Splunk>

March/2024
Deepak Rawat

Splunk

1.The Splunk Platform

1. Why Splunk

- Big data platform for machine data.
- Convert raw unstructured data into searchable events.
- Organize data in indexes.
- Users can create dashboard, alerts and reports.

Machine Data: Digital exhaust produced by servers, applications and network devices.

Examples:

- Web Access logs
- Application Logs
- Windows Event Logs
- Network packet capture
- OS Performance metrics

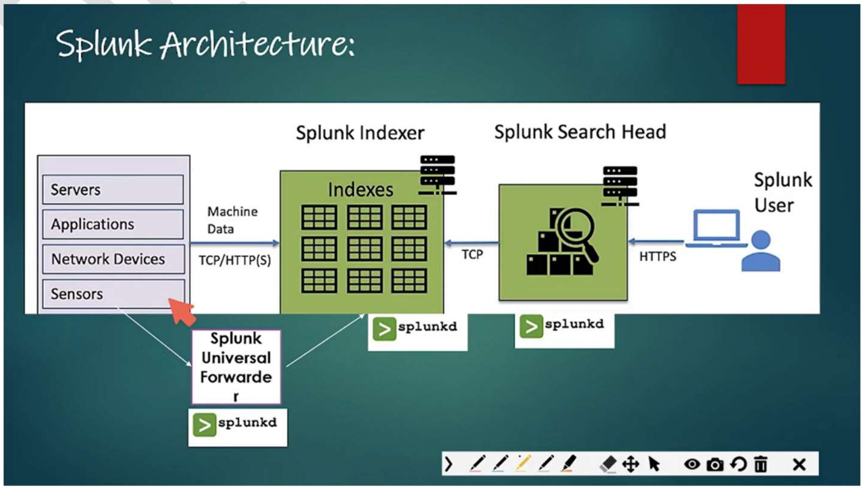
Hidden value of machine data:

- Is there latency in, my application?
- What is the error of my application service?
- Where is DOS attempts coming from?
- How many login attempts cause of wrong username?

Problems with machine data:

- Volume
- Velocity
- Unstructured
- Distributed

Splunk indexes data from any source to enable searching, reporting and visualizing at scale.



Splunk Architecture:

SPLUNK ARCHITECTURE

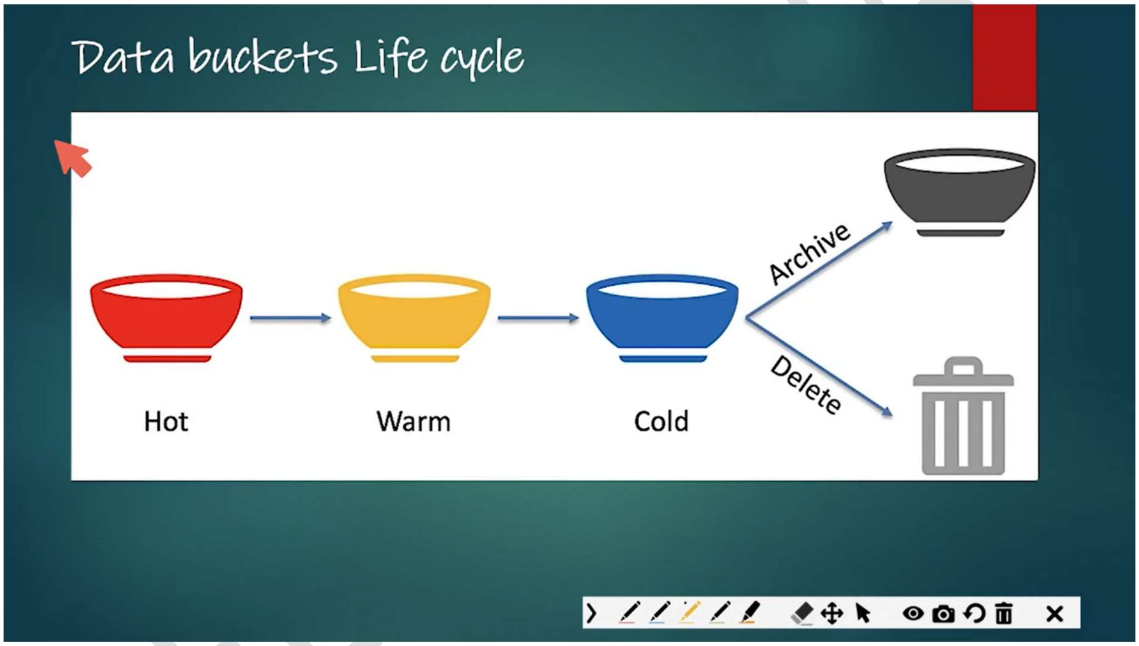
2. Components of Splunk

1. Indexer:

- Receives data from client.
- Converts raw data to searchable events.
- Executes searches.

➔ **Inside of an indexer:**

- Splunk stores data in indexes.
- Indexes contain data buckets.
- Data buckets contain raw data and index files.
- Data retention policies are configured at index level.



Data buckets Life cycle

❖ **Hot Bucket:**

- Contains newest data.
- Open for both read and write.
- Splunk Admin can configure when to roll data to warm bucket.

❖ **Warm Bucket:**

- Open for read only (no writes)
- Hot and warm buckets are kept in Faster storage.
- When data age end, it is rolled to cold from warm buckets.

❖ **Cold Buckets:**

- Open for read only (no writes).
- Cold bucket can be kept in cheaper storage.
- Depending on the configuration, data from cold buckets can either or archived to frozen buckets.

- **Frozen Bucket:**
    - Data is not searchable.
    - Data needs to be thawed first (using Splunk provided scripts) to make it searchable.

- ✓ **Splunk Security:**
    - Splunk implements RBAC (Role based Access Control)
    - Three Primary Roles: User, Power, Admin.
    - Power User can share knowledge Objects.
    - For Splunk User, knowledge objects (examples : Field Extractions, Lookups, Data Models, Tags) are private.

2. **Search Head:**
    - GUI for the User.
    - Manage Searches.
    - Distribute searches to indexes.
    - Maintains Access Control.

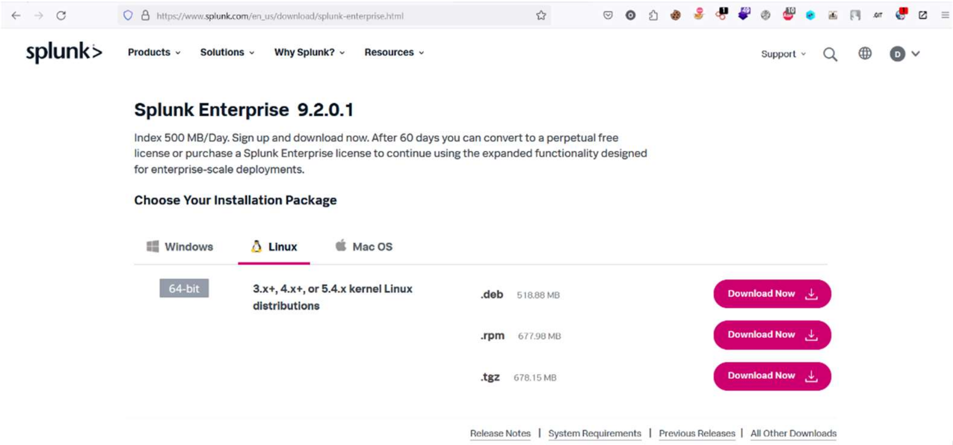
3. **Universal Forwarders**:
    - Collects Data from machine data host.
    - Keeps track of data ingestion.
    - Very lightweight and Production Ready.
4. **Other Splunk Components:**
    - Deployment Server
    - License Master
    - Heavy Forwarder
    - Monitoring Console
    - Search Head Deployer

3. Uses of Splunk

4. Installing and Setting up Splunk

1. Search Processing Language
2. Creating Statistics
3. Fields and Field Extraction
4. Grouping Events and Using Lookups
5. Creating Reports and Alerts
6. Creating Dashboards

- Splunk Trial Version:
    - Download Splunk Trial Version.
    - All features will be available for 60 days.


https://www.splunk.com/en_us/download/splunk-enterprise.html
splunk>
Products
Solutions
Why Splunk?
Resources
Support
D
Windows
Linux
Mac OS
Download Now
Download Now
Download Now
Release Notes | System Requirements | Previous Releases | All Other Downloads

Splunk Enterprise 9.2.0.1

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

64-bit	3.x+, 4.x+, or 5.4.x kernel Linux distributions	.deb	518.88 MB
		.rpm	677.98 MB
		.tgz	678.15 MB

- **Installation Guide:** https://docs.splunk.com/Documentation/Splunk/9.2.0/SearchTutorial/InstallSplunk

Install Splunk Enterprise

These steps apply only to Splunk Enterprise. If you're using Splunk Cloud Platform, go to Navigating Splunk Web.

You can install Splunk Enterprise on the following operating systems.

- Linux installation instructions
- Windows installation instructions
- macOS installation instructions

For other installers or other supported operating systems, see the step-by-step installation instructions for those platforms. After installing Splunk Enterprise, you can continue to Navigating Splunk Web.

Linux installation instructions

Splunk Enterprise provides three Linux installer options: an RPM, a DEB, or a .tgz file.

Prerequisite
You must have access to a command-line interface (CLI). When you type in the installation commands, replace `splunk_package_name` with the file name of the Splunk Enterprise installer that you downloaded.

Install the Splunk Enterprise RPM

You can install the Splunk Enterprise RPM in the default directory `/opt/splunk`, or in a different directory.

1. Use the CLI to install Splunk Enterprise.
   - To install into the default directory, type **rpm -i *splunk_package_name*.rpm**.
   - To install into a different directory, add the `--prefix` flag to the installation command.
     For example, type **rpm -i --prefix=/opt/new_directory *splunk_package_name*.rpm**.
2. Go to the steps to Launch Splunk Web.

Install the Splunk Enterprise DEB package

- You can install the Splunk Enterprise DEB only into the `/opt/splunk` directory.
- This location must be a regular directory, and cannot be a symbolic link.
- You must have access to the root user or have sudo permissions to install the package.
- The package does not create environment variables to access the Splunk Enterprise installation directory. You must set those variables on your own.

If you need to install Splunk Enterprise somewhere else, or if you use a symbolic link for `/opt/splunk`, then use a TAR file to install the software.

1. In the CLI, type **dpkg -i *splunk_package_name*.deb**.
2. Go to the steps to Launch Splunk Web.

Install the Splunk Enterprise .tgz file

Knowing the following items helps ensure a successful installation with a compressed TAR file:

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, to install in `/opt/splunk`, either `cd` to `/opt` or place the tar file in `/opt` before you run the `tar` command. This method works for any accessible directory on your host file system.
- Splunk Enterprise does not create the `splunk` user. If you want Splunk Enterprise to run as a specific user, you must create the user manually before you install.
- Confirm that the disk partition has enough space to hold the uncompressed volume of the data you plan to keep indexed.

1. To install Splunk Enterprise on a Linux system, expand the TAR file into an appropriate directory using the `tar` command. The default installation directory is `splunk` in the current working directory.

   To install into `/opt/splunk`, use the following command with the `-C` argument.
2. `tar xvzf splunk_package_name.tgz -C /opt`
3. Go to the steps to Launch Splunk Web.

Windows installation instructions

For this tutorial you will install Splunk Enterprise using the default installation settings, which run the software as the Local System user, `admin`.

1. Navigate to the folder or directory where the installer is located.
2. Double-click the `splunk.msi` file to start the installer.

3. In the Welcome panel, read the License Agreement and click **Check this box to accept the license agreement**.
4. Click **Next**.
5. A terminal window appears and you are prompted to specify an administrator userid and password to use with the Splunk Trial.

   The password must be at least 8 characters in length. The cursor will not advance as you type.
   Make note of the userid and password. You will use these credentials to login Splunk Enterprise.

6. Click **Next**.
7. (Optional) You are prompted to create a shortcut on the Start Menu. If you want to do this, click **Create Start Menu shortcut**.
8. Click **Install**.
9. In the Installation Complete panel, confirm that the **Launch browser with Splunk** check box is selected.
10. Click **Finish**.
    The installation finishes, Splunk Enterprise starts, and Splunk Web launches in a browser window.
11. Go to the steps to Launch Splunk Web.

For other user options or to perform a custom installation, see the instructions for Install on Windows in the *Installation Manual.*

macOS installation instructions

Splunk Enterprise is supported only on versions 10.14 and 10.15.

1. Navigate to the folder or directory where the installer is located.
2. Double-click the DMG file.
   A Finder window that contains the `splunk.pkg` opens.
3. Double-click the `Install Splunk` icon to start the installer.
4. The **Introduction** panel lists version and copyright information. Click **Continue**.
5. The **License** panel lists shows the software license agreement. Click **Continue**.
6. You will be asked to agree to the terms of the software license agreement. Click **Agree**.
7. In the **Installation Type** panel, click **Install**. This installs Splunk Enterprise in the default directory `/Applications/splunk`.
8. You are prompted to type the password that you use to login to your computer.
9. When the installation finishes, a popup informs you that an initialization must be performed. Click **OK**.
10. A terminal window appears and you are prompted to specify an administrator userid and password to use with the Splunk Trial.

    The password must be at least 8 characters in length. The cursor will not advance as you type.
    Make note of the userid and password. You will use these credentials to login Splunk Enterprise.

11. A popup appears asking what you would like to do. Click **Start and Show Splunk**. The login page for Splunk Enterprise opens in your browser window.
12. Close the **Install Splunk** window.

    The installer places a shortcut on the Desktop so that you can launch Splunk Enterprise from your Desktop any time.

13. Go to the steps to Launch Splunk Web.

Install on Linux

You can install Splunk Enterprise on Linux using RPM or DEB packages or a tar file, depending on the version of Linux your host runs.

To install the Splunk **universal forwarder**, see Install a *nix universal forwarder in the *Universal Forwarder* manual. The universal forwarder is a separate executable, with a different installation package and its own set of installation procedures.

Upgrading Splunk Enterprise

If you are upgrading, see How to upgrade Splunk Enterprise for instructions and migration considerations before you upgrade.

Tar file installation

What to know before installing with a tar file

Knowing the following items helps ensure a successful installation with a tar file:

- Some non-GNU versions of `tar` might not have the `-C` argument available. In this case, to install in `/opt/splunk`, either `cd` to `/opt` or place the tar file in `/opt` before you run the `tar` command. This method works for any accessible directory on your host file system.
- Splunk Enterprise does not create the `splunk` user. If you want Splunk Enterprise to run as a specific user, you must create the user manually before you install.
- Confirm that the disk partition has enough space to hold the uncompressed volume of the data you plan to keep indexed.

Installation procedure

1. Expand the tar file into an appropriate directory using the `tar` command:
2. `tar xvzf splunk_package_name.tgz`

    The default installation directory is `splunk` in the current working directory. To install into `/opt/splunk`, use the following command:

    ```
    tar xvzf splunk_package_name.tgz -C /opt
    ```

RedHat RPM installation

RPM packages are available for Red Hat, CentOS, and similar versions of Linux.

The `rpm` package does not provide any safeguards when you use it to upgrade. While you can use the `--prefix` flag to install it into a different directory, upgrade problems can occur If the directory that you specified with the flag does not match the directory where you initially installed the software.

After installation, software package validation commands (such as `rpm -Vp <rpm_file>` might fail because of intermediate files that get deleted during the installation process. To verify your Splunk installation package, use the `splunk validate files` CLI command instead.

1. Confirm that the RPM package you want is available locally on the target machine.
2. Verify that the Splunk Enterprise user account that will run the Splunk services can read and access the file.
3. If needed, change permissions on the file.
4. `chmod 644 splunk_package_name.rpm`
5. Invoke the following command to install the Splunk Enterprise RPM in the default directory `/opt/splunk`.
6. `rpm -i splunk_package_name.rpm`
7. (Optional) To install Splunk in a different directory, use the `--prefix` argument.

   ```
   rpm -i --prefix=/<new_directory_prefix> splunk_package_name.rpm
   ```

   For example, if you want to install the files into `/new_directory/splunk` use the following command:

   ```
   rpm -i --prefix=/new_directory splunk_package_name.rpm
   ```

Replace an existing Splunk Enterprise installation with an RPM package

- Run `rpm` with the `--prefix` flag and reference the existing Splunk Enterprise directory.
- `rpm -i --replacepkgs --prefix=/splunkdirectory/ splunk_package_name.rpm`

Automate RPM installation with Red Hat Linux Kickstart

- If you want to automate an RPM install with Kickstart, edit the kickstart file and add the following.
- `./splunk start --accept-license`
- `./splunk enable boot-start`

  The `enable boot-start` line is optional.

Debian .DEB installation

Prerequisites to installation

- You can install the Splunk Enterprise Debian package only into the default location, `/opt/splunk`.
- This location must be a regular directory, and cannot be a symbolic link.
- You must have access to the root user or have sudo permissions to install the package.
- The package does not create environment variables to access the Splunk Enterprise installation directory. You must set those variables on your own.

If you need to install Splunk Enterprise somewhere else, or if you use a symbolic link for `/opt/splunk`, then use a tar file to install the software.

Installation procedure

- Run the `dpkg` installer with the Splunk Enterprise Debian package name as an argument.
- `dpkg -i splunk_package_name.deb`

Debian commands for showing installation status

Splunk package status:

```
dpkg --status splunk
```

List all packages:

```
dpkg --list
```

Information on expected default shell and caveats for Debian shells

On later versions of Debian Linux (for example, Debian Squeeze), the default non-interactive shell is the `dash` shell. Splunk Enterprise expects to run commands using the `bash` shell, and `bash` to be available from `/bin/sh`. Using the `dash` shell can result in zombie processes - processes that have completed execution, yet remain in the process table and cannot be killed or removed. If you run Debian Linux, consider changing your default shell to be `bash`.

To view an example on how to change the default shell to bash, see https://unix.stackexchange.com/questions/442510/how-to-use-bash-for-sh-in-ubuntu at StackExchange.

Next steps

Now that you have installed Splunk Enterprise:

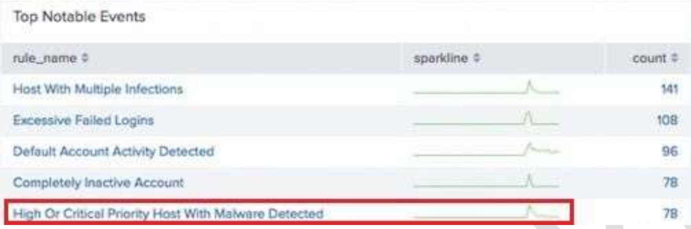
- Start it and create administrator credentials. See Start Splunk Enterprise for the first time.
- Configure it to start at boot time. See Configure Splunk software to start at boot time.
- Learn what comes next. See what happens next?

Content Topic Guidelines

Identify normal ES use cases

The Splunk ES documentation provides two primary use cases: **Detect malware**, and **Identity suspicious activity**. The first use case is detailed here, while the second should be reviewed using the Splunk Docs. Additional example use cases are available for investigating **zero-day activity**, finding **data exfiltration** and **monitoring privileged accounts** for suspicious activity. These are described in the course objectives section.

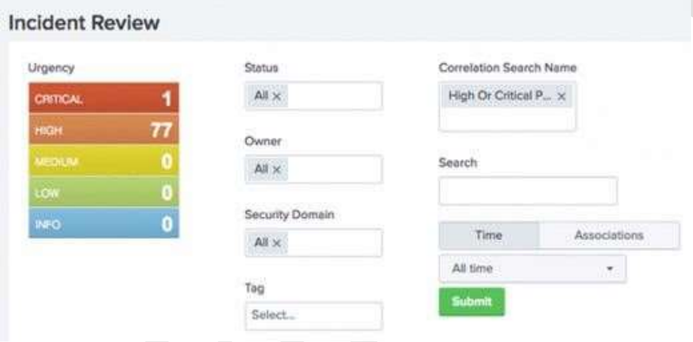
For the malware use case, Splunk ES should be indexing logs from an IDPS tool, web proxy, or endpoint security product. Start by reviewing the **Security Posture Dashboard** for **Top Notable Events**, focusing on the rule for "**High or Critical Priority Host with Malware Detected**". Observe the sparkline next to the rule name for a spike that illustrates an increasing number of infected hosts. Click on the rule name or count to drill down to the **Incident Review** dashboard.



Top Notable Events

rule_name ⇕	sparkline ⇕	count ⇕
Host With Multiple Infections		141
Excessive Failed Logins		108
Default Account Activity Detected		96
Completely Inactive Account		78
High Or Critical Priority Host With Malware Detected		78

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_SecPosDB.png



Incident Review

Urgency: CRITICAL 1, HIGH 77, MEDIUM 0, LOW 0, INFO 0

Status: All ×

Owner: All ×

Security Domain: All ×

Tag: Select...

