobileOptionPack	NA	NA
GCC_SCADA01	VMware Tools	11.0.5.15389592	VMware Inc.

Not Sending Baseline Data: 5 # Hosts

Sending Baseline Data but not Assigned: 1 # Hosts

Security Patches

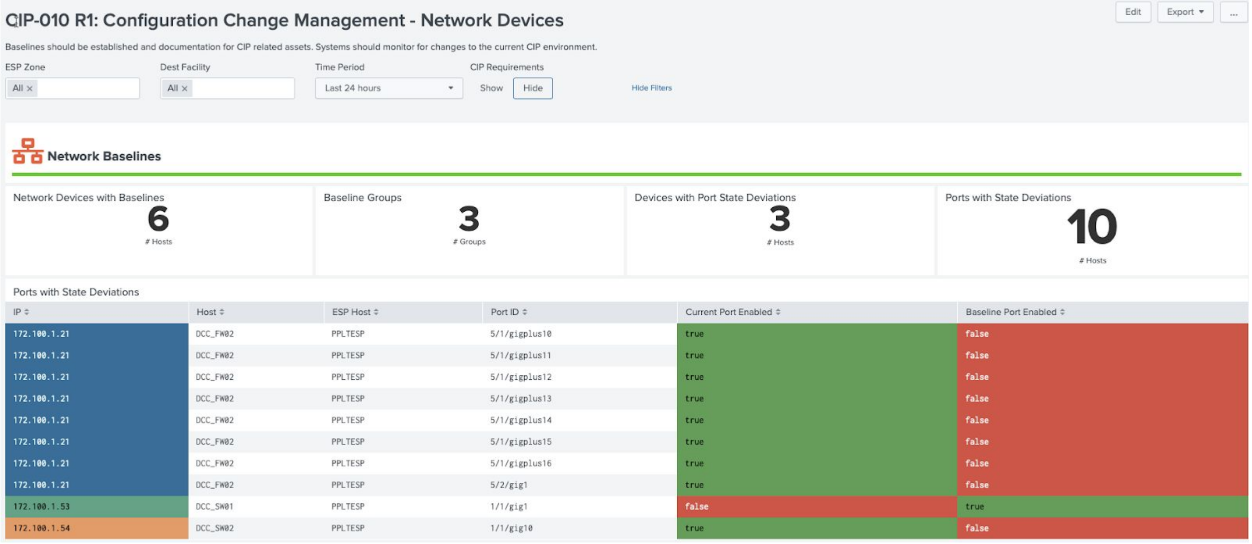
Security Patch Issues

host	Severity	KB	Title	ESP Zone	State
GCC JS01	Unspecified	309521	Windows XP Update Package October 25 2001	CPPESP	Requires Install

Security Patches Installed by Baseline Approval

Host	Severity	KB	Title	ESP Zone
GCC JS01	Unspecified	KB309521	Windows XP Update Package October 25 2001	CPPESP

Network Baseline Example (CIP 010 R1 - Network Devices):



CIP-010 R1: Configuration Change Management - Network Devices

Baselines should be established and documentation for CIP related assets. Systems should monitor for changes to the current CIP environment.

Network Baselines

Network Devices with Baselines: 6 # Hosts

Baseline Groups: 3 # Groups

Devices with Port State Deviations: 3 # Hosts

Ports with State Deviations: 10 # Hosts

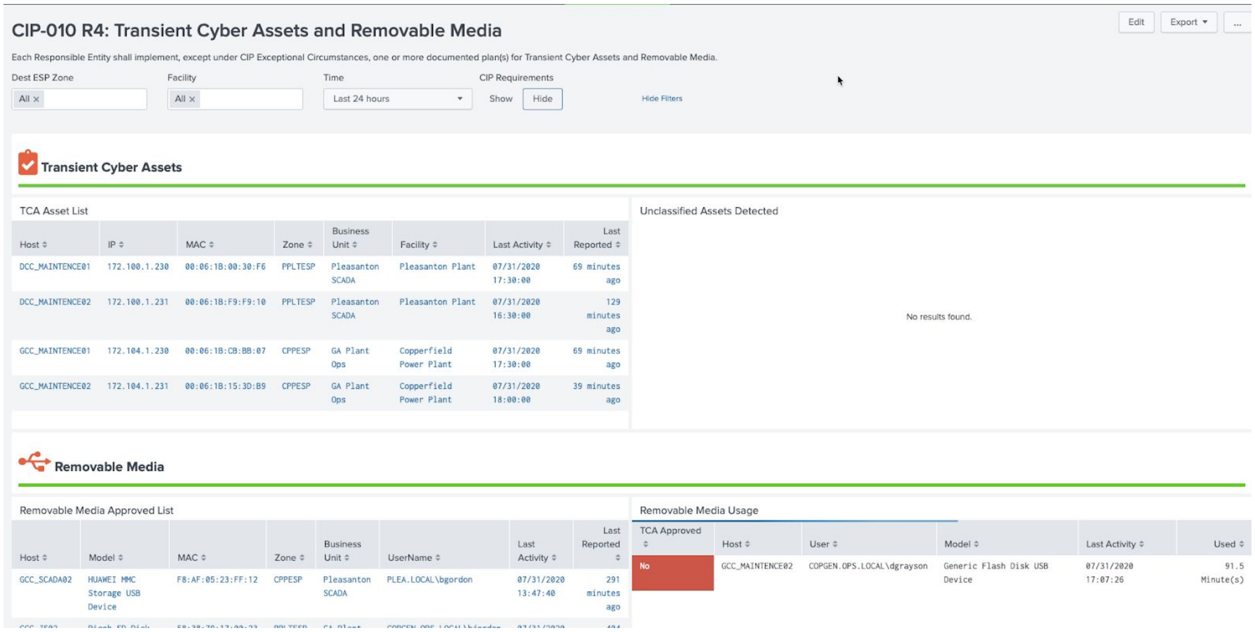
Ports with State Deviations

IP	Host	ESP Host	Port ID	Current Port Enabled	Baseline Port Enabled
172.100.1.21	DCC_FW02	PPLTESP	5/1/gigplus10	true	false
172.100.1.21	DCC_FW02	PPLTESP	5/1/gigplus11	true	false
172.100.1.21	DCC_FW02	PPLTESP	5/1/gigplus12	true	false
172.100.1.21	DCC_FW02	PPLTESP	5/1/gigplus13	true	false
172.100.1.21	DCC_FW02	PPLTESP	5/1/gigplus14	true	false
172.100.1.21	DCC_FW02	PPLTESP	5/1/gigplus15	true	false
172.100.1.21	DCC_FW02	PPLTESP	5/1/gigplus16	true	false
172.100.1.21	DCC_FW02	PPLTESP	5/2/gig1	true	false
172.100.1.53	DCC_SW01	PPLTESP	1/1/gig1	false	true
172.100.1.54	DCC_SW02	PPLTESP	1/1/gig10	true	false

NERC CIP 010: Transient Assets and Removable Media

Requirements exist to track transient assets such as laptops and maintenance equipment and removable media. Since transient assets are not continuously connected to networks and systems, their activity on the system should be closely tracked. The standard allows for certain removable media to be approved for general use. Assets and removable media should be classified as cip:TSA in the asset lookup for approved devices.

Transient Cyber Assets and Removable Media Example:



CIP-010 R4: Transient Cyber Assets and Removable Media

Each Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media.

Dest ESP Zone: All ×
Facility: All ×
Time: Last 24 hours
CIP Requirements: Show Hide

Transient Cyber Assets

TCA Asset List

Host	IP	MAC	Zone	Business Unit	Facility	Last Activity	Last Reported
DCC_MAINTENCE01	172.100.1.230	00:06:1B:00:30:F6	PPLTESP	Pleasanton SCADA	Pleasanton Plant	07/31/2020 17:30:00	69 minutes ago
DCC_MAINTENCE02	172.100.1.231	00:06:1B:F9:F9:10	PPLTESP	Pleasanton SCADA	Pleasanton Plant	07/31/2020 16:30:00	129 minutes ago
GCC_MAINTENCE01	172.104.1.230	00:06:1B:CB:BB:07	CPPESP	GA Plant Ops	Copperfield Power Plant	07/31/2020 17:30:00	69 minutes ago
GCC_MAINTENCE02	172.104.1.231	00:06:1B:15:3D:B9	CPPESP	GA Plant Ops	Copperfield Power Plant	07/31/2020 18:00:00	39 minutes ago

Unclassified Assets Detected

No results found.

Removable Media

Removable Media Approved List

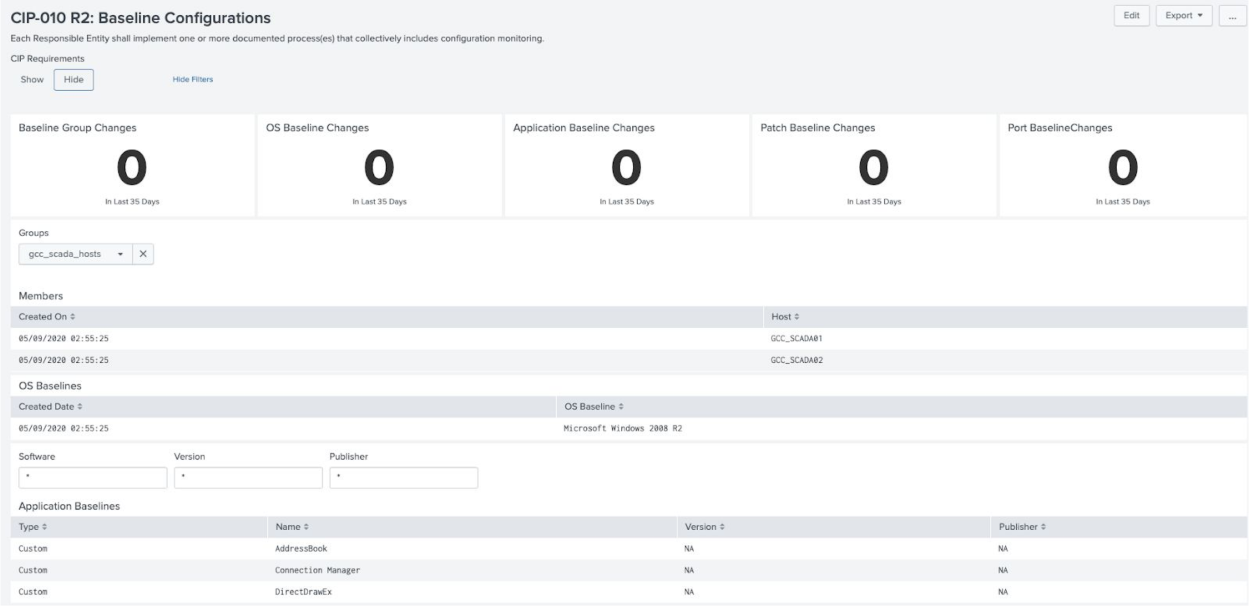
Host	Model	MAC	Zone	Business Unit	UserName	Last Activity	Last Reported
GCC_SCADA02	HUAWEI MMC Storage USB Device	F8:AF:05:23:FF:12	CPPESP	Pleasanton SCADA	PLEA.LOCAL\bgordon	07/31/2020 13:47:40	291 minutes ago

Removable Media Usage

TCA Approved	Host	User	Model	Last Activity	Used
No	GCC_MAINTENCE02	COPGEN.OPS.LOCAL\dgrayson	Generic Flash Disk USB Device	07/31/2020 17:07:26	91.5 Minute(s)

NERC CIP 010: Baseline Configuration Tool

The NERC CIP 010 Baseline Configuration Tool serves as both a tool and scorecard for baseline configuration. Through this tool it is possible to verify baseline group assignments as well as view configuration information related to the group. For example, a group containing computer assets, panels will appear showing the baselines for applications, OS, and security patches. This tool does not provide a direct method to update the baselines at this current time.



CIP-010 R2: Baseline Configurations

Each Responsible Entity shall implement one or more documented process(es) that collectively includes configuration monitoring.

CIP Requirements

Baseline Group Changes	OS Baseline Changes	Application Baseline Changes	Patch Baseline Changes	Port BaselineChanges
0	0	0	0	0
In Last 35 Days	In Last 35 Days	In Last 35 Days	In Last 35 Days	In Last 35 Days

Groups: gcc_scada_hosts

Members

Created On	Host
05/09/2020 02:55:25	GCC_SCADA01
05/09/2020 02:55:25	GCC_SCADA02

OS Baselines

Created Date	OS Baseline
05/09/2020 02:55:25	Microsoft Windows 2008 R2

Software: *

Version: *

Publisher: *

Application Baselines

Type	Name	Version	Publisher
Custom	AddressBook	NA	NA
Custom	Connection Manager	NA	NA
Custom	DirectDrawEx	NA	NA

NERC CIP Specific Lookups

KV Store Lookups

The Splunk OT Security solution contains two critical kvstore lookups that are leveraged to determine deviations from normal asset behavior. The two tables are linked and timestamped. The critical kv stores and their fields is defined below:

cip_baseline groups:

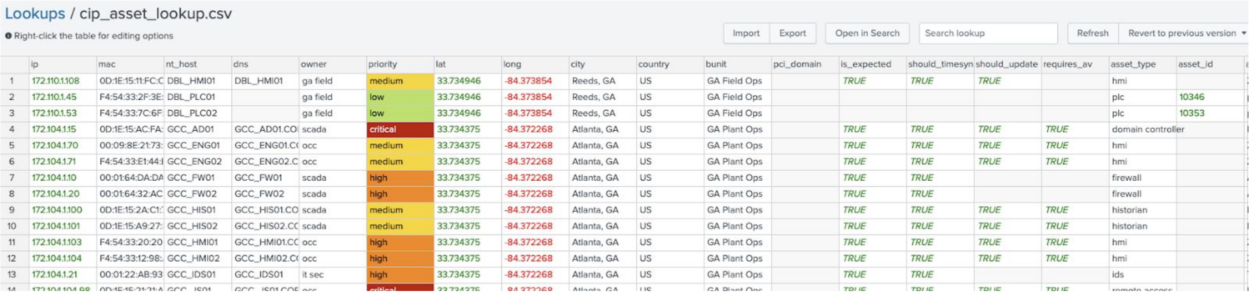
Field	Description
_key	Auto-generated by Splunk, **this key must be linked to group_id** in the system_baselines lookup (similar to a foreign key)
created_date	Time in epoch when this particular group was created. Note: new or modified groups should create a new entry so group configurations can be maintained over time.
group_members	A list of host names that belong to this group, pipe delimited
group_name	Name for the group for readability

system_baselines:

Field	Description
_key	Auto-generated by Splunk, unique identifier for this baseline
config	The actual configuration for this kind of baseline. This is normally json, but if this is not available it is possible to modify search and dashboards to use a different format.
config_asset_type	Type of asset that this configuration should be applied to - the NERC CIP app currently only uses two values: computer and network (device such as plc). It is possible to store other configuration asset types as needed but the current NERC CIP dashboards only leverage these two.
config_type	The type of configuration, for example. NERC CIP reports only use the following types: os, applications, patch, port_config. It is possible to store other configuration types (for example, services) as needed
created_date	Time in epoch when this particular configuration was created. Note: new configurations should create a new entry so configurations can be maintained over time.
group_id	This maps this configuration to a specific group in the cip_baseline_groups, telling Splunk that the two are connected. This is **an essential field** for Splunk to know which configuration to apply to a machine and what parameters to use for checking for deviations.

Various lookup tables are essential for populating dashboards with data or for presenting visualizations. The following sections break down each lookup and its intended purpose.

Lookup name: cip_asset_lookup.csv
This is the main lookup used to provide information about assets which are part of NERC CIP.

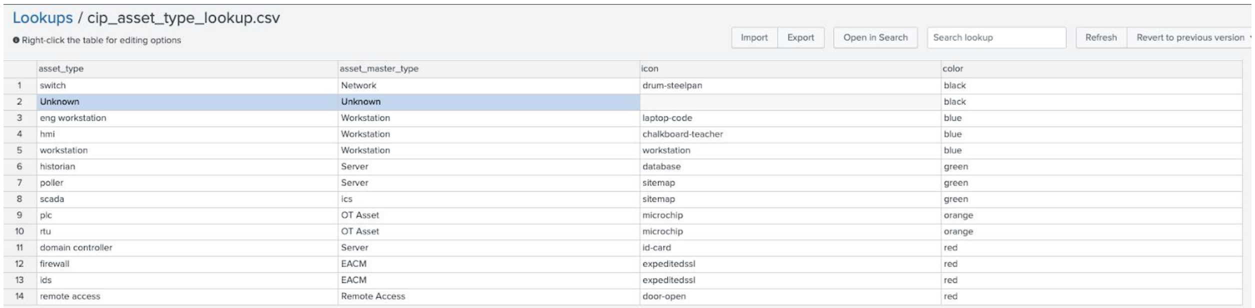


Lookups / cip_asset_lookup.csv

❶ Right-click the table for editing options

	ip	mac	nt_host	dns	owner	priority	lat	long	city	country	bunit	pci_domain	is_expected	should_timesyn	should_update	requires_av	asset_type	asset_id
1	172.110.1.108	0D:1E:15:11:FC:C	DBL_HMI01	DBL_HMI01	ga field	medium	33.734946	-84.373854	Reeds, GA	US	GA Field Ops		TRUE	TRUE	TRUE		hmi	
2	172.110.1.45	F4:54:33:2F:3E:	DBL_PLC01		ga field	low	33.734946	-84.373854	Reeds, GA	US	GA Field Ops						plc	10346
3	172.110.1.53	F4:54:33:7C:6F:	DBL_PLC02		ga field	low	33.734946	-84.373854	Reeds, GA	US	GA Field Ops						plc	10353
4	172.104.1.15	0D:1E:15:AC:FA:	GCC_AD01	GCC_AD01.CO	scada	critical	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	domain controller	
5	172.104.1.70	00:09:8E:21:73:	GCC_ENG01	GCC_ENG01.C	occ	medium	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	hmi	
6	172.104.1.71	F4:54:33:E1:44:	GCC_ENG02	GCC_ENG02.C	occ	medium	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	hmi	
7	172.104.1.10	00:01:64:DA:DA	GCC_FW01	GCC_FW01	scada	high	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE			firewall	
8	172.104.1.20	00:01:64:32:AC	GCC_FW02	GCC_FW02	scada	high	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE			firewall	
9	172.104.1.100	0D:1E:15:2A:C1:	GCC_HIS01	GCC_HIS01.CO	scada	medium	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	historian	
10	172.104.1.101	0D:1E:15:A9:27:	GCC_HIS02	GCC_HIS02.C	scada	medium	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	historian	
11	172.104.1.103	F4:54:33:20:20	GCC_HMI01	GCC_HMI01.C	occ	high	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	hmi	
12	172.104.1.104	F4:54:33:12:98:	GCC_HMI02	GCC_HMI02.C	occ	high	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	hmi	
13	172.104.1.21	00:01:22:AB:93	GCC_IDS01	GCC_IDS01	it sec	high	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE			ids	
14	172.104.104.98	0D:1E:15:21:21:A	GCC_JS01	GCC_JS01.COF	occ	critical	33.734375	-84.372268	Atlanta, GA	US	GA Plant Ops		TRUE	TRUE	TRUE	TRUE	remote access	

Lookup name: cip_asset_type_lookup.csv
This is the lookup that is used to dictate icons, colors, and master asset types when used on various tables and visualizations.

