

**Splunk (SEIM) Project
&
Documentation
CPP Student-Run SOC**

Revision: April 19,2020

Edited by Jensen Gomez

Contents

Introduction.....	pg.3
Project Process.....	pg.3
SIEM Concepts for Splunk Enterprise.....	pg.4
Splunk Definitions and SPL Basics.....	pg.6
Establishing Log Management.....	pg.7
Splunk CIM.....	pg.9
Splunk Supporting Add-on for Active Directory Installation.....	pg.10-11
Alerts.....	pg.12
Editing existing Alerts to send to SOC email.....	pg.13
Threat hunting, Endpoint Security, and Monitoring.....	pg.18
Dashboard SPL documentation.....	pg.27
TruStar Implementation.....	pg.31
Issue Log.....	pg.41
How to get access to Splunk Fundamentals 2.....	Pg.53

Introduction

The Student-Run SOC operates under Cal Poly Pomona. This is great to keep in mind because a college or university can be a very unusual place for a network security professional to work at. Due to the nature of the SOC being run by students there is a requirement to maintain an open level of access that is usually beyond business standards. Although this is a negative, allowing students this access allows open exchange of ideas and learning. This document will keep track of the enormous progress done by students that are willing to operate the Student-Run SOC. Everything from log management, endpoint security, regulatory compliance, and best practices are learned here. Splunk Enterprise is just one of the three SIEMs that will be homegrown and implemented. The CPP College of Business has granted students the chance to acquire, implement, and configure, the components of a SIEM without the cost of a fully baked commercial offering.

The student run SOC at Cal Poly Pomona is a project that students can utilize soon. SIEMS (Security information and event management) are used in the industry to protect and monitor businesses. The student run SOC will run 3 SIEMS, those being IBM Q-radar, Splunk enterprise, and LogRhythm. Students will get to use the 3-industry standard SIEMS to gain insight and hands on experience in security operations. The SOC will provide real-time analysis of security alerts generated by applications and network hardware.

A big thanks to the Splunk Pledge Program for providing the Student-Run SOC with a free 1-year license to operate. Splunk Inc. provided this license for academic instruction in mind and this would have not been possible without them. The pledge program also includes complimentary eLearning and support.

More information on the program: https://www.splunk.com/en_us/about-us/splunk-pledge.html

Project Process

Goal: To Create an operational live SOC environment using Splunk Enterprise

Tentative timeline and progress:

Establishing Log Management ✓
 Syslog and Microsoft Active directory logs ✓
 Alerts ✓
 Flow data ✓
 Assessment Data ✓
 TruStar Implementation ✓
 Automation and Orchestration

My GitHub: <https://github.com/Nukaflux/Studentrun-SOC->

SIEM Concepts for Splunk Enterprise

SIEM Concepts and processes:

A SIEM can be compared to a complex machine in that a SIEM has several moving parts, each performing a specific job, that need to work properly together or else the entire system will fail. There are variations on the standard SIEM, with additional specific parts, but a simple SIEM can be broken down into seven separate pieces or processes. Understanding this will allow you to understand Splunk's SIEM processes.

Source Device>Log Collection>Parsing>Correlation>Log Storage+Rules>Monitoring

- The source device is a device that feeds information into the SIEM. A source device is the device, application, or some other type of data that you want to retrieve logs from that you then store and process in your SIEM.
- The next step in the device or application log flow is to somehow get all these different logs from their native devices to the SIEM. This Log Collection.
- Next after the data is being forwarded to the SIEM what happens? You need to Parse the data in useable data. Lucky for us Splunk automatically categorizes data into sources, event type, and field.
- Now comes correlation. You investigate the logs and find a pattern. You might notice that a sequence of more than 200 of the same events has occurred in the past 1 minute. That would raise suspicion.
- After having suspicion, you save the log, and apply rules and logic. An example would be "If there more than 100 or more failed authentications from the same source, an alert will be sent. This is the power of log storage and rules used in parallel. I have applied this logic for a possible brute force alert in our own SOC.
- Monitoring, then comes into play. With preconfigured alerts and reports, SOC Analysts can then report the incident to a SOC Manager and Security Architect. The issue is reported, investigated, and resolved.

Windows Security Log Quick Reference

User Account Changes			
4720	Created	4722	Enabled
4723	User changed own password		
4724	Privileged User changed this user's password		
4725	Disabled	4726	Deleted
4738	Changed	4740	Locked out
4767	Unlocked	4781	Name change

Domain Controller Authentication Events		
4768	A Kerberos authentication ticket (TGT) was requested	
4771	Kerberos pre-authentication failed	See Kerberos Failure Codes
4820	A Kerberos TGT was denied because the device does not meet the access control restrictions	

Kerberos Failure Codes	
0x6	Bad user name
0x7	New computer account?
0x9	Administrator should reset password
0xC	Workstation restriction
0x12	Account disabled, expired, locked out, logon hours restriction
0x17	The user's password has expired
0x18	Bad password
0x20	Frequently logged by computer accounts
0x25	Workstation's clock too far out of sync with the DC's

Group Changes		Created	Changed	Deleted	Member	
					Added	Removed
Security	Local	4731	4735	4734	4732	4733
	Global	4727	4737	4730	4728	4729
	Universal	4754	4755	4758	4756	4757
Distribution	Local	4744	4745	4748	4746	4747
	Global	4749	4750	4753	4751	4752
	Universal	4759	4760	4763	4761	4762

Logon Types	
2	Interactive
3	Network (i.e. mapped drive)
4	Batch (i.e. schedule task)
5	Service (service startup)
7	Unlock (i.e. unattended workstation with password protected screen saver)
8	Network Cleartext (Most often indicates a logon to IIS with "basic authentication")
10	Remote Desktop
11	Logon with cached credentials

Logon Failure Codes	
0xC0000064	User name does not exist
0xC000006A	User name is correct but the password is wrong
0xC0000234	User is currently locked out
0xC0000072	Account is currently disabled
0xC000006F	User tried to logon outside his day of week or time of day restrictions
0xC0000070	Workstation restriction
0xC0000193	Account expiration
0xC0000071	Expired password
0xC0000133	Clocks between DC and other computer too far out of sync
0xC0000224	User is required to change password at next logon
0xC0000225	Evidently a bug in Windows and not a risk
0xC000015b	The user has not been granted the requested logon type (aka logon right) at this machine

Splunk Definitions and SPL Basics

Official Splunk SPL documentation:

<https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchReference/UnderstandingSPLsyntax>

Splunk Enterprise uses the search app to conduct investigations, reports, and log management. The search app uses a query language known as SPL or Splunk Processing Language. A Splunk search is a series of commands and arguments. Commands are chained together with a pipe “|” character to indicate that the output of one command feeds into the next command on the right.

```
search | command1 arguments1 |  
command2 arguments2 | ...
```

At the start of the search pipeline, is an implied search command to retrieve events from the index. Search requests are written with keywords, quoted phrases, Boolean expressions, wildcards, field name/value pairs, and comparison expressions. The AND operator is implied between search terms. For example:

```
sourcetype=access _combined error |  
top 5 uri
```

This search retrieves indexed web activity events that contain the term “error”. For those events, it returns the top 5 most common URI values. Search commands are used to filter unwanted events, extract more information, calculate values, transform, and statistically analyze the indexed data. Think of the search results retrieved from the index as a dynamically created table. Each indexed event is a row. The field values are columns. Each search command redefines the shape of that table. For example, search commands that filter events will remove rows, search commands that extract fields will add columns

Host, Source, and Source Type

A host is the name of the physical or virtual device where an event originates. It can be used to find all data originating from a specific device. A source is the name of the file, directory, data stream, or other input from which a particular event originates. Sources are classified into source types, which can be either well known formats or formats defined by the user. Some common source types are HTTP web server logs and Windows event logs. Events with the same source types can come from different sources. For example, events from the file source=/var/log/messages and from a syslog input port source=UDP:514 often share the source type, sourcetype=linux _ syslog.

Common Search Commands

chart/ timechart	Returns results in a tabular output for (time-series) charting.
dedup	Removes subsequent results that match a specified criterion.
eval	Calculates an expression. See COMMON EVAL FUNCTIONS.
Fields	Removes fields from search results.
head/tail	Returns the first/last N results.
lookup	Adds field values from an external source.
rename	Renames a field. Use wildcards to specify multiple fields.
rex	Specifies regular expression named groups to extract fields.
search	Filters results to those that match the search expression.
sort	Sorts the search results by the specified fields.
top/rare	Displays the most/least common values of a field.
table	Specifies fields to keep in the result set. Retains data in tabular format.

Optimizing Searches

The key to fast searching is to limit the data that needs to be pulled off disk to an absolute minimum. Then filter that data as early as possible in the search so that processing is done on the minimum data necessary. This can be done with the time picker which allows the search to limit results based on time.