Correlation Search Name: High Or Critical P... ×

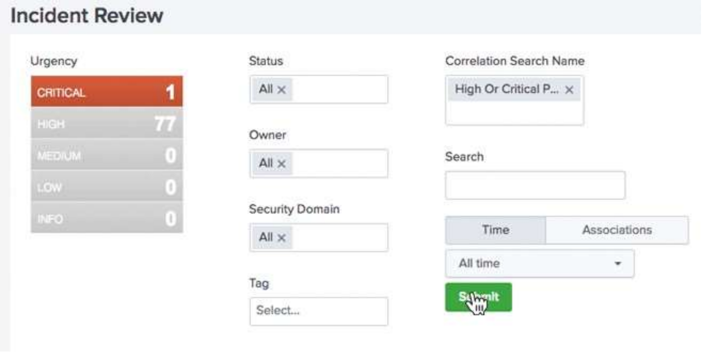
Search:

Time | Associations

All time

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_IncRevDB.png

On the Incident Review page, notable events are listed in reverse date order. In this example, we have one critical event and 77 high events. Filter only by critical events, then click submit:



Incident Review

Urgency: CRITICAL 1, HIGH 77, MEDIUM 0, LOW 0, INFO 0

Status: All ×

Owner: All ×

Security Domain: All ×

Tag: Select...

Correlation Search Name: High Or Critical P... ×

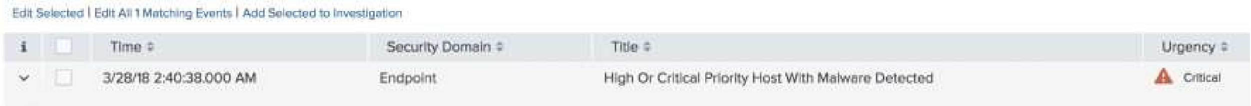
Search:

Time | Associations

All time

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_IncRevUrgency.png

From here, indicate to other analysts that this notable event is currently being analysed. Click the checkbox to select the event of interest. Alternatively, select multiple events, followed by **Edit all X matching events** to change their status in bulk. In this case, choose **Edit Selected** to update the single event. Change the **Status** to ***In Progress*** and click the **Assign To Me** link to assign your own username as the **Owner**. Add a **comment** for context if necessary, then click **Save changes** to return to the Incident Review dashboard.

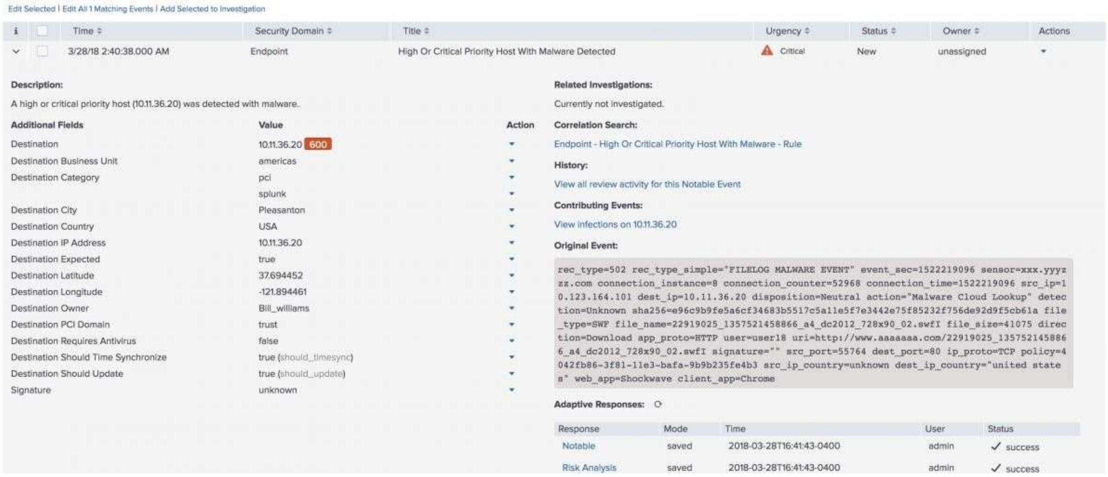


Edit Selected | Edit All 1 Matching Events | Add Selected to Investigation

i	□	Time ⇕	Security Domain ⇕	Title ⇕	Urgency ⇕
⌄	□	3/28/18 2:40:38.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	⚠ Critical

Clicking the > arrow to the left of the event will expand details to include the following:

- Description
- Additional Fields
  - ◦ Configured from ES → **Configure → Incident Management → Incident Review Settings**
  - ◦ Configured in **SA-ThreatIntelligence/local/log_review.conf**
- Related Investigations
- Correlation Search
- History
- Contributing Events
- Original Event
- Adaptive Responses



Edit Selected | Edit All 1 Matching Events | Add Selected to Investigation

i	□	Time ⇕	Security Domain ⇕	Title ⇕	Urgency ⇕	Status ⇕	Owner ⇕	Actions
⌄	□	3/28/18 2:40:38.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	⚠ Critical	New	unassigned	▾

Description:

A high or critical priority host (10.11.36.20) was detected with malware.

Additional Fields	Value	Action
Destination	10.11.36.20 600	▾
Destination Business Unit	americas	▾
Destination Category	pci	▾
	splunk	▾
Destination City	Pleasanton	▾
Destination Country	USA	▾
Destination IP Address	10.11.36.20	▾
Destination Expected	true	▾
Destination Latitude	37.694452	▾
Destination Longitude	-121.894461	▾
Destination Owner	Bill_williams	▾
Destination PCI Domain	trust	▾
Destination Requires Antivirus	false	▾
Destination Should Time Synchronize	true (should_timesync)	▾
Destination Should Update	true (should_update)	▾
Signature	unknown	▾

Related Investigations:

Currently not investigated.

Correlation Search:

Endpoint - High Or Critical Priority Host With Malware - Rule

History:

View all review activity for this Notable Event

Contributing Events:

View infections on 10.11.36.20

Original Event:

```
rec_type=502 rec_type_simple="FILELOG MALWARE EVENT" event_sec=1522219096 sensor=xxx.yyyz
zz.com connection_instance=8 connection_counter=52968 connection_time=1522219096 src_ip=1
0.123.164.101 dest_ip=10.11.36.20 disposition=Neutral action="Malware Cloud Lookup" detec
tion=Unknown sha256=e96c9b9fe5a6cf34683b5517c5a11e5f7e3442e75f85232f756de92d9f5cb61a file
_type=SWF file_name=22919025_1357521458866_a4_dc2012_728x90_02.swfI file_size=41075 direc
tion=Download app_proto=HTTP user=user18 uri=http://www.aaaaaaa.com/22919025_135752145886
6_a4_dc2012_728x90_02.swfI signature="" src_port=55764 dest_port=80 ip_proto=TCP policy=4
042fb86-3f81-11e3-bafa-9b9b235fe4b3 src_ip_country=unknown dest_ip_country="united state
s" web_app=Shockwave client_app=Chrome
```

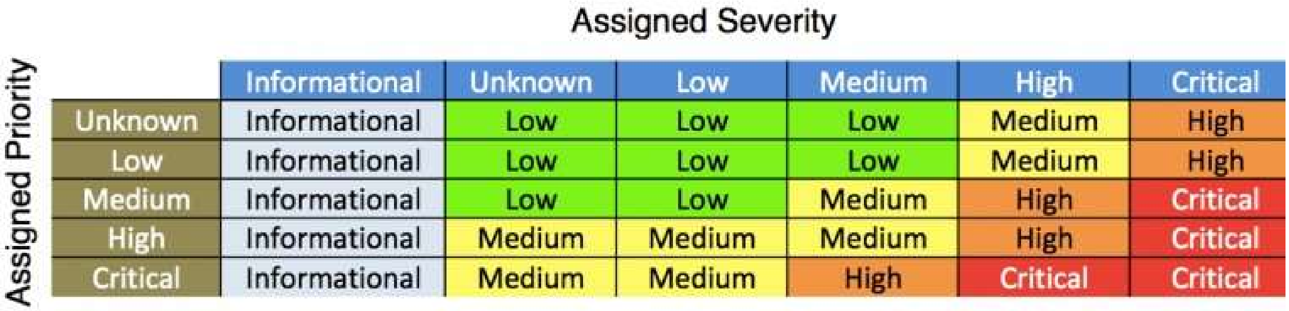
Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2018-03-28T16:41:43-0400	admin	✓ success
Risk Analysis	saved	2018-03-28T16:41:43-0400	admin	✓ success

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_IncRevDBsorted.png

In this case, the **Destination** field has a **Risk Score** of ***100*** associated with the **asset**, as shown above in orange. This will have contributed to the **urgency** rating of this event as ***critical***.

The diagram below shows how the assigned **priority** of an identity or asset, combined with the assigned **severity** of an event, contributes to the calculated **urgency** of the event in the **Incident Review** dashboard



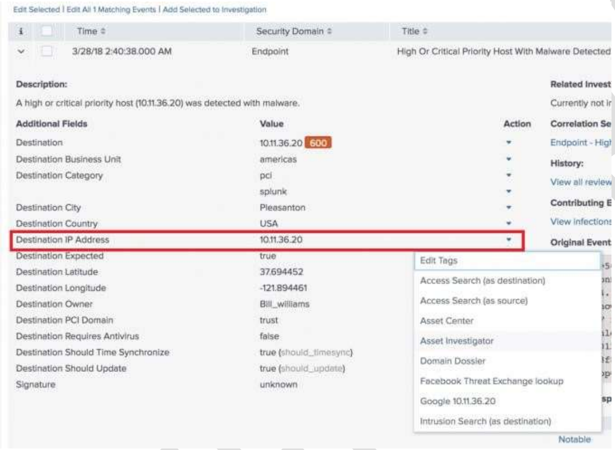
Assigned Severity

Assigned Priority	Informational	Unknown	Low	Medium	High	Critical
Unknown	Informational	Low	Low	Low	Medium	High
Low	Informational	Low	Low	Low	Medium	High
Medium	Informational	Low	Low	Medium	High	Critical
High	Informational	Medium	Medium	Medium	High	Critical
Critical	Informational	Medium	Medium	High	Critical	Critical

Source: https://docs.splunk.com/File:ES40_Notable_Urgency_table2.png

For example, a Destination IP Address corresponding to an **asset** with a **risk rating** of 100 (critical **priority**), combined with an **event severity** of critical, has resulted in the **urgency** of "Critical". If the assigned **severity** of the event was low or unknown, the resulting event **urgency** would have been "High" instead.

Returning to the Incident Review display: Each of the fields has an **Action** dropdown that allows drilling down into a variety of dashboards for further contextual details. For example, the **Action** item next to ***Destination IP Address*** provides a link to the **Asset Investigator**:



Edit Selected | Edit All 1 Matching Events | Add Selected to Investigation

i	□	Time ⇕	Security Domain ⇕	Title ⇕
⌄	□	3/28/18 2:40:38.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected

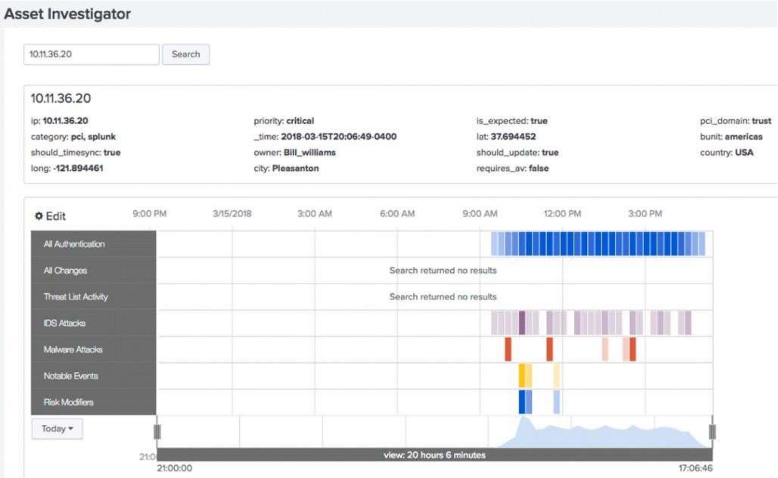
Description:

A high or critical priority host (10.11.36.20) was detected with malware.

Additional Fields	Value	Action
Destination	10.11.36.20 600	▾
Destination Business Unit	americas	▾
Destination Category	pci	▾
	splunk	▾
Destination City	Pleasanton	▾
Destination Country	USA	▾
Destination IP Address	10.11.36.20	▾
Destination Expected	true	
Destination Latitude	37.694452	
Destination Longitude	-121.894461	
Destination Owner	Bill_williams	
Destination PCI Domain	trust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	true (should_timesync)	
Destination Should Update	true (should_update)	
Signature	unknown	

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_IncRevFieldAct.png

The Asset Investigator displays details for a single host with groups of threat categories, such as ***All Authentication***, ***IDS Attacks*** or ***Malware Attacks***. Each row is presented as a **swimlane** that provides a heat map for collections of data points known as **candlesticks**. Brighter shades indicate a larger number of events within the category for that time period.


Asset Investigator

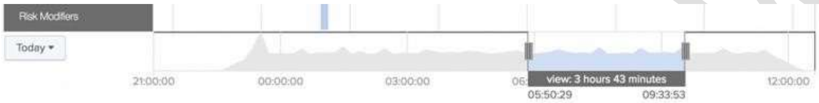
10.11.36.20 Search

10.11.36.20

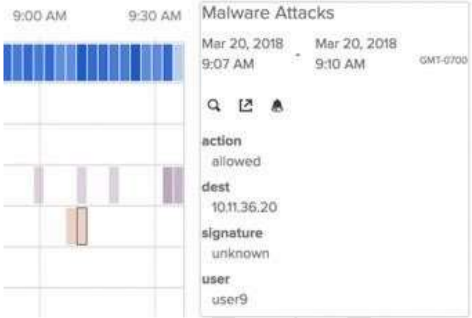
ip: **10.11.36.20** priority: **critical** is_expected: **true** pci_domain: **trust**
category: **pci, splunk** _time: **2018-03-15T20:06:49-0400** lat: **37.694452** bunit: **americas**
should_timesync: **true** owner: **Bill_williams** should_update: **true** country: **USA**
long: **-121.894461** city: **Pleasanton** requires_av: **false**

Source:

https://docs.splunk.com/images/8/83/ES51_UseCase_Malware_AssetInvest.png Use the **time sliders** to focus on a specific time range:



Click a **candlestick** to view the **Event Panel**..



Malware Attacks

Mar 20, 2018 9:07 AM - Mar 20, 2018 9:10 AM GMT-0700

action
allowed

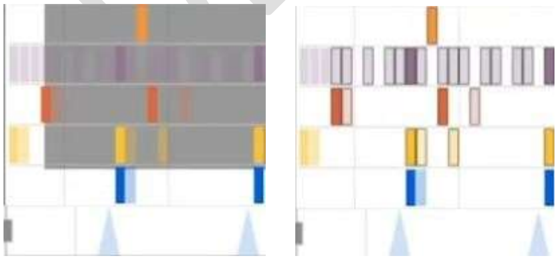
dest
10.11.36.20

signature
unknown

user
user9

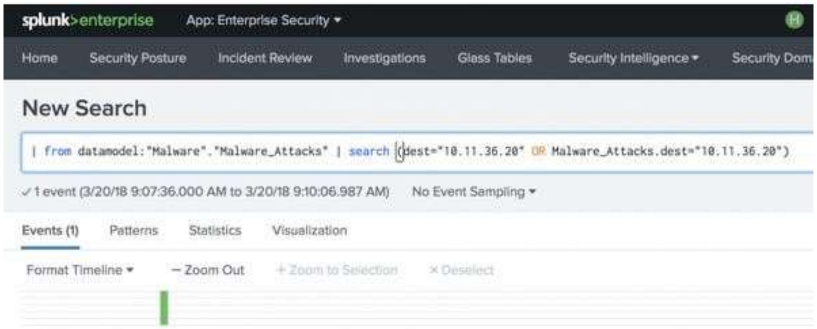
Source: https://docs.splunk.com/File:ES51_UseCase_Malware_AInvEvent.png

You can also drag your mouse over multiple **swimlanes** and timeframes to select multiple **candlesticks**, which will extrapolate common fields and a listing of field values into the **Event Panel**.



Source: https://www.youtube.com/watch?v=6XmiLxKvg6k

In the **Event Panel**, click the magnifying glass icon for **Go to Search** to drill down and search on the selected events:



```
| from datamodel:"Malware"."Malware_Attacks" | search (dest="10.11.36.20" OR Malware_Attacks.dest="10.11.36.20")
```

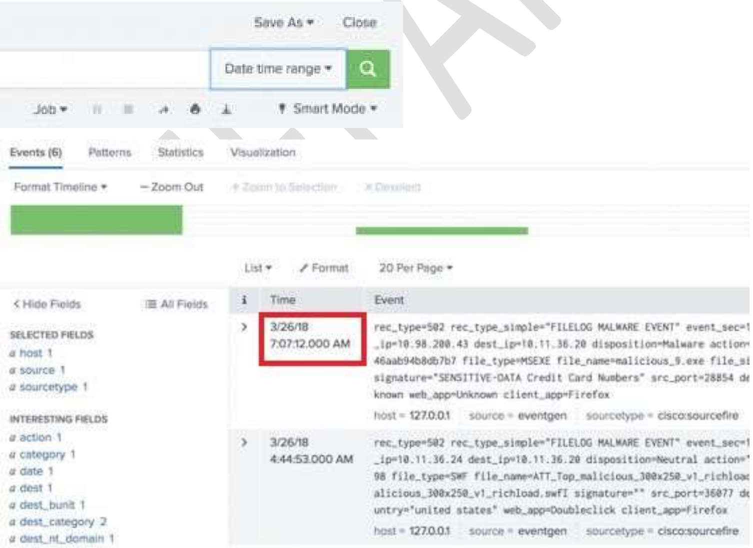
✓ 1 event (3/20/18 9:07:36.000 AM to 3/20/18 9:10:06.987 AM)

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_RawSearch1.png

The ***New Search*** dashboard shows the **App Context** of ***Enterprise Security***, which allows ES-specific field values, aliases, etc. to be applied to raw log events. The drilldown search uses the ***Malware_Attacks*** **dataset object** within the ***Malware*** **datamodel**, searching on the desired Destination IP Address of ***dest*** as an alias of the ***dest_ip*** field in the ***Malware*** data model. From a performance perspective, be aware that ES does **NOT** use accelerated data models for drilldown searches, so specifying a smaller time range will provide faster results.

With the desired results available in search, start your investigation with common key fields, such as ***source*** and ***sourcetype***. This will provide a context for what type of events are associated with the observance of malicious activity.
Extend upon this by investigating network-related fields such as ***src_ip*** and ***dest_ip*** to understand the flow of traffic. Finally, investigate host-specific values such as ***uri*** and ***client_app*** to determine what kind of requests were being made, and whether these reflect normal user behaviour.

Recall that a **candlestick** only represents a small portion of events within the timerange you selected in the **Asset Investigator**. Expand the time range from the **Date time range picker**, or from the **Event Time**.



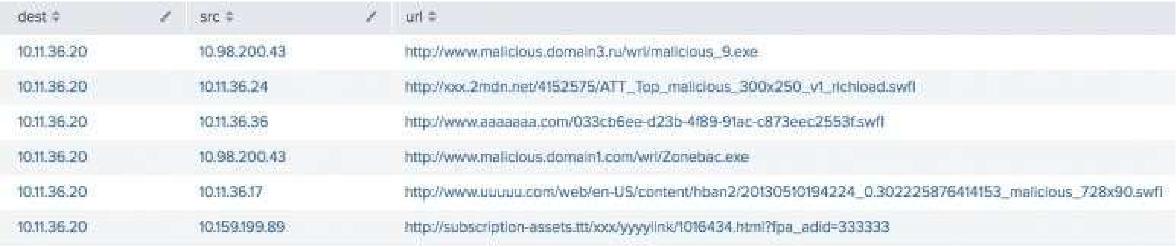
i	Time	Event

>	3/26/18
	7:07:12.000 AM
		rec_type=502 rec_type_simple="FILELOG MALWARE EVENT" event_sec=1
		_ip=10.98.200.43 dest_ip=10.11.36.20 disposition=Malware action=
		46aab94b8db7b7 file_type=MSEXE file_name=malicious_9.exe file_si
		signature="SENSITIVE-DATA Credit Card Numbers" src_port=28854 de
		known web_app=Unknown client_app=Firefox
		host = 127.0.0.1 source = eventgen sourcetype = cisco:sourcefire

>	3/26/18
	4:44:53.000 AM
		rec_type=502 rec_type_simple="FILELOG MALWARE EVENT" event_sec=1
		_ip=10.11.36.24 dest_ip=10.11.36.20 disposition=Neutral action="
		98 file_type=SWF file_name=ATT_Top_malicious_300x250_v1_richloac
		alicious_300x250_v1_richload.swfI signature="" src_port=36077 de
		untry="united states" web_app=Doubleclick client_app=Firefox
		host = 127.0.0.1 source = eventgen sourcetype = cisco:sourcefire

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_LotsOfEvents.png

Optionally, apply tabular formatting by appending `| table dest src url`, or with the fields you desire.