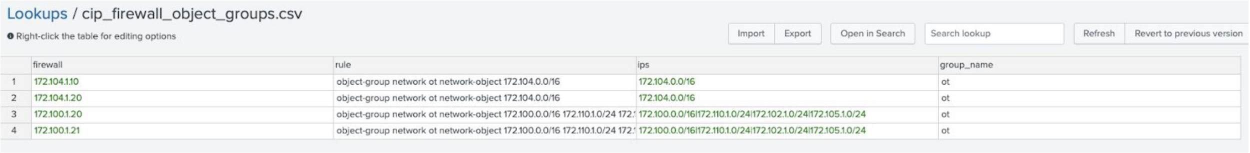


Lookups / cip_asset_type_lookup.csv

❶ Right-click the table for editing options

	asset_type	asset_master_type	icon	color
1	switch	Network	drum-steelpan	black
2	Unknown	Unknown		black
3	eng workstation	Workstation	laptop-code	blue
4	hmi	Workstation	chalkboard-teacher	blue
5	workstation	Workstation	workstation	blue
6	historian	Server	database	green
7	poller	Server	sitemap	green
8	scada	ics	sitemap	green
9	plc	OT Asset	microchip	orange
10	rtu	OT Asset	microchip	orange
11	domain controller	Server	id-card	red
12	firewall	EACM	expeditedssl	red
13	ids	EACM	expeditedssl	red
14	remote access	Remote Access	door-open	red

Lookup name: cip_firewall_object_groups.csv
This lookup is used to expand information about object groups contained in firewalls so users do not need to look up object groups. Object groups will often be contained in the cip_firewall_groups.csv.

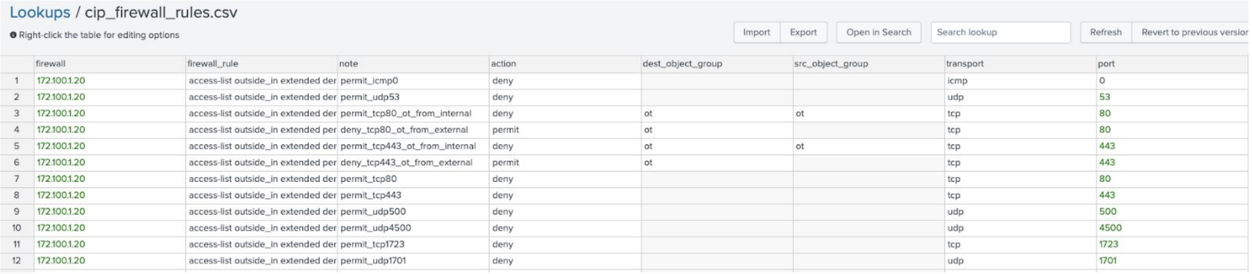


Lookups / cip_firewall_object_groups.csv

❶ Right-click the table for editing options

	firewall	rule	ips	group_name
1	172.104.1.10	object-group network ot network-object 172.104.0.0/16	172.104.0.0/16	ot
2	172.104.1.20	object-group network ot network-object 172.104.0.0/16	172.104.0.0/16	ot
3	172.100.1.20	object-group network ot network-object 172.100.0.0/16 172.110.1.0/24 172.1	172.100.0.0/16|172.110.1.0/24|172.102.1.0/24|172.105.1.0/24	ot
4	172.100.1.21	object-group network ot network-object 172.100.0.0/16 172.110.1.0/24 172.1	172.100.0.0/16|172.110.1.0/24|172.102.1.0/24|172.105.1.0/24	ot

Lookup name: cip_firewall_rules.csv
This lookup is used to hold firewall rules and annotations for NERC CIP firewalls.

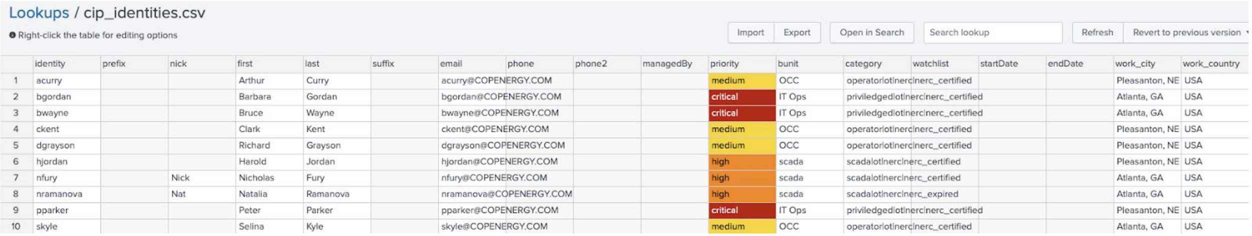


Lookups / cip_firewall_rules.csv

Right-click the table for editing options

	firewall	firewall_rule	note	action	dest_object_group	src_object_group	transport	port
1	172.100.1.20	access-list outside_in extended der	permit_icmp0	deny			icmp	0
2	172.100.1.20	access-list outside_in extended der	permit_udp53	deny			udp	53
3	172.100.1.20	access-list outside_in extended der	permit_tcp80_ot_from_internal	deny	ot	ot	tcp	80
4	172.100.1.20	access-list outside_in extended per	deny_tcp80_ot_from_external	permit	ot		tcp	80
5	172.100.1.20	access-list outside_in extended der	permit_tcp443_ot_from_internal	deny	ot	ot	tcp	443
6	172.100.1.20	access-list outside_in extended per	deny_tcp443_ot_from_external	permit	ot		tcp	443
7	172.100.1.20	access-list outside_in extended der	permit_tcp80	deny			tcp	80
8	172.100.1.20	access-list outside_in extended der	permit_tcp443	deny			tcp	443
9	172.100.1.20	access-list outside_in extended der	permit_udp500	deny			udp	500
10	172.100.1.20	access-list outside_in extended der	permit_udp4500	deny			udp	4500
11	172.100.1.20	access-list outside_in extended der	permit_tcp1723	deny			tcp	1723
12	172.100.1.20	access-list outside_in extended der	permit_udp1701	deny			udp	1701

Lookup name: cip_identities.csv
This is the main lookup used to hold information about identities for the Asset and Identity framework.

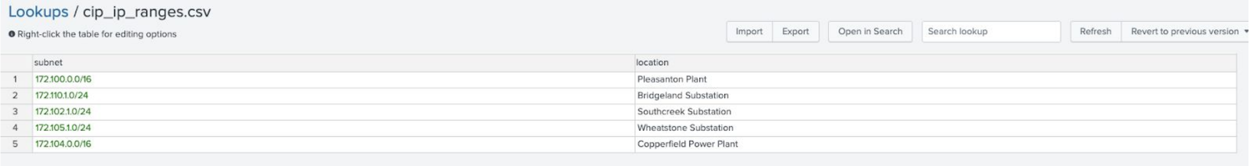


Lookups / cip_identities.csv

Right-click the table for editing options

	identity	prefix	nick	first	last	suffix	email	phone	phone2	managedBy	priority	bunit	category	watchlist	startDate	endDate	work_city	work_country
1	acurry			Arthur	Curry		acurry@COPENERGY.COM				medium	OCC	operator|ot|nerc|nerc_certified				Pleasanton, NE	USA
2	bgordan			Barbara	Gordan		bgordan@COPENERGY.COM				critical	IT Ops	priviledged|ot|nerc|nerc_certified				Atlanta, GA	USA
3	bwayne			Bruce	Wayne		bwayne@COPENERGY.COM				critical	IT Ops	priviledged|ot|nerc|nerc_certified				Atlanta, GA	USA
4	ckent			Clark	Kent		ckent@COPENERGY.COM				medium	OCC	operator|ot|nerc|nerc_certified				Pleasanton, NE	USA
5	dgrayson			Richard	Grayson		dgrayson@COPENERGY.COM				medium	OCC	operator|ot|nerc|nerc_certified				Pleasanton, NE	USA
6	hjordan			Harold	Jordan		hjordan@COPENERGY.COM				high	scada	scada|ot|nerc|nerc_certified				Pleasanton, NE	USA
7	nfury		Nick	Nicholas	Fury		nfury@COPENERGY.COM				high	scada	scada|ot|nerc|nerc_certified				Atlanta, GA	USA
8	nramanova		Nat	Natalia	Ramanova		nramanova@COPENERGY.COM				high	scada	scada|ot|nerc|nerc_expired				Atlanta, GA	USA
9	pparker			Peter	Parker		pparker@COPENERGY.COM				critical	IT Ops	priviledged|ot|nerc|nerc_certified				Pleasanton, NE	USA
10	skyle			Selina	Kyle		skyle@COPENERGY.COM				medium	OCC	operator|ot|nerc|nerc_certified				Atlanta, GA	USA

Lookup name: cip_ip_ranges.csv
This lookup is used to define subnets that are considered part of OT environments. Subnets can be single IP’s or use CIDR notation.

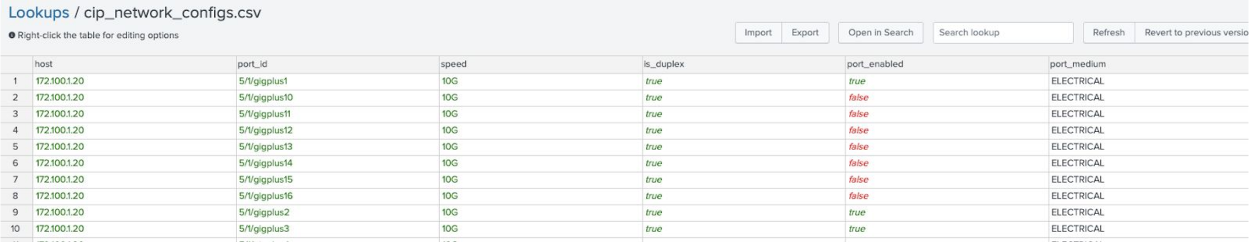


Lookups / cip_ip_ranges.csv

Right-click the table for editing options

	subnet	location
1	172.100.0.0/16	Pleasanton Plant
2	172.110.1.0/24	Bridgeland Substation
3	172.102.1.0/24	Southcreek Substation
4	172.105.1.0/24	Wheatstone Substation
5	172.104.0.0/16	Copperfield Power Plant

Lookup name: cip_network_configs.csv
This lookup is used to contain information on network devices as well as port and state information. This lookup will normally be populated from network configs, either regularly or statically.

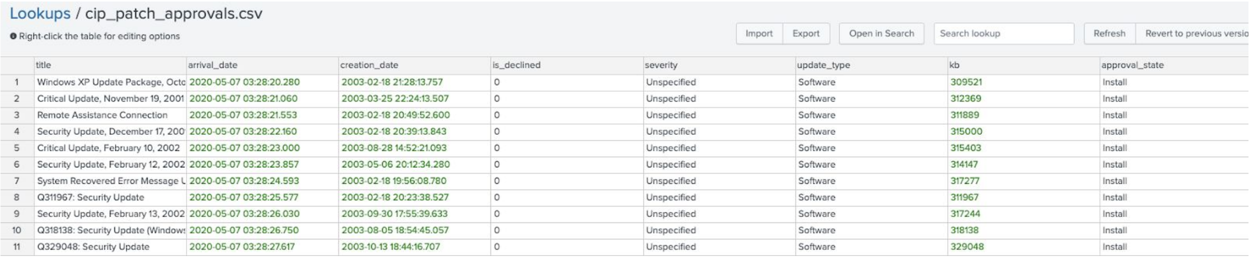


Lookups / cip_network_configs.csv

Right-click the table for editing options

	host	port_id	speed	is_duplex	port_enabled	port_medium
1	172.100.1.20	5/1/gigplus1	10G	true	true	ELECTRICAL
2	172.100.1.20	5/1/gigplus10	10G	true	false	ELECTRICAL
3	172.100.1.20	5/1/gigplus11	10G	true	false	ELECTRICAL
4	172.100.1.20	5/1/gigplus12	10G	true	false	ELECTRICAL
5	172.100.1.20	5/1/gigplus13	10G	true	false	ELECTRICAL
6	172.100.1.20	5/1/gigplus14	10G	true	false	ELECTRICAL
7	172.100.1.20	5/1/gigplus15	10G	true	false	ELECTRICAL
8	172.100.1.20	5/1/gigplus16	10G	true	false	ELECTRICAL
9	172.100.1.20	5/1/gigplus2	10G	true	true	ELECTRICAL
10	172.100.1.20	5/1/gigplus3	10G	true	true	ELECTRICAL

Lookup name: cip_patch_approvals.csv
This lookup is used to contain information about patches and whether they are approved. This data will often be populated from the patching management system (e.g. WSUS). It can also be used to generate baselines.

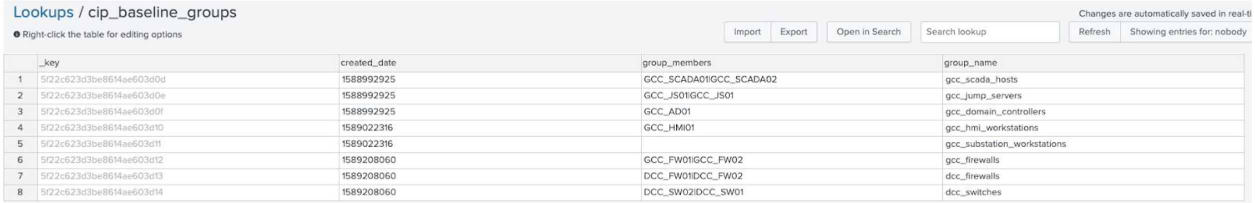


Lookups / cip_patch_approvals.csv

● Right-click the table for editing options

	title	arrival_date	creation_date	is_declined	severity	update_type	kb	approval_state
1	Windows XP Update Package, Octo	2020-05-07 03:28:20.280	2003-02-18 21:28:13.757	0	Unspecified	Software	309521	Install
2	Critical Update, November 19, 2001	2020-05-07 03:28:21.060	2003-03-25 22:24:13.507	0	Unspecified	Software	312369	Install
3	Remote Assistance Connection	2020-05-07 03:28:21.553	2003-02-18 20:49:52.600	0	Unspecified	Software	311889	Install
4	Security Update, December 17, 200	2020-05-07 03:28:22.160	2003-02-18 20:39:13.843	0	Unspecified	Software	315000	Install
5	Critical Update, February 10, 2002	2020-05-07 03:28:23.000	2003-08-28 14:52:21.093	0	Unspecified	Software	315403	Install
6	Security Update, February 12, 2002	2020-05-07 03:28:23.857	2003-05-06 20:12:34.280	0	Unspecified	Software	314147	Install
7	System Recovered Error Message L	2020-05-07 03:28:24.593	2003-02-18 19:56:08.780	0	Unspecified	Software	317277	Install
8	Q311967: Security Update	2020-05-07 03:28:25.577	2003-02-18 20:23:38.527	0	Unspecified	Software	311967	Install
9	Security Update, February 13, 2002	2020-05-07 03:28:26.030	2003-09-30 17:55:39.633	0	Unspecified	Software	317244	Install
10	Q318138: Security Update (Windows	2020-05-07 03:28:26.750	2003-08-05 18:54:45.057	0	Unspecified	Software	318138	Install
11	Q329048: Security Update	2020-05-07 03:28:27.617	2003-10-13 18:44:16.707	0	Unspecified	Software	329048	Install

Lookup name: cip_baseline_groups (kvstore)
This lookup is used to contain information about groupings of assets for baselining purposes. For more information on the fields see the section on NERC CIP 010. **This lookup is directly connected with system_baselines.**



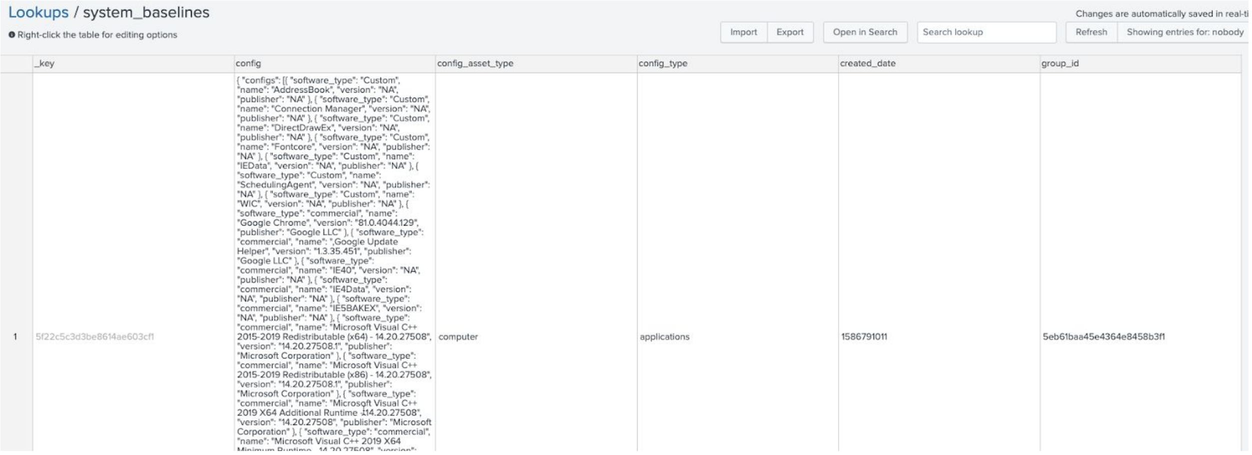
Lookups / cip_baseline_groups

● Right-click the table for editing options

Changes are automatically saved in real-ti

	_key	created_date	group_members	group_name
1	5f22c623d3be8614ae603d0d	1588992925	GCC_SCADA01|GCC_SCADA02	gcc_scada_hosts
2	5f22c623d3be8614ae603d0e	1588992925	GCC_JS01|GCC_JS01	gcc_jump_servers
3	5f22c623d3be8614ae603d0f	1588992925	GCC_AD01	gcc_domain_controllers
4	5f22c623d3be8614ae603d10	1589022316	GCC_HMI01	gcc_hmi_workstations
5	5f22c623d3be8614ae603d11	1589022316		gcc_substation_workstations
6	5f22c623d3be8614ae603d12	1589208060	GCC_FW01|GCC_FW02	gcc_firewalls
7	5f22c623d3be8614ae603d13	1589208060	DCC_FW01|DCC_FW02	dcc_firewalls
8	5f22c623d3be8614ae603d14	1589208060	DCC_SW02|DCC_SW01	dcc_switches

Lookup name: system_baselines (kvstore)
This lookup is used to contain all the baseline configurations for computers and network devices. For more information on the fields see the section on NERC CIP 010. **This lookup is directly connected with cip_baseline_groups.**