Last 24 hours ▾

Q

Presets

REAL-TIME

30 second window
1 minute window
5 minute window
30 minute window
1 hour window
All time (real-time)

RELATIVE

Today
Week to date
Business week to date
Month to date
Year to date
Yesterday
Previous week
Previous business week
Previous month
Previous year

OTHER

Last 15 minutes
Last 60 minutes
Last 4 hours
Last 24 hours
Last 7 days
Last 30 days
All time

> Relative

> Real-time

> Date Range

> Date & Time Range

> Advanced

Establishing Log Management

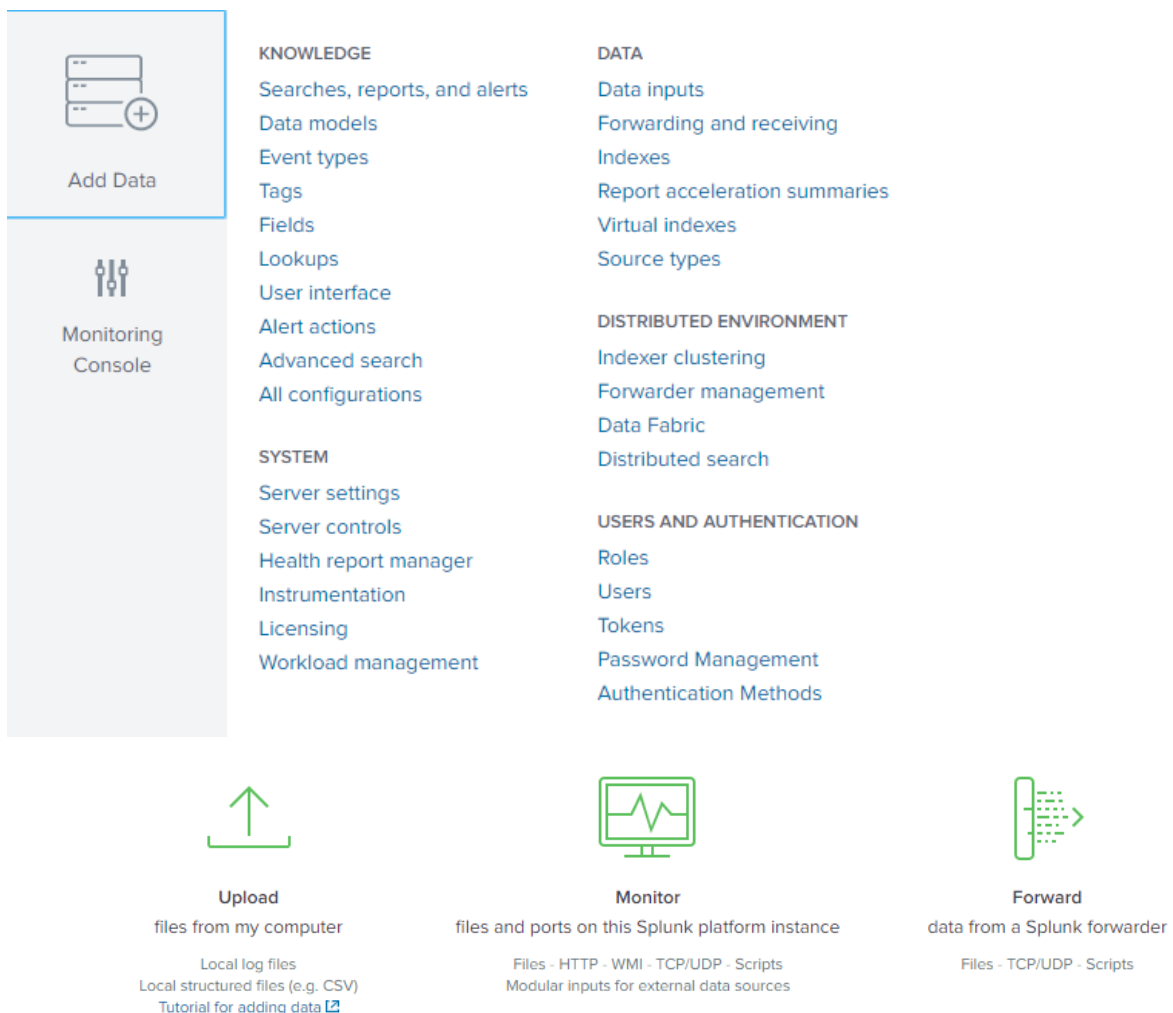
A SIEM solution is nothing without logs. Without them, there is simply no information to extract.

- **Which brings us to our first question:** How and what kind of information logs do we want our SIEM (Splunk) to retain and analyze?

Splunk takes a reasonably user-friendly approach to interface design by making the initial experience easier on the less practiced admin. You can set up your Splunk server to receive live syslog feeds, monitor a local machine, or drop in existing log files.

Adding Data/logs to Splunk Enterprise:

1. Settings
2. Click Add Data
3. Choose a method of Data upload



The screenshot displays the Splunk Enterprise web interface. On the left is a sidebar with two main sections: 'Add Data' (represented by a server icon with a plus sign) and 'Monitoring Console' (represented by a wrench and screwdriver icon). The main content area is divided into three columns of links. The first column, under 'KNOWLEDGE', includes links for Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; and All configurations. The second column, under 'SYSTEM', includes links for Server settings; Server controls; Health report manager; Instrumentation; Licensing; and Workload management. The third column, under 'DATA', includes links for Data inputs; Forwarding and receiving; Indexes; Report acceleration summaries; Virtual indexes; and Source types. Below these columns are three large green icons representing different data upload methods: 'Upload' (an upward arrow), 'Monitor' (a computer monitor with a pulse line), and 'Forward' (a server rack with an arrow pointing right). Each icon has a title and a list of supported data sources below it.

Method	Supported Data Sources
Upload	files from my computer Local log files Local structured files (e.g. CSV) Tutorial for adding data
Monitor	files and ports on this Splunk platform instance Files - HTTP - WMI - TCP/UDP - Scripts Modular inputs for external data sources
Forward	data from a Splunk forwarder Files - TCP/UDP - Scripts

Choosing data:

- Log information can be produced by virtually every device on your network and, in the case of servers and workstations, could be produced by both operating systems and applications. Furthermore, each log source can usually be tuned to provide a record of virtually everything it is doing.
- Before we choose data, we need to look at several questions:

Which devices will you collect events from?

- Endpoint devices, firewalls, routers, SDC-AD

Which events will you collect?

- Logging onto devices,
- configuration changes, and software changes

How long will you keep the logs?

- There are two ways to decide how long. A maximum length of time will provide the best possible data set for several desirable goals such as identifying growth trends for capacity planning, discovering, and remediating long-standing issues of network security. Retaining logs for a long period time also can lead to opening your organization to potentially damaging discoveries.
- For the Student Run SOC we are keeping logs at the maximum length for demo purposes.

Where will you store the logs?

On a dedicated VM.

Our Splunk Box info is:

DNS Name: splunk.sdc.local

IP Addresses: 172.16.64.105

How will Splunk organize our data?

Splunk CIM official documentation:

<https://docs.splunk.com/Documentation/CIM/4.15.0/User/Setup>

- For our instance we will use the Splunk Common Information Model app. The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. CIM add-on models data or building apps to pivot and report. The CIM add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. You can use these data models to normalize and validate data at search time, accelerate key data in searches and dashboards, or create new reports and visualizations with Pivot. CIM models are accelerated models.

Preconfigured Models provided by Splunk CIM

Data model	File name
Alerts	Alerts.json
Application State	Application_State.json
Authentication	Authentication.json
Certificates	Certificates.json
Change	Change.json
Change Analysis	Change_Analysis.json
CIM Validation (S.o.S)	Splunk_CIM_Validation.json
Databases	Databases.json
Data Loss Prevention	DLP.json
Email	Email.json
Endpoint	Endpoint.json
Event Signatures	Event_Signatures.json
Interprocess Messaging	Interprocess_Messaging.json
Intrusion Detection	Intrusion_Detection.json
Inventory	Compute_Inventory.json
Java Virtual Machines (JVM)	JVM.json
Malware	Malware.json
Network Resolution (DNS)	Network_Resolution.json
Network Sessions	Network_Sessions.json
Network Traffic	Network_Traffic.json
Performance	Performance.json
Splunk Audit Logs	Splunk_Audit.json
Ticket Management	Ticket_Management.json
Updates	Updates.json
Vulnerabilities	Vulnerabilities.json
Web	Web.json

Now that we have Splunk CIM we can then move on to gathering logs.

Establishing Splunk enterprise as a SIEM solution requires AD logs and Syslogs. We will need this to:


- To generate events based on the contents of an Active Directory
- To augment events with information from an Active Directory

Splunk Supporting Add-on for Active Directory Installation:

- 1) [Download the Splunk Supporting Add-on for Active Directory](#) from Splunk Apps
The file downloads with a .tar.gz extension. Do not run this file.
- 2) Log into Splunk Web on the Splunk Enterprise instance on which you want to install the app.
- 3) Once logged in, click 'App' from the menu bar.
- 4) Click **Manage apps...**
- 5) On the next page, click the **Install app from file** button.
- 6) On the upload screen, click **Browse...**
- 7) Select the downloaded splunk-support-for-active-directory-xxxx.tar.gz file.
- 8) Click **Open**.
- 9) Click **Upload**.
Splunk Enterprise opens the splunk-support-for-active-directory-xxxx.tar.gz package and installs the application.
- 10) Click the **Restart Splunk** button or the link in the banner to restart Splunk.
- 11) A dialog box asking you if you are sure you want to restart Splunk may appear. Click **OK** to restart Splunk.
- 12) Once Splunk restarts, click **OK** to return to the Splunk login page.
- 13) [Configure the Splunk Supporting Add-on for Active Directory](#)
(Official Splunk Documentation)

Splunk Supporting Add-on for Active Directory Configuration:
[Official Documentation from Splunk](#)

1. On the main webpage for Splunk Web interface click on Splunk Supporting Add-on for Active Directory.
2. In the app Click Configuration.
3. Fill the following fields as follows