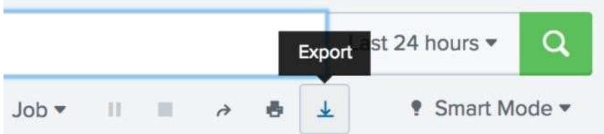
dest	src	url
10.11.36.20	10.98.200.43	http://www.malicious.domain3.ru/wrl/malicious_9.exe
10.11.36.20	10.11.36.24	http://xxx.2mdn.net/4152575/ATT_Top_malicious_300x250_v1_richload.swfl
10.11.36.20	10.11.36.36	http://www.aaaaaaa.com/033cb6ee-d23b-4f89-91ac-c873eec2553f.swfl
10.11.36.20	10.98.200.43	http://www.malicious.domain1.com/wrl/Zonebac.exe
10.11.36.20	10.11.36.17	http://www.uuuuu.com/web/en-US/content/hban2/20130510194224_0.302225876414153_malicious_728x90.swfl
10.11.36.20	10.159.199.89	http://subscription-assets.ttt/xxx/yyyylink/1016434.html?fpa_adid=333333

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_SortedEvents.png

In this example, there are three Shockwave Flash (SWF) files and three executables visible from the **sourcetype** of ***cisco:sourcefire***. A Shockwave Flash vulnerability likely acted as the point of entry, which then resulted in generation or download of additional malicious executables. This sourcetype shows network activity, but we should drill down on the ***src*** field to observe other sourcetype activity from a host of interest. Tabling the output by URL and file name, then sorting the results can verify this suspicion.

Following a standard incident response procedure, the malicious host is identified, and the containment phase follows to quarantine or isolate as appropriate.

Next, drill down into the ***uri*** field to find other hosts potentially infected by the same malware, extending the search as necessary to ensure all relevant hosts are identified. Tabulating this output by `| table src url file_name` allows the data to be more readily exported for reporting, as seen below:



Source: https://docs.splunk.com/File:ES51_UseCase_Malware_SuspiciousTableExport.png

From here, update the **notable event** created earlier. Select the notable event and click **Add Selected to Investigation**. Details of Splunk **Investigations** are covered later in the course objectives. Place the notable event in ***Pending*** until the investigation is concluded, then mark the event as **Closed** with appropriate notes to summarise Containment, Eradication, Response, and Lessons Learned.

NB: These incident response workflows are not an explicit part of Splunk Enterprise Security, but should be documented to better assist preparation for future incident response.

Review the second use case on your own for identifying initial malware infection using DNS data. Prerequisites include adding asset & identity data into Splunk ES, normalising anti-malware logs into the ***Malware*** CIM data model, normalising DNS lookup data to the ***Network Resolution*** CIM data model, and normalising web activity to the ***Proxy*** object of the ***Web*** CIM data model. For the exam, be prepared for questions on CIM, data models & normalisation.

If DNS queries are not collected by a third party sensor, they can be collected by the **Splunk Stream** app. Details of mapping source types to Data Models through **Field Aliases** and the **Add-on Builder** are discussed in the course objectives section of this document. The incident response process should start with preparation and identification, followed by containment, eradication, response, and lessons learned. https://docs.splunk.com/Documentation/ES/6.6.0/Usecases/Overview
https://docs.splunk.com/Documentation/ES/6.6.0/User/Howurgencyisassigned

Examine deployment requirements for typical ES installs

Deployment requirements are described in the course objectives.

https://docs.splunk.com/Documentation/ES/6.6.0/Install/DeploymentPlanning

https://docs.splunk.com/Documentation/ES/6.6.0/Install/Indexes

Know how to install ES and gather information for lookups

Details of ES installation and information gathering for lookups are described in the course objectives.

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallEnterpriseSecurity

https://docs.splunk.com/Documentation/ES/6.6.0/Install/Planyourdatainputs

Know the steps to set up inputs using Technology Add-ons (TAs)

TAs may be updated regularly and are unique for each add-on. Click **Apps** → **Manage Apps** → **Edit Properties** to set an app as **visible** to access its configuration. Add-ons, in contrast to apps, should be set to non-visible when configuration is complete. Custom TAs can be created using the **Splunk Add-on Builder**, where the configuration page will be defined by the fields you specify during its building and testing. You can also review the **inputs.conf** file of existing or custom created TAs to understand how these add-ons are structured. Further details are available in the course objectives.

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallTechnologyAdd-ons

Create custom correlation searches

Custom correlation searches are described in the course objectives.

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Correlationsearchoverview

Configure ES risk analysis, threat and protocol intelligence

Relevant ES dashboards for risk analysis and intelligence are described in the course objectives.

https://docs.splunk.com/Documentation/ES/6.6.0/User/RiskAnalysis

https://docs.splunk.com/Documentation/ES/6.6.0/User/ThreatIntelligence

https://docs.splunk.com/Documentation/ES/6.6.0/User/ProtocolIntelligence

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Createriskobjects

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Managethreatintelligenceuponupgrade

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Addgenericintel

Fine tune ES’s settings and other customizations

ES customisation is described in the course objectives.

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Generalsettings

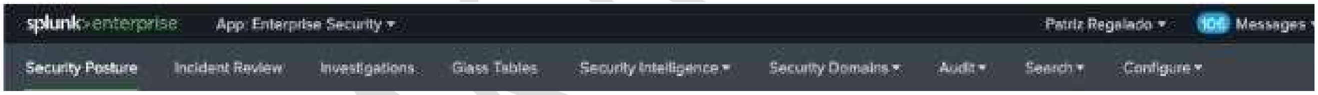
Course Objectives

1.0 Enterprise Security (ES) Introduction (5%)

1.1 Overview of ES features and concepts

Splunk ES uses search and correlation capabilities, based on operational intelligence, to allow users to capture, monitor and report on data from security devices, systems & applications. These are categorised under domains of access, endpoint and network threats. Security analysts can then identify, investigate and resolve alerts and incidents pertaining to these threats.

Dashboards support analysis and investigations, starting with **Security Posture** for a high level overview, and the **Incident Review** dashboard for details of notable events. **Investigations** supports workbenches, as well as a timeline and summary, for review & collaboration of incidents requiring additional investigation.



Source: https://splunkproducttours.herokuapp.com/tour/splunk-enterprise-security-es

More than 100 dashboards are available, supporting risk analysis, intelligence sources, asset & identity monitoring, as well as domain dashboards that provide an overview of access, endpoints, network, and asset & identity information. Audit dashboards monitor the Splunk ES environment.

This section is intentionally short. By learning, practising and reviewing the following sections, you will gain a more holistic overview of ES features and concepts.

https://docs.splunk.com/Documentation/ES/6.6.0/User/Overview

Splunk Enterprise Security Guided Product Tour | Thanks

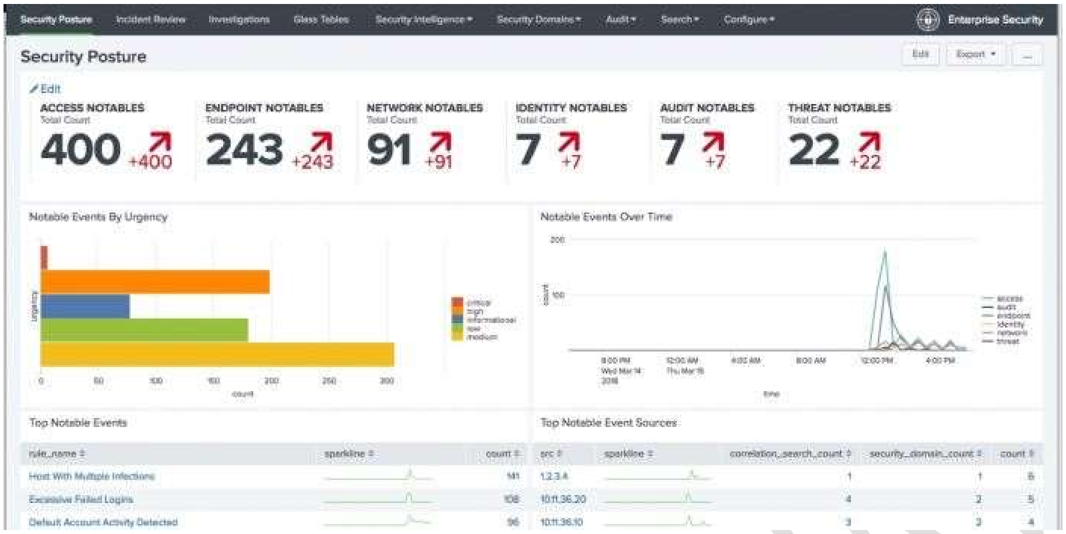
2.0 Monitoring and Investigation (10%)

2.1 Security Posture

The Security Posture dashboard provides an overview appropriate for a SOC wallboard, showing all events and trends over 24 hours, as well as real-time event information & updates.

Security posture dashboard panels include:

- **Key [Security] Indicators**: Count of notable events over 24 hours. **Indicators** are customisable, with default indicators as follows:
  - **Access** Notables
  - **Endpoint** Notables
  - **Network** Notables
  - **Identity** Notables
  - **Audit** Notables
  - **Threat** Notables
  - **UBA** [User Behaviour Analytics] Notables (if UEBA is available)
- **Notable Events by Urgency**: Based on asset priority and severity assigned tot he correlation search. Supports drilldown into **Incident Review** for associated events over the last 24 hours.
- **Notable Events Over Time**: Timeline of notable events by domain that can drill down into **Incident Review** for the selected ***security domain*** and timeframe.
- **Top Notable Events**: Displays ***rule names***, ***count*** and ***sparkline*** of activity over time. Drilldown opens the ***Incident Review*** dashboard scoped to the selected rule.
- **Top Notable Event Sources**: Displays the top 10 notable events by `src`, including total count, count per correlation & domain, and ***sparkline***. Drilldown opens **Incident Review** scoped to the selected `src`.



Security Posture

ACCESS NOTABLES Total Count	ENDPOINT NOTABLES Total Count	NETWORK NOTABLES Total Count	IDENTITY NOTABLES Total Count	AUDIT NOTABLES Total Count	THREAT NOTABLES Total Count
400 ↗ +400	243 ↗ +243	91 ↗ +91	7 ↗ +7	7 ↗ +7	22 ↗ +22

Top Notable Events

rule_name ⇕	sparkline ⇕	count ⇕
Host With Multiple Infections		141
Excessive Failed Logins		108
Default Account Activity Detected		96

Top Notable Event Sources

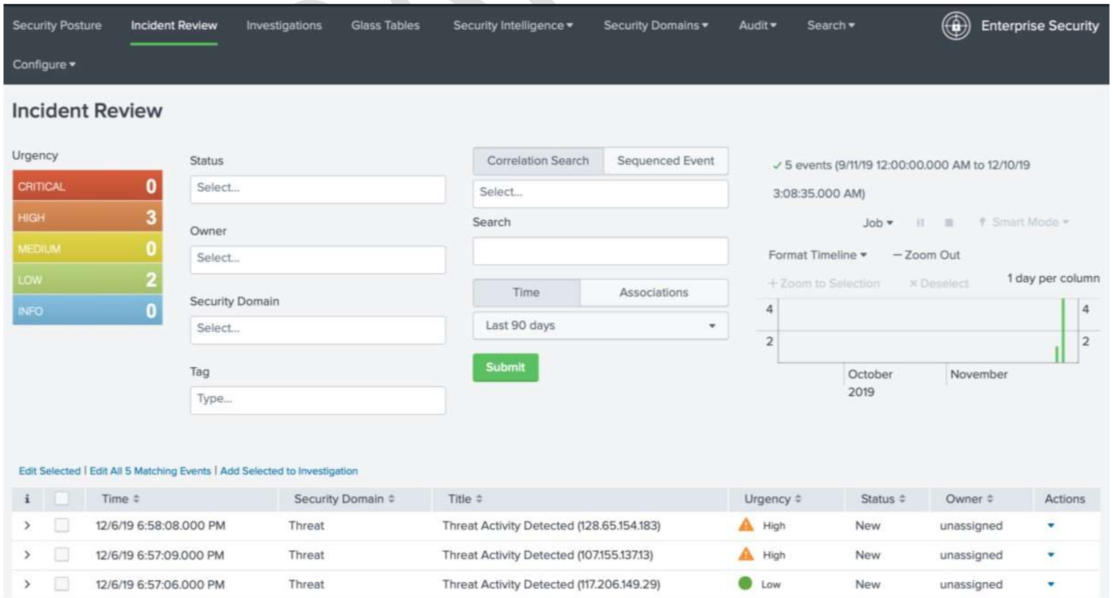
src ⇕	sparkline ⇕	correlation_search_count ⇕	security_domain_count ⇕	count ⇕
1.2.3.4		1	1	5
10.11.36.20		4	2	5
10.11.36.10		3	2	4

Source: https://docs.splunk.com/File:ES51_UseCase_Malware_SecPosDB.png
https://docs.splunk.com/Documentation/ES/6.6.0/User/SecurityPosturedashboard

2.2 Incident Review

Correlation searches are designed and developed to detect suspicious patterns and create notable events.

The **Incident Review dashboard** then displays notable events in descending date order, with their current status. Unlike the Security Posture dashboard, which provides an overview of notable events, the Incident Review dashboard provides individual details of notable events. Notable events can be filtered or sorted by field, and each event may represent one or more incidents detected by a correlation search.



Incident Review

Urgency

CRITICAL	0
HIGH	3
MEDIUM	0
LOW	2
INFO	0

Status: Select...

Owner: Select...

Security Domain: Select...

Tag: Type...

Select...

Search

Last 90 days

✓ 5 events (9/11/19 12:00:00.000 AM to 12/10/19 3:08:35.000 AM)

i	□	Time ⇕	Security Domain ⇕	Title ⇕	Urgency ⇕	Status ⇕	Owner ⇕	Actions
>	□	12/6/19 6:58:08.000 PM	Threat	Threat Activity Detected (128.65.154.183)	⚠ High	New	unassigned	▾
>	□	12/6/19 6:57:09.000 PM	Threat	Threat Activity Detected (107.155.137.13)	⚠ High	New	unassigned	▾
>	□	12/6/19 6:57:06.000 PM	Threat	Threat Activity Detected (117.206.149.29)	● Low	New	unassigned	▾

Analysts use this dashboard to examine, assign, or triage alerts, which may lead to an **Investigation**.

By default, notable event statuses include the following:

- Unassigned
- New [default]
- In Progress
- Pending
- Resolved
- Closed

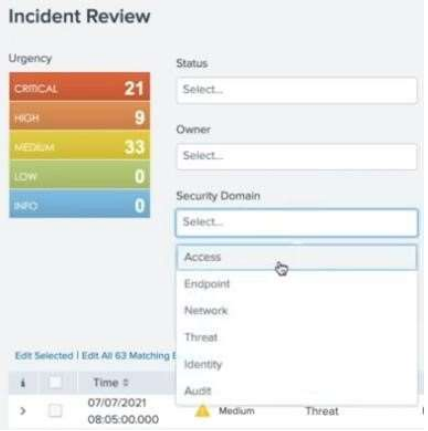
Incident Review progresses through stages of:

1. **Assignment** to an analyst
2. Updating the **status** of the event from “New” to “In Progress”
3. Performing investigative **actions** for triage, which might include **adaptive response** actions
4. Adding appropriate **comments** as triage continues
5. Optionally, assigning the notable event to an **Investigation** for more thorough analysis
6. Updating the notable event **status** to “Resolved”
7. Peer Review to validate the resolution before updating the notable event **status** to “Closed”

Two of the fields not mentioned in this example are ***Unassigned*** and ***Pending***. The ***Unassigned*** status indicates that the current analyst is no longer working on the event, and that another analyst can pick up where they left off. The ***Pending*** state indicates that the analyst is waiting on a third party such as a vendor, a client, or a change approval.

In cases like the above, it may be necessary to change the configuration of Incident Handling to add additional Notable Event Statuses. Examples might include “Pending Change”, “In Progress – Team X”, “Resolved – False Positive” or “Resolved – Mitigated”. This allows the dashboard to provide a clear picture of each incident state, while improving reporting and use cases. For example, a high number of False Positives for a specific notable event indicates the need to improve correlation searches for a specific use case.

The ***Security Domain*** on the **Incident Review** page aligns with the key indicators from the **Security Posture** dashboard. Note that if User & Endpoint Behavioural Analytics (UEBA) is not in use, this option will not be available. In a later section on dashboards, you’ll see how the ***access***, ***endpoint***, ***network*** and ***identity*** security domains are presented visually via the **Security Domains** menu. ***Threats*** are more nuanced, as they can pertain to malware on endpoints, network intrusions or vulnerabilities; or to threat intelligence, which falls under the **Security Intelligence** menu. ***Audit*** events are observable in separate dashboards under the **Audit** menu.



Source: https://www.youtube.com/watch?v=6XmiLxKvg6k

https://docs.splunk.com/Documentation/ES/6.6.0/User/IncidentReviewdashboard

2.3 Notable events management

Notable events can be seen from two lenses; an operational view, and an administrative view.

From an operational perspective, notable events are managed through ***triage***. This means assigning notables to specific owners, prioritising actions to resolve security events, and accelerating triage by using ***filters***, ***tags*** or ***dispositions***. NB: dispositions are a new feature, so may not be referenced in the current version of the Splunk ES Administration exam. As described above, custom notable event statuses can be used for earlier versions of Splunk ES, or as an interim solution to support backward compatibility with existing business processes.

Selecting a notable and choosing **Edit selected** allows you to take action on that event. Selecting multiple events, then clicking **Edit all selected**, or clicking **Edit all X matching events** allows you to take action on multiple events.

Once selected, you may select an **Owner**, or choose **Assign To Me** to assign it to yourself. You can also change the **Status** as described above, customise the **Urgency** if needed, and optionally add a **Comment** to describe actions taken.

When ready to proceed, **Save changes** and **Close** the dialog box if not closed automatically.

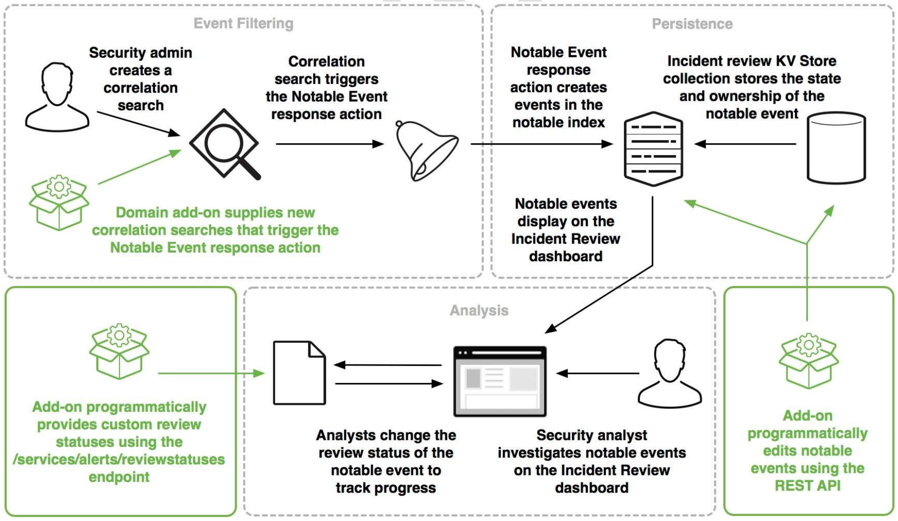
Ways to triage notables faster include:

- **Sorting** or **Filtering** by:
  - **Urgency** (Critical, High, Medium, Low, Informational)
  - **Status** (New, In Progress, Pending, Resolved, Closed, or custom status)
  - **Owner**
  - **Security Domain** (Access, Endpoint, Network, Threat, Identity, Audit, or custom domain)
  - **Type** (All Notables, ***Risk Notables***, or [Non-risk] Notables)
- **Filtering** by:
  - **Search Type** (correlation search or sequenced search)

    - **Time** (e.g. Last 24 hours, Last 30 days) or **Association** (Specific investigations, **Short ID** of alert, or running attack templates associated with notables)
    - **Correlation Search Name** (E.g. "Use Case T001: Detect Malware on Endpoint")
- Grouping Notables (**Saved Filters**)
- Manage filters for notables
- Add **Dispositions** for notables
    - From the Splunk ES menu bar, click **Incident Review**, select a notable, then **Edit Selected**
    - Choose one of the following **Dispositions**
        - **Undetermined** [default]
        - **True Positive** – Suspicious Activity (e.g. legitimate malware)
        - **Benign Positive** – Suspicious but Expected (e.g. legitimate privilege escalation)
        - **False Positive** – Incorrect Analytic Logic (e.g. entropy instead of UEBA or MLTK)
        - **False Positive** – Inaccurate Data (e.g. incorrect data ingest or parsing)
        - <Custom Disposition>

Notable events can be generated in several ways:

- as an adaptive response to a correlation search
- via the ES menu bar under **Configure → Incident Management**
- via the ***/services/alerts/reviewstatuses*** REST API endpoint
- via the **Event Panel** of the **Asset Investigator** dashboard



Event Filtering
Security admin creates a correlation search
Correlation search triggers the Notable Event response action
Domain add-on supplies new correlation searches that trigger the Notable Event response action
Persistence
Notable Event response action creates events in the notable index
Incident review KV Store collection stores the state and ownership of the notable event
Notable events display on the Incident Review dashboard
Analysis
Add-on programmatically provides custom review statuses using the /services/alerts/reviewstatuses endpoint
Analysts change the review status of the notable event to track progress
Security analyst investigates notable events on the Incident Review dashboard
Add-on programmatically edits notable events using the REST API

Source: https://dev.splunk.com/enterprise/static/SES-460-notable-compressor-38128bbe320a63023373269dfddef322.png

Notable event review statuses can be configured in ***reviewstatuses.conf*** within **SA-ThreatIntelligence**.