Lookups / system_baselines

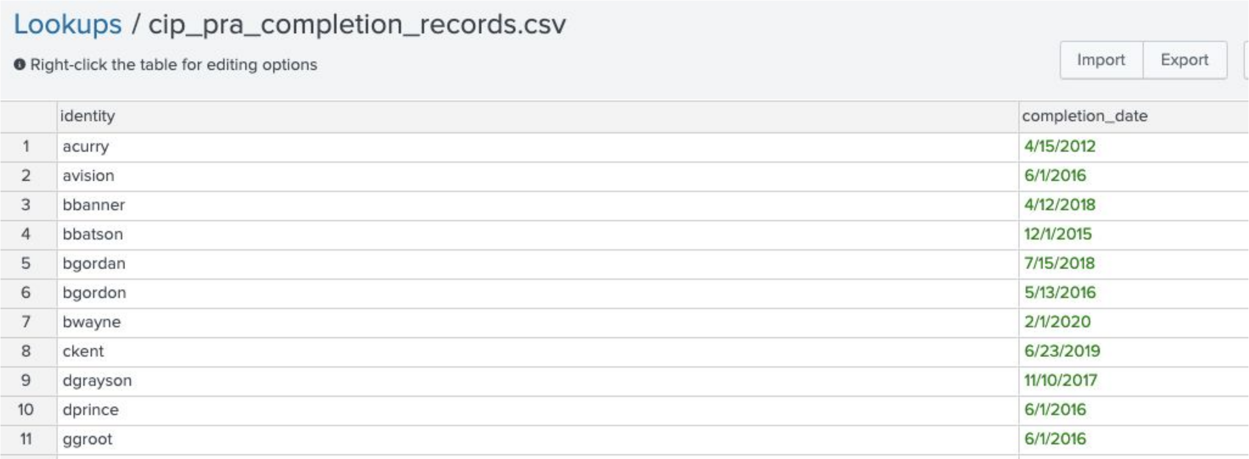
● Right-click the table for editing options

Changes are automatically saved in real-ti

	_key	config	config_asset_type	config_type	created_date	group_id
1	5f22c5c3d3be8614ae603cf1	{ "configs": [{ "software_type": "Custom", "name": "AddressBook", "version": "NA", "publisher": "NA" }, { "software_type": "Custom", "name": "Connection Manager", "version": "NA", "publisher": "NA" }, { "software_type": "Custom", "name": "DirectDrawEx", "version": "NA", "publisher": "NA" }, { "software_type": "Custom", "name": "Fontcore", "version": "NA", "publisher": "NA" }, { "software_type": "Custom", "name": "IEData", "version": "NA", "publisher": "NA" }, { "software_type": "Custom", "name": "SchedulingAgent", "version": "NA", "publisher": "NA" }, { "software_type": "Custom", "name": "WIC", "version": "NA", "publisher": "NA" }, { "software_type": "commercial", "name": "Google Chrome", "version": "81.0.4044.129", "publisher": "Google LLC" }, { "software_type": "commercial", "name": ",Google Update Helper", "version": "1.3.35.451", "publisher": "Google LLC" }, { "software_type": "commercial", "name": "IE40", "version": "NA", "publisher": "NA" }, { "software_type": "commercial", "name": "IE4Data", "version": "NA", "publisher": "NA" }, { "software_type": "commercial", "name": "IE5BAKEX", "version": "NA", "publisher": "NA" }, { "software_type": "commercial", "name": "Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.20.27508", "version": "14.20.27508.1", "publisher": "Microsoft Corporation" }, { "software_type": "commercial", "name": "Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.20.27508", "version": "14.20.27508.1", "publisher": "Microsoft Corporation" }, { "software_type": "commercial", "name": "Microsoft Visual C++ 2019 X64 Additional Runtime - 14.20.27508", "version": "14.20.27508", "publisher": "Microsoft Corporation" }, { "software_type": "commercial", "name": "Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.20.27508", "version":	computer	applications	1586791011	5eb61baa45e4364e8458b3f1

Lookup name: cip_pra_completion_records

Lookup file with a list of users and when their last personal risk assessment was completed. This lookup is used to verify individuals had a risk assessment completed at least every 15 months.

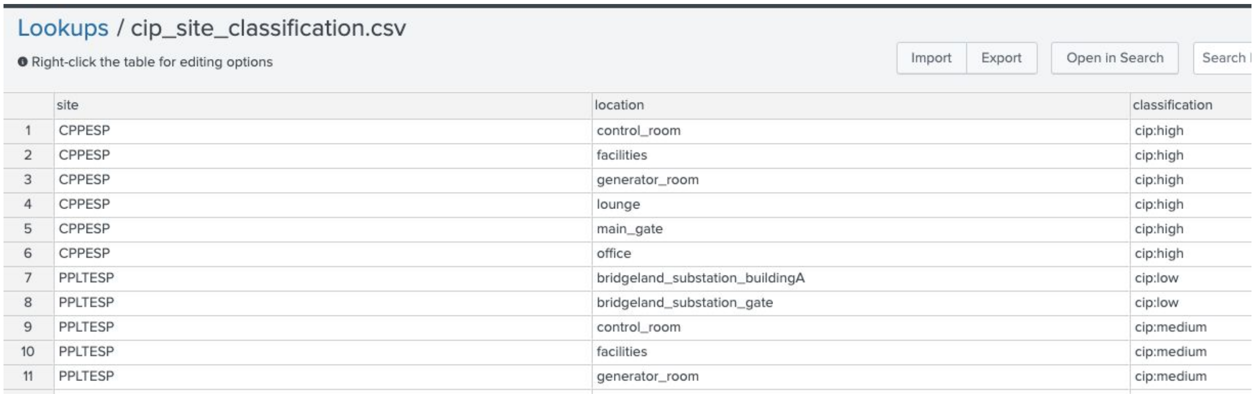


Lookups / cip_pra_completion_records.csv

	identity	completion_date
1	acurry	4/15/2012
2	avision	6/1/2016
3	bbanner	4/12/2018
4	bbatson	12/1/2015
5	bgordan	7/15/2018
6	bgordon	5/13/2016
7	bwayne	2/1/2020
8	ckent	6/23/2019
9	dgrayson	11/10/2017
10	dprince	6/1/2016
11	ggroot	6/1/2016

Lookup name: cip_site_classification

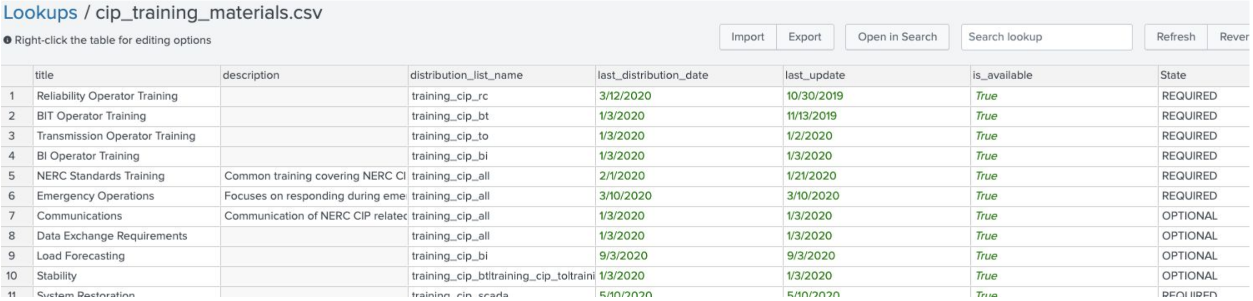
This lookup is used to classify physical security sites and locations and their respective CIP BES classification. While often sites may be classified as a single BES level this lookup provides flexibility to use alternative mechanisms for classification. Note: classifications should follow the naming convention of other lookups to include <regulation>:<classification>.



Lookups / cip_site_classification.csv

	site	location	classification
1	CPPESP	control_room	cip:high
2	CPPESP	facilities	cip:high
3	CPPESP	generator_room	cip:high
4	CPPESP	lounge	cip:high
5	CPPESP	main_gate	cip:high
6	CPPESP	office	cip:high
7	PPLTESP	bridgeland_substation_buildingA	cip:low
8	PPLTESP	bridgeland_substation_gate	cip:low
9	PPLTESP	control_room	cip:medium
10	PPLTESP	facilities	cip:medium
11	PPLTESP	generator_room	cip:medium

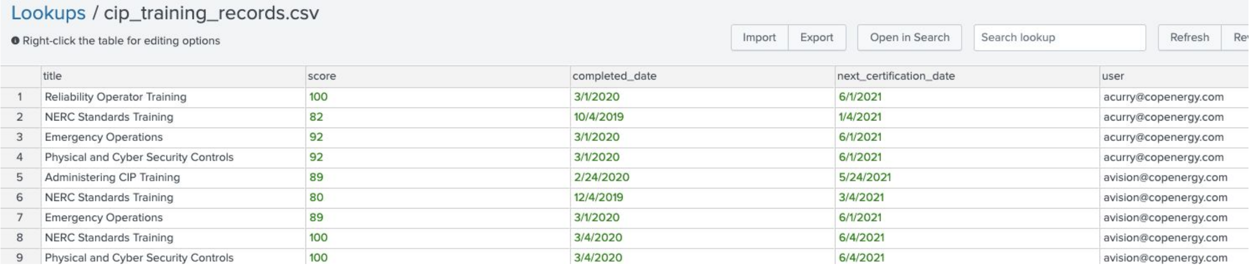
Lookup name: cip_training_materials
This lookup contains a list of all the training courses and materials that are available, including the title, description, the last time course updates were distributed, and whether the training is required or optional. It also included which groups are available to take the training.



❶ Right-click the table for editing options

	title	description	distribution_list_name	last_distribution_date	last_update	is_available	State
1	Reliability Operator Training		training_cip_rc	3/12/2020	10/30/2019	*True*	REQUIRED
2	BIT Operator Training		training_cip_bt	1/3/2020	11/13/2019	*True*	REQUIRED
3	Transmission Operator Training		training_cip_to	1/3/2020	1/2/2020	*True*	REQUIRED
4	BI Operator Training		training_cip_bi	1/3/2020	1/3/2020	*True*	REQUIRED
5	NERC Standards Training	Common training covering NERC CI	training_cip_all	2/1/2020	1/21/2020	*True*	REQUIRED
6	Emergency Operations	Focuses on responding during eme	training_cip_all	3/10/2020	3/10/2020	*True*	REQUIRED
7	Communications	Communication of NERC CIP relatec	training_cip_all	1/3/2020	1/3/2020	*True*	OPTIONAL
8	Data Exchange Requirements		training_cip_all	1/3/2020	1/3/2020	*True*	OPTIONAL
9	Load Forecasting		training_cip_bi	9/3/2020	9/3/2020	*True*	OPTIONAL
10	Stability		training_cip_btltraining_cip_toltraini	1/3/2020	1/3/2020	*True*	OPTIONAL
11	System Restoration		training_cip_scada	5/10/2020	5/10/2020	*True*	REQUIRED

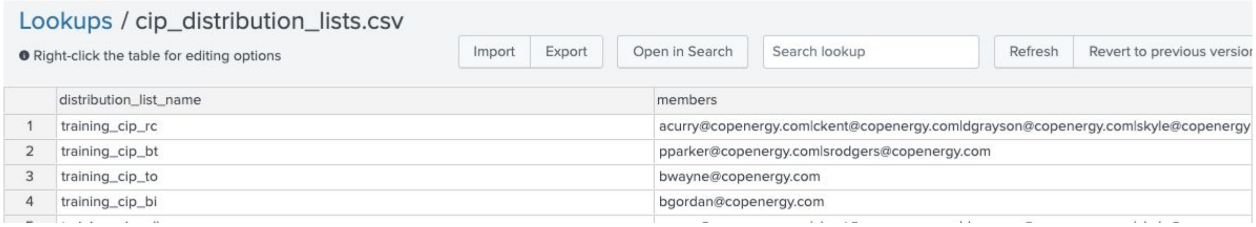
Lookup name: cip_training_records
This lookup functions as a list of courses that have been taken by individuals including when the training was completed and when it needs to be repeated. The course title should be contains in the cip_training_materials lookup.



❶ Right-click the table for editing options

	title	score	completed_date	next_certification_date	user
1	Reliability Operator Training	100	3/1/2020	6/1/2021	acurry@copenergy.com
2	NERC Standards Training	82	10/4/2019	1/4/2021	acurry@copenergy.com
3	Emergency Operations	92	3/1/2020	6/1/2021	acurry@copenergy.com
4	Physical and Cyber Security Controls	92	3/1/2020	6/1/2021	acurry@copenergy.com
5	Administering CIP Training	89	2/24/2020	5/24/2021	avision@copenergy.com
6	NERC Standards Training	80	12/4/2019	3/4/2021	avision@copenergy.com
7	Emergency Operations	89	3/1/2020	6/1/2021	avision@copenergy.com
8	NERC Standards Training	100	3/4/2020	6/4/2021	avision@copenergy.com
9	Physical and Cyber Security Controls	100	3/4/2020	6/4/2021	avision@copenergy.com

Lookup name: cip_distribution_lists
This lookup contains a list of distribution groups and the members of each group for cip training. Distribution_list_names are used in the cip_training_materials to identify individuals who would need specific training for NERC CIP compliance. Members of each list are pipe-delimeted.


Lookups / cip_distribution_lists.csv
Import
Export
Open in Search
Search lookup
Refresh
Revert to previous versior

❶ Right-click the table for editing options

	distribution_list_name	members
1	training_cip_rc	acurry@copenergy.com|ckent@copenergy.com|dgrayson@copenergy.com|skyle@copenergy
2	training_cip_bt	pparker@copenergy.com|srodgers@copenergy.com
3	training_cip_to	bwayne@copenergy.com
4	training_cip_bi	bgordan@copenergy.com

Section 7: Event typing and Alerting

Event types

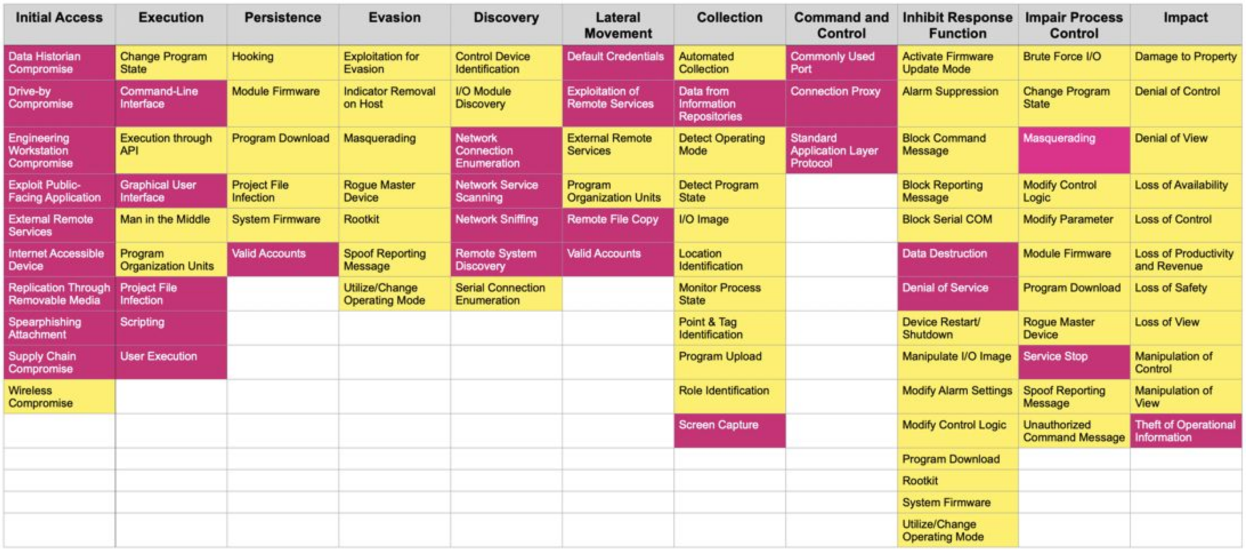
Event types provide a mechanism to classify logs and events and tag them with categories that can be searched and aggregated across multiple indexes, sources, and source types. The OT Security Add-on for Splunk includes event typing specific to MITRE ICS alerts and data from third-party OT Security solutions. The following event types are used within the solution:

mitre_ics_alert: this event type is used for all MITRE ICS-related alerts and requires the macro *get_ot_security_alerts* to define which data sources should be included. This event type is used in the correlation search *Threat - MITRE - ICS Alert Rule* to generate notable alerts. In addition, the tag mitre_ics can be used to identify these same events.

MITRE ICS Alerts

The MITRE ICS ATT&CK model was released in January 2020 and provides a framework of common technique, tactics, and procedures (TTP) for attacks on Industrial Control Systems (ICS) and OT environments. While some of these TTP's can be identified using Splunk alone, several of them require third-party support of industrial and network protocols. As a result, the OT Security Add-on for Splunk has two main kinds of alerts, those in which a TTP is identified by a third-party OT Security product or those which can be detected with Splunk alone.

The following table divides TTP's into those two categories. Items in magenta are supported by Splunk alone, while cells in yellow indicate alerts that would come from an external OT Security product. As Splunk's features evolve and integrations improve with other products, Splunk will re-evaluate which TTP's can be covered natively within Splunk.



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Correlation rules for items in magenta are covered by specific correlation searches named OT Sec - <TTP> (e.g. *OT Sec - Data Historian Compromise*). Items in yellow are covered by the *OT Sec - MITRE ICS Alert* correlation search. This correlation search requires a TTP identifier (specifically a field named technique_id) present in the events sent by the third-party product. This field is already supported by several third-party partner integrations.

Third-party OT Security Product Alerts

Third-party OT Security products often generate alerts and events relevant to Splunk Enterprise Security. These alerts are particularly valuable when they leverage the Alerts data model included in Splunk's Common Information (CIM). To include these events as notables within Splunk, enable the correlation search *OT Sec - Generic OT Security Alert*. We recommend that this correlation search is run and results are validated and searches tuned prior to enabling the rule globally. This will prevent unnecessary alerts showing up in the Enterprise Security Incident Review dashboard.

Additional OT Security Alerts

Several alerts related to NERC CIP regulations are also available in the solution. Splunk will continue to evaluate specific OT Security alerts outside of MITRE ICS on an as-needed basis. The *Access Granted for Uncertified Individual* alert can be used to identify users accessing a NERC CIP asset without the appropriate certifications. The *Unapproved Removable Media on Critical Asset* alert can be used to identify when an unauthorized removable media device has been attached to a NERC CIP asset.