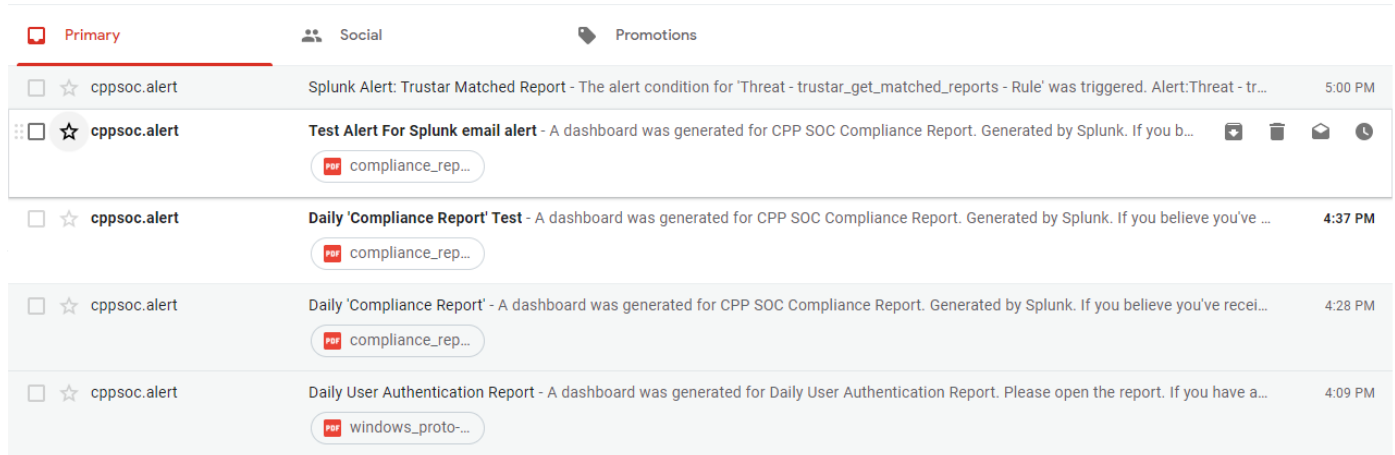
Domain name *	<input type="text" value="default"/>
Alternate domain name *	<input type="text" value="SDC"/>
Base DN *	<input type="text" value="dc=sdc,dc=local"/>
LDAP Server	
Hostname *	<input type="text" value="SDC-AD.sdc.local"/>
Port	<input type="text" value="636"/>
SSL	<input checked="" type="checkbox"/>
Credentials	
Bind DN	<input type="text" value="splunkldap@sdc.local"/>
Password	<input type="password"/>
Connection status	<div> Untested</div> <div>Test connection</div>

Save

4. Click Test Connection.
5. If Successful click save.

1) Setting up Alerts

- Splunk Enterprise provides the ability to correlate events and trigger actions, such as sending emails under certain conditions or causing a script to run. When you know what you are looking for in advance, this can be a way of achieving a level of SIEM-like function with a single tool. In this section I will be showcasing how to set up alerts in Splunk to trigger an email send.

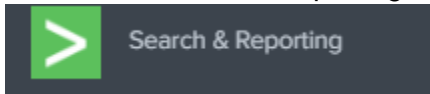


Things to keep in mind: Accelerated models vs normal searches

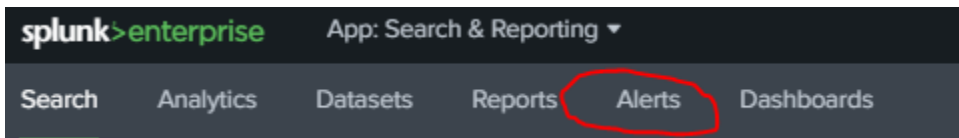
- You cannot have a real time alert using an accelerated model.
- In a SIEM solution use a detection query that is not using an accelerated data model to effectively respond to threats in real time.
- Accelerated models are more effective for reports and dashboards. They help ease the burden of performance and keeps the indexer from being overwhelmed.

Accessing the Alerts Page in Splunk:

1. Click on Search and Reporting

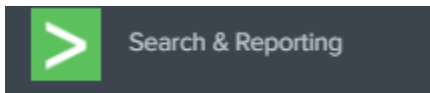


2. Click on Alerts

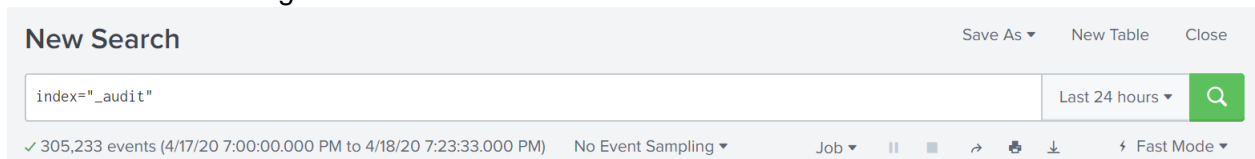


Saving an existing search as an alert, dashboard, or report in Splunk:

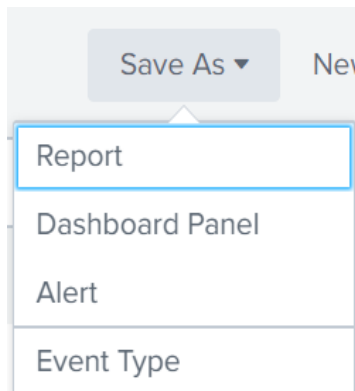
1. Click on Search and Reporting



2. Create a search using the search bar.



3. Click "save as" and choose between Report, Dashboard Panel and Alert.



Splunk Documentation on Data Models:

<https://docs.splunk.com/Documentation/Splunk/8.0.0/Knowledge/Aboutdatamodels?ref=hk>

Editing existing Alerts to send to SOC email:

1. Access the Alerts page! Search and Reporting/Alerts
2. Click edit on an existing alert.

splunk>enterprise App: Search & Reporting ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Analytics Datasets Reports **Alerts** Dashboards > Search & Reporting

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

9 Alerts All Yours This App's filter 🔍

i	Title ^	Actions	Owner ↕	App ↕	Sharing ↕	Status ↕
>	Brute Force Attack	Open in Search Edit ▾	nobody	InfoSec_App_for_Sp...	Global	Enabled
>	Critical Severity Intrusion	Open in Search Edit ▾	nobody	InfoSec_App_for_Sp...	Global	Enabled
>	Geographically Improbable Access	Open in Search Edit ▾	nobody	InfoSec_App_for_Sp...	Global	Enabled
>	High Severity Intrusion	Open in Search Edit ▾	nobody	InfoSec_App_for_Sp...	Global	Enabled
>	Locked Out Accounts	Open in Search Edit ▾	nobody	InfoSec_App_for_Sp...	Global	Enabled
>	Notable Events to TruSTAR	Open in Search Edit ▾	nobody	TA_trustar	Global	Enabled
>	Suspected Network Scanning	Open in Search Edit ▾	nobody	InfoSec_App_for_Sp...	Global	Enabled
>	Threat - trustar_get_matched_reports - Rule	Open in Search Edit ▾	nobody	TA_trustar	Global	Enabled
>	_phantom_app_Critical Vulnerabilities	Open in Search Edit ▾	nobody	phantom	Global	Enabled

3. Once in the edit page for alerts. Scroll down to Add action.

Edit Alert

At 0:00 ▾

Expires 24 hour(s) ▾

Trigger Conditions

Trigger alert when Number of Results ▾

is greater than ▾ 0

Trigger Once For each result

Throttle ? ☐

Trigger Actions

+ Add Actions ▾

When triggered

>	🔔 Add to Triggered Alerts	Remove
>	✉ Send email	Remove






Cancel Save

4. Click add action and click Send email notification.

Edit Alert ×



At

Run a Phantom playbook on this event.

-  Run a script
Invoke a custom script
-  **Send email notification**
Send email based on notification settings
-  Send notification to slack
Send a message on a Slack channel based on notification settings
-  Send notification to victorops
Notify victorops of changes in alerts for which victorops alerting is enabled
-  Send to Phantom

+ Add Actions ▾

When triggered

>	 Add to Triggered Alerts	Remove
>	 Send email	Remove

hour(s) ▾

of Results ▾

0



For each result

5. Fill out the following fields:

To: CPP.SROC@gmail.com

Subject: (Name of the alert)

When triggered

>	 Add to Triggered Alerts	Remove
▼	<div> Send email</div> <div><div>To</div><div>CPP.SRSOC@gmail.com</div></div> <div><div>Comma separated list of email addresses.</div><div>Show CC and BCC</div></div> <div><div>Priority</div><div>Highest ▼</div></div> <div><div>Subject</div><div>Splunk Alert: Possible Brute Force</div></div> <div><div>The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More</div></div> <div><div>Message</div><div>The alert condition for '\$name\$' was triggered.</div></div>	Remove

Cancel Save

6. Click Save

Threat hunting, Endpoint Security, and Monitoring

Threat Hunting

- A **SIEM** needs the ability to effectively investigate events to determine possible intrusions. A well-deployed SIEM solution could identify an attack while it is underway. Other options a SIEM may have is the ability to perform endpoint security. Endpoint security is the managing of endpoints (typically client nodes) on the network from a centralized location or management system, as well as managing the security of the network by protecting it from the endpoints
- One way to this with Splunk is to take full advantage of SPL to create automatic queries that detect an attack or threat.
- **Splunk's SPL** code for search queries is very good at allowing a user to effectively detect and create investigations on the fly. In this section I will be showcasing Splunk's ability to detect threats.