Risk Event Notables include two fields:

- **Risk Events**: Events that created the notable alert
- **Aggregated Risk Score**: Sum of scores associated with each of the contributing events, such that three events with risk scores of 10, 20 and 40 would have an aggregated risk score of 70.

Click the value in the ***Risk Events*** field for the notable of interest. This opens a window with two panels.

The top panel displays a timeline of contributing risk events, while the bottom panel includes a table with detailed event information

Sort the contributing risk events in the table by ***Time***, ***Risk Rule*** or ***Score***.

Expand the notable in the **Contributing Risk Events** table to analyse the following fields:

- Risk Object
- Source
- Risk Score
- Risk Message
- Saved Search Description
- Threat Object
- Threat Object Type

Click **View Raw Event** for information on the ***contributing events*** that triggered the ***risk event***.

Correlate risk events with dates and risk scores in the ***timeline visualisation*** to identify threats. The timeline may also use colour codes to indicate severity, aligning with colours used in the contributing risk event table.

Up to 100 ***Contributing Risk Events*** can be viewed at a time. If more than 100 contributing events exist, the event count displays as 100+ on the header, with a link to the search page to display all risk events.

Hover over the colour coded icons in the timeline visualisation for more risk event information, including:

- Risk Score
- Event Name
- Description
- Time
- MITRE Tactic
- MITRE Technique

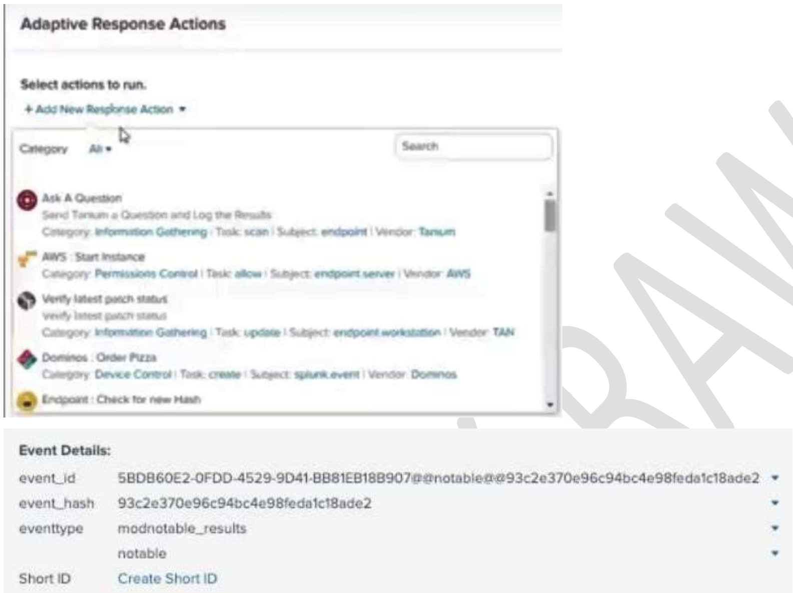
Clicking a notable in the timeline highlights the associated row in the ***Contributing Risk Events*** table.

Identify the **Risk Object Type** as ***User***, ***System***, ***Network Artifact*** or ***Other*** via the timeline header.

Other components in the **Incident Review** for a given alert include:

- **History**: View recent activity for the notable event to see comments and status changes

- **Related Investigations**
- **Correlation search**: Understand why the notable event was created or generated
- **Contributing events**: What source events caused the notable to be created
- **Asset and Identity Risk Scores**: Drill down on risk analytics
- **Adaptive Response**: Review automatically completed actions for the event with drill down for more details, and Adaptive Response Invocations for the associated raw audit events
- **Next Steps**: Defines what triage actions should be taken next
- **Create Short ID**: Found under ***Event Details*** for sharing with other analysts or to reference this notable event



Adaptive Response Actions

Select actions to run.

+ Add New Response Action ▾

Category All ▾ Search

Ask A Question
Send Tanium a Question and Log the Results
Category: Information Gathering | Task: scan | Subject: endpoint | Vendor: Tanium

AWS : Start Instance
Category: Permissions Control | Task: allow | Subject: endpoint.server | Vendor: AWS

Verify latest patch status
verify latest patch status
Category: Information Gathering | Task: update | Subject: endpoint.workstation | Vendor: TAN

Dominos : Order Pizza
Category: Device Control | Task: create | Subject: splunk.event | Vendor: Dominos

Endpoint : Check for new Hash

Event Details:

event_id 5BDB60E2-0FDD-4529-9D41-BB81EB18B907@@notable@@93c2e370e96c94bc4e98feda1c18ade2 ▾
event_hash 93c2e370e96c94bc4e98feda1c18ade2 ▾
eventtype modnotable_results ▾
notable ▾
Short ID Create Short ID

Source: https://www.domaintools.com/assets/blog_image/how-we-made-investigations-in-splunk-powerful-effectiveimage-4.jpg

Investigations, **Correlation Searches** and **Adaptive Response** will be addressed in detail in a later section

Sequenced events from sequence templates are also listed in the selected notable alert details, allowing drill down into each of the events in the sequence that contributed to the notable event being generated.

The focus here is on managing notables rather than investigating notables, but further details on notable investigation can be found in the first link below:

https://docs.splunk.com/Documentation/ES/6.6.0/User/Triagenotableevents

https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/notableeventsplunkes/

2.4 Managing Investigations

The **Investigations** page shows the following attributes of investigations assigned to you:

- Titles

- Descriptions
- Time Created
- Last Modified Time
- Collaborators

If you have the capability to manage all investigations, you can see these details for all investigations, not just for those on which you are collaborating.

Use the **Filter** box to search on title and description to find an Investigation. Alternatively, follow the below process to start a new investigation.

1. Create an Investigation
    1. Directly from the Investigations page;
    2. via **Incident Review** while triaging notable events;
    3. From an event workflow action; or
    4. Using the investigation bar at the bottom of any dashboard page
2. Add colleagues to the investigation as **collaborators**.
3. Open the investigation and start investigating on the **workbench**.
4. Add **artifacts** to the investigation scope, in addition to those added automatically from notable events.
5. Review the tabs and panels for information relevant to your investigation, such as additional affected **assets** or details about the affected assets that can accelerate your investigation.
    1. As you investigate, add helpful or insightful events, actions, and artifacts to the investigation to record the steps you took in your investigation.
    2. Run searches, adding useful **searches** to the investigation from your **action history** with the **investigation bar** or relevant **events** using **event actions**. This makes it easy to replicate your work for future, similar investigations, and to comprehensively record your investigation process.
    3. **Filter** dashboards to focus on specific elements, like narrowing down a **swim lane search** to focus on a specific **asset** or **identity** on the asset or identity investigator dashboards. Add insightful filtering actions from your action history to the investigation using the investigation bar.
    4. Triage and investigate potentially-related notable events. Add relevant notable events to the investigation.
6. Add **notes** to record other investigation steps, such as notes from a phone call, email or chat conversations, links to press coverage or social media posts. **Upload files** like screenshots or forensic investigation files.
7. Complete the investigation and **close** the investigation and *optionally*, **close** associated notable events.
8. Review the investigation **summary** and share it with others as needed.

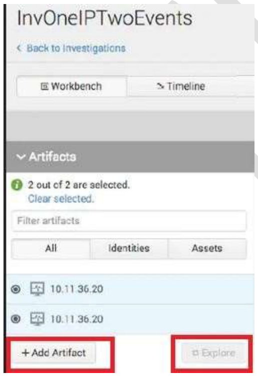
Once an investigation is created, open and has assigned collaborators, you can add **artifacts** to the **scope** of the investigation. This may include **assets**, **identities**, **files** and **URLs** to verify whether they are affected by, or participants in, the overall security incident. You can add an artifact to an investigation as follows:

- Add artifacts **automatically** from a notable event
- Add artifacts **manually**
- Add artifacts from a **workbench panel**
- Add artifacts from an **event** on the investigation

Artifacts can be freely added to the scope of the investigation, and later viewed from the **timeline**. Within the scope, review relevant panels for additional context, then add **events** or details that provide further insight. NB: **Assets** and **Identities** added as artifacts to the scope do not have to form part of the ***Asset and Identity framework*** within Splunk Enterprise Security.

To manually add an artifact:

1. Open the relevant investigation to view the associated workbench.
2. On the Artifacts panel, click **Add Artifact**, entering the **Artifact** value and **Type**
    1. NB: An Artifact **Type** of **File** may be a ***filename***, ***file hash*** or ***file path***
3. Optionally add a **description** and one or more comma-separated **labels** to contextualise the entry
4. If choosing the **Add multiple artifacts** tab, all artifacts must be the same **Type**.
    1. Separate the entries using a delimiter of choice, and specify this as the **Separator**.
    2. As with a single artifact, optionally add a description and comma-separated labels
5. Optionally, click **Expand Artifacts** to look up an ***asset*** or ***identity*** in the corresponding lookup (where available), and add the correlated artifacts to the investigation in scope
6. Click **Add to Scope** to add the artifacts to your investigation scope



InvOneIPTwoEvents

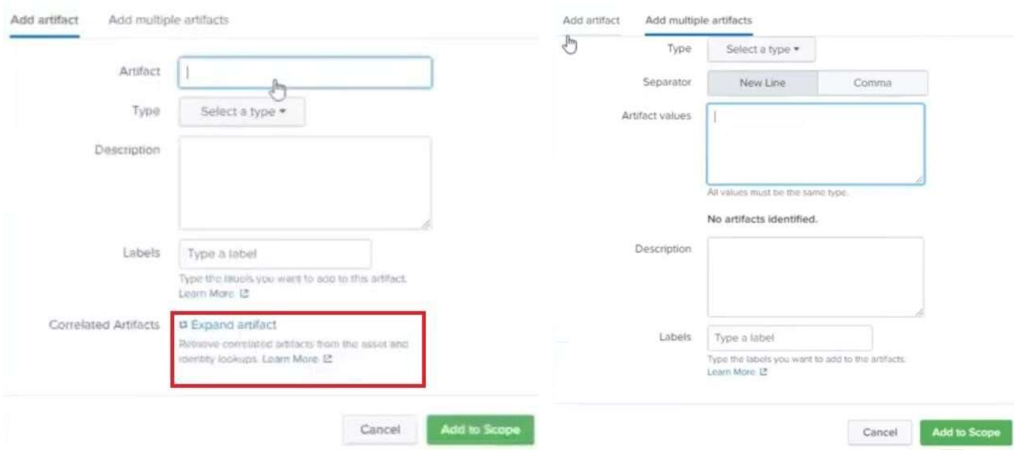
‹ Back to Investigations

2 out of 2 are selected.
Clear selected.

10.11.36.20

10.11.36.20

Image: Adding and exploring artifacts from a workbench panel



Type the labels you want to add to this artifact. Learn More

Remove correlated artifacts from the asset and identity lookups. Learn More

All values must be the same type.

No artifacts identified.

Type the labels you want to add to the artifacts. Learn More

Source: https://www.youtube.com/watch?v=KoIY-_2ItSc

Manually added artifacts are automatically selected so that you can click **Explore** and continue investigating with the new artifacts. Hovering over the artifacts and selecting the **information icon (i)** will show the corresponding labels. Labels can also be seen under the summary tab.

If a workbench panel has drilldown enabled, you can add field values as artifacts from the panel:

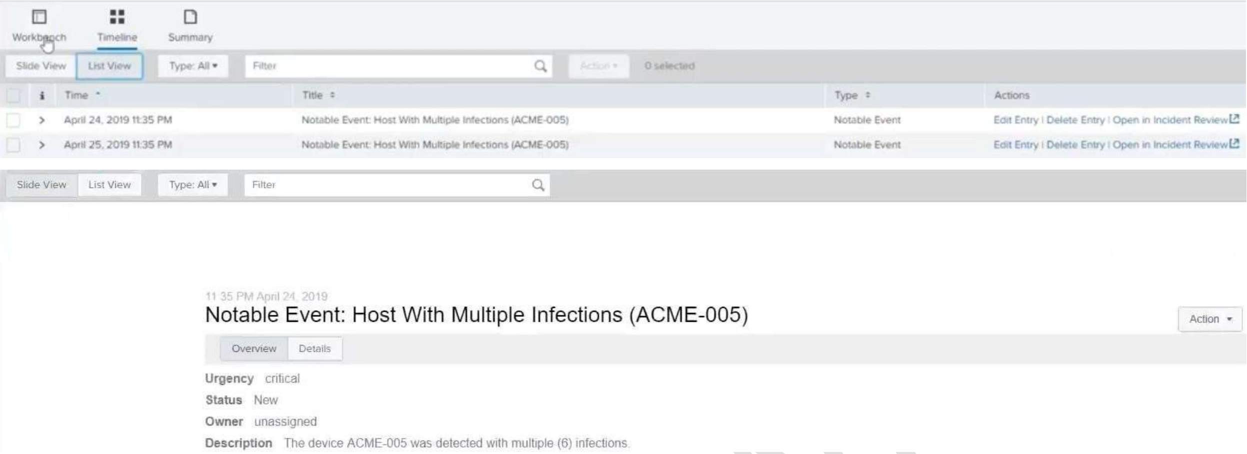
1. Select artifacts on the workbench and click **Explore**
2. In a panel, click a **field value** and complete the pre-populated **Add Artifact** dialog box
3. Optionally add a **description** and **labels** for the artifact
4. Optionally click **Expand Artifacts** to look up asset and identity information in asset or identity lookups and add correlated artifacts to the investigation scope
5. Click **Add to Scope** to add the desired artifact to the investigation scope

New **panels**, **tabs** and **profiles** can be added to the workbench to simplify investigations.

1. Open an **Investigation** and click **Explore** to explore artifacts
2. Click **Add Content**
3. Click **Load profile** or **Add single tab**, make a selection, and save
4. New panels are created via the ES Menu Bar 1. **Configure → Content → Content Management**
   2. For a Prebuilt panel:
      1. Create **New Content → Panel**
      2. Type a **Prebuilt panel ID**, select a **Destination App**, Type **prebuilt panel XML**, and **Save**
      3. Alternatively, convert a dashboard panel to a prebuilt panel
   3. For a standard (Workbench) panel
      1. Create **New Content → Workbench Panel**
      2. Select the panel from the list
      3. Optionally add a **Label** or **Description**

4. Add a **token** to replace the token in the panel search

5. Select the artifact **Type**, **Apply**, **Save**, and **Save** again In addition to the workbench view, there is the timeline view:



	i	Time ˄	Title ⇕	Type ⇕	Actions
□	>	April 24, 2019 11:35 PM	Notable Event: Host With Multiple Infections (ACME-005)	Notable Event	Edit Entry | Delete Entry | Open in Incident Review
□	>	April 25, 2019 11:35 PM	Notable Event: Host With Multiple Infections (ACME-005)	Notable Event	Edit Entry | Delete Entry | Open in Incident Review

11:35 PM April 24, 2019

Notable Event: Host With Multiple Infections (ACME-005)

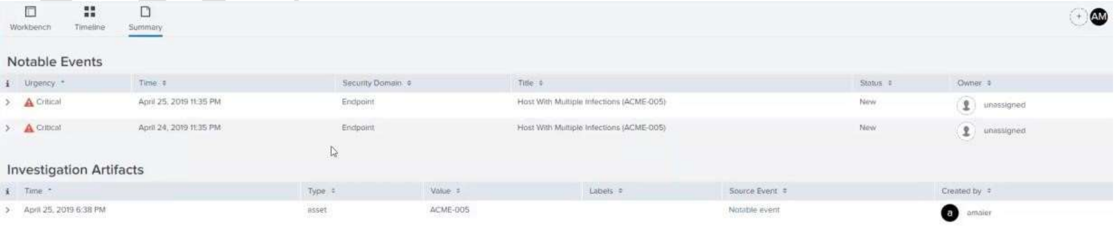
Urgency critical
Status New
Owner unassigned
Description The device ACME-005 was detected with multiple (6) infections.

Source: https://www.youtube.com/watch?v=KoIY-_2ItSc

After adding an event to the investigation, individual field values from the raw event can be added as artifacts:

1. View the **Timeline** of the investigation and locate the event in the **Slide View**
2. Click **Details** to view a table of fields and values in the event
3. Click the value to add to the investigation scope and complete the **Add Artifact** dialog box
4. Optionally add a **description** and **labels** for the artifact
5. Optionally click **Expand Artifacts** to look up asset or identity information and add correlated artifacts to the investigation scope
6. Click **Add to Scope** to add the raw event field values to the investigation scope

Finally, there is a **Summary** view, which provides an overview of notable events and artifacts linked to the investigation, as well as their respective owners and creators. The list of **contributors** remains visible in this view, with the option to add additional contributors as required.

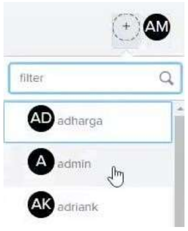


Notable Events

i	Urgency ˄	Time ⇕	Security Domain ⇕	Title ⇕	Status ⇕	Owner ⇕
>	Critical	April 25, 2019 11:35 PM	Endpoint	Host With Multiple Infections (ACME-005)	New	unassigned
>	Critical	April 24, 2019 11:35 PM	Endpoint	Host With Multiple Infections (ACME-005)	New	unassigned

Investigation Artifacts

i	Time ˄	Type ⇕	Value ⇕	Labels ⇕	Source Event ⇕	Created by ⇕
>	April 25, 2019 6:38 PM	asset	ACME-005		Notable event	amaier

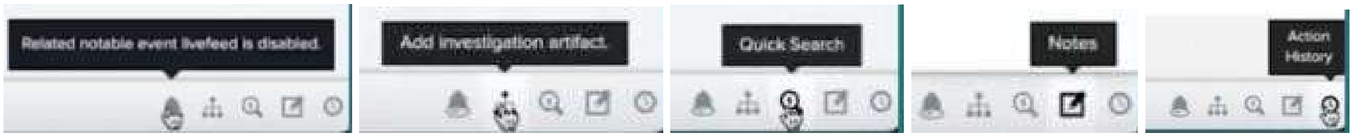


Source: https://www.youtube.com/watch?v=KoIY-_2ItSc

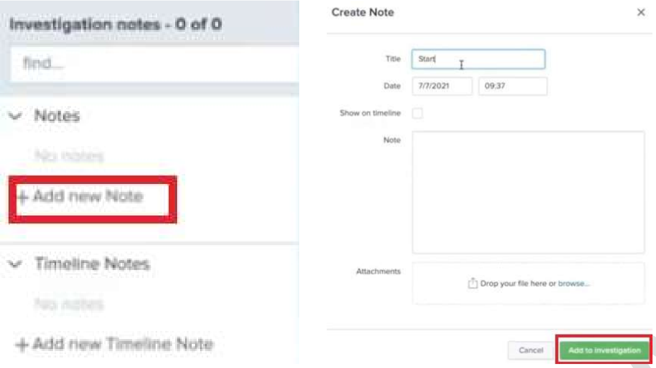
For any of these views, there are also options in the bottom right-corner to:

- View a live feed of relevant notable events
- Perform a Quick Search
- Add an investigation artifact

- View or add **Notes**, or add a **Timeline Note**
- **View Action History**


Related notable event livefeed is disabled.
Add investigation artifact.
Quick Search
Notes
Action History

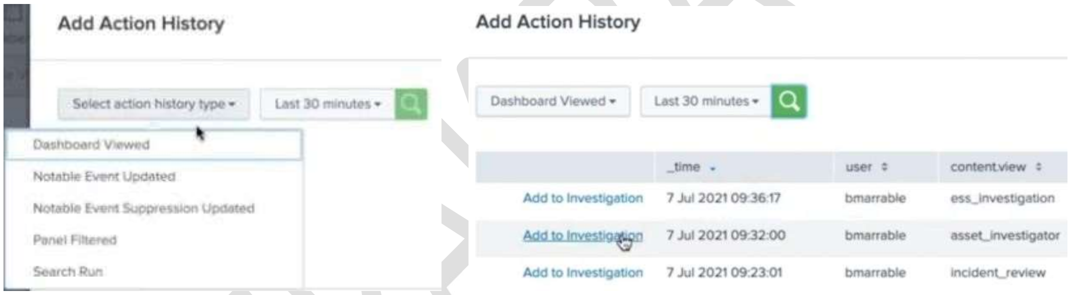
Notes are for standard work performed on the workbench, such as observations or additional information. In contrast, timeline notes are for inline comments that help describe the timeline of events, visible at the time you specify.