Section 8: Phantom OT Security Extension

Goal

The goal for the document is to provide OT security users with guidance on the following topics:

- Overview of the Phantom OT Security Extension ("the extension")
- Introduce content and architecture
- Define requirements and steps for installation
- Provide step-by-step configuration instructions
- Recommendations on how to customize a deployment

Purpose

About the Phantom OT Security Extension

Reduce search and decision time with "bionic" capabilities

Automated research and response actions

Help every OT analyst become equally excellent

Improve decision quality and consistency across analysts

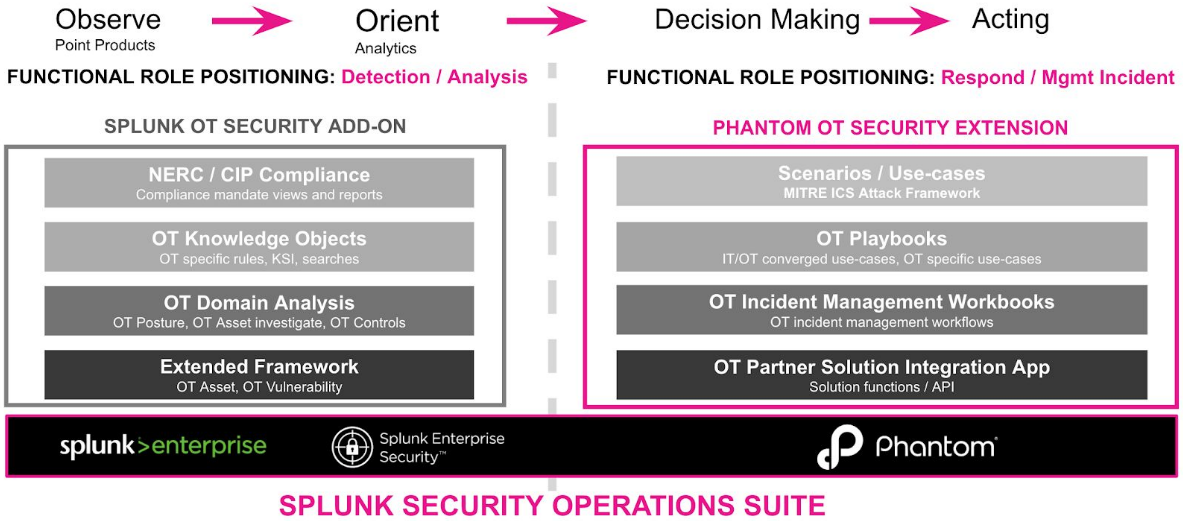
Mature OT security operations with MITRE ICS

Best-practice approach to implement extensive industry standards to sec ops

Splunk Phantom is a Security Orchestration, Automation, and Response (SOAR) system. The Splunk Phantom platform combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate your team, processes, and tools to help you orchestrate security workflows, automate repetitive security tasks, and quickly respond to threats.

The Phantom OT Security Extension ("the extension") is a content pack of workbooks and playbooks, published in Phantom community Github (https://github.com/splunk/playbooks ,https://github.com/splunk/security_content), for use in any Phantom deployment Version 4.9 or greater. The extension is tightly integrated with the Splunk OT Security Add-on for ES. As ES detects MITRE ICS ATT&CK ("MITRE ICS") tactics, the extension maps individual MITRE ICS response recommendations. With the extension, a security organization that holds responsibility for monitoring an OT environment is able to more rapidly implement automation and orchestration tactics that support MITRE ICS recommendations.

Rationale


Observe
Point Products
Orient
Analytics
Decision Making
Acting
FUNCTIONAL ROLE POSITIONING: Detection / Analysis
FUNCTIONAL ROLE POSITIONING: Respond / Mgmt Incident
SPLUNK OT SECURITY ADD-ON
NERC / CIP Compliance
Compliance mandate views and reports
OT Knowledge Objects
OT specific rules, KSI, searches
OT Domain Analysis
OT Posture, OT Asset investigate, OT Controls
Extended Framework
OT Asset, OT Vulnerability
PHANTOM OT SECURITY EXTENSION
Scenarios / Use-cases
MITRE ICS Attack Framework
OT Playbooks
IT/OT converged use-cases, OT specific use-cases
OT Incident Management Workbooks
OT incident management workflows
OT Partner Solution Integration App
Solution functions / API
splunk>enterprise
Splunk Enterprise Security™
Phantom
SPLUNK SECURITY OPERATIONS SUITE

The Phantom OT Security Extension provides templates in the form of *workbooks*, *playbooks* and actions. Workbooks map response/remediation processes (“workflows”). Playbooks are subtasks within workbooks used to automate actions. Actions are tasks, often involving connectivity to 3rd party systems, and perform discrete functions on behalf of the user or with their approval. The Phantom OT Security extensions perform actions to gather information and optionally issue commands for various OT security technologies.

- **Workbooks** are templates providing a list of standard tasks that analysts can follow when evaluating containers or cases. Workbooks can be nested within each other to create a more layered flow for cumulative events, cumulative cases, or cases that start out as one type of incident but end up as a different type of incident.
- **Playbooks** are intended to be more discreet than workbooks and are used to define a series of automation tasks that act on new data entering Splunk Phantom. For example, you can configure a playbook to perform a set of steps (“tasks”) for all new containers with a specific label.
- **Actions** are made available to Splunk Phantom by apps, providing API interactions to various security products, including Splunk Enterprise Security. See Add and configure apps and assets to provide actions in Splunk Phantom in the Administer Splunk Phantom manual.

The purpose of workbooks, playbooks and actions are to automate manual OT investigation and generate responses for consideration by security analysts, so the repetitive manual processes are reduced while responses are faster, accurate and structured.

Included Content

- **Workbooks**: OT security incident management
    - **OT security incident response -** Based on NIST 800-61, this default workbook is provided as a primary response model.
    - **MITRE ICS TTP ("Tactics Techniques Procedures") incident response --** A series of workbooks to address a subset of MITRE ICS TTPs. . These workbooks are designed to both structure and accelerate response by incorporating specific MITRE recommendations such as rapid evaluation of the proscribed mitigations within each TTP.

- **Playbooks**: OT security incident response actions
    - **Use-case orchestration playbook -** A series of investigation playbooks, ordered to execute as an incident is determined as a specific MITRE TTP incident.
    - **Playbook actions for OT security investigations -** Set of automation actions for security investigations and validations that interacts with Splunk Enterprise Security.
    - **Response automation templates -** Set of response automation templates, include sets of phantom actions (From phantom apps), that could interact with security / OT security solutions for remediation/response actions. Examples include opening tickets, quarantining a host, shutting down ports, disable users etc.

Overview

Workbooks and playbooks included within the OT security extension are designed to apply industry standards from organizations such as MITRE and NIST in responding to cyber incidents. Applied standards include NIST 800-82, 800-83, 800-61 alongside the MITRE ICS framework provide a solid foundation for OT security response. This section will review how Splunk has assembled parts of these standards into a template format which is designed to be further extended or modified at the time of deployment.

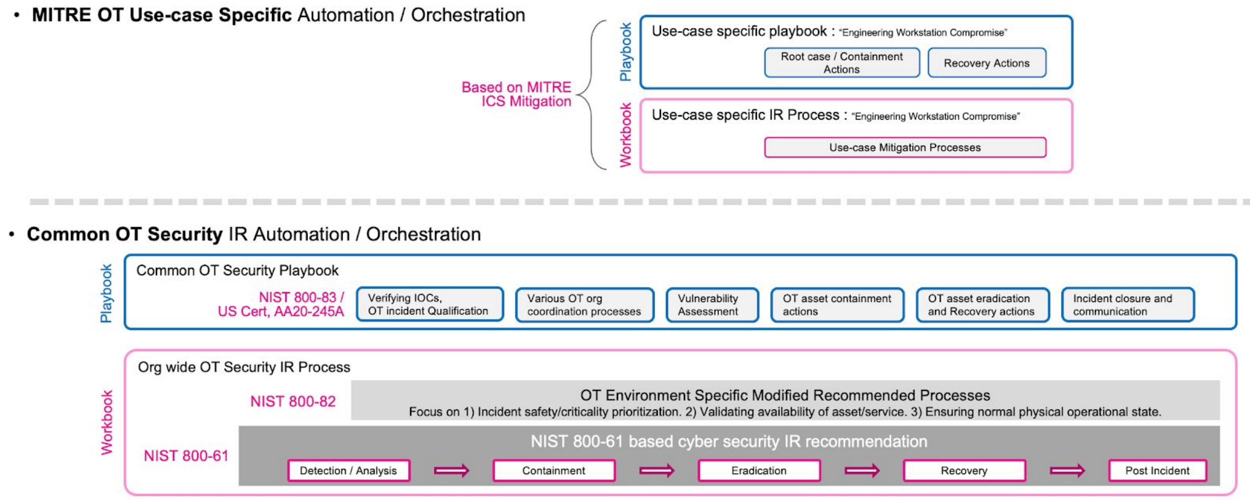

• MITRE OT Use-case Specific Automation / Orchestration
Based on MITRE ICS Mitigation
Playbook
Use-case specific playbook : "Engineering Workstation Compromise"
Root case / Containment Actions
Recovery Actions
Workbook
Use-case specific IR Process : "Engineering Workstation Compromise"
Use-case Mitigation Processes
• Common OT Security IR Automation / Orchestration
Playbook
Common OT Security Playbook
NIST 800-83 / US Cert, AA20-245A
Verifying IOCs, OT incident Qualification
Various OT org coordination processes
Vulnerability Assessment
OT asset containment actions
OT asset eradication and Recovery actions
Incident closure and communication
Workbook
Org wide OT Security IR Process
NIST 800-82
OT Environment Specific Modified Recommended Processes
Focus on 1) Incident safety/criticality prioritization. 2) Validating availability of asset/service. 3) Ensuring normal physical operational state.
NIST 800-61
NIST 800-61 based cyber security IR recommendation
Detection / Analysis
Containment
Eradication
Recovery
Post Incident

Figure 1

The design outlined in ***Figure 1*** allows organizations to easily customize the OT response process while reducing repetitive content maintenance. The provided design is to link a default OT Incident Response workbook with one or more modular MITRE ICS TTP workbook within the default OT Incident Response workbook.

Relationship between Workbooks:

- **Default OT Incident Response workbook:** Designed to provide organizational OT Incident Response process management, often OT response tasks that apply to all OT incidents.
- **MITRE ICS TTP workbook**: Designed to provide each MITRE ICS TTP specific processes. Each of these TTP workbooks is intended to be embedded within the Default OT Incident Response workbook and can be chained together in a modular fashion.

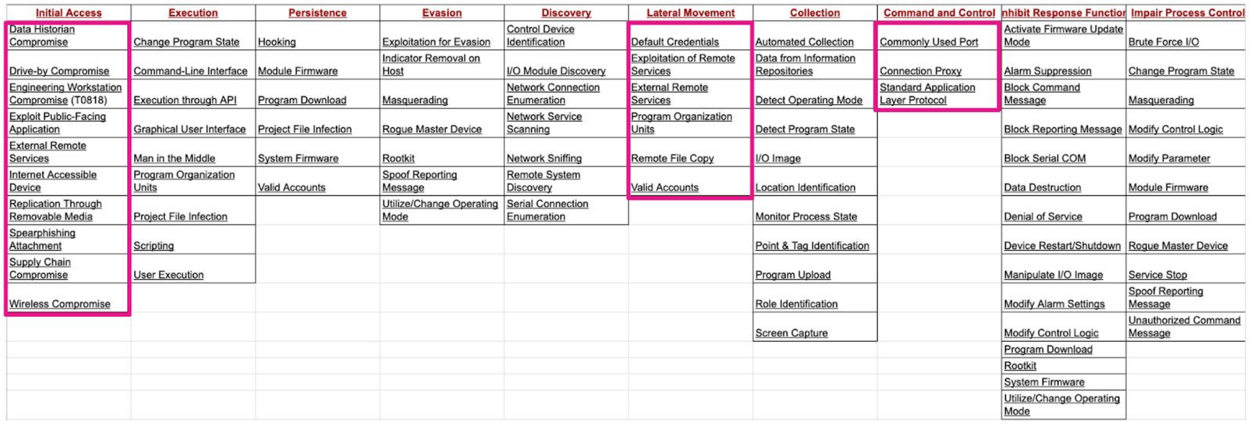
Leveraged standards for OT security workbook / playbook design include:

Documents ID	Document Descriptions
NIST SP 800-40 R2	NIST SP 800-40, Rev 2, "Creating a Patch and Vulnerability Management Program,"
NIST SP 800-53	NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems – Information Security," July 2009
NIST SP 800-61	NIST SP 800-61, Rev. 1, "Computer Security Incident Handling Guide," March 2008.
NIST SP 800-82	NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security, Final Public Draft 2009.

NIST SP 800-83	NIST SP 800-83, “Guide to Malware Incident Prevention and Handling,” November 2005
NIST SP 800-86	NIST SP 800-86, “Guide to Integrating Forensic Techniques into Incident Response,” August 2006
NIST SP 800-92	NIST SP 800-92, “Guide to Computer Security Log Management,” September 2006
US Cert, AA20-245A	Technical Approaches to Uncovering and Remediating Malicious Activity https://us-cert.cisa.gov/ncas/alerts/aa20-245a
Homeland Security ICS Security Response	Developing an Industrial Control Systems Cybersecurity Incident Response Capability

Figure 2

The included workbooks and playbooks consist of 3 categories of TTP from MITRE ICS, “Initial Access”, “Lateral Movement”, “Command and Control”. These TTP’s cover activities in the early phase of penetration and also cover broad coverage of network assets and visibility. They provide enough variety to establish a working model for how to advance a MITRE ICS approach using Phantom. Future releases may include additional MITRE ICS attack TTP categories.



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	nhibit Response Functior	Impair Process Control
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State
Engineering Workstation Compromise (T0818)	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message
						Screen Capture		Modify Control Logic	Unauthorized Command Message
								Program Download	
								Rootkit	
								System Firmware	
								Utilize/Change Operating Mode	

Figure 3

Architecture

Splunk Components

- Splunk OT Security Add-on on ES
    - Focused on detection of potential incidents, serving in the role of SIEM for combined IT/OT security. OT add-on detects and categorizes alerts based on the MITRE ICS, attaching the categorization of alerts to Phantom

- Phantom OT Security Extension
    - Receives classified alerts based on MITRE ICS, then applies automation and remediation recommendations by each MITRE ICS TTPs. Also after the automated investigations are executed, a broad-set of out-of-the-box Phantom app actions can be leveraged to contain and manage the response process.

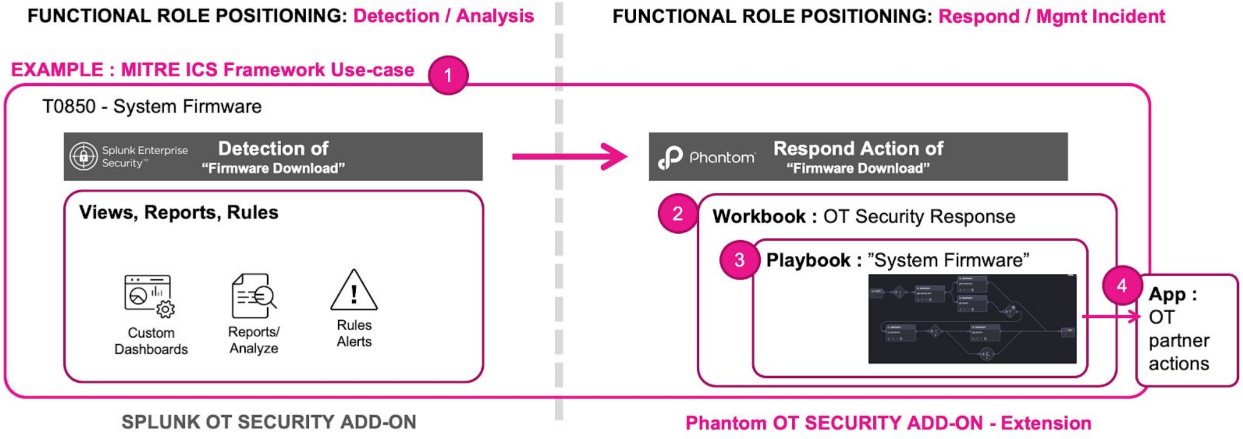

FUNCTIONAL ROLE POSITIONING: Detection / Analysis
FUNCTIONAL ROLE POSITIONING: Respond / Mgmt Incident
EXAMPLE : MITRE ICS Framework Use-case
1
T0850 - System Firmware
Splunk Enterprise Security
Detection of "Firmware Download"
Phantom
Respond Action of "Firmware Download"
Views, Reports, Rules
Custom Dashboards
Reports/ Analyze
Rules Alerts
2
Workbook : OT Security Response
3
Playbook : "System Firmware"
4
App : OT partner actions
SPLUNK OT SECURITY ADD-ON
Phantom OT SECURITY ADD-ON - Extension

Figure 4

Requirements

Environment Requirements

OT Security Add-On for Splunk: The use of Phantom OT security extension requires a completed implementation of OT Security Add-on for Splunk on Enterprise Security. Following capabilities must be ready and validated for Phantom OT security extension.

- ES environment with OT Security Add-on for Splunk
- OT Security Add-on version 2.0.1 or greater with alerts enriched with MITRE ICS T00 IDs.
- Integration between ES and Phantom, using one or more of the models outlined in ***Figure 5***
- ES data ingestion requirements

- OT asset inventory
- OT network traffic sessions
- OT network authentication sessions

Phantom Configuration

- Installation of OT security extension workbooks
- Installation of OT security extension playbooks

Required Apps

There are multiple apps required to integrate the Phantom OT Security Extension on both Phantom and Splunk ES for Phantom OT Security Extension. The intent of this section is to address preparing ES and Phantom environments for you to immediately use Phantom OT security extension with minimal customizations.

Here are required apps for ES and Phantom integrations:

Application	**Install Target**	**Usage**
Splunk App for Phantom	Phantom	Pull event data from Splunk, push event data to Splunk, add Splunk actions to Phantom playbooks.
Phantom App for Splunk	Splunk	Push Splunk/ES event data to Phantom. (https://splunkbase.splunk.com/app/3411/)
Phantom OT Security Extension	Phantom	Packages from Splunk security github. https://github.com/philroyer-phantom/playbooks

Figure 5

Installation

Installation Steps

STEP 1: Validate ES install and status of OT Security Add-on:

Validation of ES environment with OT security add-on - prior to the installation of Phantom OT security extension content, following capability and readiness must be verified. Detailed instructions covered in other parts of the OT Security solution document.

- Verify capability of asset Integration and search
- Verify data integrations, by running SPL queries on the following CIM models / Index.
  - Network
  - Authentication
  - Endpoint
  - OS/System

STEP 2: Install Phantom

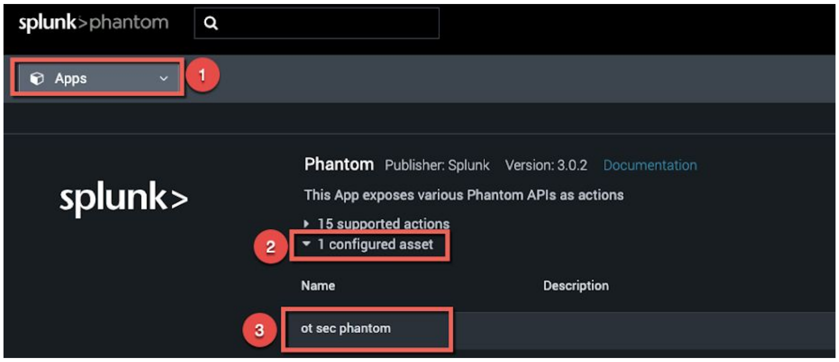
Installation procedure for Phantom can vary depending on the type of environment you have and based that your environment requirements, you can choose a different installation method of install ; Phantom on prem, self-managed cloud or as an AMI/Image from your cloud provided.