Endpoint Security

- Many **SIEM** systems have the capability to perform endpoint security. Endpoint security is the managing the security of the many endpoints (typically client nodes) on the network from a centralized location or management system, as well as managing the security of the network by protecting it from the endpoints.
- In our instance we will focus on **Host Intrusion Detection**.

The screenshot displays the Splunk Enterprise Search & Reporting interface. At the top, the navigation bar includes 'splunk>enterprise', 'App: Search & Reporting', and user options like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this, the 'Search' tab is active, showing a 'New Search' form with the query 'source=WinEventLog:Security'. The search results show 40,890 events from 4/18/20 12:00:00.000 AM to 4/19/20 12:01:48.000 AM. The interface includes a timeline visualization and a table of results.

Time	Event
4/19/20 12:01:47.000 AM	04/18/2020 09:01:47 PM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4688 EventType=0 Show all 41 lines

Basic Brute Force Attack Detection Tutorial:

A brute force attack is an attempt to crack a password or username or find a hidden web page, or find the key used to encrypt a message, using a trial and error approach, and hoping, eventually, to guess correctly. This is an old attack method, but it is still effective and popular with hackers. In a Splunk search, monitoring Authentication logs is the best place to detect abnormal login patterns.

Data Requirements in Splunk for successful detection:

- Must have Windows Security, linux_secure, or CIM Authentication data
- Must have the src field defined

SPL:

```
index=* (source="*WinEventLog:Security" OR sourcetype=linux_secure OR tag=authentication) user!=""  
| stats count(eval(action="success")) as successes count(eval(action="failure")) as failures by src  
| where successes>0 AND failures>100|
```

Steps:

1. Start your search with **index=***. This insures to search all indexes.
 - This is typically a bad practice, due to search performance, so use the index that contains your organization's security logs.
2. **sourcetype to source="*WinEventLog:Security" OR sourcetype=linux_secure OR tag=authentication) user!=""**
 - This is to look through Windows Logs or Linux Logs
3. **| stats count(eval(action="success")) as successes count(eval(action="failure")) as failures by src**
 - **Stats+eval is used to count how many events where a login is a success or the action is a failure, by source.**
4. Narrow all those successful and failed authentications to a search result where there is at least once success and more than 100 failures.
 - **where successes>0 AND failures>100**

Brute force implementation (Accelerated Model):

```
| tstats summariesonly=t allow_old_summaries=t count from datamodel
    =Authentication by Authentication.action, Authentication.src
| rename Authentication.src as source, Authentication.action as action
| chart last(count) over source by action
| where success>0 and failure>20
| sort -failure
| rename failure as failures
| fields - success, unknown
```

This is our use of brute force detection. This detects a possible brute force attack using WINCOLLECT events. Specifically, with when authentication returns failed login attempts more than 20 times and a successful logon after.

- Note that in our live environment we are using an accelerated model from CIM. Instead of the one present in our tutorial. This is to ensure better performance when conducting searches in a report.
- Report acceleration and summary indexing *speed up individual searches*, on a report by report basis. They do this by building collections of precomputed search result aggregates.
- The tstats command is used to perform statistical queries on indexed fields. The indexed fields can be from normal index data, tscollect data, or accelerated data models. In this case we are using tstats to perform a query on an accelerated data model titled Authentication. This data model specifies failure, success, and denied logins.
- Keep in mind this report does not work with real time search. For real time response, we are using index.

When this query is running into a search in Splunk. We are returned with a tstats table that returns failure and success. |where success>0 and failure>20 searches for events in the model that return returns failed login attempts more than 20 times and a successful logon after.

Network Scan Detection tutorial:

Scanning is a way for attackers to discover the attack surface of your organization (effectively, perform discovery), so they can prepare for an attack, or prepare for the next phase of an attack. It should only ever happen from authorized sources (e.g., vulnerability scanners) internally, and if someone else is doing scanning, you should know about it

- Our detection looks for hosts that reach out to more than 500 hosts, or more than 500 ports in a short period of time, indicating scanning.

Data Requirements in Splunk for successful detection:

- Must have Firewall data
- Must have a dest_ip and dest_port field

SPL (Live Data Approach):

```
1 index=* ( (tag=network tag=communicate) OR sourcetype=pan*traffic OR sourcetype=opsec OR sourcetype=cisco:asa) earliest=-1h
2 | stats dc(dest_port) as num_dest_port dc(dest_ip) as num_dest_ip by src_ip
3 | where num_dest_port > 500 OR num_dest_ip > 500
```

SPL (Accelerated model Approach):

```
1 | tstats summariesonly=t allow_old_summaries=t dc(All_Traffic.dest_port) as num_dest_port dc
  (All_Traffic.dest_ip) as num_dest_ip from datamodel=Network_Traffic where earliest=-1h by
  All_Traffic.src_ip
2 | where num_dest_port > 500 OR num_dest_ip > 500
```

- This is our live detection of hosts that are reaching out to more than 500 hosts.
- You will notice that we are again using a CIM accelerated data model for performance.
- The data model in use here is datamodel=Network_Traffic
- This model contains fields such as destination ports, ip addresses, and many more pertaining to Network Traffic.

Steps:

1. | tstats summariesonly=t allow_old_summaries=t dc(All_Traffic.dest_port) as num_dest_port dc(All_Traffic.dest_ip) as num_dest_ip from datamodel=Network_Traffic where earliest=-1h by All_Traffic.src_ip

- First, we bring in our basic dataset, Firewall Logs, from the last hour via our accelerated data model which is generated from Splunk CIM. We then get the distinct count (aka unique count) of ips and ports that were used per source IP.

2. | where num_dest_port > 500 OR num_dest_ip > 500

- Finally, we can filter for more than 500 src_ips or dest_ports.

Concentration of Attacker Tools by Filename:

It is uncommon to see attacker tools used in rapid succession on an endpoint. This search will identify tools by filename, and look for multiple executions

“Certain commands are frequently used by malicious actors and infrequently used by normal users. By looking for execution of these commands in short periods of time, we can not only see when a malicious user was on the system but also get an idea of what they were doing.”

Taken from: <https://car.mitre.org/analytics/CAR-2013-04-002/>

By correlating the process names being executed on endpoints with a list of 'known hacker tool executable names' we can detect this suspicious activity.

On our Splunk Instance, tools.csv is a complete list of known executable names that are executed on endpoints within succession of each other by hackers with malicious intent.

Commands of interest:

- arp.exe
- at.exe
- attrib.exe
- cscript.exe
- dsquery.exe
- hostname.exe
- ipconfig.exe
- mimikatz.exe
- nbstat.exe
- net.exe
- netsh.exe
- nslookup.exe
- ping.exe
- quser.exe
- qwinsta.exe
- reg.exe
- runas.exe
- sc.exe
- schtasks.exe
- ssh.exe
- systeminfo.exe
- taskkill.exe
- telnet.exe
- tracert.exe
- wscript.exe
- xcopy.exe

SPL:

```

1 index=* source="*WinEventLog:Security" EventCode=4688
2 [| inputlookup tools.csv WHERE discovery_or_attack=attack | stats values(filename) as search | format]
3 | transaction host maxpause=5m
4 | where eventcount>=4
5 | fields - _raw closed_txn field_match_sum linecount

```

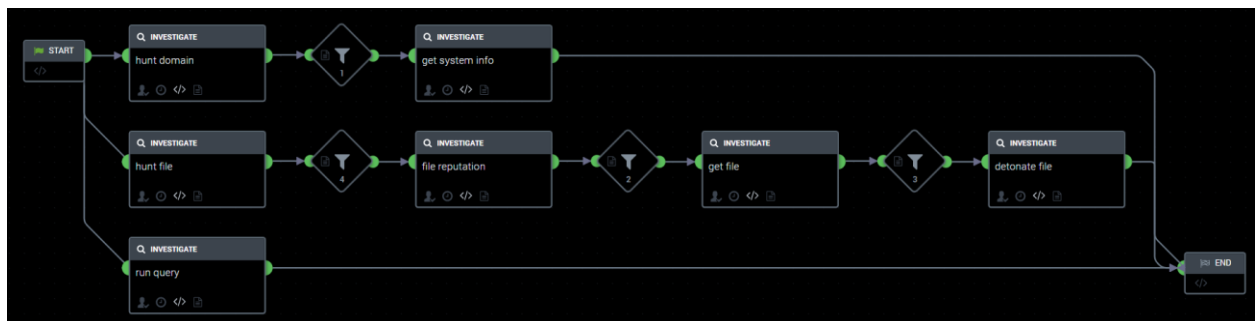
- Note: using index=* is bad practice due to the performance of the search. In our own instance we refer index to the index containing WinEventLogs. You always want to be specific.
- Tools.csv contains a list of known processes that executed in succession.
- maxpause=5m lets us continue grouping together any events that have no more than 5 minutes between each one.
- From line 1-3, we have grouping of suspicious process launches, but also transaction has added a few new fields, such as duration and eventcount. Eventcount lets us see how many process launches are in each transaction (each grouping of suspicious process launches), so we can filter for when there are at least 4 launch events together.

False Positives:

This search should trigger very few false positives because it's filtered to just very specific launches, and even more, looking for multiple process launches in a short period of time. The only scenario where you will expect to see this happen is if your organization happens to use some of those unusual tools for normal sysadmin tasks and have them scripted.