Title: Start

Date: 7/7/2021 09:37

Image: View and Add Notes



	_time ⌄	user ⇕	contentview ⇕
Add to Investigation	7 Jul 2021 09:36:17	bmarrable	ess_investigation
Add to Investigation	7 Jul 2021 09:32:00	bmarrable	asset_investigator
Add to Investigation	7 Jul 2021 09:23:01	bmarrable	incident_review

Image: View and Add Action History

Detailed procedures for performing investigation are not included in this document, but you are encouraged to follow the directions at the following link to become familiar with the process of adding details to an investigation, making changes, collaborating, reviewing, referring to action history, and sharing results https://docs.splunk.com/Documentation/ES/6.6.0/User/Timelines

https://www.splunk.com/en_us/blog/security/use-investigation-workbench-to-reduce-time-to-contain-and-time-to-remediate.html

3.0 Security Intelligence (5%)

3.1 Overview of security intelligence tools

In addition to the Security Intelligence dashboards, Splunk includes a selection of generic or **non-threat intelligence sources** which can be configured via the Splunk ES tool bar under **Configure** → **General** → **General Settings**:

- Mozilla Public Suffix List (enabled by default)
- MITRE ATT&CK Framework (enabled by default)
- ICANN Top-level Domains List (enabled by default)
- Cisco Umbrella 1 Million Sites
- Alexa Top 1 Million Sites
- MaxMind GeoIP ASN databases (IPv4 and IPv6) **Threat intelligence sources** include:
- Emerging Threats (compromised IPs and firewall IP rules)
- Malware domain host list (Hail a TAXII)
- iblocklist (LogMeIn, Priatebay, Proxy, Rapidshare, Spyware, Tor, Web attacker)
- Phishtank Database
- SANS blocklist

You can also add **custom or third party intelligence sources** through:

- Downloading Internet feeds, using a ***URL-based threat source*** or ***TAXII feed***
- Uploading a structured threat intelligence file, such as ***STIX*** (JSON) or ***OpenIOC*** (XML) format
  - See examples of STIX JSON and OpenIOC XML files in the appendix
- Uploading a custom ***CSV*** file with threat intelligence
- Adding threat intelligence from ***Splunk events***
- Adding threat intelligence with a ***custom lookup file***

Once configured, verify that you have added threat intelligence successfully via the ES menu bar, by clicking on **Audit →** **Threat Intelligence Audit**. Ensure the ***download_status*** indicates “threat list downloaded” or “Retrieved document from TAXII feed” as appropriate. Also review the **Intelligence Audit Events** for any errors associated with ***lookups*** used for threat intelligence.

Types of threat intelligence stored in KV (key-value) stores include:

- X509 Certificates (***certificate_intel***)
- Email (***email_intel***)
- File names or hashes (***file_intel***)
- URLs (***http_intel***)
- IP addresses and domains (***ip_intel***)
- Processes (***process_intel***)
- Registry entries (***registry_intel***)
- Services (***service_intel***)
- Users (***user_intel***)

These sources are referenced by **collections.conf** in **DA-ESS-ThreatIntelligence**. Each source has a unique rating called **weight**, which defaults to 60, but can be specified in **inputs.conf** within **SA-**

ThreatIntelligence. Higher weighting results in higher risk scores for corresponding intelligence matches.

Threat Intelligence is managed from the ES menu bar under **Configure → Data Enrichment → Threat Intelligence Management**. Threat intelligence is automatically processed, but you can select a workload action to trigger for other intelligence, such as running a user-defined saved search. This streamlines the parsing and processing of intelligence documents to extend and improve performance of the threat intelligence framework.

Threat Intelligence Management also provides the tools to:

- Disable intelligence sources;
- Disable individual threat artifacts;
- Edit an intelligence source;
- Configure threat source retention; and
- Configure threat intelligence file retention

Generic intelligence can be configured from the ES menu under **Configure → Data Enrichment → Intelligence Downloads**. For non-threat intelligence, leave ***Sinkhole*** unchecked, and deselect the check box for ***Is Threat Intelligence***. The ***weight*** field is irrelevant in a non-threat context. The default ***interval*** is 43200 seconds, or every 12 hours. Do not use the ***Maximum age*** setting. Fill out the ***Parsing Options*** to ensure your list parses correctly, and change ***Download Options*** as required. **Intelligence documents** can be configured to trigger specific ***workloads*** or ***actions*** each time they are uploaded or downloaded.

Use the **inputintelligence** command to add intelligence from the threatlist directory to your search results. Think of this as an intelligence lookup. E.g. **inputintelligence** ***cisco_top_one_million_sites***.

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Addthreatintel

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Addgenericintel

4.0 Forensics, Glass Tables and Navigation Control (10%)

4.1 Explore forensics dashboards

The three primary dashboards for day to day operational activities will likely be the following: • **Security Posture**: Customisable overview of notable events over the past 24 hours

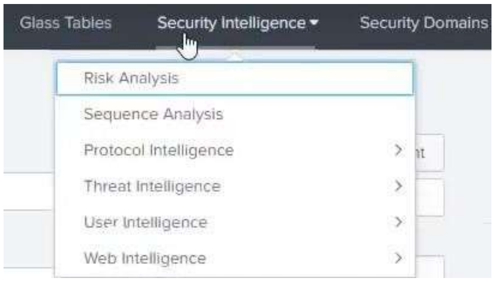
  - **Key Indicators**: Notable events by security domain
  - **Notable Events by Urgency**: Calculated from asset priority and severity assigned to the correlation search. Drilling down opens the Incident Review dashboard filtered to the selected urgency
  - **Notable Events over Time**: Displays a timeline of events by security domain. Drilling down shows all notable events in the selected security domain and timeframe
  - **Top Notable Events**: Top notable events by rule name, including a total count and sparkline. Drilling down opens Incident Review scoped to the selected rule.
  - **Top Notable Event Sources**: Top 10 notable events by `src`, including total count, count per correlation & domain, and sparkline. Drilling down opens Incident Review scoped to the `src`.

- **Incident Review**: Details of notable events to support triage and assignment
- **Investigations**: Track progress and activity while investigating multiple related security incidents

Investigations is the most prominent forensic dashboard, and is typically accessed via the incident review pages, as an escalation from notable event triage.

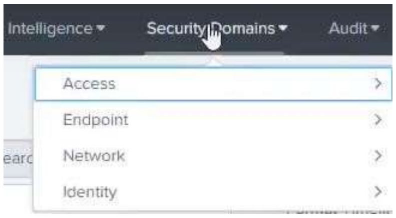
Security intelligence dashboards enhance investigations in the following areas:

- **Risk analysis**: Assess risk scores of systems and users to identify environmental risks
- **Sequence analysis**: Provides context into running sequence correlation searches
- **Protocol intelligence**: Packet capture data from stream capture apps provide insights into network activity including suspicious traffic, DNS, SSL, email, and other relevant connections & protocols
- **Threat intelligence**: Integrated and additional sources provide context to security incidents and help identify known malicious activity
- **User intelligence**: Investigate and monitor user & asset activity, and review access anomalies
- **Web intelligence**: Analyse web traffic by HTTP category, user agent, URL length, and new domains



Security domain dashboards monitor events and status of important security domains:

- **Access**: Authentication and access-related data, such as login attempts, access control events, and default account activity
- **Endpoint**: Malware infections, patch history, system configurations, and time synchronisation
- **Network**: Traffic data from firewalls, routers, IDPS, vulnerability scanners, proxy servers and hosts
- **Identity**: Data from asset and identity lists, as well as types of sessions in use



Security Intelligence supports correlation searches and alerts, including contributing risks, events and anomalous or notable behaviour. **Security Domains** provides environmental context better suited to investigations, and may be more closely associated with governance, compliance, audits and security maturity.

As this objective is to **explore** dashboards, you should interact with each of the dashboards, and think about when each dashboard might be used in a variety of scenarios. You are not expected to memorise individual panels or their underlying searches, but should be able to associate individual dashboards with their corresponding security domain.

https://docs.splunk.com/Documentation/ES/6.6.0/User/Domaindashboards

https://docs.splunk.com/Documentation/ES/6.6.0/User/SecurityPosturedashboard

4.2 Examine glass tables

Glass tables support design and development of custom visualisations tailored to particular audiences. Unlike dashboards, glass tables provide a more holistic view to assist with governance, risk and compliance. For example, notable events for the network security domain can overlay a diagram of the network topology to provide visual indication of where additional support or resources may be required.

From the ES menu, click **Glass Tables**. Next, click **Create New Glass Table**, enter a **Title** and **Description**, and set **Permissions**. Finally, click **Create Glass Table**. Use the editing tools at the top to add images, shapes, icons and text. Use the **Security Metrics** on the left to present results of ad hoc searches, display metric data, and to add connections that describe the relationships between metrics.

Click and drag key indicator search **widgets** onto the drawing canvas, which will update in real time. Click on a widget to customise the related ***Search***, ***Earliest Time***, ***Threshold*** details, ***Custom Drilldown***, and visual elements. Click **Save** to save your new glass table.

Though glass tables are not present in ES 6.6, they are supported in ES 6.4, which continues to be supported by the latest version of Splunk Enterprise (v8.2.2 at the time of writing). The **Dashboard Studio** app is the current recommendation for providing this type of graphical functionality.

https://www.splunk.com/en_us/resources/videos/splunk-enterprise-security-glass-tables.html

https://docs.splunk.com/Documentation/ES/6.4.1/User/CreateGlassTable

4.3 Configure navigation and dashboard permissions

To configure **navigation**, from the ES menu bar, select **Configure → General → Navigation** Locate a preferred view for when opening Splunk and hover over the checkmark next to the view's name to "Set this as the default view". Click **Save** to save changes, and **OK** to refresh the page.

Additional options exist to:

- Edit the existing menu bar navigation
- Add a single view or a collection to the menu bar
- Add a view to an existing collection
- Add a link to the menu bar
- Restore the default navigation

To configure **permissions**, from the ES menu bar, select **Configure → General → Permissions** Select the checkbox for the role and the permissions you want to assign to that role, and save.

To update general dashboard permissions, open the Search & Reporting app, click on Dashboards, and under Actions, select Edit → Edit Permissions. You can then choose **Owner** to make the dashboard ***private***, **App** to share the dashboard in the current ***app context***, or **All apps** to make the dashboard accessible throughout the platform instance.
https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Customizemenubar
https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Managepermissions
https://docs.splunk.com/Documentation/Splunk/8.2.2/Viz/DashboardPermissions

5.0 Enterprise Security (ES) Deployment (10%)

5.1 Identify deployment topologies

Deployment topologies or architectures include the following:

- **Single instance** deployment: Search head and indexer, suitable for a lab or test environment. Forwarders collect data and send it to the single instance for parsing, storing and searching
- **Distributed search** deployments: Dedicated search head or search head cluster. Forwarders collect data and send it to one or more indexers. Improve search performance by using an index cluster consisting of a master and multiple nodes. In a distributed search deployment, and to implement search head clustering, the search head must forward all data to the indexers.
- **Cloud deployment**: Splunk Cloud Platform (SCP) customers work with Splunk support to set up, manage, and maintain their cloud infrastructure
- **Hybrid search deployment**: An on-premises Splunk ES search head can search indexers in another cloud environment. Consider the effect of added latency, bandwidth concerns and adequate hardware to support the search head

If using a deployment server for Enterprise Security apps and add-ons, Enterprise Security will not finish installing. For Splunk ES add-ons, deploy them using the **Distributed Configuration Management** tool. If add-ons are managed by the deployment server, **remove** the **deploymentclient.conf** file that references the deployment server. **Distributed Configuration Management** helps to configure & download **Splunk_TA_ForIndexers**. Further modifications can be made after download, such as site retention settings and other storage options.

https://docs.splunk.com/Documentation/ES/6.6.0/Install/DeploymentPlanning

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallTechnologyAdd-ons

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallTechnologyAddons#Create_the_Splunk_TA_ForIndexers_and_manage_deployment_manually

5.2 Examine the deployment checklist

High level deployment overview:

1. Install Splunk ES on your search head or search head cluster
2. Determine which add-ons to install on forwarders
3. Deploy add-ons to forwarders
4. Deploy add-ons to indexers

No official checklist was observed when researching this topic. However, the YouTube source below specifies this deployment checklist, with sizing, scoping and scaling prior to ES download & installation:

1. Determine size and scope of installation

2. Configure additional servers if needed
3. Obtain ES software
4. Determine software installation requirements for SHs, indexers & forwarders
5. Install all ES apps on SH(s)
6. Deploy indexer configurations

A number of procedural steps are also available in the Installation and Upgrade Manual.

https://www.youtube.com/watch?v=pOOJNyAUN7s

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallTechnologyAdd-ons

5.3 Understand indexing strategy for ES

In a **single instance** deployment, ES creates the indexes in the default data storage path. This defaults to the $SPLUNK_DB path of $SPLUNK_HOME/var/lib/splunk.

In a **Splunk Cloud Platform (SCP)** deployment, customers work with Splunk Support to set up, manage and maintain cloud index parameters

In a **distributed** deployment, create indexes on all Splunk platform indexers or search peers

Splunk ES does not provide configuration settings for the following, so these must be addressed separately:

- Multiple storage paths
- Accelerated data models
- Data retention
- Bucket sizing
- Use of volume parameters

https://docs.splunk.com/Documentation/ES/6.6.0/Install/Indexes

5.4 Understand ES Data Models

Data models use scheduled summarization searches initiated on the search head and performed on the indexers. This searches only newly indexed data while using the data model as a filter. I.e. **summariesonly** = ***true***. Resulting matches are saved to disk alongside the index bucket for quick access. Splunk ES leverages data model acceleration to populate dashboards and views, and to provide correlation search results. Data models are defined and provided in the ***Common Information Model*** (CIM) add-on (**Splunk_SA_CIM**), which is included with Splunk ES.

CIM can constrain indexes searched by data models to improve performance, and adjust data model acceleration settings including ***backfill time***, ***max concurrent searches***, ***manual rebuilds***, and ***scheduling priority***.

In addition to leveraging the data models included with the CIM, Enterprise Security implements and uses the following custom data models:

- **Assets and Identities** (All_Assets, All_Identities, Expired_Identity_Activity)

    - ◦ Data generated by the ES ***Asset and Identities* framework**
- **Domain Analysis** (All_Domains)
    - ◦ Data generated by the WHOIS modular input
- **Incident Management** (Notable_Events_Meta, Notable_Events, Suppressed_Notable_Events, Incident_Review, Correlation_Search_Lookups.*, Notable_Event_Supressions.*)
    - ◦ Data generated by the ES ***notable event* framework**
- **Risk Analysis** (All_Risk)
    - ◦ Data generated by the ES ***risk* framework**
- **Threat Intelligence** (Threat_Activity)
    - ◦ Data generated by the ES ***threat intelligence* framework**
- **User and Entity Behavior Analytics** or **UEBA** (All_UEBA_Events, All_UEBA_Events.*)
    - ◦ Data communicated by Splunk UBA for use in ES, when the **SA-UEBA** add-on is enabled

Each data model uses a different retention period, such as 1 year for domain analysis, 0 for Incident Management, and All
Time for Threat Intelligence. A REST API can be used to query values for all available data models such as Web, Endpoint, Network Traffic and Authentication. Use the CIM Setup page in the Splunk CIM app to modify these retention settings. **Data model acceleration** settings can be viewed from **Settings → Data Models**, or from the link below.

https://docs.splunk.com/Documentation/ES/6.6.0/Install/Datamodels

https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/datamodelsusedbyes/

6.0 Installation and Configuration (15%)

6.1 Prepare a Splunk environment for installation

General considerations:

- Review the Splunk platform requirements for Splunk ES
    - ◦ 64-bit CPU, 32GB RAM, 16 CPU cores
- If a deployment server manages any of the apps or add-ons included with Splunk ES, **remove** the ***deploymentclient.conf*** file that contains references to the deployment server and restart Splunk services, or the installation will not complete
- Your user account must have the ***admin* role** and the ***edit_local_apps* capability**. The admin role is assigned this capability by default
- Ensure there is at least 1GB of free space in the /**tmp** directory for installation or upgrade to complete Perform the following **before you start an upgrade**:

1. Review compatible versions of the Splunk platform
2. Review hardware requirements
3. Review known issues with the latest ES release
4. Review deprecated features in the latest ES release
5. Back up the search head, including the KV store
6. Ensure at least 1GB of free space is available in the /tmp directory for the upgrade

Upgrade recommendations include:

1. Upgrade the Splunk platform and ES in the same maintenance window
2. Upgrade Splunk ES to a compatible version
3. Upgrade Splunk platform instances
4. Upgrade Splunk ES
5. Review, upgrade and deploy add-ons
6. See the post-installation version-specific upgrade notes

There are additional prerequisites for installing ES in a **Search Head Cluster (SHC)** environment. ES supports installation on Linux-based SHCs only. You should also verify that you have:

- One deployer
- The same version of Splunk Enterprise on the deployer and SHC cluster nodes
- The same app versions of any other apps on the deployer and SHC nodes
- A backup of **etc/shcluster/apps** on the deployer
- A backup of **etc/apps** from one of the SHC nodes
- A backup of the KV store from one of the SHC nodes
- Global or "/system/local" server.conf shclustering configuration

```
[server] export = system
```

https://docs.splunk.com/Documentation/ES/6.6.0/Install/Beforeupgrading

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallEnterpriseSecurity

https://docs.splunk.com/Documentation/ES/6.6.0/RN/Enhancements

6.2 Download and install ES on a search head

Step 1. Download Splunk Enterprise Security

1. Log in to splunk.com with your Splunk.com user name and password.
2. Download the latest Splunk Enterprise Security product. You must be a licensed Enterprise Security customer to download the product.
3. Click Download and save the Splunk Enterprise Security product file to your desktop.

        1. At the time of writing, you may instead be prompted to “Contact Sales”

4. Log in to the search head as an administrator.

Step 2. Install Splunk Enterprise Security

The installer dynamically detects if you're installing in a single search head environment or search head cluster environment. The installer is also bigger than the default upload limit for Splunk Web. 1. Increase the Splunk Web upload limit to 1 GB by creating a file called

$SPLUNK_HOME/etc/system/local/web.conf with the following stanza.

```
[settings]
max_upload
_size =
1024
```

2. Click Settings → Server controls → Restart Splunk.
3. Click Apps → Manage Apps → Install App from File.
4. Click Choose File and select the Splunk Enterprise Security product file.
5. Click Upload to begin the installation.
6. Click Set up now to start setting up Splunk Enterprise Security

When installing in a Search Head Cluster environment, ensure you have met the prerequisites described in the section above, and follow these steps:

1. Prepare the deployer per the **prerequisites**.
2. Install Enterprise Security on the **deployer**.
    1. Increase the Splunk Web upload limit, for example to 1GB, by creating a file called $SPLUNK_HOME/etc/system/local/web.conf with the following stanza.

       ```
       [settings]
       max_upload
       _size =
       1024
       ```

    2. On the Splunk toolbar, select Apps > Manage Apps and click Install App from File.
    3. Click Choose File and select the Splunk Enterprise Security product file.
    4. Click Upload to begin the installation.
    5. Click Continue to app setup page

       Note the message that ES is being installed on the **deployer** of a SHC environment and that Technology Addons (TAs) will **not** be installed as part of the **post-install** configuration.
3. Click **Start Configuration Process**.
4. If you are not using Secure Sockets Layer (SSL) in your environment, do one of the following steps when you see the SSL Warning message:

   1. (**Recommended**) Click **Enable SSL** to turn on SSL and start using https:// for encrypted data transfer.

      (Side note: free certificate services are accessible through organisations like LetsEncrypt)

   2. (**Not Advised**) Click **Do Not Enable SSL** to keep SSL turned off and continue using http:// for data transfer.

5. Wait for the process to complete.
6. Move SplunkEnterpriseSecuritySuite from $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/apps

   If you use the **btool** command line tool to verify settings, use it only **after** you move the SplunkEnterpriseSecuritySuite from ***etc/apps*** to ***etc/shcluster/appssearches*** directory. If SplunkEnterpriseSecuritySuite remains in the ***etc/apps*** directory. btool checks may cause errors because add-ons like **SA-Utils** that contain .spec files are not installed on the deployer.

   The DA-ESS and SA apps are automatically extracted and deployed throughout the search head cluster.