Refer to the following Splunk Phantom documentation to get started with the right option: https://docs.splunk.com/Documentation/Phantom/4.10.2/Install/Overview

STEP 3: Connect Phantom to ES (Configuring Splunk App for Phantom)

The **Splunk App for Phantom** is a Phantom app used to connect Phantom to Splunk. Phantom apps that are built by Splunk are installed in Phantom by default, so no installation is required, however, connection configuration to Splunk instances is needed.

In the asset settings, Phantom administrator needs the IP/hostname of your Splunk instance as well as a Splunk user with sufficient access to the data to be searched.

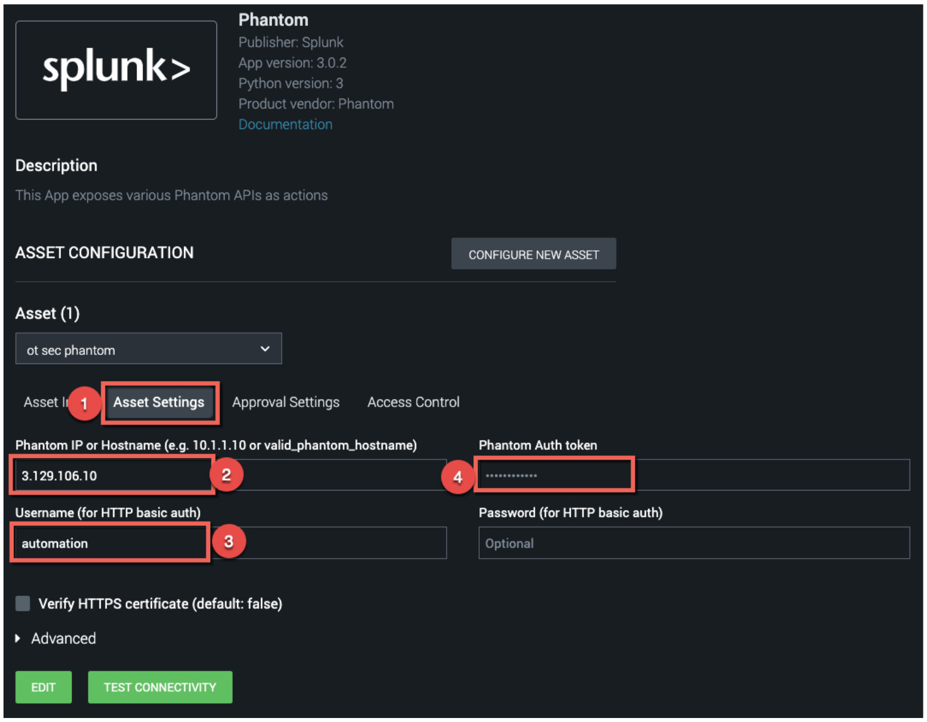


Phantom Publisher: Splunk Version: 3.0.2 Documentation

This App exposes various Phantom APIs as actions

- 15 supported actions
- 1 configured asset

Name	Description
ot sec phantom	



Phantom
Publisher: Splunk
App version: 3.0.2
Python version: 3
Product vendor: Phantom
Documentation

Description

This App exposes various Phantom APIs as actions

ASSET CONFIGURATION

Asset (1)

ot sec phantom

Phantom IP or Hostname (e.g. 10.1.1.10 or valid_phantom_hostname): 3.129.106.10

Phantom Auth token: ••••••••••••

Username (for HTTP basic auth): automation

Password (for HTTP basic auth): Optional

☐ Verify HTTPS certificate (default: false)

The Splunk App for Phantom can do the following:

- Post data to Splunk as events
- Update notable events
- Run SPL queries
- Pull events from Splunk to Phantom.

To pull events from Splunk to Phantom, configure the asset settings and ingest settings in the configured asset (> Main dropdown > App) interface. It is recommended that a new label in Phantom for the events to be pulled in from Splunk be created, which will make it easier to find the events in the Analyst Queue in Phantom.

There are four included actions which can be used in playbooks:

- get host events – retrieves events about a specific host from Splunk
- post data – creates an event in your Splunk instance

- run query – runs an SPL query in Splunk and returns the results of the search to Phantom
- update event – updates specified notable events within your Splunk Enterprise Security instance

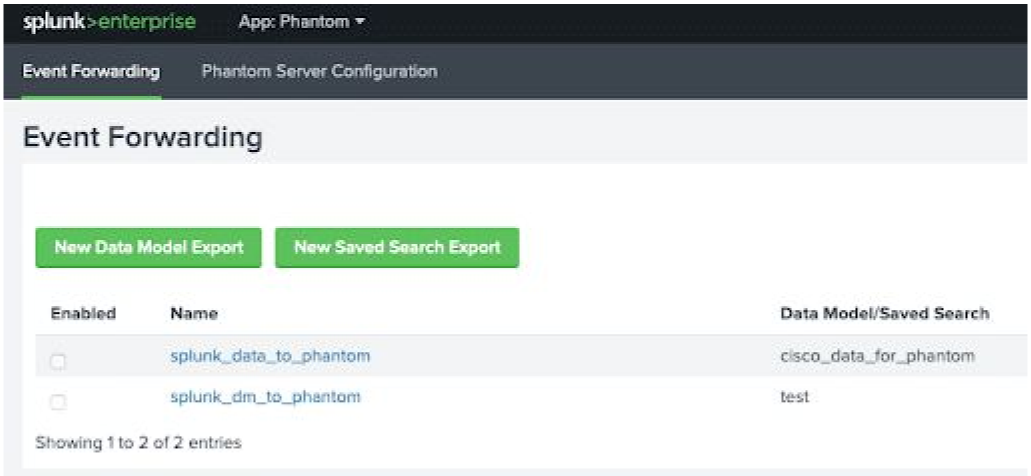
For specific details on using these actions, search for “Splunk” on the Apps page in Phantom and click the Documentation link. (https://docs.splunk.com/Documentation/Phantom/4.10.1/Admin/AppsAssets)

STEP 4: Connect Splunk ES to Phantom (Configuring Phantom App for Splunk)

The Phantom App for Splunk is a Splunkbase app that is installed in Splunk and connects Splunk to Phantom. The main function of this app is to send data from Splunk to Phantom.

First, go through the Phantom Server Configuration page to connect Splunk to Phantom, which will require an automation user in Phantom.

To send events to Phantom, create a saved search in Splunk where the results of the search are the events you want ingested into Phantom. Open the Phantom App for Splunk and create a New Saved Search Export to start sending events over. There is also an option to create a Data Model Export, which follows the same set of steps used for exporting saved search results to Phantom:



Event Forwarding

Enabled	Name	Data Model/Saved Search
□	splunk_data_to_phantom	cisco_data_for_phantom
□	splunk_dm_to_phantom	test

Showing 1 to 2 of 2 entries

As optional features to understand, this app also contains alert actions that can be used in Splunk Enterprise Security:

- Send to Phantom – sends the event(s) that triggered the alert to Phantom
- Run Playbook in Phantom – sends the event(s) that triggered the alert to Phantom and runs the specified playbook on them

For more information about the Phantom App for Splunk, review the following documents:

- https://docs.splunk.com/Documentation/PhantomApp
- https://my.phantom.us/4.6/docs/admin/splunk

STEP 5: Workbook Installation

To install OT security workbooks, access the Phantom server's shell then run the import script to import shared OT security workbooks. To do this, download the latest zipped workbooks from Github, then upload it to Phantom server.

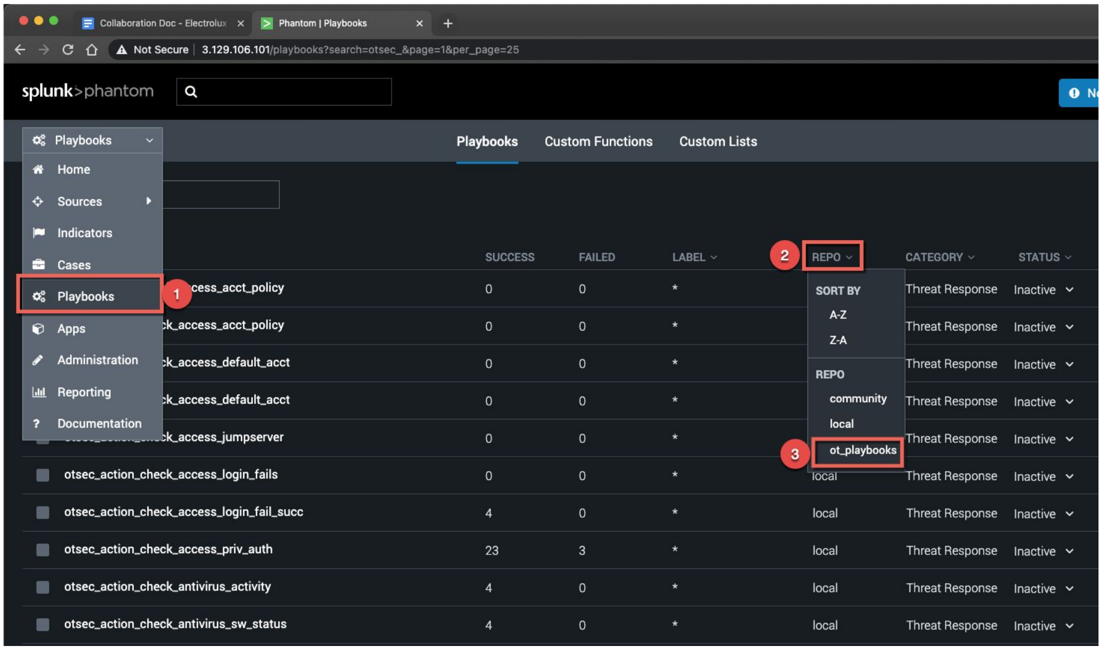
- Download zip files with OT security workbooks
    - URL: https://github.com/splunk (To Be confirmed)
- Unzip the downloaded workbook file ot_security_workbooks.tar.gz. sftp / scp over to Phantom server.
    - scp ot_security_workbooks.tar.gz splunk@PHANTOM_IP:/tmp/
- Get access to Phantom server linux shell
    - ssh splunk@PHANTOM_IP
    - cd /tmp/
    - tar xvfz ot_security_workbooks.tar.gz
- Importing workbooks
    - Syntax:
        - case_templates_import_export.py --import "exported_workbook_filename"

```
# case_templates_import_export.py --import
ot_sec_workbook_export_01
```

STEP 6: Playbook Installation

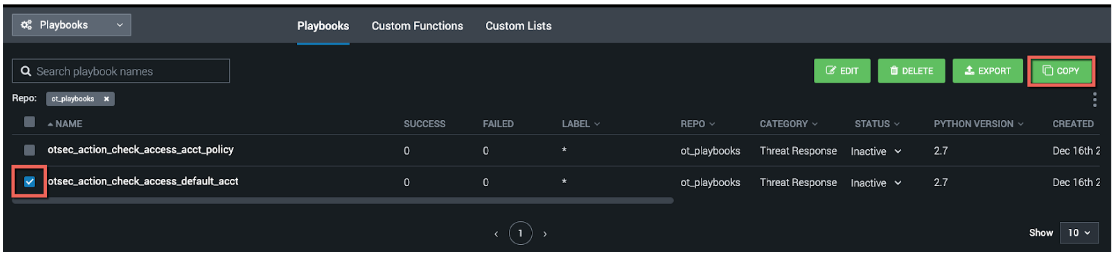
To install the playbook, use the product community GIThub to access the extension content by selecting the repo as "ot_playbooks" in your phantom product, then save them into your "local" repo before you customize the playbook for your environment.

- Go to Playbook administration interface, select "**REPO**" column to select ot_playbooks community repo. This will bring all the playbooks in the community ot_playbooks repo.



	SUCCESS	FAILED	LABEL ⌄	REPO ⌄	CATEGORY ⌄	STATUS ⌄
cess_acct_policy	0	0	*		Threat Response	Inactive ⌄
k_access_acct_policy	0	0	*		Threat Response	Inactive ⌄
k_access_default_acct	0	0	*		Threat Response	Inactive ⌄
k_access_default_acct	0	0	*		Threat Response	Inactive ⌄
k_access_jumpserver	0	0	*		Threat Response	Inactive ⌄
otsec_action_check_access_login_fails	0	0	*	local	Threat Response	Inactive ⌄
otsec_action_check_access_login_fail_succ	4	0	*	local	Threat Response	Inactive ⌄
otsec_action_check_access_priv_auth	23	3	*	local	Threat Response	Inactive ⌄
otsec_action_check_antivirus_activity	4	0	*	local	Threat Response	Inactive ⌄
otsec_action_check_antivirus_sw_status	4	0	*	local	Threat Response	Inactive ⌄

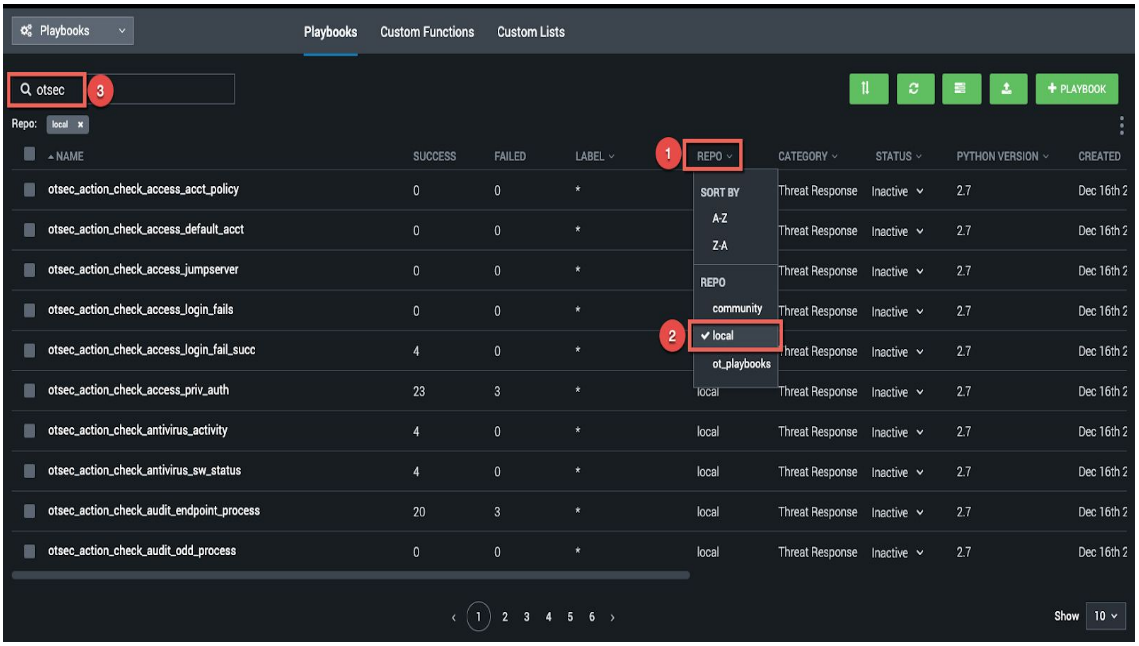
- From the ot_playbooks repo, select the playbook to install, then copy it to the local repo for you to create a local version of the playbook for customization.



	▴ NAME	SUCCESS	FAILED	LABEL ⌄	REPO ⌄	CATEGORY ⌄	STATUS ⌄	PYTHON VERSION ⌄	CREATED
□	otsec_action_check_access_acct_policy	0	0	*	ot_playbooks	Threat Response	Inactive ⌄	2.7	Dec 16th 2
☑	otsec_action_check_access_default_acct	0	0	*	ot_playbooks	Threat Response	Inactive ⌄	2.7	Dec 16th 2

- Set the “Playbook Name” same as the original OT security playbook, and just save it to the “local” repo. This saves the playbook into the local Phantom instance so you can modify them. Repeat the procedure to copy all other playbooks from “ot_playbooks” community repo to “local’ repo for the playbook installation.

- Once all the playbooks are copied to local instance, select “REPO” to “local” and search for “otsec” playbooks installed in your local instance.



NAME	SUCCESS	FAILED	LABEL	REPO	CATEGORY	STATUS	PYTHON VERSION	CREATED
otsec_action_check_access_acct_policy	0	0	*		Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_access_default_acct	0	0	*		Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_access_jumpserver	0	0	*		Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_access_login_fails	0	0	*		Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_access_login_fail_succ	4	0	*		Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_access_priv_auth	23	3	*	local	Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_antivirus_activity	4	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_antivirus_sw_status	4	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_audit_endpoint_process	20	3	*	local	Threat Response	Inactive	2.7	Dec 16th 2
otsec_action_check_audit_odd_process	0	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2

Workbook Customization Guide

The reasons for customizing different types of workbooks included with Phantom OT security extensions are as follows:

- OT security incident response workbook - Customize the OT response process specific to your organization, adding specific tasks to address internal Incident response or supporting OT asset owner requested requirements
- MITRE ICS TTP workbooks - Phantom OT Security extension playbooks includes tasks suggested by each of MITRE ICS TTP use-case recommendations. If there are additional tasks per MITRE ICS TTP level to address conditions such as special topology or solutions owned by the sec operations, administrators should add / modify tasks per TTP.

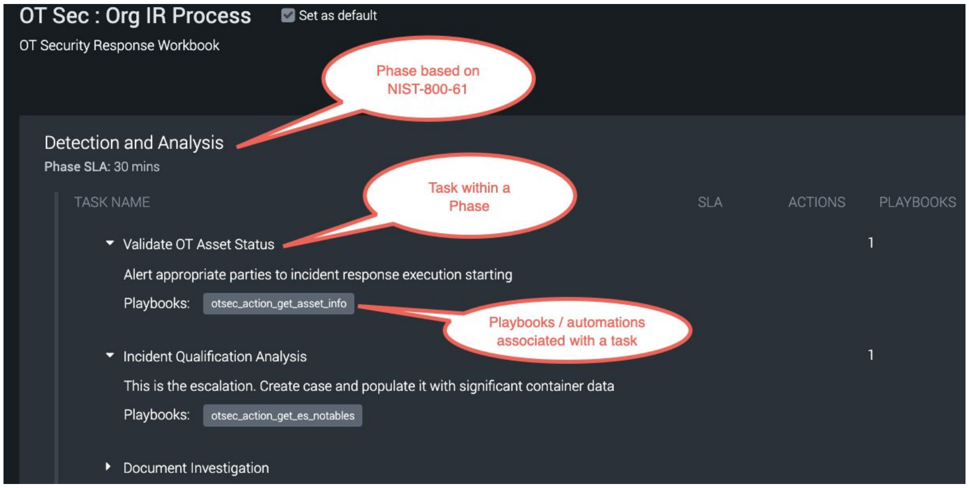
Customizing OT Incident Response (IR) workbooks

Guidance on “Org OT incident IR” workbooks:

- **Phase** - Defined as a phase of a response process. According to NIST 800-61, typically phases include: Detection, Analysis, Containment, Eradication and Post. While it is uncommon to add additional phases beyond those outlined by NIST, specific organizational approaches to incident response can be substituted as needed.
- **Tasks** - Each task belongs to a “Phase” of the workbook. For example, “Validate OT Asset Status,” which looks up the asset detail involved in an incident, is a

task performed during “Detection and Analysis”. Additional tasks each may be added to support organizational or site specific workflows.