Future Plans:

- Creating a Phantom Playbook! Based on this type of threat hunting.



Authentication Against a New Domain Controller (daily report)

```

source="*WinEventLog:Security" index=* 4776 EventCode=4776           // First we start with our basic dataset of WinSecurity logs with
                                                                    EventCode 4776, which will only originate from a domain controller.

| rename ComputerName as DomainControllerName                       // We then rename the ComputerName to DomainController name for
                                                                    clarity

| table _time DomainControllerName user                             // Then we use table to include just the fields we're apt to care
                                                                    about. (Technically we need to use | table for this app because we
                                                                    show you the intermediate results, but in production you should drop
                                                                    this line because it will reduce search performance.)

| stats earliest(_time) as earliest latest(_time) as latest by user, // Here we use the stats command to calculate what the earliest and
DomainControllerName                                                the latest time is that we have seen this combination of fields.

| eval maxlatest=now()                                              // This line is for convenience, where we store the current timestamp
                                                                    so that we can use it in the next line.

| eval isOutlier=(if(earliest >= relative_time(maxlatest, "-1d@d"), 1, // If the earliest time we have seen that value was within the last
0)                                                                    day, that means the first time we've ever seen it just happened, and
                                                                    it qualifies as anomalous.

```

Event ID 4776 (or in a Splunk search, EventCode=4776) returns authentication logs from a domain controller. A common indicator for lateral movement is when a user starts logging into new domain controllers.

- If privileged access to a domain controller is obtained by a malicious user, that adversary can modify, corrupt, or destroy the AD DS database and, along with all of the systems and accounts that are managed by Active Directory.
- By monitoring both successful and unsuccessful authentication attempts organizations can identify anomalies such as time of day, frequency and other suspicious patterns that may indicate compromised assets or credentials.

Windows Event Log Clearing Events (Windows Audit Log tampered)

```
index=* (source="*WinEventLog:Security" AND          // First we load our Windows Event Log data and
(EventCode=1102 OR EventCode=1100)) OR              filter for the Event Codes that indicate the
((source="*WinEventLog:System") AND EventCode=104)   Windows event log is being cleared. You can see
                                                      there are a few possibilities.

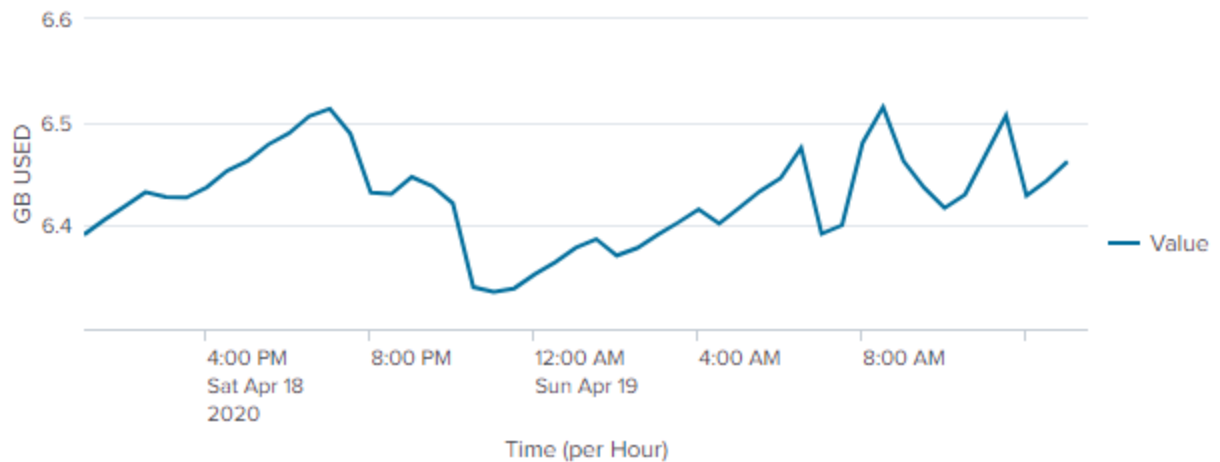
| stats count by _time EventCode sourcetype host     // Then, because we respect analysts, we put it in
                                                      a nice easy-to-consume table.
```

- This use case looks for Windows event codes that indicate the Windows Audit Logs were tampered with.

80
8000

Dashboard and Search Query Documentation

Memory Domain controller Usage (Last 24 Hours)

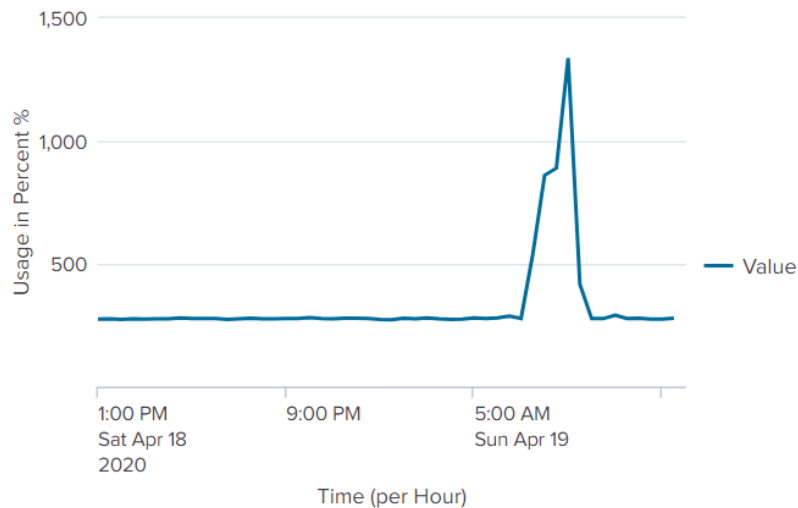
**SPL:**

```
1 host="SDC-AD" source="Perfmon:Available Memory" | eval Value=(32-Value/1e+9) |timechart avg(Value) as Value
```

- Host is set the SDC Active Directory box
- source= "perform:" Available Memory" only gives the available memory in bytes. The purpose of this query is to show Memory Usage. So, we resort to using an eval function.
- eval value=(32-Value/1e+9). We eval the value from available memory divide it by 1e+9 to convert our value from bytes to gigabytes. We then subtract the number GBs in our SDC AD box which 32 GB.
- timechart then takes the avg value of used memory per hour and creates a visual representation of the memory usage in a 24 hour span.

CPU Usage Dashboard:

CPU Domain Controller Usage (Last 24 Hours)



SPL:

```
| eventtype="perfmon_windows" (Host="*") Host="*" object="Processor" counter="% Processor Time" | eval value=Value*100
| fillnull value="avg" instance|timechart avg(value) as Value
```

- eventtype is set to perfmon_windows
- Host is set equal to "*" in the off chance this query needs changes. Supplementing SDC-AD.sdc.local as host also works.
- Object is set to processor monitor processor
- Setting a counter to that object to %Processor Time. In windows % Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread.
- I evaluate the value returned from processor time. I was returned a decimal so I multiplied it by 100 to get returned the processor time in percent. In windows every 100% is one full core being utilized. This is how it is possible to get percentages over 100%
- I then get the value to return an average and set the value to a 24 hour timechart.

Events Received in last 30 Days

26,896,581

SPL:

```
1 | tstats count where index="*"
```

- This counts all the events in every index.
- Using a time picker, I then limit the search to return a count in last 30 days.
- I choose to use a time picker that way the counter is flexible.
- For the visualization picker, I selected a single value. If you want to this using pure SPL code and hard code the visualization use "| timechart count"
- To have the dashboard count up every second I set the refresh value to 1 second.

Auto Refresh Delay ?

Custom ▼

1s

TruStar Implementation & Collaboration with LACL

LACL introduction

LA Cyber Lab is a non-profit organization focused on providing a way for companies to share cybersecurity threat information.

- LA Cyber Lab's intelligence sharing has taken two forms: a daily threat report distributed by email and a regularly shared comma-separated value (CSV) file containing "indicators of compromise" (IOCs)—fingerprints for known attacks that businesses can use to detect attacks.
- LA Cyber Lab has offered us the opportunity to receive threat feeds into our own SIEMS using a TruStar implementation.
- This will be used to keep a constant list of threats that can be updated and run against our playbooks.

LACL's Official Website: <https://www.lacyberlab.org/>

TruSTAR integration without Splunk Enterprise Security edition SETUP:

- This section explains the required Dependencies to install TruSTAR onto our Splunk Instance here at the SDC.