7. Use the deployer to deploy Enterprise Security to the cluster members. From the deployer, run this command:

```
splunk apply shcluster-bundle --answer-yes -target
<URI>:<management_port> -auth <username>:<password>
```

Perform the following for standard command line installation of Splunk ES

1. Download Splunk ES and place it on the search head.
2. Start the installation process on the search head. Install with the **./splunk install app <*filename*>** command or

   perform a REST call to start the installation from the server command line. E.g.

   curl -k -u admin:password https://localhost:8089/services/apps/local -d filename="true" -d name="<file name and directory>" -d update="true" -v

   DO NOT use **./splunk install app** when **upgrading** the Splunk Enterprise Security app.

You can upgrade Splunk ES on the CLI using the same process as other Splunk apps or add-ons. After the app is installed, run the **essinstall** command with the appropriate flags as shown in the next step. 3. On the search head, use the Splunk software command line to run the following command:

splunk search '| essinstall' -auth admin:password You can also run this search command from Splunk Web:

```
| essinstall
```

When installing from the command line, **ssl_enablement** defaults to "***strict***." If you don't have SSL enabled, the installer will exit with an error. As a workaround or for testing purposes, you can set **ssl_enablement** to "***auto***".

If you run the search command to install Enterprise Security in Splunk Web, you can review the progress of the installation as search results. If you run the search command from the command line, you can review the **installation log** in: **$SPLUNK_HOME/var/log/splunk/essinstaller2.log.**

Perform the following for command line installation of Splunk ES on a SHC:

1. Download ES as above and place it on the deployer.
2. Install with the **./splunk install app** <filename> command or perform a REST call to start the installation from the server command line. For example: **curl -k -u admin:password https://localhost:8089/services/apps/local -d filename="true" -d name="<file name and directory>" -d update="true" -v** 3. On the deployer, use the Splunk software command line to run the following command:

   ```
   splunk search '| essinstall --deployment_type shc_deployer' -auth admin:password
   ```

4. Restart with **./splunk restart** only if SSL is changed from disabled to enabled or vice versa. 5. Use the deployer to deploy ES to the cluster members. From the deployer, run this command:

```
splunk apply shcluster-bundle
```

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallEnterpriseSecurity

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallEnterpriseSecuritySHC

6.2a Test a new install

For a standard ES installation, test installation and setup as follows:

1. Download Splunk Enterprise Security and place it on the search head.
2. Start the installation process on the search head. Install with the **./splunk install app <filename>** command or perform a REST call to start the installation from the server command line. E.g.

   ```
   curl -k -u admin:password https://localhost:8089/services/apps/local -d
   filename="true" -d name="<file name and directory>" -d update="true" -v
   ```

3. From **Splunk Web**, open the **Search and Reporting** app.
4. Type the following search to perform a dry run of the installation and setup.

   ```
   | essinstall --dry-run
   ```

For a SHC installation of ES, verify that ES is deployed to the cluster members:

1. From the GUI of a cluster member, check the Help → About menu to check the version number.
2. From the CLI of a cluster member, you can check the /etc/apps directory to verify the **Supporting Add-ons (SA)** and **Domain Add-ons (DA)** for Enterprise Security:

    1. DA-ESS-AccessProtection, DA-ESS-EndpointProtection, DA-ESS-IdentityManagement, DA-ESSNetworkProtection, DA-ESS-ThreatIntelligence,
    2. SA-AccessProtection, SA-AuditAndDataProtection, SA-EndpointProtection, SA-IdentityManagement, SA-NetworkProtection, SA-ThreatIntelligence, SA-UEBA, SA-Utils,
    3. Splunk_DA-ESS_PCICompliance, SplunkEnterpriseSecuritySuite, Splunk_SA_CIM, Splunk_ML_Toolkit, and Splunk_SA_Scientific_Python_linux_x86_64 (or Splunk_SA_Scientific_Python_windows_x86_64 for windows)

3. From the CLI of a cluster member, you can check the $SPLUNK_HOME/etc/apps/SplunkEnterpriseSecuritySuite/local/inputs.conf file to see that the data model accelerations settings are enabled.

Although **Technology Add-ons (TAs)** are bundled in the installer, they are not deployed as part of the installation process for a SHC. You must deploy them manually if you want to use them

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallEnterpriseSecurity#Step_3._Set_up_Splunk_Enterprise_Se curity

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallEnterpriseSecuritySHC

6.3 Understand ES Splunk user accounts and roles

ES adds three roles to the default roles provided by Splunk. These support access to specific functions based on a user’s access requirements. Three categories of **users** are defined as follows:

- **Security Director** (Splunk ES role - **ess_user**): Primarily reviews the **Security Posture**, **Protection Centers** and **Audit** dashboards
- **Security Analyst** (Splunk ES role - **ess_analyst**): Uses the **Security Posture** and **Incident Review** dashboards to manage and investigate security incidents. Analysts also review the **Protection Centers**, determine what constitutes a security incident, and define thresholds for correlation searches and dashboards. Analysts must be able to edit notable events
- **Solution Administrator** (Splunk ES role - **admin** or **sc_admin**): Installs and maintains the Splunk platform and Splunk Apps. Responsible for configuring ***workflows***, adding new ***data sources***, ***tuning***, and ***troubleshooting*** the application

Splunk ES roles inherit from other roles, while adding additional functionality:

- **ess_user** (inherits **user**): Replaces the user role for ES users. Permits real-time search, list search head clustering, edit splunk eventtypes in the **Threat Intelligence** TA, and manage notable event suppressions.
- **ess_analyst** (inherits **user**, **ess_user**, **power**): Replaces the power role for ES users. Adds the capabilities to create, edit and own notable events and perform all transitions, edit glass tables, and create and modify investigations.
- **ess_admin** (inherits **user**, **ess_user**, **power**, **ess_analyst**): Cannot be assigned directly to a user. You must use the Splunk platform **admin** or **sc_admin** roles. **ess_admin** inherits

ess_analyst and adds several other **capabilities** pertinent to performing ES administrative tasks.

The **admin** role inherits all unique ES **capabilities**, and **sc_admin** is the equivalent for **Splunk Cloud (SC)** environments. These roles are required to respectively administer an Enterprise Security installation.

The key takeaway here is that **ess_admin** is NOT assigned directly to users. If privileges beyond that of **ess_analyst** need to be assigned to an ES user, they can be assigned **admin** or **sc_admin**, or a custom role with the relevant capabilities.

These can be added via the ES menu bar under **Configure → General → Permissions**, finding the **role** and **ES Component** you want to add to it, selecting the check box for the component, then clicking **Save**.

Capabilities are beyond the scope of this discussion of users and roles, but you are encouraged to visit the link below to view details of capabilities and their corresponding functions.

For the exam, consider how users, roles and capabilities fit into the variety of resources available in Splunk Enterprise Security, and how these should best be configured for the most appropriate access. https://docs.splunk.com/Documentation/ES/6.6.0/Install/ConfigureUsersRoles

6.4 Post-install configuration tasks

The installation process effectively stops upon clicking **Set up now**, at which point the post-install configuration tasks begin. On the setup page, click **Start** and choose to either ***Enable SSL*** or ***Do Not Enable SSL***. The Post-Install Configuration page indicates the status as the setup progresses.

Choose to exclude selected add-ons from being installed, or install and disable them. When the setup is done, you will be prompted to **Restart Splunk** to finish the post-installation configuration. If you encounter problems during this process, ensure you followed the earlier instructions in regards to **deploymentclient.conf**, role capabilities, disk space, hardware requirements, and app installation instructions for search head clusters

If you enabled SSL as part of this process, you will need to update the Splunk Web URL to use https and if a custom port is configured, you will need to specify this as well.

When upgrading, following the upgrade of of Splunk ES and restart of Splunk Web, click **Continue to app setup page** to **Start** the ES setup. The **Splunk Enterprise Security Post-Install Configuration** page indicates the upgrade status as it moves through the stages of installation. When complete, you may be prompted to **Restart Splunk** if you opted to enable SSL before the setup.

If upgrading, review the version-specific upgrade notes for any additional required steps to complete.

Once all steps are completed, navigate to the ES menu bar, and click on **Audit → ES Configuration Health**. Review potential conflicts and changes to the default settings. If pages fail to load, you may need to clear the browser cache.

After installation or upgrade completes, review the installation log at **$SPLUNKHOME$/var/log/splunk/essinstaller2.log**.
https://docs.splunk.com/Documentation/ES/6.6.0/Install/Upgradetonewerversion#Step_4._Set_up_Splunk_Enterprise_Se curity

7.0 Validating Enterprise Security (ES) Data (10%)

7.1 Plan ES inputs

Splunk ES add-ons are designed to parse and categorise known data sources and other technologies for CIM compliance. For each data source:

1. **Identify the add-on**: Identify the technology and determine the corresponding add-on. The primary sources are the TAs provided with Enterprise Security and the CIM-compatible content available on Splunkbase. If the add-on you want to use is not already compatible with the CIM, modify it to support CIM data schemas. Refer to Splunk Docs for more details on this process.
2. **Install the add-on**: Install the add-on on the ES search head. Install add-ons that perform index-time processing on each indexer. The add-on might also be needed on a heavy forwarder, if present. Splunk Cloud Platform customers must work with Splunk Support to install add-ons on search heads and indexers, but are responsible for on-premises forwarders.
3. **Configure the server, device, or technology where necessary**: Enable logging or data collection for the device or application and/or configure the output for collection by a Splunk instance.
4. **Customise the add-on where necessary**: If required, customisation may include setting the location or source of the data, or other unique settings.
5. **Set up a Splunk data input and confirm the source type settings**: Review the TA's README file for information about the source type setting associated with the data, or customisation notes about configuring the input.

Data input considerations include:

- **Monitoring files**: Set the source type on the forwarder using an input configuration, or use a deployment server to centrally manage and standardise this configuration
- **Monitoring network ports**: Examples include a syslog server, or listener ports on a forwarder. Each network source should be sent on a distinct port.
- **Monitoring Windows data**: See the documentation below for available methods of collecting various source data including event logs, file system changes, AD, WMI, registry data, performance metrics, and host, print & network information
- **Monitoring network wire data**: Splunk Stream supports real-time capture of wire data
- **Scripted inputs**: Collects data from an API or other remote data interfaces and message queues using shell scripts, python scripts. Windows batch files, PowerShell or other utility that can format and stream desired data

New data inputs can be configured via the GUI using Settings → Data inputs → Add new → Save

Asset and Identity information provides data enrichment and additional context for analysis. This is described in a later section, but be aware that collection of asset and identity information is highly beneficial to risk based alerting as well as the analytical and investigative process. Ensure that appropriate add-ons are selected to configure appropriate data inputs in order to capture relevant data. https://docs.splunk.com/Documentation/ES/6.6.0/Install/Planyourdatainputs

https://docs.splunk.com/Documentation/CIM/4.20.0/User/UsetheCIMtonormalizedataatsearchtime

https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/HowtogetWindowsdataintoSplunk

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Addassetandidentitydata

7.2 Configure Technology Add-ons (TAs)

There are three main types of add-ons pertaining to Splunk Enterprise Security:

- **Supporting Add-ons (SAs)**: Provides normalisation through a variety of file types, including the schemas to map data sources into the CIM for data model analysis. SAs also host asset and identity information and correlation searches for alerts and events.
- **Domain Add-ons (DAs)**: Provides views into the security domain, such as search knowledge for investigation and data summarisation. Each domain includes summary dashboards of security metrics and drill down views for more information to help investigate and explore abnormal behaviour.
- **Technical Add-ons (TAs)**: Also simply referred to as “add-ons” - Collects and formats incoming data, and can also provide adaptive response actions. Abstracts data from specific technologies from the higher level configuration in Splunk ES. TAs also contain search-time knowledge mappings that assign fields and tags to the data used by the search layer

This topic only references configuration of TAs. Even though many of these TAs come packaged with Splunk ES, many of these add-ons are also available separately from Splunkbase, where you read an overview of the add-on as well as configuration instructions or links to additional documentation. Additional information may also be available in a
README file or directory within the add-on, or from .spec files, such as inputs.conf.spec, to specify which configuration items are available and what settings are valid for each item.

https://docs.splunk.com/Documentation/ES/6.6.0/Install/InstallTechnologyAdd-ons

https://dev.splunk.com/enterprise/docs/devtools/enterprisesecurity/abouttheessolution/

8.0 Custom Add-ons (5%)

8.1 Design a new add-on for custom data

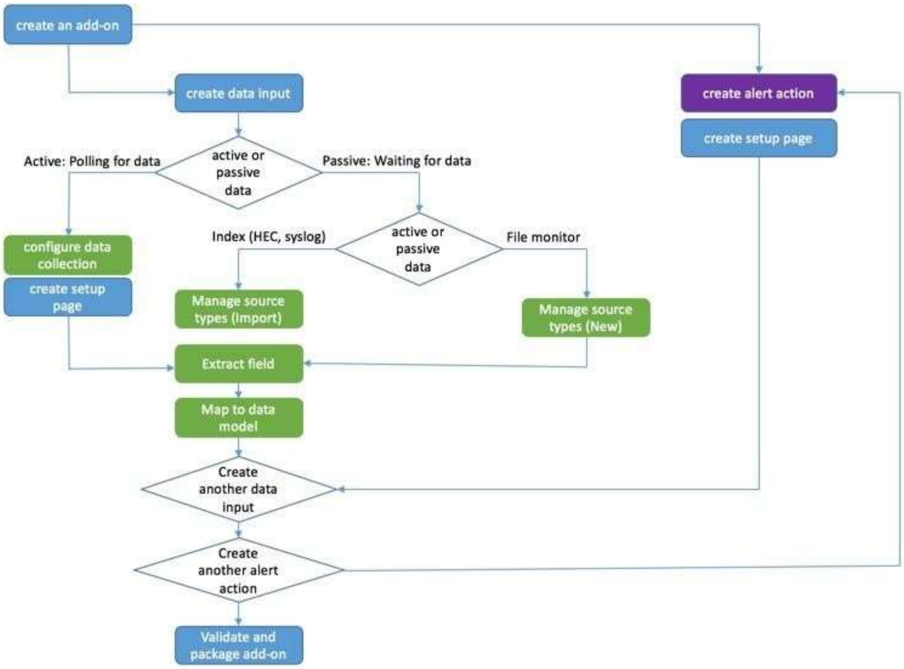
The **Add-on Builder** is a Splunk app that allows you to build new add-ons in a non production environment for deployment into a production environment. Follow the instructions on Splunkbase, ensuring that the version of the Addon Builder is supported by the installed version of Splunk Enterprise.

Once installed, consider the following before building the add-on:

- Be familiar with your data and understand the data that you want to extract from it.
- Determine the method you will use to gather your data. If you plan to use file monitors, network listeners, or the **HTTP Event Collector (HEC)**, you do not need to build a **modular input** and can skip the **input options** requirement.
- **Modular inputs** may query a third-party API or a data type that is not natively supported by Splunk. If you plan to create a modular input, have sample data and/or a test account for the system that the module will contact. Know the input options that are required to access your data. The Add-on Builder helps to generate **Python** code for the data input, or you can write your own Python code for the data input and input arguments. This code can then be **validated** by the Add-on Builder.
- Know which parts of the **Common Information Model (CIM)** to which you want to map data. For example, almost all data sources produce **Authentication** and **Change Analysis** events, but few produce **Intrusion Detection** events.

In addition to automatically extracted or customer fields from Splunk Enterprise, the Splunk Add-on Builder lets you add custom fields to support field mapping at index and/or search time. This data can then be normalised against the fields in any of the CIM's 22 predefined data models, or a custom data model of your choosing. This process starts by creating a project for a new add-on.

Different steps are taken depending on whether data is being passively collected, or if actively polling for data (E.g. REST API), as well as whether the data is already present. Optionally, additional data inputs or alert actions can be added prior to validating and packaging the add-on:



Source: https://docs.splunk.com/File:AOB2.2_overall_procedure1.jpg

Practice using this app with a variety of data to understand the process. Review this design process after following the instructions below for using the add-on builder to build a new add-on.

https://docs.splunk.com/Documentation/AddonBuilder/4.0.0/UserGuide/BeforeYouBegin

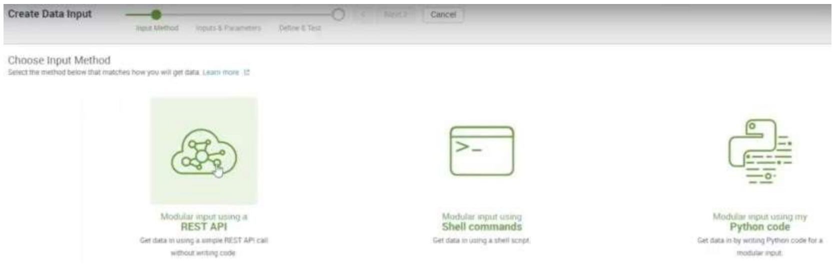
https://docs.splunk.com/Documentation/AddonBuilder/4.0.0/UserGuide/NameProject

8.2 Use the Add-on Builder to build a new add-on

Follow the above flowchart for building the new add-on, starting with the Create Add-on phase. Fill in the required fields including name, author, version and description, and click Create. The Add-on Folder Name will automatically be determined from the specified Add-on name.

Next, **Configure Data Collection** with a new input. In the first video below, a **REST API** is used as the source of the data input, and is **actively** being queried to pull the data down to Splunk. There is also an option to **Create Alert Actions**, which is not discussed in any detail here

Configure Data Collection
Click to add new data inputs.
Create Alert Actions
Click to create alert actions.



Choose Input Method

Select the method below that matches how you will get data. Learn more

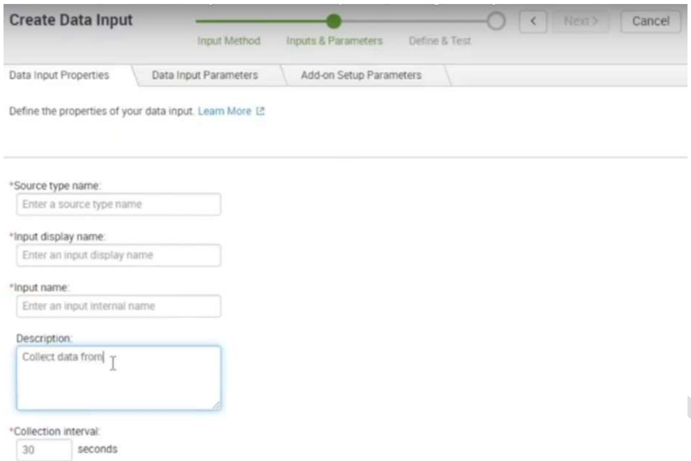
Modular input using a **REST API**
Get data in using a simple REST API call without writing code

Modular input using **Shell commands**
Get data in using a shell script.

Modular input using my **Python code**
Get data in by writing Python code for a modular input.

Other modular inputs include **shell commands** or **Python code**. Recall that this step is not required for **passive** data collection, e.g. where the data is available from a file monitor, for already indexed data, or for a manual file upload.

Active data sources require data input properties and parameters to be provided. Data input **properties** include the ***source type name***, ***input display name***, ***input name***, ***description*** and ***collection interval***.



Create Data Input

Input Method — Inputs & Parameters — Define & Test

< Next > Cancel

Data Input Properties | Data Input Parameters | Add-on Setup Parameters

Define the properties of your data input. Learn More

*Source type name: Enter a source type name

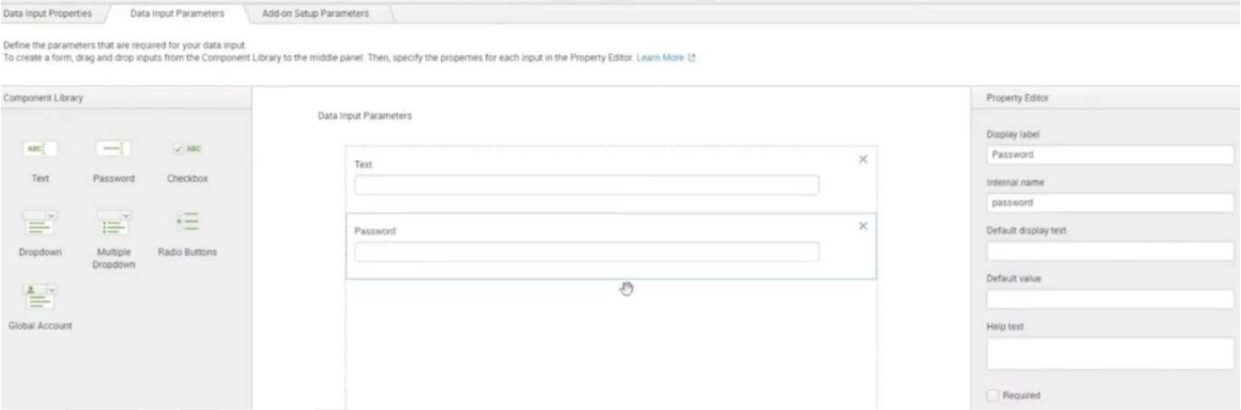
*Input display name: Enter an input display name

*Input name: Enter an input internal name

Description: Collect data from

*Collection interval: 30 seconds

Data input **parameter types** include ***text***, ***password***, ***checkbox***, ***radio button***, ***dropdown***, ***multiple dropdown*** or ***global account***. Drag and drop the relevant fields, specifying labels, help text or default text and values as appropriate.