- **Playbooks** - Automation playbooks get assigned to a task to automate that particular task. Organization and site specific customization to add/subtract automation playbooks is supported.



OT Sec : Org IR Process ☑ Set as default

OT Security Response Workbook

Detection and Analysis

Phase SLA: 30 mins

TASK NAME	SLA	ACTIONS	PLAYBOOKS
▾ Validate OT Asset Status Alert appropriate parties to incident response execution starting Playbooks: otsec_action_get_asset_info			1
▾ Incident Qualification Analysis This is the escalation. Create case and populate it with significant container data Playbooks: otsec_action_get_es_notables			1
▸ Document Investigation			

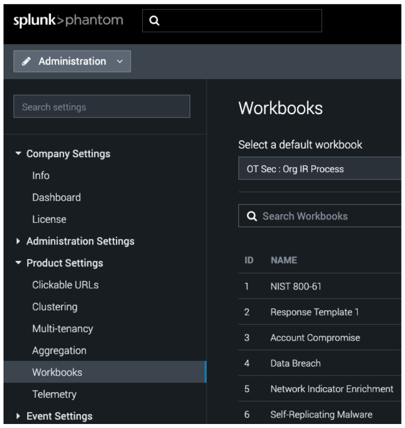
Phase based on NIST-800-61

Task within a Phase

Playbooks / automations associated with a task

Instructions on accessing MITRE ICS TTP Workbooks:

- Open Phantom Administration for workbook: > Administration > Product Settings > Workbooks

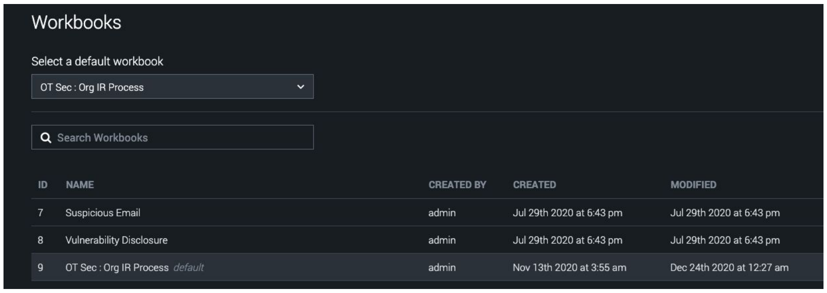


Workbooks

Select a default workbook: OT Sec : Org IR Process

ID	NAME
1	NIST 800-61
2	Response Template 1
3	Account Compromise
4	Data Breach
5	Network Indicator Enrichment
6	Self-Replicating Malware

- Select “OT Sec: Org IR Process” to edit OT Sec: Org IR Process workbook



Workbooks

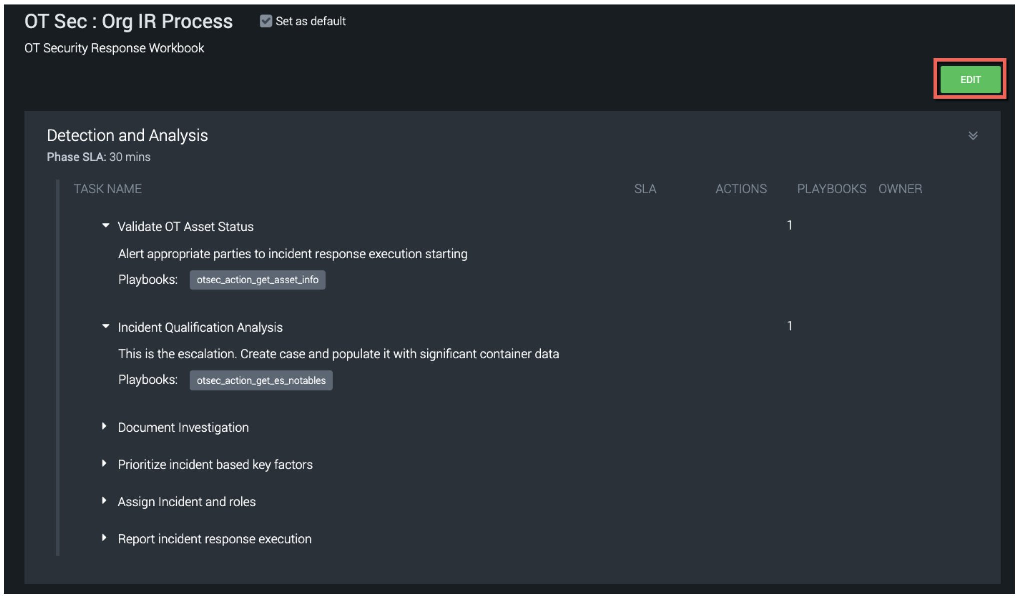
Select a default workbook

OT Sec : Org IR Process

Search Workbooks

ID	NAME	CREATED BY	CREATED	MODIFIED
7	Suspicious Email	admin	Jul 29th 2020 at 6:43 pm	Jul 29th 2020 at 6:43 pm
8	Vulnerability Disclosure	admin	Jul 29th 2020 at 6:43 pm	Jul 29th 2020 at 6:43 pm
9	OT Sec : Org IR Process *default*	admin	Nov 13th 2020 at 3:55 am	Dec 24th 2020 at 12:27 am

- Select “Edit” to edit the template. Here add your organization specific processes. As an example, an organization might require that asset owners be notified of any incident occurring within Purdue model layerL2 or below. To support this requirement, define a process within “Containment and Eradication” to add such a task.



OT Sec : Org IR Process ☑ Set as default

OT Security Response Workbook

Detection and Analysis

Phase SLA: 30 mins

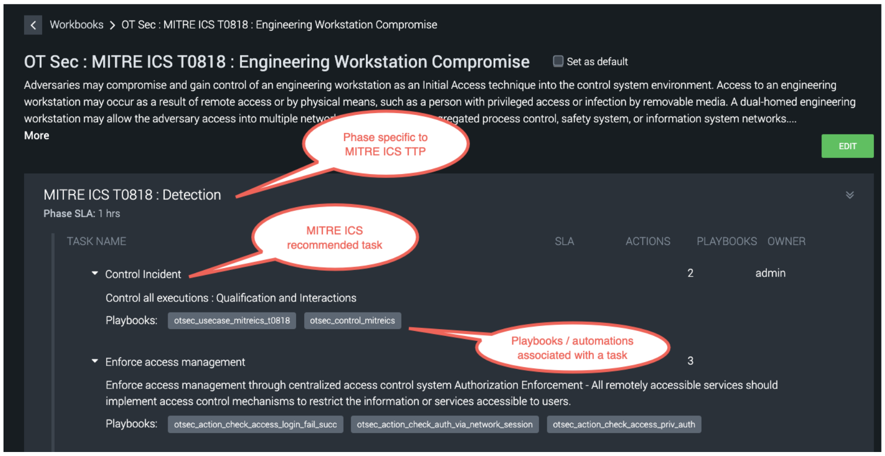
TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▾ Validate OT Asset Status Alert appropriate parties to incident response execution starting Playbooks: otsec_action_get_asset_info			1	
▾ Incident Qualification Analysis This is the escalation. Create case and populate it with significant container data Playbooks: otsec_action_get_es_notables			1	
▸ Document Investigation				
▸ Prioritize incident based key factors				
▸ Assign Incident and roles				
▸ Report incident response execution				

Customizing MITRE ICS TTP workbooks

Guidance on “MITRE ICS TTP” workbooks:

- **Phase** - Added phase for each categorized incident, so the phase name will be the MITRE ICS TTP. Note: customized or newly added TTP workbooks ***will not be changed or overridden*** by future updates as Splunk releases more content
- **Tasks** - According to MITRE ICS mitigation recommendations, specific mitigations are recommended as default. Additional tasks can be added/subtracted for specific site requirements, but these TTP use-case content should be used as default. These tasks can be updated with future release of the extension.

- **Playbooks** - Similar to the tasks, additional automation playbooks can be added or subtract the default automation playbook.


Workbooks > OT Sec : MITRE ICS T0818 : Engineering Workstation Compromise
□ Set as default
More
EDIT

OT Sec : MITRE ICS T0818 : Engineering Workstation Compromise

Adversaries may compromise and gain control of an engineering workstation as an Initial Access technique into the control system environment. Access to an engineering workstation may occur as a result of remote access or by physical means, such as a person with privileged access or infection by removable media. A dual-homed engineering workstation may allow the adversary access into multiple netwo regated process control, safety system, or information system networks....

Phase specific to MITRE ICS TTP

MITRE ICS T0818 : Detection

Phase SLA: 1 hrs

MITRE ICS recommended task

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
Control Incident			2	admin
Enforce access management			3	

Control Incident: Control all executions : Qualification and Interactions

Playbooks: otsec_usecase_mitreics_t0818 otsec_control_mitreics

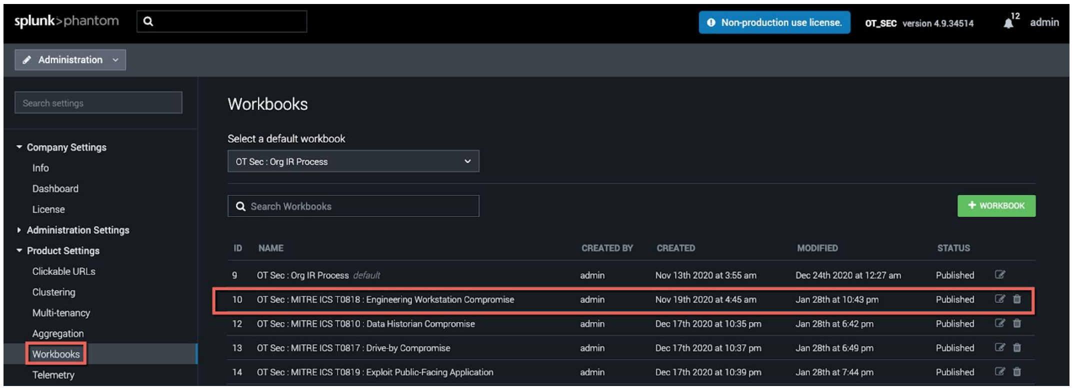
Playbooks / automations associated with a task

Enforce access management: Enforce access management through centralized access control system Authorization Enforcement - All remotely accessible services should implement access control mechanisms to restrict the information or services accessible to users.

Playbooks: otsec_action_check_access_login_fail_succ otsec_action_check_auth_via_network_session otsec_action_check_access_priv_auth

Instruction on accessing MITRE ICS TTP Workbooks:

- Enter into Phantom administration for workbook: > Administration > Product Settings > Workbooks, then select workbooks with “OT Sec: MITRE ICS Txx: ….”

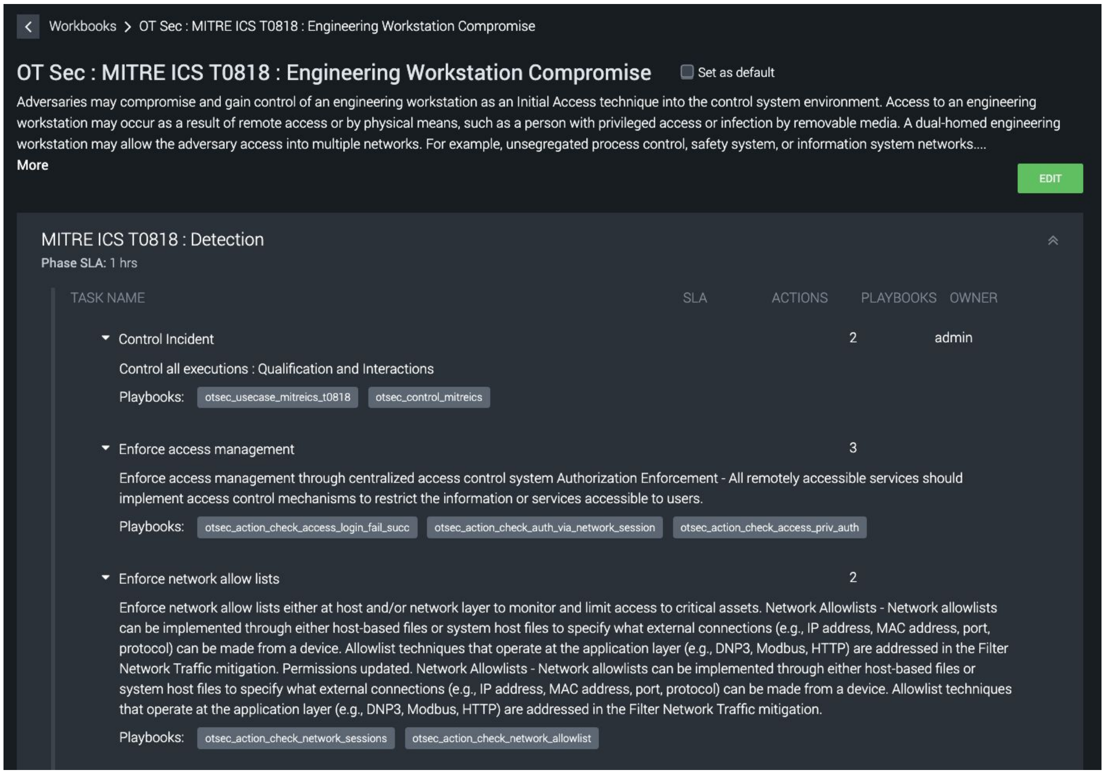


Workbooks

Select a default workbook: OT Sec : Org IR Process

ID	NAME	CREATED BY	CREATED	MODIFIED	STATUS
9	OT Sec : Org IR Process *default*	admin	Nov 13th 2020 at 3:55 am	Dec 24th 2020 at 12:27 am	Published
10	OT Sec : MITRE ICS T0818 : Engineering Workstation Compromise	admin	Nov 19th 2020 at 4:45 am	Jan 28th at 10:43 pm	Published
12	OT Sec : MITRE ICS T0810 : Data Historian Compromise	admin	Dec 17th 2020 at 10:35 pm	Jan 28th at 6:42 pm	Published
13	OT Sec : MITRE ICS T0817 : Drive-by Compromise	admin	Dec 17th 2020 at 10:37 pm	Jan 28th at 6:49 pm	Published
14	OT Sec : MITRE ICS T0819 : Exploit Public-Facing Application	admin	Dec 17th 2020 at 10:39 pm	Jan 28th at 7:44 pm	Published

- Select “Edit” to enter into workbook edit mode.



Workbooks > OT Sec : MITRE ICS T0818 : Engineering Workstation Compromise

OT Sec : MITRE ICS T0818 : Engineering Workstation Compromise

□ Set as default

Adversaries may compromise and gain control of an engineering workstation as an Initial Access technique into the control system environment. Access to an engineering workstation may occur as a result of remote access or by physical means, such as a person with privileged access or infection by removable media. A dual-homed engineering workstation may allow the adversary access into multiple networks. For example, unsegregated process control, safety system, or information system networks....

More

EDIT

MITRE ICS T0818 : Detection

Phase SLA: 1 hrs

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▾ Control Incident			2	admin

Control all executions : Qualification and Interactions

Playbooks: otsec_usecase_mitreics_t0818 otsec_control_mitreics

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▾ Enforce access management			3	

Enforce access management through centralized access control system Authorization Enforcement - All remotely accessible services should implement access control mechanisms to restrict the information or services accessible to users.

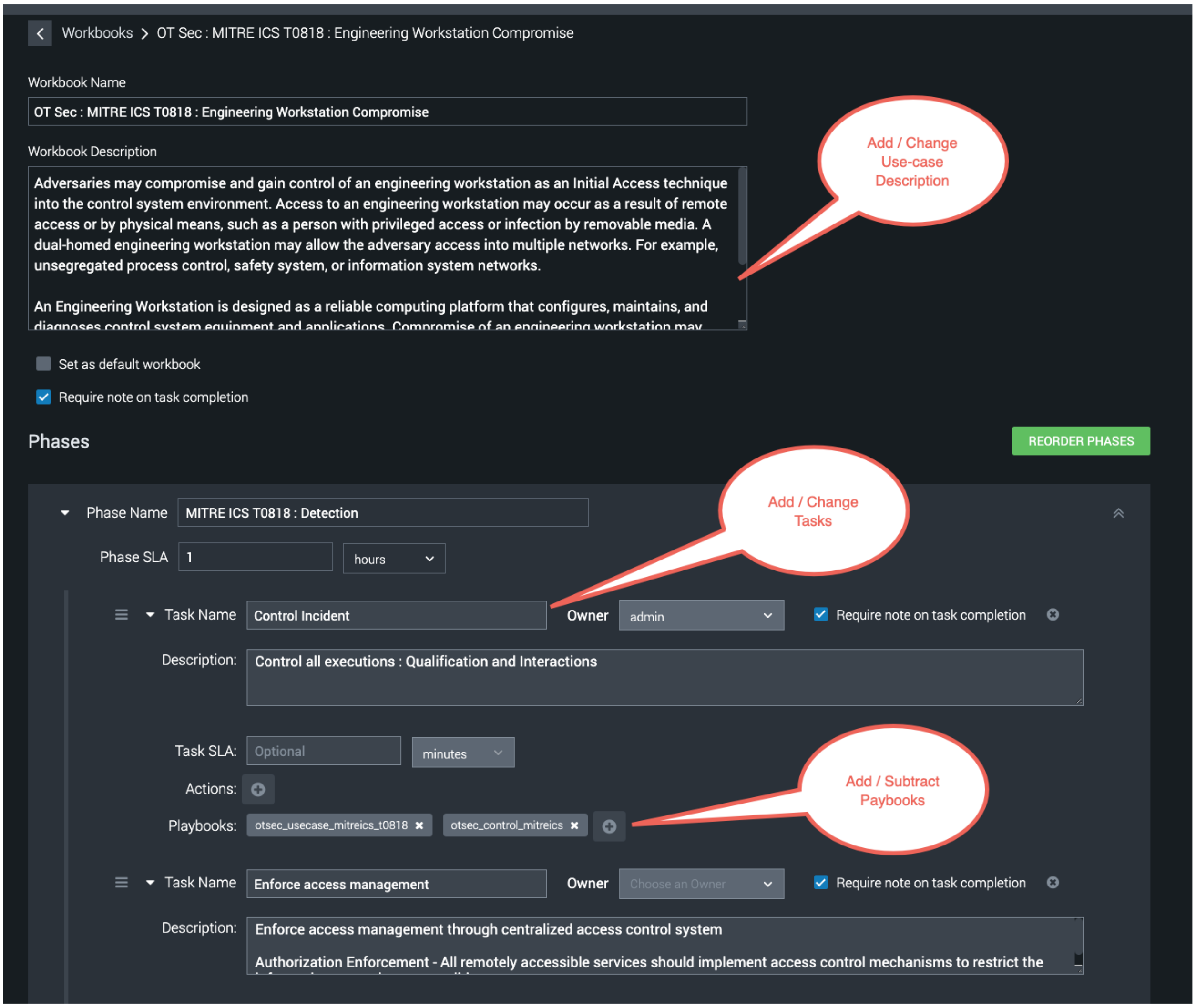
Playbooks: otsec_action_check_access_login_fail_succ otsec_action_check_auth_via_network_session otsec_action_check_access_priv_auth

TASK NAME	SLA	ACTIONS	PLAYBOOKS	OWNER
▾ Enforce network allow lists			2	

Enforce network allow lists either at host and/or network layer to monitor and limit access to critical assets. Network Allowlists - Network allowlists can be implemented through either host-based files or system host files to specify what external connections (e.g., IP address, MAC address, port, protocol) can be made from a device. Allowlist techniques that operate at the application layer (e.g., DNP3, Modbus, HTTP) are addressed in the Filter Network Traffic mitigation. Permissions updated. Network Allowlists - Network allowlists can be implemented through either host-based files or system host files to specify what external connections (e.g., IP address, MAC address, port, protocol) can be made from a device. Allowlist techniques that operate at the application layer (e.g., DNP3, Modbus, HTTP) are addressed in the Filter Network Traffic mitigation.