Required dependencies:

- **TruSTAR App for Splunk (App):** This is the user interface component for the TruSTAR integration. It is composed of an overview dashboard and tables that display IOCs and reports from Station. The App monitors the indexes you specify for the presence of IOCs that the TruSTAR TA has copied from Station into the Splunk index you've chosen.
- **Technology Add-on for TruSTAR (TA):** The back-end component fetches reports and IOC data from selected enclaves in TruSTAR Station and indexes them for use with the Splunk search tool.
- Creating a single index that the TruSTAR TA can forward data to.
- Configuring the TruSTAR TA to refer to the created index. In this case our current named index is set to forward to `trustar_app_ta_logs`. To edit this, login to the Splunk web app and navigate to Settings/DATA/Indexes
 - An API key, API Secret Key, and LACL Enclave ID from your TruStar Account.
- **TruStar Technology Add-On:** [Download Link](#)
- **TruStar App for Splunk:** [Download Link](#)

Procedure:

1. Created the Index trustar_app_ta

- Navigated to Settings/DATA/Indexs
- Created index titled: trustar_app_ta
- Click save

The screenshot displays the Splunk Enterprise web interface. The top navigation bar includes links for Apps, Admin, Messages, Settings, Activity, and Help. The main content area is titled 'Indexes' and shows a list of 30 indexes. The 'trustar_app_ta' index is highlighted in the list.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event
_audit	Edit Delete Disable	Events	system	1.16 GB	488.28 GB	5.64M	8 months ago	a few seconds ago
_internal	Edit Delete Disable	Events	system	4.61 GB	488.28 GB	31.6M	a month ago	a few seconds ago
_introspection	Edit Delete Disable	Events	system	3.1 GB	488.28 GB	3.66M	23 days ago	a few seconds ago
_metrics	Edit Delete Disable	Metrics	system	1.27 GB	488.28 GB	13.8M	23 days ago	a few seconds ago
_telemetry	Edit Delete Disable	Events	system	3 MB	488.28 GB	934	8 months ago	13 hours ago
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0		
cim_modactions	Edit		Splunk_SA_	1 MB	488.28 GB	0		

The 'New Index' modal is open, showing the following configuration details:

- Index Name:** trustar_app_ta
- Index Data Type:** Events
- Home Path:** optional
- Cold Path:** optional
- Thawed Path:** optional
- Data Integrity Check:** Enable
- Max Size of Entire Index:** 500 GB
- Max Size of Hot/Warm/Cold Bucket:** auto GB
- Frozen Path:** optional
- App:** TruSTAR App for Splunk
- Storage Optimization:** Tsidx Retention Policy (Enable Reduction)

2. Installation of Both TruSTAR App for Splunk (App) and technology Add-on for TruSTAR (TA):

- Downloaded the files App files for both TruStar Apps. The app on splunk base is not up to date (version 1.0.9 as of 2/25/19).
- Login using Admin Credentials on Splunk Web App
- Install the TruSTAR files using the Splunk web app user interface
- Select Apps -> Manage Apps from the main menu bar.
- Click on install app from file
- Splunk Enterprise will Restart for each app

[Browse more apps](#)
[Install app from file](#)
[Create app](#)

3. Configuration of TA app!

- Login to the Splunk node with admin account. Admin Credentials in KeePass Database for the SOC.
- Went to Settings -> Data -> Data Inputs to display the Inputs page
- Selected TruSTAR Configuration in the Local Inputs **section**.

Local Inputs		
Type	Inputs	Actions
Files & Directories Index a local file or monitor an entire directory.	16	+ Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	2	+ Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	2	+ Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	3	+ Add new
Scripts Run custom scripts to collect or generate more data.	19	+ Add new
Modular Action Relay Relay modaction from remote splunk search head.	0	+ Add new
REST REST API input for polling data from RESTful endpoints	2	+ Add new
Wire data Passively capture wire data from network traffic.	1	+ Add new
TruSTAR Configuration REST API input for polling data from TruSTAR endpoints	1	+ Add new
PCAP Files Upload pcap data for indexing.	0	+ Add new

URL To Connect *	<input type="text" value="https://station.trustar.co"/>
API Authentication Key *	<input type="text"/>
API Secret *	<input type="text"/>
Confirm API Secret	<input type="text"/>
Date (UTC in 'YYYY-MM-DD hh:mm:ss' format)	<input type="text"/>
	Date since when you want to fetch reports and indicators from TruSTAR during first polling. Default will be 90 days ago.
SSL Certificate Path	<input type="text"/>
	Path for the custom certificate.
HTTPS Proxy Address	<input type="text"/>
	Use proxy address starting with (http:// or https://) to communication with the TruSTAR station, e.g. http://10.10.1.10 or https://10.0.1.10
HTTPS Proxy Port	<input type="text"/>
	Proxy port to use for communication with the TruSTAR station, e.g. 3128
HTTPS Proxy Username	<input type="text"/>
	Username to use for communication with the TruSTAR station.
HTTPS Proxy Password	<input type="text"/>
Confirm HTTPS Proxy Password	<input type="text"/>
Data Collection	Enabled
	To enable data collection select "Enabled".
Enclave IDs	<input type="text" value="a28684aa-d047-4770-bac7-1c5a6717dadb"/>
	Enter Enclave ID's to pull data from. If multiple ID's, use comma separated values.
Enclave types for fetching Priority Score	<input type="text" value="INTERNAL"/>
	Enter Enclave types in capital letters to fetch priority score. Possible Enclave types are (INTERNAL,CLOSED,OPEN). If multiple types, use comma separated values.
Tags	<input type="text"/>
	Enter tags to filter by indicators list. If multiple tags, use comma separated values.

☐ More settings

- Filled in the configuration details (see TA Configuration Parameters below).
- Entered Api Key and Api Secret key from TruStar Account (profile/API on company website)
- Entered LACL enclave id
- Enabled data collection
- Click>save

TruStar Configuration Parameters

Parameter	Required	Description
Rest Input Name	Yes	The name of rest modular input. Each Modular Input name must be unique and use alphanumeric characters only; you cannot use special characters. Name it "trustar001" - If you need to delete this REST input and create a new one in future, you will need to use a new name (Ex: "trustar002").
URL to Connect	Yes	The TruSTAR station URL from which data is collected by executing API calls. Set this parameter to https://station.trustar.co
API Authentication Key	Yes	Used to make API calls. You can find this Key in the TruSTAR Station web interface under Settings-> API. How to find your API Key The Key is in clear text at the time of new modular input creation. On save of Modular input, the Key is encrypted and stored at the /storage/password entity of Splunk.
API Secret	Yes	Used when making API calls. Available under Settings-> API on TruSTAR Station. How to find your API Secret The Secret in clear text at the time of new modular input creation. On save of Modular input, Secret key is encrypted and stored at the /storage/password entity of Splunk.
Date (UTC in "YYYY-MM-DD hh:mm:ss" format)	Optional	Submission date/timestamp for the oldest report you want to import into Splunk. The default (blank) will import data from all enclaves you specify for the past 90 days.
SSL Certificate Path	Optional	Path of SSL Certificate that will be used while executing any API request to TruSTAR station. Leave this parameter blank if you are using a CA signed certificate.
Enable Data Collection	Yes	Signals TA to begin importing data from the TruSTAR enclaves specified in the Enclave IDs field as soon as the configuration changes are saved.
Enclave IDs	Yes	The enclave(s) to import data from. Specify the Enclave ID (alphanumeric id next to enclave name in TruSTAR Station). To

		<p>import data from multiple enclaves, separate each enclave ID with a comma and no spaces:</p> <p>In this case Input LACL Enclave ID!</p> <p>649b15c1-dfb8-408d-b3</p> <p>Retrieving your Enclave IDs</p> <p>Best Practices</p> <ul style="list-style-type: none"> • Avoid importing from more enclaves than you need to as each one takes time to process. • To import data from enclaves whose data quality/reliability is unknown, consider setting up the TruSTAR TA on an a different Splunk Heavy Forwarder and use secondary TA to import data from those enclaves into the same index as your primary heavy forwarder/TA, but using a different set of API credentials than your primary TA. TruSTAR limits the number of API calls a set of API credentials can make each minute. • If you need to reach further back in time for certain enclaves, set up additional TAs on other heavy forwarders and configure each TA to import from a unique set of enclaves and time windows. Make sure that all of the TAs import the data into the same index so the TruSTAR App can view and search all the data.
HTTPS Proxy Address	Optional	<p>Proxy address to use for communication with the TruSTAR station, e.g. http://10.10.1.10</p> <p>Note: If you are using a ZScaler proxy and have issues communicating with Station, contact TruSTAR support.</p>
HTTPS Proxy Port	Optional	<p>Proxy port to use for communication with the TruSTAR station e.g. 3128</p>
HTTPS Proxy Username	Optional	<p>Proxy username. Check with your system administrator or helpdesk for this information.</p>
HTTPS Proxy Password	Optional	<p>Proxy password. Check with your system administrator or helpdesk for this information.</p>

Enclave types for fetching Priority Score	Optional	<p>Type of enclaves being accessed. Values are INTERNAL (default), OPEN, CLOSED, or blank. If you specify multiple types, use commas to separate the values (no spaces are allowed). Note: On-premises installations should leave this field blank. If you cannot save the configuration settings with this field left blank, set the value to OPEN and restrict the Station user account access to only those open-source enclaves that you want to import into Splunk.</p> <p>Best Practices</p> <ul style="list-style-type: none"> • Don't have the TA fetch any priority scores, as this will drastically increase the amount of time it takes to get indicators into your index. • Do not have the TA not import any data from Open Sources enclaves into your Splunk index. You can see the types of enclaves being accessed in the Web user interface where you view reports. • Ensure that the Station user account whose API credentials you are using in the Splunk rest input has read-only permission in Station to the enclaves you want to import to your Splunk index.
Interval	Optional	<p>Polling interval in seconds. This is the amount of time (in seconds) that the TA will wait before polling the TruSTAR enclaves whose IDs you entered in the "Enclave IDs" box for new indicators or reports to import into Splunk.</p> <p>Best Practices</p> <ul style="list-style-type: none"> • Set the value to 86400 (once/day) initially. After it has completed the initial download, you can lower the interval to 3600 (once/hr). • Avoid importing data from TruSTAR far back in time. The further back in time you go, the longer the import process takes before the indicators actually post to your index).
Set sourcetype	Optional	Standard Splunk field. Options are AUTOMATIC (default) or MANUAL.
Index	Optional	The index to be used for TruSTAR data. You should see the trustar