Data Input Properties | Data Input Parameters | Add-on Setup Parameters

Define the parameters that are required for your data input.
To create a form, drag and drop inputs from the Component Library to the middle panel. Then, specify the properties for each input in the Property Editor. Learn More

Display label: Password

Internal name: password

Default display text:

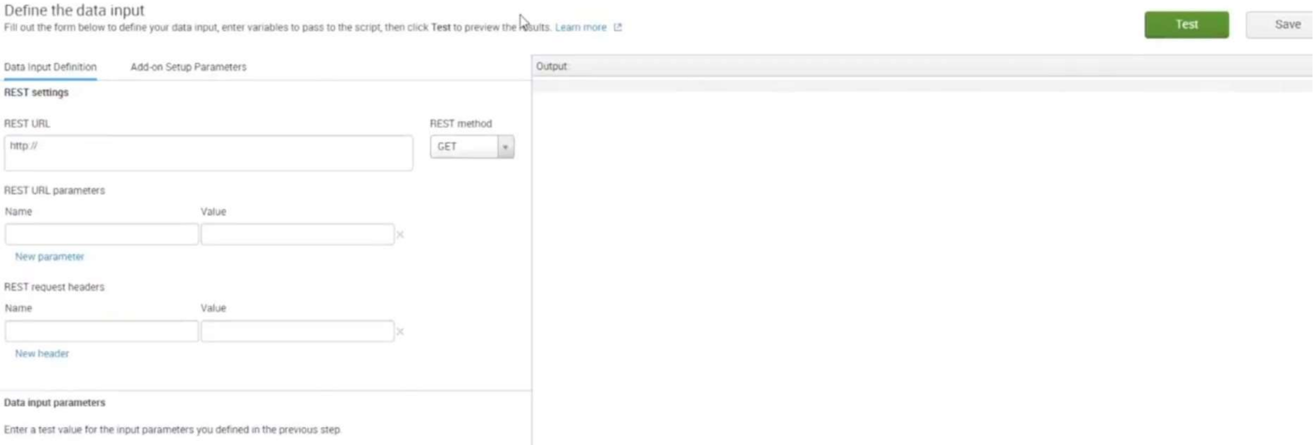
Default value:

Help text:

□ Required

Once **Data Input Properties** and **Data Input Parameters** are configured, proceed to **Add-on Setup Parameters**. This may include **proxy settings** or **global account settings**.

Next, **define** the data input and **test** settings to ensure expected data is received without error. REST inputs will use a REST ***URL***, URL ***parameters*** and ***request headers***, as well as the data input parameters that you specified earlier.



Define the data input

Fill out the form below to define your data input, enter variables to pass to the script, then click **Test** to preview the results. Learn more

REST settings

REST URL: http://

REST method: GET

REST URL parameters

Name	Value

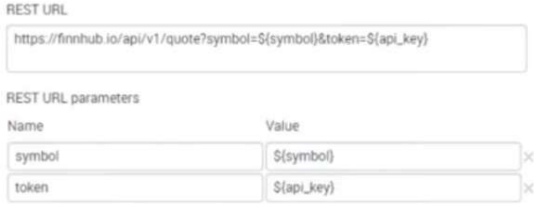
REST request headers

Name	Value

Data input parameters

Enter a test value for the input parameters you defined in the previous step

The form values for the parameters are captured using ${field_name} and specified the same way in the REST URL:

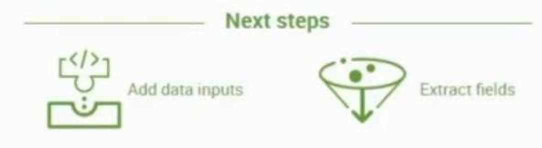


REST URL: https://finnhub.io/api/v1/quote?symbol=${symbol}&token=${api_key}

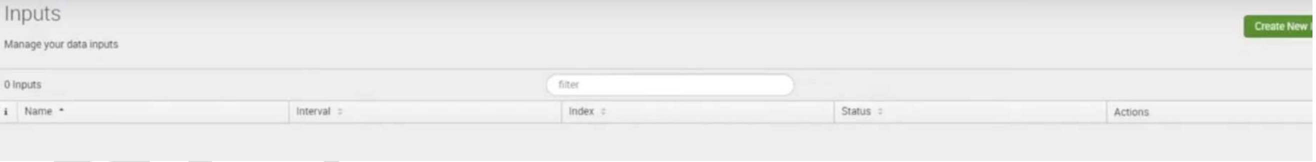
REST URL parameters

Name	Value
symbol	${symbol}
token	${api_key}

Test the configuration settings, troubleshooting as required, and **Save** when ready. You will be advised when the process is Done with the option to add additional data inputs or field extractions:



At this point, the add-on is created on the local system with the name you specified, and the setup page can be validated. Open the newly created add-on, and click on **Add New Input**.



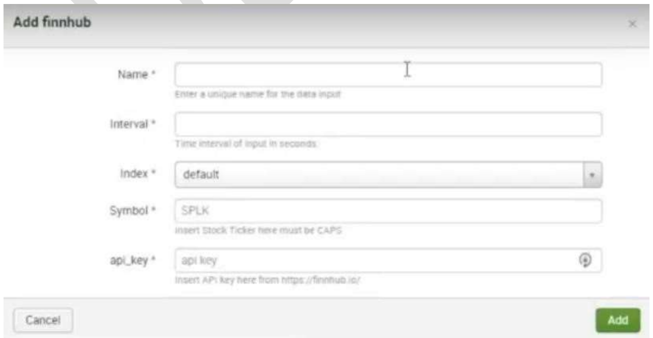
Inputs

Manage your data inputs

0 Inputs

i	Name	Interval	Index	Status	Actions

Specify a relevant index with the rest of the configuration, and click **Add** when ready.



Add finnhub

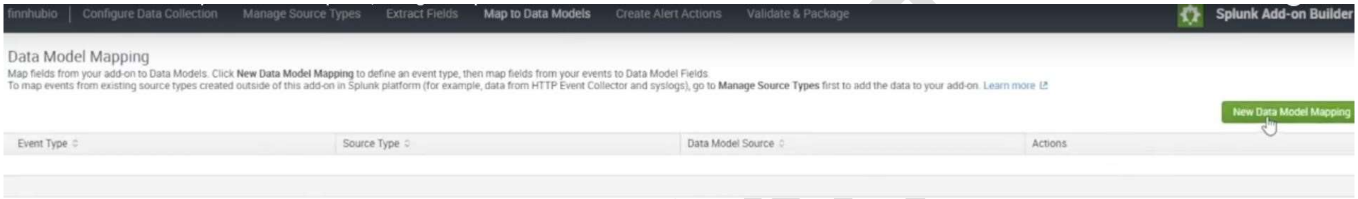
Name *	 Enter a unique name for the data input
Interval *	 Time interval of input in seconds
Index *	default
Symbol *	SPLK Insert Stock Ticker here must be CAPS
api_key *	api key Insert API key here from https://finnhub.io/

Though not listed in the flow diagram above for the polling of active data, **Manage Source Types** ensures appropriate event and line breaking, as well as timestamp extraction. This should be a familiar process based on content covered in Splunk Administration or earlier courses.

Review the data and the current extracted fields. There will likely be fields that aren't intuitive, or don't align with the field names used in CIM data models, so **field aliases** are required to provide this **mapping**. Start by returning to the Addon Builder to open the newly created add-on, and click on **Extract Fields** in the menu bar.

Review the **source types** and the **Parsed Format**. If this shows as **Unparsed Data**, click on **Assisted Extractions** to update this to the relevant type such as **Key Value**, **JSON**, **Table** or **XML** data, and click **Save**. If the data is unstructured, no further changes are required here.

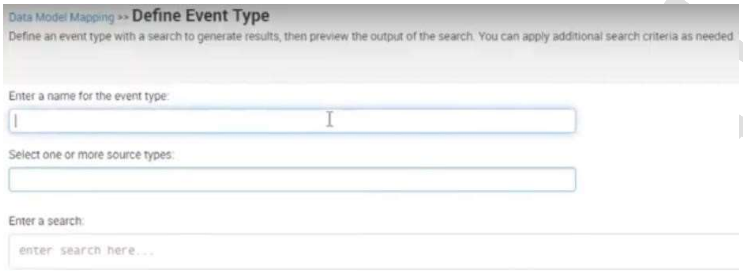
Click on **Map to Data Models** in the menu bar. **Create a New Data Model Mapping**, and you will be prompted to enter a name of the **event type**, select one or more **source types**, and enter a **search**. Upon selecting the source type, the search will automatically populate to reference your selection. Click **Save**.



Data Model Mapping

Map fields from your add-on to Data Models. Click **New Data Model Mapping** to define an event type, then map fields from your events to Data Model Fields.
To map events from existing source types created outside of this add-on in Splunk platform (for example, data from HTTP Event Collector and syslogs), go to **Manage Source Types** first to add the data to your add-on. Learn more

Event Type	Source Type	Data Model Source	Actions



Data Model Mapping >> Define Event Type

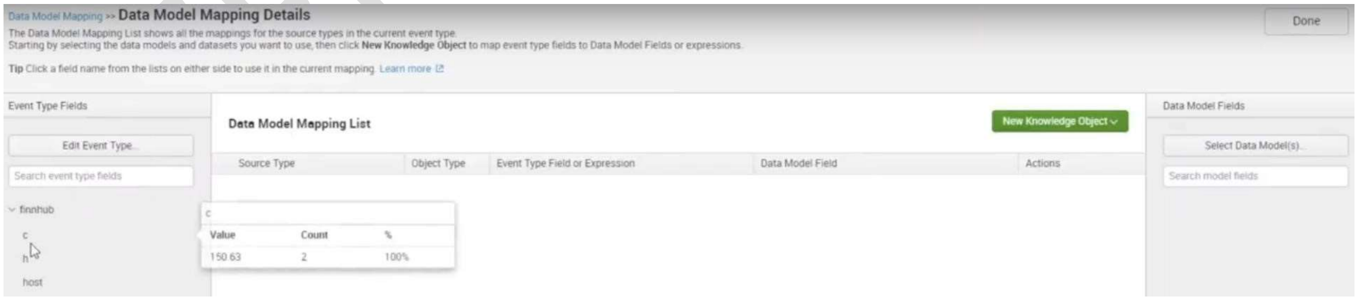
Define an event type with a search to generate results, then preview the output of the search. You can apply additional search criteria as needed.

Enter a name for the event type:

Select one or more source types:

Enter a search:

The next screen will provide **event type** fields on the **left**, and **data model** fields on the **right**. In the middle section, click on **New Knowledge Object** and choose **FIELDALIAS**. Click on the event type field from the left hand side to populate the field in the middle. If a data model is selected, the data model field can be selected. Otherwise, simply type the name of the desired **Data Model Field** and click **OK**. When all the required mappings are entered, click on **Done** to return to the Data Model Mapping page.



Data Model Mapping >> Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type.
Starting by selecting the data models and datasets you want to use, then click **New Knowledge Object** to map event type fields to Data Model Fields or expressions.

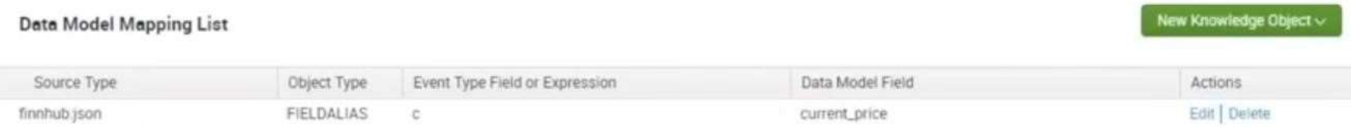
Tip Click a field name from the lists on either side to use it in the current mapping. Learn more

Data Model Mapping List

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions

c

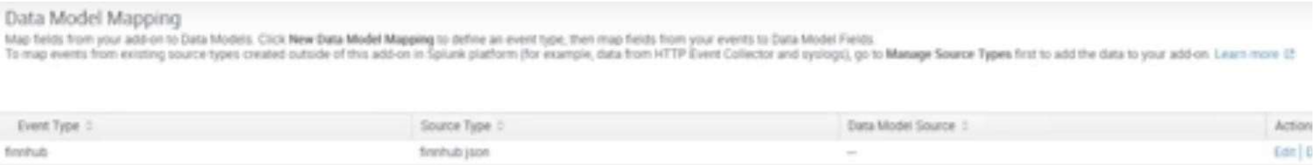
Value	Count	%
150 63	2	100%



Data Model Mapping List

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions
finnhub json	FIELDALIAS	c	current_price	Edit | Delete

Note that if a data model was not selected, the **Data Model Source** will display as a dash, but the field aliases are present. Searching on the index will now display both the original field names and the corresponding field aliases.



Data Model Mapping

Map fields from your add-on to Data Models. Click **New Data Model Mapping** to define an event type, then map fields from your events to Data Model Fields.
To map events from existing source types created outside of this add-on in Splunk platform (for example, data from HTTP Event Collector and syslogs), go to **Manage Source Types** first to add the data to your add-on. Learn more

Event Type	Source Type	Data Model Source	Action
finnhub	finnhub json	—	Edit |

Finally, click on **Validate & Package** and click on **Validate**. If prompted, click on **Update Settings** to provide your credentials to connect to the App Certification service on Splunk.com. **Test** the credentials and **Save** when ready.

Once this has been configured, click on **Validate** to produce an **Overall Health Report**. If the package looks good and has no errors, click on **Download Package** to download the SPL file, which can be renamed to a .zip extension for manual examination of the add-on configuration files.

The second YouTube video below shows a passive collection approach using test data and an existing CIM model for Network Traffic. I encourage you to watch both videos and gain hands-on experience in progressing through the stages of creating an add-on using either passive or active data sources. As a challenge, try following the process for creating a new source type using custom data of your choosing, and for bonus points, try creating your own datamodel and datasets.

Though there are numerous steps above, the overall process is reasonably straightforward once you've got some hands-on experience. Though this topic has a low weighting, it's possible that you one question may reflect the entire 5%, so following along with the videos and practicing with the free add-on builder will be far easier than attempting to memorise the above. https://docs.splunk.com/Documentation/AddonBuilder/4.0.0/UserGuide/UseTheApp

https://www.youtube.com/watch?v=-pzyvQMLmf0

https://www.youtube.com/watch?v=cJw3IAgbBV0

9.0 Tuning Correlation Searches (10%)

9.1 Configure correlation search scheduling and sensitivity

Correlation searches underpin the generation of notable events for alerting on potential security incidents. They are managed from the ES menu under **Content Management**. From here, locate the correlation search you want to change, and in the **Actions** column, you have the option to change between **real-time** and **scheduled** searches.

Use a **real-time** scheduled search to prioritise **current** data and **performance**. These are **skipped** if the search cannot be run at the scheduled time. Real-time schedule searches **do not backfill** gaps in data that occur if the search is skipped. Use a **continuous** schedule to prioritise data **completion**, as these are never skipped.

Optionally modify the **cron** schedule to control the search frequency. Higher frequency facilitates faster response, but if related data is expected over an extended period, reduced frequency may be more appropriate. If you are not familiar with cron schedules, take a look at https://crontab.guru for more information.

Optionally specify a **schedule window** for the search. A value of **0** means that a schedule window will not be used, while **auto** allows the scheduler to automatically set a schedule window. Manual configuration can also be defined in **minutes**. If multiple scheduled reports run at the same time, a schedule window allows this search to be deferred in favour of higher-priority searches. Optionally specify a schedule **priority** such as **High** or **Highest** to ensure it runs at the earliest available instance for the scheduled time.

If manually converting a real time search to a scheduled search, review the time range, which defaults as -5m@m to
+5m@m, and consider updating use of | **datamodel** from real-time searches to | **tstats** for efficiency. If you use **Guided Mode** to convert the search, it can automatically switch from **datamodel** to **tstats** for you. You will either have the option to edit a Guided Mode search or manually edit the search, but not both. Choosing to **Edit search in guided mode** will replace the existing search with a new search.

In regards to sensitivity, correlation searches typically have trigger conditions for adaptive response actions, such as the generation of notable events. From the ES menu bar, click **Configure → Content → Content Management** and select the title of the correlation search you want to edit.

Type a **Window duration**. Unlike the **schedule window** duration above, which is the time allowed for the search to run, a **Window duration** is the period of time for which no future alerts will be generated by the matching events. Be careful not to confuse these two terms. The **Fields to group by** specifies which fields to use when matching similar events. If the fields listed here match a generated alert, the correlation search will not create a new alert. Multiple fields can be defined based on the fields returned by the correlation search.

E.g. A window duration of 30m with grouping fields of ***src*** and ***dest*** means that events with the same ***src*** AND the same ***dest*** will not generate additional alerts during the 30m period, but events with the same ***src*** and different ***dest***, or the same ***dest*** and different ***source*** WILL generate new alerts for this period. Be careful not to filter out unique actions that should be investigated. Window duration is appropriate when the additional events represent **duplicate** alerts or would result in doubling up on investigate efforts from analysts.
https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Configurecorrelationsearches

9.2 Tune Enterprise Security (ES) correlation searches

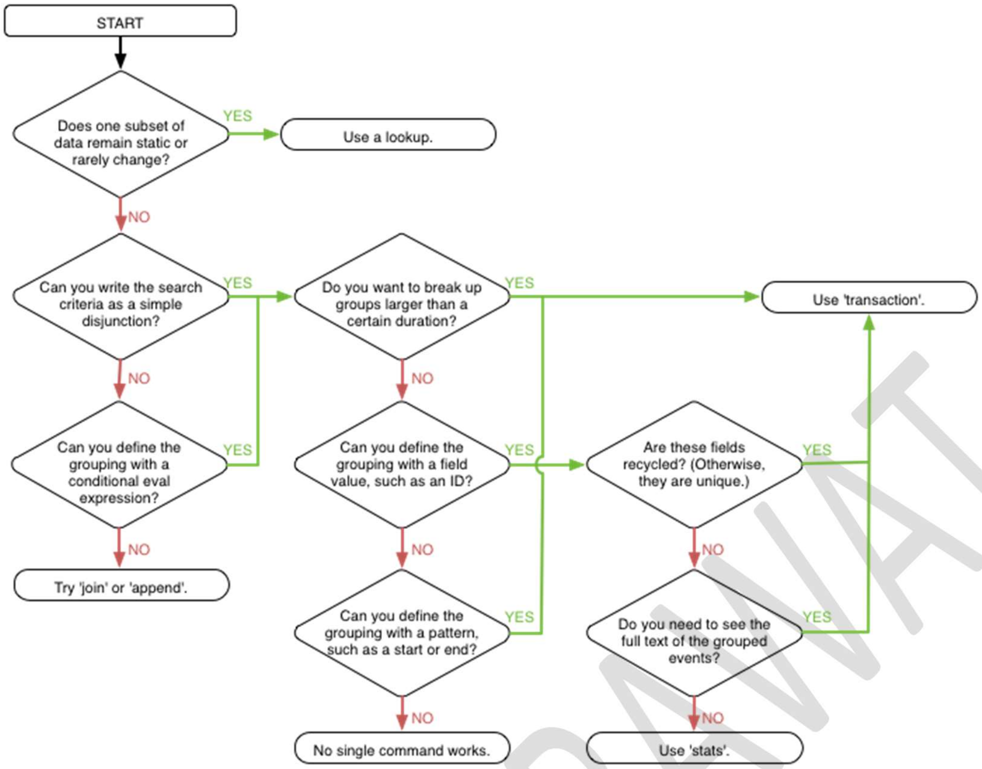
There are some instances where you want to continue detecting on events, but make an exception for a period of time to prevent these alerts from appearing on the **Incident Review** dashboard. **Notable event suppressions** provides this function to users with the ***ess_user*** role by default. Suppressed notable events continue to contribute to the notable event counts on the **Security Posture** and **Auditing** dashboards, but will not display on the **Incident Review** dashboard. When suppression ends, notable events will become visible on the Incident Review dashboard again. Suppressions are appropriate for incidents that need to be handled at a later date.

To create a suppression, click **Configure → Incident Management → Notable Event Suppressions → Create New Suppression** and enter a ***Name*** and ***Description*** for the suppression filter. Enter a ***Search*** used to find notable events to be suppressed. Set the ***Expiration Time*** as a time limit for the suppression filter.

NB: The expiration time applies to the **filter**, and not the period for which the notable events are detected. When the expiration time is reached, the filter is lifted and previously filtered events will be seen in the **Incident Review** history for the time that the notable would have originally been visible.

Though possible to set a suppression without an expiry, it could be forgotten. It may also suggest that the correlation search requires tuning to remove unwanted noise or false positives. Suppression is used for events on which you cannot currently act and do not want to appear in dashboards at this time. Notable event suppressions can be audited in the **Suppression Audit** dashboard.