Playbooks: otsec_action_check_network_sessions otsec_action_check_network_allowlist

- From the workbook editor: edit / change TTP descriptions, add change “Tasks”, and/or add/subtract “playbooks” to modify the behavior of any existing or newly added MITRE ICS TTP workbook.



Workbooks > OT Sec : MITRE ICS T0818 : Engineering Workstation Compromise

Workbook Name

OT Sec : MITRE ICS T0818 : Engineering Workstation Compromise

Workbook Description

Adversaries may compromise and gain control of an engineering workstation as an Initial Access technique into the control system environment. Access to an engineering workstation may occur as a result of remote access or by physical means, such as a person with privileged access or infection by removable media. A dual-homed engineering workstation may allow the adversary access into multiple networks. For example, unsegregated process control, safety system, or information system networks.

An Engineering Workstation is designed as a reliable computing platform that configures, maintains, and diagnoses control system equipment and applications. Compromise of an engineering workstation may

□ Set as default workbook

☑ Require note on task completion

Phases

Phase Name: MITRE ICS T0818 : Detection

Phase SLA: 1 hours

Task Name: Control Incident | Owner: admin | ☑ Require note on task completion

Description: Control all executions : Qualification and Interactions

Task SLA: Optional minutes

Actions:

Playbooks: otsec_usecase_mitreics_t0818 ✖ otsec_control_mitreics ✖

Task Name: Enforce access management | Owner: Choose an Owner | ☑ Require note on task completion

Description: Enforce access management through centralized access control system

Authorization Enforcement - All remotely accessible services should implement access control mechanisms to restrict the

Playbook Customization Guide

The reasons for customizing different types of playbooks included with Phantom OT security extensions are:

- MITRE ICS TTP automation playbooks - Use the “metrics” labeled playbooks to orchestrate automations of multiple response actions in the desired order for each TTP use-cases.
- OT security response actions playbooks - These are specific action level playbooks that accomplish an action, where an action can be a investigation search/report, changing the state of an element, or

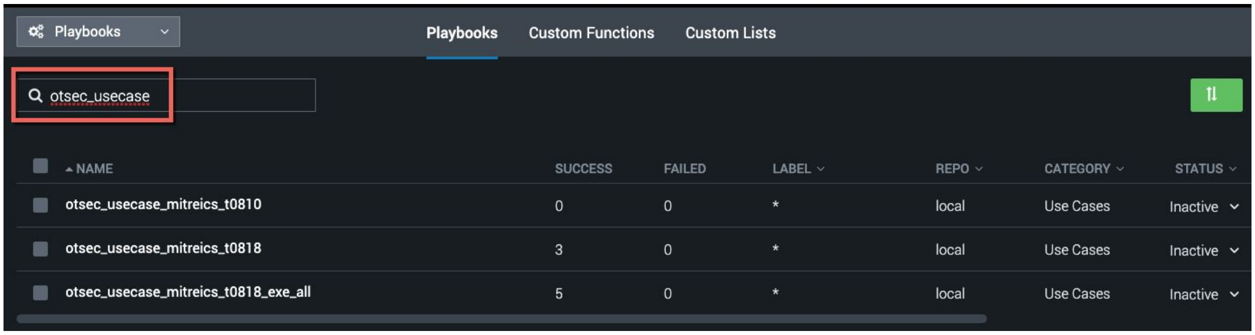
Customizing MITRE ICS TTP automation playbooks

Guidance on “MITRE ICS TTP” automation playbooks:

- The purpose of the MITRE ICS TTP automation playbooks is to automate execution of all tasks related to a categorized MITRE incident. Use the provided example as the template defines what will be automated for that peculiar MITRE ICSincident type. This playbook calls many of the smaller “OT security response actions playbooks” to automatically kick-off multiple tasks actions associated with an incident.
- Here is the recommendation on what to be customized:
    - Adding playbooks or actions the organization additionally wants to add, those are not included as the part of this extension.
    - If the organization doesn't want to automate the entire sequence of the playbooks for the MITRE ICS use-case, and rather prefers an analyst to manually and selectly execute automated actions, then those playbook actions should be removed from the MITRE ICS TTP automation playbooks.

Accessing “MITRE ICS TTP” automation playbooks:

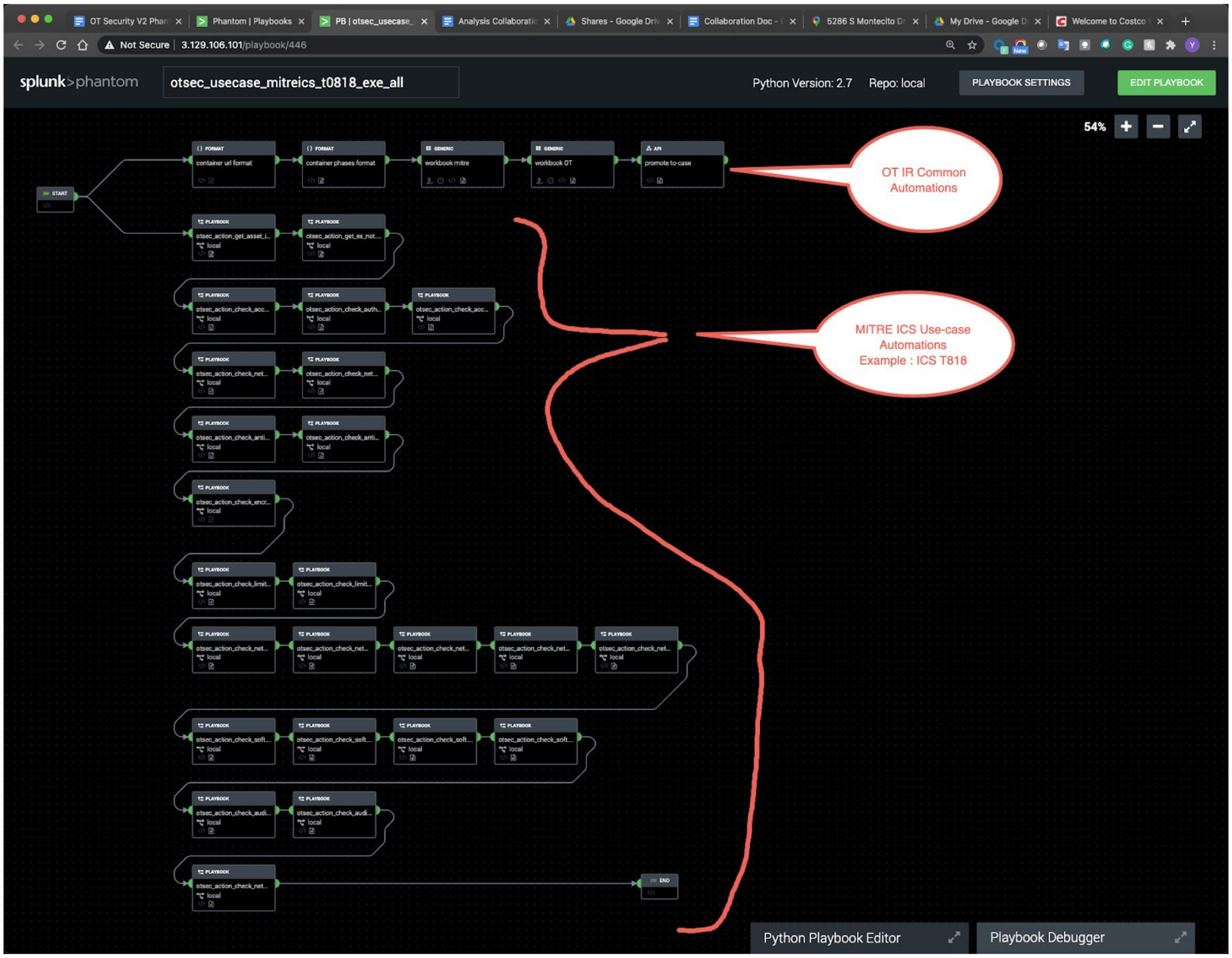
- Enter into Phantom “Playbooks” interface: > Main interface dropdown selection > “Playbooks”, then search for “otsec_usecase”



otsec_usecase

NAME	SUCCESS	FAILED	LABEL	REPO	CATEGORY	STATUS
otsec_usecase_mitreics_t0810	0	0	*	local	Use Cases	Inactive
otsec_usecase_mitreics_t0818	3	0	*	local	Use Cases	Inactive
otsec_usecase_mitreics_t0818_exe_all	5	0	*	local	Use Cases	Inactive

- Select a “otsec_usecase” playbook for editing


Not Secure 3.129.106.101/playbook/446
splunk>phantom
PLAYBOOK SETTINGS
EDIT PLAYBOOK
54%
START
FORMAT
container url format
FORMAT
container phases format
GENERIC
workbook mitre
GENERIC
workbook OT
API
promote to-case
PLAYBOOK
otsec_action_get_asset_i...
otsec_action_get_es_not...
otsec_action_check_acc...
otsec_action_check_auth...
otsec_action_check_net...
otsec_action_check_anti...
otsec_action_check_encr...
otsec_action_check_limit...
otsec_action_check_soft...
otsec_action_check_audi...
local
END
Python Playbook Editor
Playbook Debugger

otsec_usecase_mitreics_t0818_exe_all

Python Version: 2.7 Repo: local

OT IR Common Automations

MITRE ICS Use-case Automations Example : ICS T818

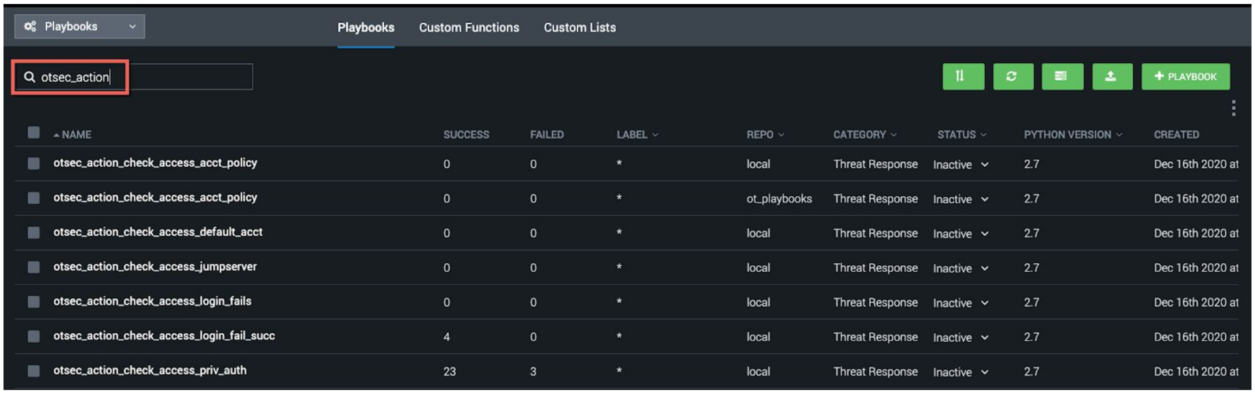
Customizing OT security response action playbooks

Guidance on “OT security response actions” automation playbooks:

- Most of the playbooks help automate investigation and gathering important context if it exists. Many of these playbooks use Enterprise Security and/or access CIM models to do various searching and analysis to address MITRE mitigation ICS recommendations. That means as the reference architecture, we recommend various security solutions to be integrated to ES, to store all necessary investigative details for each point security solution. If the deployment follows the reference architecture suggested, the idea is that many automation playbooks should work out of the box with minimal adjustment.
- Here are a couple of reasons why some of the instigation automation playbook supplied by this OT extension should be modified:
    - Most likely situation - Required some tuning of the investigated search syntax already embedded in the supplied playbook because there some site specific adjustment needs to be made. Like defining zones that are site specific, if the search references some condition about zones.
    - Not recommended - Not all the security point solutions are integrated with ES, where the collected data is properly stored in CIM.
    - Not recommended - Prefers direct communication with point security solution instead of ES integration for collecting the relevant data

Instruction on accessing “OT response actions” playbooks:

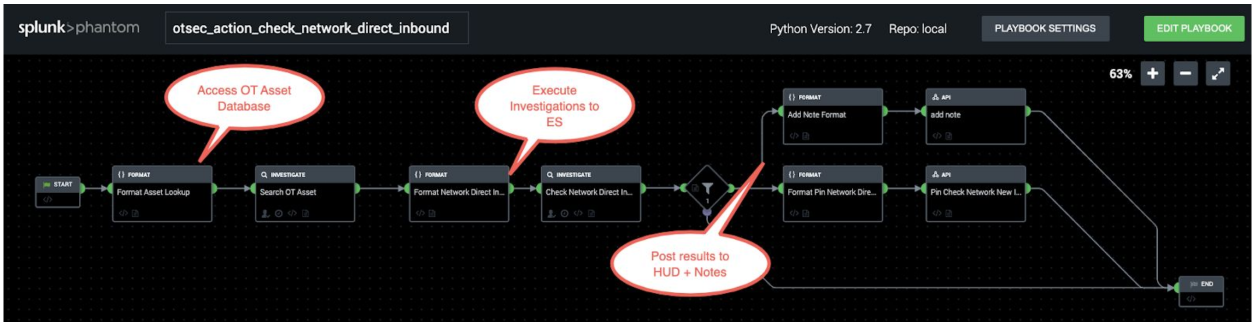
- Enter into Phantom “Playbooks” interface: > Main interface dropdown selection > “Playbooks”, then search for “otsec_usecase”.



otsec_action

NAME	SUCCESS	FAILED	LABEL	REPO	CATEGORY	STATUS	PYTHON VERSION	CREATED
otsec_action_check_access_acct_policy	0	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2020 at
otsec_action_check_access_acct_policy	0	0	*	ot_playbooks	Threat Response	Inactive	2.7	Dec 16th 2020 at
otsec_action_check_access_default_acct	0	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2020 at
otsec_action_check_access_jumpserver	0	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2020 at
otsec_action_check_access_login_fails	0	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2020 at
otsec_action_check_access_login_fail_succ	4	0	*	local	Threat Response	Inactive	2.7	Dec 16th 2020 at
otsec_action_check_access_priv_auth	23	3	*	local	Threat Response	Inactive	2.7	Dec 16th 2020 at

- Select the playbook with “otsec_action” label



Phantom OT Security Extension Workbook Catalog

Workbook Name	Description
OT Sec: Org IR Process	OT Incident default workbook, gets assign to all OT incidents
OT Sec: MITRE ICS T0818: Engineering Workstation Compromise	MITRE ICS TTP workbook for T0818 “TTP” workbooks are additional workbooks that get attached.
OT Sec: MITRE ICS T0810: Data Historian Compromise	MITRE ICS TTP workbook for T0810
OT Sec: MITRE ICS T0817: Drive-by Compromise	MITRE ICS TTP workbook for T0817
OT Sec: MITRE ICS T0819: Exploit Public-Facing Application	MITRE ICS TTP workbook for T0819
OT Sec: MITRE ICS T0822: External Remote Services	MITRE ICS TTP workbook for T0822
OT Sec: MITRE ICS T0883: Internet Accessible Device	MITRE ICS TTP workbook for T0883
OT Sec: MITRE ICS T0847: Replication Through Removable Media	MITRE ICS TTP workbook for T0847
OT Sec: MITRE ICS T0865: Spearphishing Attachment	MITRE ICS TTP workbook for T0865
OT Sec: MITRE ICS T0862: Supply Chain Compromise	MITRE ICS TTP workbook for T0862
OT Sec: MITRE ICS T0860: Wireless Compromise	MITRE ICS TTP workbook for T0860
OT Sec: MITRE ICS T0807: Command-Line Interface	MITRE ICS TTP workbook for T0807
OT Sec: MITRE ICS T0823: Graphical User Interface	MITRE ICS TTP workbook for T0823
OT Sec: MITRE ICS T0873: Project File Infection	MITRE ICS TTP workbook for T0873
OT Sec: MITRE ICS T0853: Scripting	MITRE ICS TTP workbook for T0853
OT Sec: MITRE ICS T0863: User Execution	MITRE ICS TTP workbook for T0863
OT Sec: MITRE ICS T0841: Network Service Scanning	MITRE ICS TTP workbook for T0841
OT Sec: MITRE ICS T0842: Network Sniffing	MITRE ICS TTP workbook for T0842
OT Sec: MITRE ICS T0846: Remote System Discovery	MITRE ICS TTP workbook for T0846
OT Sec: MITRE ICS T0812: Default Credentials	MITRE ICS TTP workbook for T0812
OT Sec: MITRE ICS T0866: Exploitation of Remote Services	MITRE ICS TTP workbook for T0866
OT Sec: MITRE ICS T0867: Remote File Copy	MITRE ICS TTP workbook for T0867
OT Sec: MITRE ICS T0859: Valid Accounts	MITRE ICS TTP workbook for T0859
OT Sec: MITRE ICS T0811: Data from Information Repositories	MITRE ICS TTP workbook for T0811

OT Sec: MITRE ICS T0861: Point & Tag Identification	MITRE ICS TTP workbook for T0861
OT Sec: MITRE ICS T0845: Program Upload	MITRE ICS TTP workbook for T0845
OT Sec: MITRE ICS T0852: Screen Capture	MITRE ICS TTP workbook for T0852
OT Sec: MITRE ICS T0885: Commonly Used Port	MITRE ICS TTP workbook for T0885
OT Sec: MITRE ICS T0884: Connection Proxy	MITRE ICS TTP workbook for T0884
OT Sec: MITRE ICS T0869: Standard Application Layer Protocol	MITRE ICS TTP workbook for T0869
OT Sec: MITRE ICS T0809: Data Destruction	MITRE ICS TTP workbook for T0809