		<p>index in the drop-down menu. If you do not, the Heavy Forwarder may not be correctly configured (see the FAQ - Splunk Integration file), or it may not be communicating properly with your indexers/indexer cluster. You must also change the macro definition. See the Changing Macro Definition instructions below.</p>
--	--	--

Compliance Controls to Implement

NIST Framework

AC - Access Control

AU - Audit and Accountability

AT - Awareness and Training

CM - Configuration Management

CP - Contingency Planning

IA - Identification and Authentication

IR - Incident Response

MA – Maintenance

MP - Media Protection

RA - Risk Assessment

CA - Security Assessment and Authorization

SC - System and Communications Protection

SI - System and Information Integrity

SA - System and Services Acquisition

PS - Personnel Security

PE - Physical and Environmental Protection

PL – Planning

PM - Program Management

Strategy is to have as many controls possible being monitored through Splunk

Example of easy ones:

- **Account Management: AC-2 • Incident Monitoring: IR-5 • Continuous Monitoring: CA-7**

Examples of interesting ones:

- **Information System Backup: CP-9**
- **Information System Component Inventory: CM-8**
- **System and Information Integrity Policy and Procedures: SI-1**

Change Log

4/19/20

Company API Usage

ALLOWED CALLS PER DAY 1500

DAILY USAGE:  4/1500

Next reset at 12:00am UTC

- **TruStar API calls reaching max due to Splunk implementation. May need to see if the model is accelerated which is causing that calls.**
- **Turned off integration with Phantom**

3/24/2020

LDAP for Phantom:

Apps > LDAP

Microsoft

LDAP

Publisher: Phantom

App version: 1.2.40

Python version: 2.7

Product vendor: Microsoft

[Documentation](#)

Description

This app implements various actions that can be carried out on an AD server

ASSET CONFIGURATION

CONFIGURE NEW ASSET

Asset (0)

Select existing asset

Asset Info

Asset Settings

Approval Settings

Access Control

Server IP/Hostname

Required

☒ Force use of SSL

Administrator username

Required

Administrator password

Required

Advanced

Supported Actions

get users - Get the list of users

reset password - Force the user to change the password at the next logon

set password - Set the password of a user

get system attributes - Gets the attributes of a computer/system

get user attributes - Gets the attributes of a user

set system attribute - Set the value of an attribute of a computer/system

change system ou - Change the OU of a computer/system

list user groups - Get the groups that the user is a member of

enable user - Enables the specified user

disable user - Disables the specified user

test connectivity - Validate the asset configuration for connectivity. This action logs into the device to check the connection and credentials

MAIL ALERTS AND MAIL

Mail Server Settings

Mail host

smtp.gmail.com:587

Set the host that sends mail for this Splunk instance.

Email security

☐ none
 ☐ Enable SSL
 ☒ Enable TLS

Check with SMTP server admin. When SSL is enabled, mail host should include the port. IE: smtp.splunk.com:465

Username

CPP.SRSOC@gmail.com

Username to use when authenticating with the SMTP server. Leave empty for no authentication.

Password

.....

Password to use when authenticating with the SMTP server.

Confirm password

Email Format

Link hostname

Set a hostname for generating URLs in outgoing notifications. Enclose IPv6 addresses in square brackets (eg. [2001:db8:0:1]). Leave empty to autodetect.

Send emails as

SDC-Splunk

Email footer *

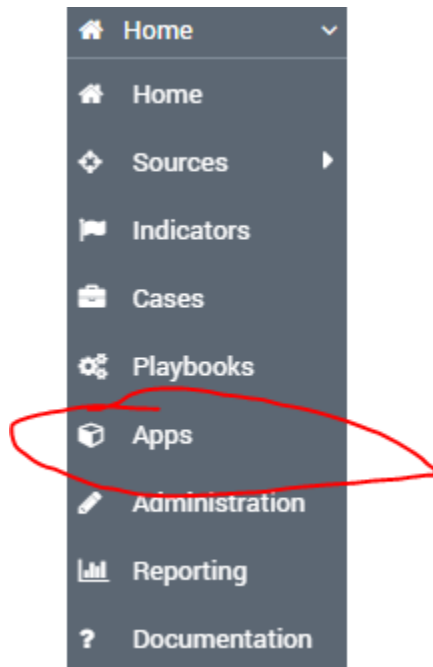
If you believe you've received this email in error, please see your Splunk administrator(K).

splunk > the engine for machine data

3/23/2020

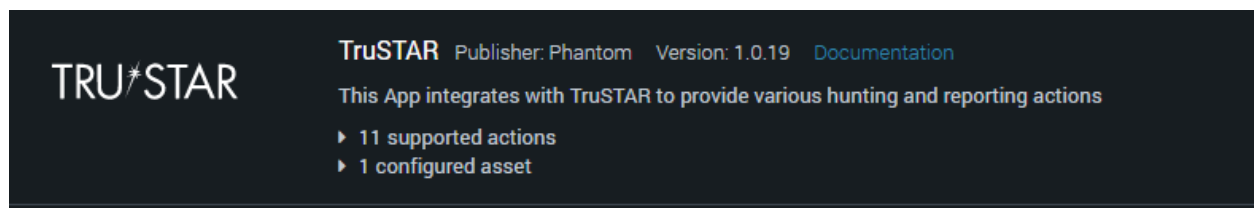
Splunk Phantom is a work in progress:

- Playbooks and automation require sources.
- These can be managed under apps.



- Currently Splunk Phantom is hooked up to LACL, the problem is that no playbooks have been made to fully utilize TruStar integration.


TruStar Integration in Splunk Phantom is found under Apps/TruStar/Configuration



- Here is the TruStar Configuration
- API key is found from TruStar/Profile/API on TruStar Website
- Current Creds Used:
- API: 1f70a497-d852-45b8-b19b-c89c81b372a8

API secret key: PIYzND490DcerDPOdRpkxiA2

< Apps > TruSTAR



TruSTAR
 Publisher: Phantom
 App version: 1.0.19
 Python version: 2.7
 Product vendor: TruSTAR Technology
[Documentation](#)

Description
 This App integrates with TruSTAR to provide various hunting and reporting actions

ASSET CONFIGURATION

CONFIGURE NEW ASSET

Asset (1)

lacl

Asset Info

Asset Settings

Approval Settings

Access Control

URL (eg: https://api.trustar.co)

https://api.trustar.co

(,) separated TruSTAR-generated enclave IDs

Optional

OAuth client ID

1f70a497-d852-45b8-b19b-c89c81b372a8

OAuth client secret key

▶ Advanced

EDIT

TEST CONNECTIVITY

3/16/2020

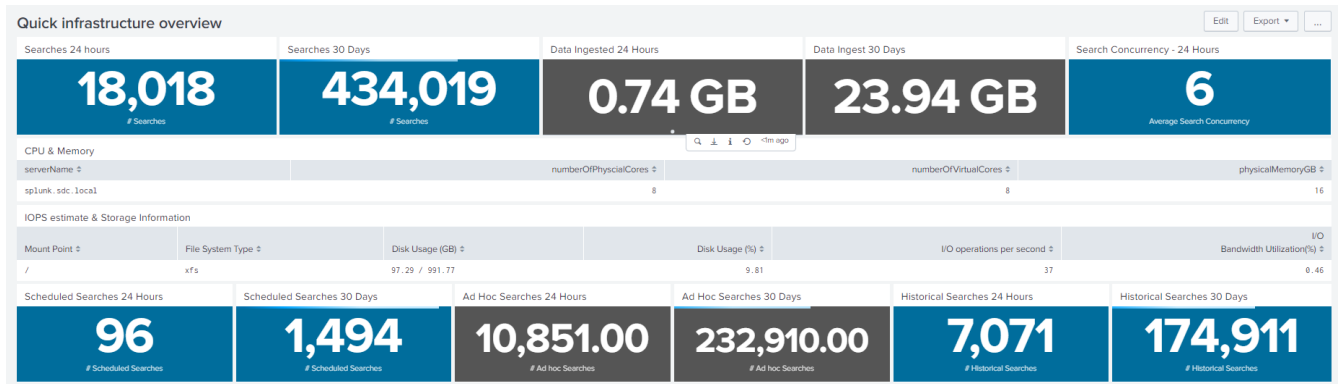
Raspberry Pis: Ubuntu xcf flashed on Pis. (I have the micro sd cards and a pi 4 at home) This allows me to work on the Pis at home durring the Covid-19 outbreak.

- VPN works out of the box and at boot
- SOC wallpaper on all Pis.

- Host names are the same as listed in Logins, Password, and Useful Information section

Dashboard Changes:

- Introducing a new dashboard that gives a quick view into the inner workings of our Splunk instance.