Phantom OT Security Extension Playbook Catalog

Playbook Name	Description
otsec_action_check_access_acct_policy	CIM: Authentication Investigates account policy violations from authentication model
otsec_action_check_access_default_acct	CIM: Authentication Investigates default account type accesses authentications
otsec_action_check_access_jumpserver	CIM: None Investigates account access activities from jump server internal auth logs
otsec_action_check_access_login_fails	CIM: Authentication Investigates excessive failed logins from OT assets
otsec_action_check_access_login_fail_success	CIM: Authentication Report all authentication activities with src host information
otsec_action_check_access_priv_auth	CIM: Authentication Investigates any escalated priv access to OT assets
otsec_action_check_antivirus_activity	CIM: Endpoint Investigates virus activities on the host
otsec_action_check_antivirus_sw_status	CIM: None Investigates antivirus software update status
otsec_action_check_audit_endpoint_process	CIM: Endpoint Investigates processes on the endpoint
otsec_action_check_audit_odd_process	CIM: Endpoint Investigates odd processes on the endpoint
otsec_action_check_audit_port_change	CIM: Endpoint Investigates any network port activity changes on the endpoint

otsec_action_check_auth_via_network_session	CIM: Network Investigates any authentication session detected on the network. (port 22,23,25,21)
otsec_action_check_encrypt_info	CIM: None Investigates hardware encryption status on the endpoint
otsec_action_check_endpoint_activity	CIM: Endpoint Investigates any notable endpoint activities on the endpoint
otsec_action_check_es_notables	CIM: ES Alerts Investigates any detected ES notables related to the host
otsec_action_check_excessive_login_fail	CIM: Authentication Investigate access failures on the endpoint
otsec_action_check_irregular_access_hr	CIM: Authentication Investigate odd hour access to the systems
otsec_action_check_limit_hw_reboots	CIM: None Investigates any systems reboots detected on the endpoint
otsec_action_check_limit_hw_usb_activity	CIM: None Investigates any USB activity detected on the endpoint.
otsec_action_check_login_success_fail	CIM: Authentication Investigate all login session to the endpoint
otsec_action_check_login_unusual_loc	CIM: Authentication Investigate all improper location access
otsec_action_check_multi_ip_short_time	CIM: Network Investigates networks sessions from x multiple hosts in a given window.
otsec_action_check_network_active_changed_host	CIM: Network Investigates dramatic changes in the activities for the host.
otsec_action_check_network_allowlist	CIM: None Reports network allowlist setting for the host
otsec_action_check_network_behavior_change	CIM: Network Investigates dramatic network behavior changes in the host.
otsec_action_check_network_conf	CIM: None Reports network configuration setting for the host
otsec_action_check_network_direct_inbound	CIM: Network Investigates direct network activities from enterprise network to OT asset
otsec_action_check_network_intrusion	CIM: Intrusions Investigates all outstanding IPS/IDS intrusion alerts on the host
otsec_action_check_network_new_inbound	CIM: Network Investigates newly detected network session to the OT host
otsec_action_check_network_outbound	CIM: Network

	Investigates any outbound / OT asset initiated activities.
otsec_action_check_network_outbound_url	CIM: Network Investigates any outbound / OT asset initiated activities accusing a public URL
otsec_action_check_network_sessions	CIM: Network Reports summary of network activities for the host
otsec_action_check_network_unauth_app_traffic	CIM: Network Investigates any authorized network traffic type related with the host
otsec_action_check_network_volume_change	CIM: Network Investigates network behavior changes related to daily traffic volume per OT asset
otsec_action_check_network_vpn_activity	CIM: Network Investigates unusual VPN activities related to OT assets
otsec_action_check_software_browser	CIM: None Investigates vulnerable browser version on the OT assets
otsec_action_check_software_new_detected	CIM: None Investigates newly detected software on the endpoint
otsec_action_check_software_not_allowed	CIM: None Investigates unauthorized software on the endpoint
otsec_action_check_software_sandbox_status	CIM: None Investigates status on sandbox capability on the endpoint.
otsec_action_check_software_updates	CIM: None Investigates any recent software update on the host
otsec_action_check_software_vuln	CIM: None Investigates any vulnerabilities matching for installed software
otsec_action_check_software_vuln_bulletin	CIM: None Investigates newly update vulnerability bulletins on NIST ICS feed
otsec_action_check_traffic_outbound	CIM: Network Investigates traffic coming in from outside/exposed side of the OT network
otsec_action_check_uniq_login_attempt	CIM: Authentication Investigate a new uniquely detected authentication activities on the host
otsec_action_check_web_malicious	CIM: Web Investigate a malicious urls access through proxy or DNS
otsec_action_check_web_malicious_artifacts	CIM: Web Investigate a malicious artifacts accessed by the host
otsec_action_get_asset_info	CIM: OT Asset Lookup Get OT asset details for each OT assets.

otsec_action_get_es_notables	CIM: ES Notables Investigate all other notables matching the OT asset
otsec_usecase_mitreics_t0818	Example of MITRE T818 auto execution playbooks

Section 9: Example Implementation and Scenario

Hypothetical Scenario: Detection and Mitigation of a threat like Triton using Splunk Enterprise, Enterprise Security, and the Splunk OT Security Solution

Ilium Works is a publicly-traded, multinational provider of energy and resources with production and distribution facilities around the globe. With corporate headquarters in the United States and more than 100,000 employees, they are regularly a target of cyber threats from both insider and outsider actors.

Like many large corporations, Ilium's IT department manages all things technology, both corporate and customer facing. This responsibility ranges from making sure that the company's internal emails get to where they're going, the breakroom kiosks are displaying important information about the day's events, and that the back-office business systems expertly manage the company's supply chain, human resources, AR and expenses, and customer facing website.

Ilium's CISO, Paul Proteus, has his hands full keeping the company secure and as resistant to cyber attack as possible. He has spent the last four years working with his team and his vendors to implement a corporate-wide cybersecurity intelligence platform that includes Splunk Enterprise as the primary repository and search, reporting and analytics tool for cybersecurity-relevant data.

As Ilium continued through its decade-long plan for Digital Transformation, Proteus and his team decided to expand their Splunk Security Platform with Splunk's SIEM offering, Splunk Enterprise Security (ES). Now Security Analysts at Ilium have fully integrated the investigative workflow and mitigation techniques in ES into their daily operations. Both known and unknown threats to the corporate network are regularly identified, sandboxed, investigated, and deactivated before they have a chance to negatively impact data security, application availability, and customer experience.

In early 2017, Ilium was hit by an unforeseen threat. Three production facilities were hit by a piece of malware named Triton, also known as "the world's most murderous malware". Designed by nation-state malicious actors to find and disable key electronic safety systems in industrial plants, Triton infiltrated several servers at Ilium running outdated versions of the Microsoft Windows operating system. Fortunately, Ilium did not run the specific safety systems targeted by Triton, so the threat didn't have the chance to cause the disablement and destruction for which it was designed.

At the time, Proteus and his team wondered how this threat may have infiltrated the supposedly air-gapped systems on the Operational Technology (OT) side of the house. While the OT systems are a bit of a black-box to the CISO team, they had searched through all of their security relevant data in Splunk, and determined that the threat had not entered through the corporate network, nor had it moved between the corporate and OT networks at any point. The CISO team felt like they had dodged a bullet for sure.

At Ilium's distribution facility in Washington, DC, Bud Calhoun, VP of Instrumentation and Automation wasn't so sure. Yes, they were lucky that Triton didn't find its intended target in his plants, but that may not be the case the next time for the next threat. On top of that, removal and further mitigation of the Triton threat required OT server upgrades and other control system and network changes which would risk significant downtime and be a large expense for the company and Calhoun's department. Because of this, and because the Ilium systems were deemed to have immunity, the Triton malware was allowed to reside on the servers in a dormant and "isolated" state. To Calhoun, this was an unacceptable risk to his equipment and network, and more importantly, his team of operators who work that equipment every day.

In March of 2020, Ilium, like most of the world, had their day to day operations turned on their head. This time, the virus wasn't cyber. COVID-19 immediately forced 50% of Ilium's employees to work from home, and the remaining essential employees to work long shifts short-handed. Calhoun knew that this could be a recipe for disaster. Ilium was now facing a decade-worth of Digital Transformation in a period of months, with new systems, applications, cloud migration, and remote access protocols being installed on a daily basis. Never mind the changes in standard operating procedures as employees had to both self-distance and produce - a massive challenge his team had handled surprisingly well.

Once Calhoun and his team found a new normal for daily operations at the plant, Calhoun revisited his concerns for cyber security risk in his operations. His team was stretched thin and stressed, and a cyber threat was just not something they would be equipped to handle at this time. Calhoun decided to reach out to CISO Proteus and ask for some help from his team.

"It wasn't us" seemed like a trite response, but Proteus wasn't wrong. He'd made the investment in team and technology to be sure that the corporate IT network was closely monitored and his team was highly capable of anticipating and mitigating unknown cyber threats. Calhoun had his own budget, and his own team, and the same access to the same vendors as the CISO office.

What Proteus didn't consider, though, was how different managing the OT environment was when compared to his state of the art IT Security approach. Asset life cycles were measured in decades in OT, not months like in IT. Some OT servers ran operating systems and applications that were years out of vendor support, and updating, upgrading, or replacing those systems would result in downtime which would be unacceptable to Ilium and its customers, especially in the middle of a global pandemic.

OT was in a constant battle to "keep it running" and "make it work", and Proteus remembered similar situations in his junior years in the datacenter where a memory upgrade could take down a company's customer relations management system. But Ilium's IT department now enjoyed all the benefits of modern approaches to virtualization, cloud services, and continuous and online upgrades - options the OT team just didn't have yet. Proteus scheduled a meeting to get his top

Splunkers on a Zoom meeting with Calhoun and his senior staffers. The meeting was productive and led to several immediate action items and opportunities for follow up.

The following is their joint action plan for initial integration and collaboration between the OT and IT departments for the purpose of improving the OT departments ability to detect and respond to cyber threats.

Action Item 1: OT Data Collection and Integration

- Asset Inventory: There is no "OT CMDB", and using IT tools like port scanners and vuln scanners is a non-starter. The OT team is aware of several OT Security Vendors whose tools use OT-friendly methods to create and monitor a network for OT devices. OT team to follow up and pick a vendor whose solution is already integrated with Splunk.
- Windows Events: Windows Event Logs are active, and viewer application is available on each machine, but there is no centralization of logs to allow correlation between applications and machines. IT and OT teams will collaborate on the best method to centralize Windows Events, including key application, hardware, authentication and hardware metrics to Splunk via Universal Forwarder or Windows Event Log Forwarding.
- Network Infrastructure Logs: IT team to provide a virtualized Syslog ng server inside the OT DMZ to centralize all Syslog messages from switches, routers, and endpoint protection devices on the OT network. OT Teams will work with their hardware vendor and system integrators to configure the delivery of this data to the Syslog ng server.
- Other Network Activity: In the interest of catching network activity outside the scope of OT Asset Inventory tools and Syslog reporting, IT team will provide documented best practices for using Zeek safely and securely on critical networks.
- Data Egress Point(s): Data needs to securely move from the Splunk forwarders inside the OT firewall to IT's Splunk Environment (currently half on premises and half in Splunk Cloud). Team will research and evaluate opportunities to leverage existing secure interconnects, traffic isolation tools such as data diodes, and will document the limited number of outbound ports utilized by Splunk Forwarders so that an agreement and shared responsibility for any related traffic can be maintained between OT and IT.

Action Item 2: Updating Asset Awareness in Splunk Enterprise and Enterprise Security for OT needs

- Asset Framework: IT leverages the Asset Framework in Splunk ES, but there are several pieces of information that are key to OT asset security management that are missing, including asset criticality. The CISO team will install and implement the DA-OTSEC add-on from Splunk to enable additional fields in the Splunk Asset Framework and will configure the necessary knowledge objects in Splunk to be ready for OT data described above when it starts to flow.

- Asset Detection and Model Creation in Splunk: The OT Asset Discovery tool chosen by the OT team will regularly forward key information about new assets discovered on the OT network, as well as configuration and other changes related to the operation of those assets to Splunk. Splunk will be configured to automatically update the asset framework and related enrichment tables immediately upon receipt of new information about an asset.

Action Item 3: Enabling centralized threat detection for OT and IT systems

- Known threats: The Splunk OT Security solution can take advantage of a community developed app “CVE Lookup” which will gather and report on information from the NIST National Vulnerability Database, including vulnerabilities specific to OT vendor software and hardware. The IT team will securely download the app directly from Splunkbase and install and configure in their Splunk environment per the documentation. In addition the Splunk OT Solution provides a number of rules which will identify known OT threats. The IT team will configure these rules as needed.
- Unknown threats: Splunk team is currently evaluating Splunk User and Entity Behavior solution, as well as Splunk’s Machine Learning Toolkit - pending this process team will use existing security-focused anomaly detection in Splunk Enterprise and Enterprise Security.
- Alerts, dashboards and reports: IT will monitor critical OT assets alongside IT assets using the Splunk solution, and will forward alerts to the OT operator on duty using Splunk Victor Ops. In addition, existing dashboards for threat detection and investigation will now include OT assets where applicable. Finally, OT will provide user access to the Splunk system for key OT stakeholders to access with their enterprise network connected mobile devices and laptops/desktops. Read only dashboards will be made available to OT teams who have remote VPN access to the enterprise network so they and company security investigators can collaborate during incidents without being forced to travel to the office and meet in person.

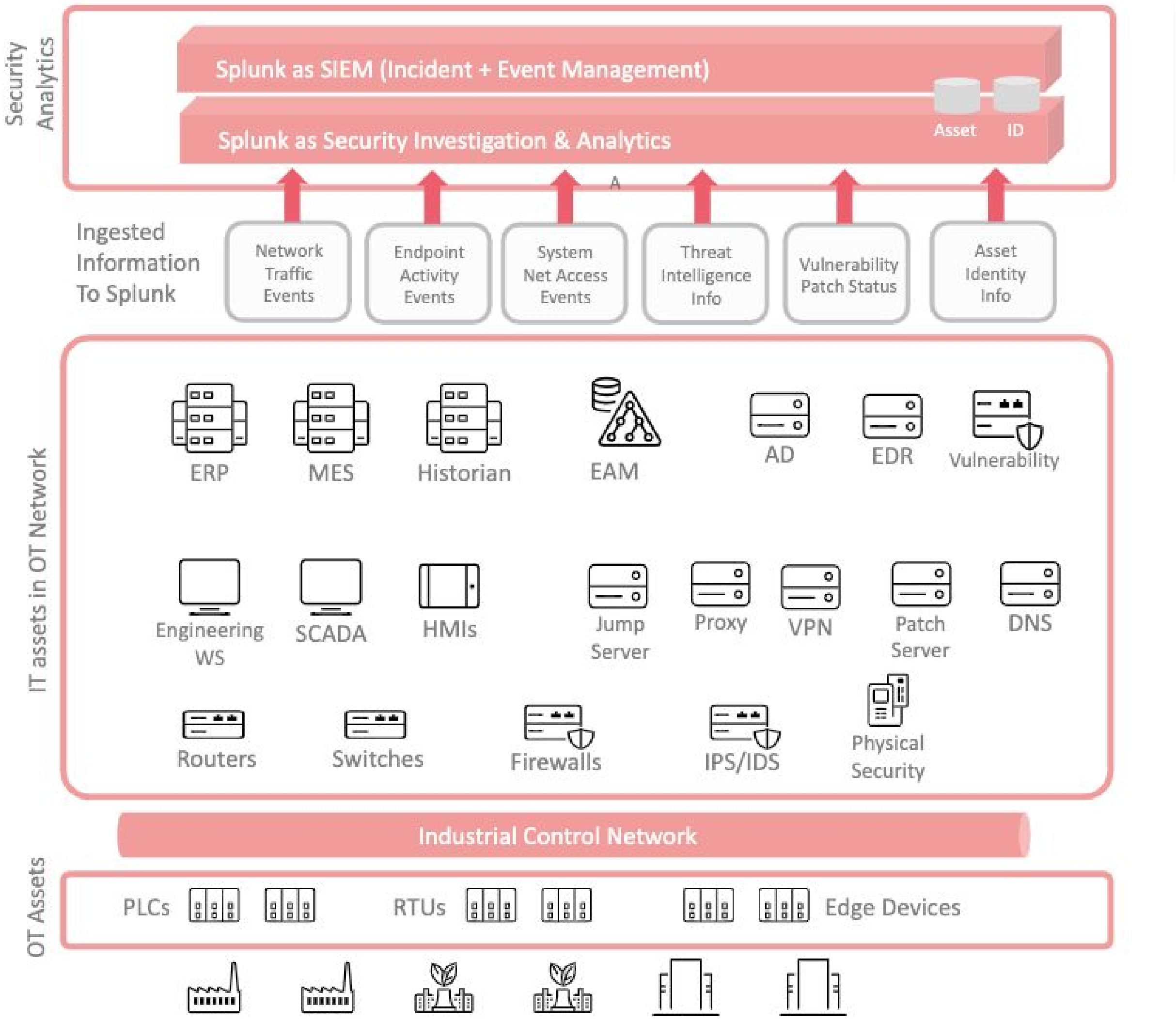
Action Item 4: Implementing MITRE ICS@TTACK Framework rules for better detection of OT threats

- OT Team will specify which of the MITRE ICS@TTACK framework-based correlation rules apply to their environment, and the Splunk team will enable these rules to execute regularly.
- Any additional requests for MITRE framework rules will be forwarded to the Splunk OT Security SME team for consideration and may be implemented immediately by Ilium Splunk Admins or Splunk and Splunk Partner professional services.

Action Item 5: Activating mitigation playbooks when OT threats are detected

- Until final decision is made on corporate-wide adoption of Splunk Phantom, team will use Victor Ops tool to inform OT operator-on-duty who will act per newly documented OT Security Threat Mitigation standard operating procedures. OT team has agreed to keep SOPs updated so that they can be eventually codified in Splunk Phantom.

Related Documents: Ilium OT Security Strategy Architectures



Conclusion:

As you can imagine, this wasn’t an overnight process. Over a period of three months, the teams implemented the procedures to collect and safely transport many of the OT events, alarms, metrics, and asset discovery data to Ilium’s new Splunk Cloud Environment in near-real-time.

Within six months, and driven by the positive outcomes related to onboarding the first data sources, OT data was fully integrated into Ilium's security monitoring and threat identification procedures. By the next March, almost one year to the date from the first conversation between the OT and IT teams, IT detected anomalous network activity between an IP address on the OT network and a remote process historian running in the compliance team's virtualized environment. Was this Triton again, or something new and possibly worse?

END OF DOCUMENT