Splunk Changes:

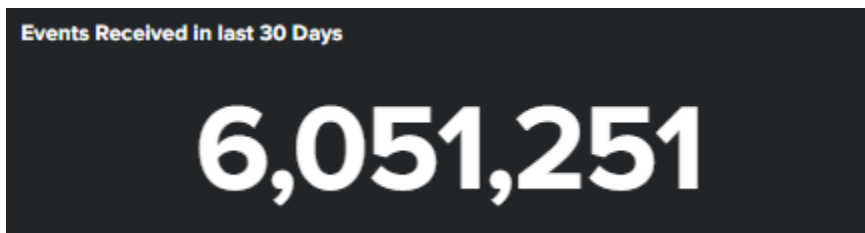
- Installed splunk app for infrastructure

3/11/20

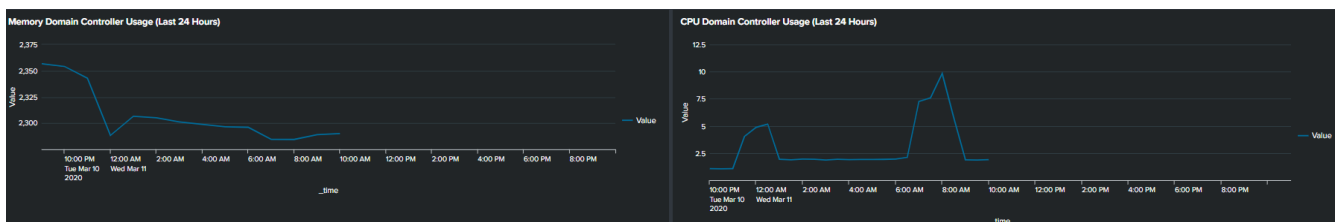
Raspberry Pis: installing Ubuntu on the Pi4s. Able to get this working by installing ubuntu mate and then installing xfce GUI in terminal interface.

Dashboard changes:

Added event counter to SDC monitoring dashboard. It is to update and refresh every 1 second to show the counter going up in real time.



- CPU and Memory domain controller down? Servers might be undergoing Maintenance or down.



Monitoring changes:

In the process of streamlining alerts. The suspected brute force attack alert is triggered by excessive user login attempts.

- Planning to create an alert dashboard that will rotate with the current SDC monitoring dashboard.

- Here below is the SPL (Splunk Programming Language) query that detects an excessive login.
- Alert is set to real time, working on a dashboard to display such alerts.

2/26/20

Raspberry Pi Progress:

- Flashed Raspbian Distro on both Pis
- Installed OVPN on both Pis
- 4k native support confirmed working, through direct hdmi plugin behind the TV.
- Changed wallpapers to SOC wallpaper
- Renamed each pi's hostname to each siem
- TODO: install SDC VPN .ovpn files on all three pis
- Current problems, Sometimes the undervolts and crashes, will look into it

Splunk Progress:

- Installed and integrated TruSTAR LACL threat feed!
- In progress: phantom playbooks and automation

Resources regarding Splunk Threat hunting.

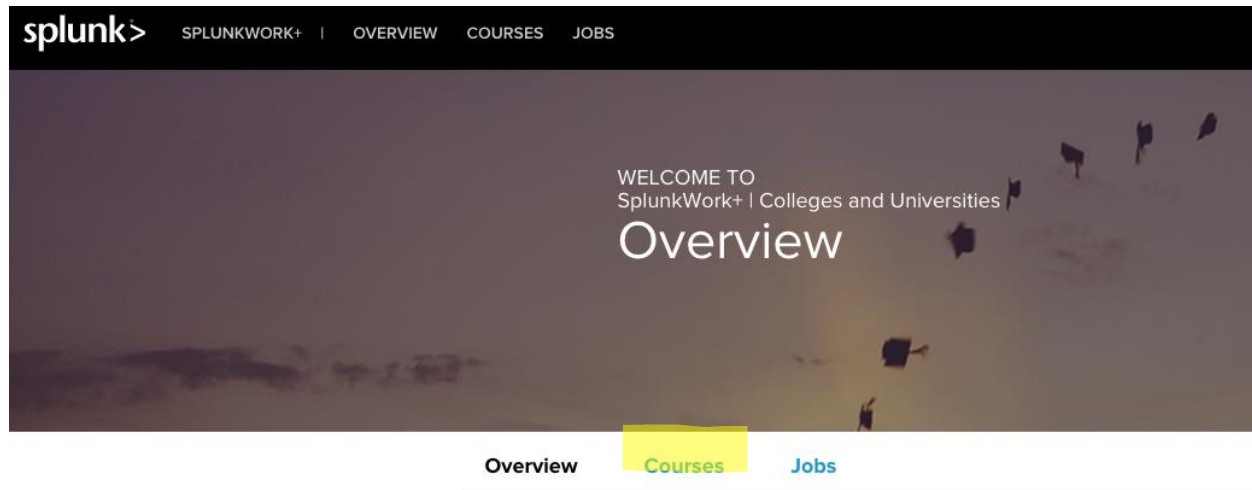
- [Lookup Before You Go-Go...Hunting](#)
Using the Lookup command in Splunk to compare IOCs or other items of interest against your Splunk dataset
- [Finding Islands in the Stream \(of Data\)...](#)
Using Splunk Stream to find malicious activity in your network
- [Work\(flow\)ing Your OSINT](#)
Using Workflow actions and Open Source Intelligence sources
- [MetaData > MetaLore](#)
Using metadata and tstats to quickly establish situational awareness
- [Peeping Through Windows \(Logs\)](#)
Tips for some of the most valuable places to start hunting in your Windows logs
- [I Need to Do Some Hunting. Stat!](#)
Using the three different stats commands for hunting adversaries in Splunk
- [This is NOT the Data You Are Looking For \(OR is it\)](#)
Introducing a set of foundational Splunk threat-hunting techniques that will help you filter data
- [Rex Groks Gibberish](#)
Using the rex and regex commands in SPL to rip apart data when you're hunting
- [UT parsing Domains Like House Slytherin](#)
Using the URL Toolbox to break apart URLs and DNS queries into domains, subdomains, TLDs, and more
- [You Can't 'Hyde' from Dr. Levenshtein When You Use URL Toolbox](#)
Using the URL Toolbox to analyze Splunk fields for Shannon entropy and Levenshtein distance
- [Do We Calculate, Appraise, Classify, Estimate? Yes. But We Do It All with Evaluate \(eval\)](#)
Using the eval command in Splunk to help modify data (on the fly) and enrich fields
- [Tall Tales of Hunting with TLS/SSL Certificates](#)
Using TLS and SSL certificates to hunt advanced adversaries
- [Finding NEW Evil: Detecting New Domains with Splunk](#)
Using Splunk (and Splunk Enterprise Security) to find domains that are "new" to your organization
- [Being Your Own Detective with SA-Investigator](#)
Using the new SA-Investigator add-on for Splunk Enterprise Security to dig deep into your data models and find the evil lurking within
- [Hunting Your DNS Dragons](#)
Using Splunk to "hunt" for malicious DNS behaviour in your network
- [A Salacious Soliloquy on Sysmon](#)
Using Sysmon data for hunting in Splunk
- [I Have a Fever, and the Only Cure for It Is More Feedback](#)
Providing feedback from hunting into security operations
- [Hunting in a New Savanna](#)
Hunting in a new environment, including BOSS of the SOC at .conf18
- [The Future is Cloudy with a Chance of Microsoft Office 365](#)
Using Microsoft Office 365 data to hunt in Splunk

- [I Azure You, This Will Be Useful](#)
Using Azure Active Directory for basic hunting and discovery
- [November Spawned an Osquery](#)
Hunting through osquery logs
- [Spotting the Signs of Lateral Movement](#)
Using Splunk core to identify lateral movement in an organization
- [CloudTrail - Digital Breadcrumbs for AWS](#)
Using AWS CloudTrail as a security logging source and how to hunt in it
- [Go with the Flow - Network Telemetry \(VPC Data\) in AWS](#)
Using VPC data from AWS in Splunk to hunt, hunt, hunt
- [Hunting COVID Themed Attacks With IOCs](#)
Leveraging crowdsourced IOCs and implementing them in Splunk

Accessing Splunk Fundamentals 2

1. Create an account under your “cpp.edu” email at https://www.splunk.com/page/sign_up/

2. Head to <https://workplus.splunk.com/universities> and click on courses.



Welcome Students

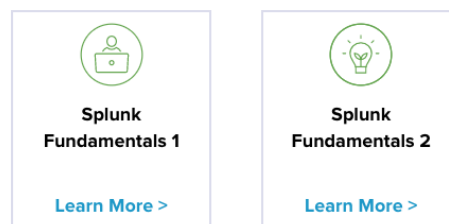
Training the workforce of tomorrow with the students of today

3. Once on this page you should have a pending status under the both of these trainings. You will receive an email from Splunk once approved.

Splunk Online Trainings

Fundamentals

This certification track prepares you to become Splunk Certified Power Users. In addition to attending the required class(es), participants take part in an online final exam. This certification is a prerequisite to the Splunk Certified Admin certification. You have 30 days from the point of registration to complete each module. No exceptions.



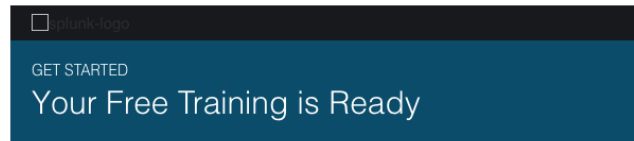
[Search Splunk Jobs](#)

4. Once approved you will receive an email from workforcetraining@splunk.com and instructions to access.

Ex: Welcome to Splunk - Your Free Training is Ready



workforcetraining@splunk.com
Wed 6/17/2020 1:01 PM
To: [REDACTED]



Hi [REDACTED]

[Congratulations!](#) Your application has been approved to join the SplunkWork+ community.

Thank you for letting Splunk be a small part of your career journey. Log in to SplunkWork+ to take advantage of complimentary Splunk training and to view thousands of Splunk jobs available with leading companies right now.

Please visit SplunkWork+ to learn more and to register for courses today!

[Get Started Now](#)