Scheduling and sensitivity relate to quantity, whereas tuning relates to quality. Suppression may be used while tuning takes place, and correlation searches can be tuned through the appropriate use of **lookups**, disjunctions (**AND**, **OR**, **NOT**), **transaction** (grouping by duration or field), and use of aggregate commands like **stats**.


START
Does one subset of data remain static or rarely change?
YES
Use a lookup.
NO
Can you write the search criteria as a simple disjunction?
YES
NO
Can you define the grouping with a conditional eval expression?
YES
NO
Try 'join' or 'append'.
Do you want to break up groups larger than a certain duration?
YES
NO
Use 'transaction'.
Can you define the grouping with a field value, such as an ID?
YES
NO
Can you define the grouping with a pattern, such as a start or end?
YES
NO
No single command works.
Are these fields recycled? (Otherwise, they are unique.)
YES
NO
Do you need to see the full text of the grouped events?
YES
NO
Use 'stats'.

https://docs.splunk.com/File:Search_event_grouping_flowchart.png

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Configurecorrelationsearches

https://docs.splunk.com/Documentation/Splunk/latest/Search/Abouteventcorrelation

https://docs.splunk.com/Documentation/ES/3.0.1/Install/NotableEventSuppression

10.0 Creating Correlation Searches (10%)

10.1 Create a custom correlation search

Custom correlation searches can be broken down into 5 parts:

- Plan the use case for the correlation search
- Create the correlation search
- Schedule the correlation search
- Choose available adaptive response actions for the correlation search

Correlation searches identify data patterns that can indicate a security risk, which might include high-risk users, malwareinfected machines, vulnerability scanning, access control, or evidence of compromised accounts.

Start by defining a use case, being explicit with what you want to detect using the search. What data are you searching, what are you searching for, what thresholds apply to the search, and how will this data be presented? E.g. search authentication sources for unsuccessful login attempts, where 10 attempts are made within a rolling 60 minute interval and present as a timechart.

Once the use case is defined, determine where the relevant data can be found. In this case, the ***Authentication*** data model is a good candidate, but there may be authentication sources that are not CIM compliant or have not yet been mapped to this data model. Take this opportunity to create the relevant CIM mappings so additional authentication searches can reference a single datamodel source rather than multiple indexes and sourcetypes.

Next, create the search by navigating from the ES toolbar to **Configure → Content → Content Management**. Choose **Create New Content → Correlation Search** and enter a **search name** and **description**. Select an appropriate **app**, such as ***SA-AccessProtection*** for excessive failed logins. Set the **UI Dispatch Context** to ***None***. If an app is selected, it will be used by links in email and other adaptive response actions.

Correlation searches can then be created in **Guided mode**. From the correlation search, select ***Mode → Guided*** and ***Continue*** to open the guided search editor. Select the appropriate data source, such as a **Data Model** or **Lookup File**. If these aren't feasible options, a ***manual*** search may be necessary.

For the example above, set the **Data source** to ***Data Model***, and select the ***Authentication*** **Data Model** and

Failed_Authentication **Dataset**. Set **Summaries only** to ***Yes*** to only search accelerated data. Set **Time Range** to last 60 minutes, **Preview** the search, then click **Next**.

You can also filter the data to exclude specific field values, such as ***where 'Authentication.dest' != "127.0.0.1"***. In this example, leave the filter condition blank and click Next.

The remaining two steps are to **aggregate** and **analyse** your data. Aggregations typically involve **count**, but may also include **values**. In this example, click **Add a new aggregate**, select the **Function** of ***values***, and the **Field** of ***Authentication.tag***. Type ***tag*** in the **Alias** field.

Add additional aggregates for **dc**(Authentication.user) as ***user_count***, **dc**(Authentication.dest) as ***dest_count***, and the **count** Function, with no attributes or alias field defined, for the overall count.

In the next section, **split** the aggregates by application (***Authentication.app***) and source (***Authentication.src***), aliasing as ***app*** and ***src*** respectively, then click Next to define the correlation search match criteria.

To recap, we have aggregated tag values, with a count of users, destinations and events, and these aggregated events are being split by the application and source values. E.g.

tags	**user_count**	**dest_count**	**count**	**app**	**src**
-	1	1	1	AppA	1.1.1.1
-	2	2	4	AppB	1.1.1.1
-	3	3	10	AppB	2.2.2.2
-	1	5	10	AppC	2.2.2.2

To alert on a specific user with 10 or more failed logins from the same source and target application:

From the **Analyze** page, select a **Field** of ***count***, and a **Comparator** of ***Greater than or equal to***, with a **Value** of ***10***, then click **Next**.

In reality, it's unlikely that a single ***src*** would have a ***user_count*** greater than one for a given one-hour interval. However, it appears that this alert could trigger if multiple users failed authentication 10 or more times from the same source IP.

One possible resolution would be to split by the **user** field as well.

Open a new tab in the browser, navigate to Splunk search, and run the final correlation search string to validate the expected results:

- If the search does not parse correctly, but parsed during filtering, return to the correlation search guided editor aggregates and split-bys to identify errors.
- If the search parses but does not produce expected events, adjust elements of the search as needed Once validated in the new search tab, return to the guided search editor and click **Done**.

Configure scheduling using a real-time or continuous schedule. For a fast response for failed logins, choose a real-time scheduled search with a Cron Schedule of */5 * * * * (every 5 minutes). Optionally set a **schedule window** or **schedule priority**, with the priority overriding the schedule window setting. In this case, leave the **Schedule Priority** as ***Default***. Recall that the **schedule window** is different from the **window duration**.

Configure the **Window Duration** to ***1 day***, grouping by ***app*** and ***src*** fields. This should match the split-by aggregate fields. Future triggers will not alert again within 24 hours for the same ***app*** and ***src*** values.

Sequence Correlation Searches are groupings of correlation searches based on **Sequence Templates** and performed by the **Event Sequencing Engine**. Sequence templates are recorded in the sequence_templates.conf file. Once created, a sequence template is available for execution within 5 minutes.

Sequence Templates allow correlation searches to be grouped into batches of events by a specific sequence, by specific attributes, or both. A **Workflow** runs the correlation searches in an order of your choice, similar to a script, allowing automation of actions that would otherwise be performed manually.

The **Workflow** consists of a **Start** section that matches on a correlation search or an expression. This is followed by **Transitions**, which define the sequence. **Transitions** each have their own match conditions, and are matched chronologically by default, but may be customised in an order-independent way. The workflow finishes on an **End** section, which defines the termination criteria for the sequence template. This occurs when:

- "All transitions are complete and the event satisfying match condition is found. The event sequencing engine will consider this outcome as a successful run of a template and will trigger the sequenced event creation"
- "The template has reached the configured max time to live (**max_ttl**). As the template has not reached its end state in the desired time, the event sequencing engine will discard this run and no sequenced event will be created"

IMPORTANT: Before Sequence Templates can be used, open the Splunk ES Menu Bar and click on **Configure→ General → General Settings**, then click **Enable** for the **Event Sequencing Engine**.

To create a Sequence Template:

- From the Splunk ES menu bar, select **Configure** → **Content** → **Content Management** → **Create New Content** → **Sequence Template**
- Enter a ***Name*** and ***Description*** for the template, and an ***App context*** for the search
- In the **Start** section add the ***Correlation Search***, ***Expression*** to match on, and any ***States*** to store for use in a later correlation search. ***Field*** specifies the existing field name, while ***Label*** specifies how that field will be referenced by future correlation searches
- In the **Transition** section:

  ◦ Choose whether to ***Enforce Ordering***

  ◦ Enter a ***Title***

  ◦ Select the ***Correlation Search*** to run next

  ◦ Type the ***Expression*** to match on
- In the **End** section, select the ***Correlation Search*** to end with, the ***Expression*** to match on, and the ***Time Limit*** for when the search should expire
- In the **Actions** section, type the ***Event Title***, ***Description***, ***Urgency*** and ***Security Domain*** for Incident Review and click **Save**

Other than tuning the correlation searches themselves, a Sequence Template may need to be adjusted to ensure that correlation search results are being captured in the correct order, which requires the **enforce order** check box to be checked.

If left unchecked, transitions can be matched in any order, but once matched, corresponding transitions will be considered complete. Matches can also utilise **Wildcards**, allowing for the sequence to fork, and **Aggregates**, which will add any notable events or risk modifiers to provide additional context to the final sequenced event.
https://docs.splunk.com/Documentation/ES/6.6.0/Tutorials/CorrelationSearch
https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Sequencecorrelationsearches

10.2 Configure adaptive responses

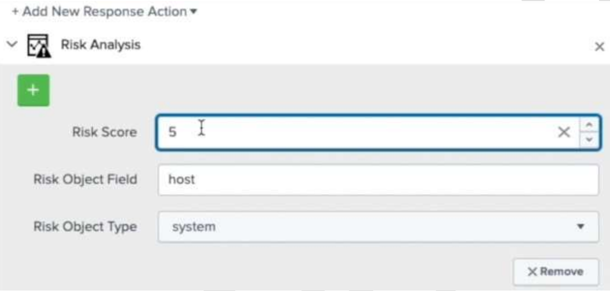
The most common adaptive response action for a correlation search is the notable event:

- Click **Add New Response Action** and select *Notable*
- Type a **Title** of ***Excessive Failed Logins (10)***
- Type a **Description** of ***System src failed app authentication $count$ times using $user_count$ username(s) against $dest_count$ target(s) in the last hour***
- Select a **security domain** of *Access* and **Severity** of ***medium***
- Leave the **Default Owner** and **Default Status** as ***leave as system default***
- Type a **Drill-down name** of ***View all login failures by system src for application app***
- Type a **Drill-down search** of | ***from datamodel:"Authentication"."Failed_Authentication"*** | ***search src="src" app="app"***

- Type a **Drill-down earliest offset** and **latest offset** of ***$info_min_time$*** and ***$info_max_time$***. NB: These values are derived from the **addinfo** command as part of summary indexing, and may not be available by default for correlation searches that do not use datamodels.
- Optionally, add **Investigation Profiles** relevant to the notable event
- Add ***src***, ***dest***, ***dvc*** and ***orig_host*** fields in **Asset Extraction** to add the values of those fields to the **investigation workbench** as **artifacts** when the notable event is added to an investigation
- Type ***src_user*** and ***user*** fields in **Identity Extraction** for the same reason
- Optionally add **Next Steps** to assist analysts triaging the notable event. You can only type plain text and links to **response actions** in the format of ***[[action|ping]]***
- Optionally add **Recommended Actions** for an analyst to run when triaging this notable event

Additional response actions can be added to perform a variety of actions. A common secondary response action is to increase the risk score of the system or user associated with the failed logins.

- **Add New Response Action → *Risk Analysis***
- Type a **Risk Score** of ***60***, **Risk Object Field** of ***src***, and **Risk Object Type** of ***System***



Risk Score: 5

Risk Object Field: host

Risk Object Type: system

Source: https://splunkvideo.hubs.vidyard.com/watch/4y6kUbbkCWnXrX2yVQcoCy

The **base** risk score from systems and users can then be modified using the **Risk Factor** editor.

Additional included **adaptive response actions** include:

- Send an **email**
- Run a **script**
- Start a **stream capture** with Splunk Stream
- **Ping** a host
- Run **Nbtstat**
- Run **Nslookup**
- Add **threat intelligence**
- Create a **Splunk Web message**

See the link below on **configure adaptive response** for details on how to configure each of these.

When ready, **Save** the correlation search https://docs.splunk.com/Documentation/ES/6.6.0/Tutorials/ResponseActionsCorrelationSearch

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Configureadaptiveresponse

https://docs.splunk.com/Documentation/Splunk/8.2.2/Knowledge/Usesummaryindexing

10.3 Search export/import

Search data export can be performing using

- Splunk Web
- CLIs
- SDKs
- REST API
- The internal, unsupported, experimental **dump** search command
- Data forwarding

The export method chosen depends on data volume and level of interactivity. The Splunk Web and CLI methods are significantly more accessible, and respectively support on-demand export of low and medium volume data respectively. The CLI facilitates tailored searches to external applications using the various Splunk SDKs. The REST API works from the CLI as well, but is recommended only for internal use. REST and SDK support high volume, automated exports, with REST working underneath the SDK.

Method	**Volume**	**Interactivity**	**Remarks**
Splunk Web	Low	On-Demand, Interactive	Easy to obtain on-demand exports
CLI	Medium	On-Demand, Low Interactive	Easy to obtain on-demand exports
REST	High	Automated, best for computer-to-computer	Works underneath SDK
SDK	High	Automated, best for computer-to-computer	Best for automation

Data can be exported into **formats** including CSV, JSON, XML, PDF (for reports) and raw event format (for search results that are raw events, and NOT calculated fields)

CLI export:

```
splunk search [eventdata] -preview 0 -maxout 0 -output
[rawdata|json|csv|xml] > [myfilename.log] ...
```

NB: **rawdata** is presented similarly to syslog data. **PDF** exports are only available from Splunk web exports.

```
splunk search "index=_internal earliest=09/14/2015:23:59:00
latest=09/16/2015:01:00:00 "
-output rawdata -maxout 200000 > c:/test123.dmp
```

In this example, up to 200,000 events of _internal index data in the given timerange are output in **raw data** format to test123.dmp. Also, note the **earliest** and **latest** time formats of mm/dd/yyyy:hh:mm:ss. As this section addresses data export, focus on the use of the **-output** parameter, and the available output formats.

REST API Export:

First, **POST** to the /**services**/**search**/**jobs**/ endpoint on the management interface:

```
curl -k -u admin:changeme https://localhost:8089/services/search/jobs/ -d
search="search sourcetype=access_* earliest=-7d"
```

Retrieve the <sid> value in the <response> for the search job ID. If you inadvertently close the window before capturing the ID, it can also be retrieved from Activity → Jobs by opening the Job Manager. Locate the job you just ran and click Inspect to open the Search Job Inspector, which contains the search job ID.

Next, use a **GET** request on the /**results** endpoint for the services **namespace** (NS) to export the search results to a file. I.e. /servicesNS/<user>/<app>/search/jobs/<sid>/**results**/. Ensure you identify the following details:

- Object endpoints (visible from https://localhost:8089/servicesNS/<user>/<app>/)
- Search job user and app (as part of the URI path)
- Output format (**atom** | **csv** | **json** | **json_cols** | **json_rows** | **raw** | **xml**)

Note the extra REST output options of **atom**, **json_cols** and **json_rows**. An Atom Feed or Atom Syndication Format is a standard XML response format used for a REST API

E.g. export results to a JSON file using REST API:

```
curl                 -u                 admin:changeme                 -k
https://localhost:8089/servicesNS/admin/search/search/jobs/1423855196.339
/results/ --get -d output_mode=json -d count=5
```

To summarise, a **curl -d** request POSTs to generate a search, and returns the **SID**. A second **curl** request uses the **--get** parameter to retrieve the search, specifying the username from the previous search, the app name (search), the SID for the /**search**/**jobs**/ endpoint, followed by the /**results**/ endpoint.

SDK Export:

Splunk SDKs support data export via **Python** SDK, **Java** SDK, **JavaScript Export** or **C#** SDK. See the appendix for an example of a Python SDK export.

https://docs.splunk.com/Documentation/Splunk/8.2.2/Search/Exportsearchresults https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Uploaddata

https://docs.splunk.com/Documentation/Splunk/8.0.2/RESTUM/RESTusing

11.0 Lookups and Identity Management (5%)

11.1 Identify ES-specific lookups

Asset and identity management is derived from a number of defined lookups that contain data from specific sources such as Active Directory. Custom identity and asset lookups can also be added and prioritised to enrich asset and identity data. This data is then processed into categorised lookups.

Finally, a number of macros and datamodels can be used to query data elements, or the entire set of asset or identity data.

Assets:

```
| makeresults | eval src="1.2.3.4" |
`get_asset(src)` | `assets`
|`datamodel("Identity_Management", "All_Assets")`
|`drop_dm_object_name("All_Assets")`
```

Identities:

```
| makeresults | eval user="VanHelsing" |
`get_identity4events(user)` | `identities`
|`datamodel("Identity_Management", "All_Identities")`
|`drop_dm_object_name("All_Identities")`
```

The macro **`drop_dm_object_name`** removes the “All_Assets.” or “All_Identities.” prefix respectively from results, making it much easier to reference the relevant fields. If multiple fields of the same name exist in different datasets, you may choose not to pipe this macro to the end of the query.

Once individual asset and identity sources are defined and prioritised, they are merged into categorised lookups for asset strings (zu), assets by CIDR range (zv), identity strings (zy) and default field correlation (zz). Each of these categories aligns with a KV store collection, or a default fields correlation lookup for asset or identity. **Merged asset and Identity data**

String-based asset correlation	assets_by_str KV store collection	LOOKUP-zu-asset_lookup_by_str-dest LOOKUP-zu-asset_lookup_by_str-dvc LOOKUP-zu-asset_lookup_by_str-src
CIDR subnet-based asset correlation	assets_by_cidr KV store collection	LOOKUP-zv-asset_lookup_by_cidr-dest LOOKUP-zv-asset_lookup_by_cidr-dvc LOOKUP-zv-asset_lookup_by_cidr-src
String-based identity correlation	identities_expanded KV store collection	LOOKUP-zy-identity_lookup_expanded-src_user LOOKUP-zy-identity_lookup_expanded-user
Default field correlation	identity_lookup_default_fields.csv asset_lookup_default_fields.csv	LOOKUP-zz-asset_identity_lookup_default_fields-dest LOOKUP-zz-asset_identity_lookup_default_fields-dvc LOOKUP-zz-asset_identity_lookup_default_fields-src LOOKUP-zz-asset_identity_lookup_default_fields-src_user LOOKUP-zz-asset_identity_lookup_default_fields-user

You can also locate lookups under Settings → Lookups. Ensure you are familiar with the process of troubleshooting lookups, and how lookups relate to the asset and identity management framework. Lookups can also be used for a number of other purposes as seen in the tables below:

Lookup type	**Description**	**Example**
List	Small, relatively static lists used to enrich dashboards.	Categories
Asset or identity list	Maintained by a modular input and searches.	Assets
Threat intelligence collections	Maintained by several modular inputs.	Local Certificate Intel

Tracker Search-driven lookups used to supply data to dashboard panels. Malware
Tracker

Per-panel filter lookup Used to maintain a list of per-panel filters on specific dashboards. HTTP
Category Analysis Filter

Internal lookups that you can modify:

Action History Search Tracking List Whitelist		Add searches to this whitelist to prevent them from creating action history items for investigations.
Administrative Identities	List	You can use this lookup to identify privileged or administrative identities on relevant dashboards such as the Access Center and Account Management dashboards.
Application Protocols	List	Used by the Port and Protocol dashboard.
Asset/Identity Categories	List	You can use this to set up categories to use to organize an asset or identity. Common categories for assets include compliance and security standards such as PCI or functional categories such as server and web_farm. Common categories for identities include titles and roles.
Assets	Asset list	You can manually add assets in your environment to this lookup to be included in the asset lookups used for asset correlation.
Demonstration Assets	Asset list	Provides sample asset data for demonstrations or examples.
Demonstration Identities	Identity list	Provides sample identity data for demonstrations or examples.
ES Configuration Health Filter	Per-panel filter lookup	Per-panel filtering for the ES Configuration Health dashboard.
Expected Views	List	Lists Enterprise Security views for analysts to monitor regularly.
HTTP Category Analysis Filter	Per-panel filter lookup	Per-panel filtering for the HTTP Category Analysis dashboard
HTTP User Agent Analysis	Per-panel filter lookup	Per-panel filtering for the HTTP User Agent Analysis dashboard
Identities	Identity list	You can manually edit this lookup to add identities to the identity lookup used for identity correlation.
IIN and LUHN Lookup	List	Static list of Issuer Identification Numbers (IIN) used to identify likely credit card numbers in event data.
Interesting Ports	List	Used by correlation searches to identify ports that are relevant to your network security policy.
Interesting Processes	List	Used by a correlation search to identify processes running on hosts relevant to your security policy.
Interesting Services	List	Used by a correlation search to identify services running on hosts relevant to your security policy.
Local * Intel	Threat intel lookup	Used to manually add threat intelligence.
Modular Action Categories	List	Used to categorize the types of adaptive response actions available to select.
New Domain Analysis	Per-panel filter lookup	Per-panel filtering for the New Domain Analysis dashboard.

PCI Domain Lookup	Identity list	Used by the Splunk App for PCI Compliance to enrich the pci_domain field. Contains the PCI domains relevant to the PCI standard.
Primary Functions	List	Identifies the primary process or service running on a host. Used by a correlation search.
Prohibited Traffic	List	Identifies process and service traffic prohibited in your environment. Used by a correlation search.
Risk Object Types	List	The types of risk objects available.
Security Domains	List	Lists the security domains that you can use to categorize notable events when created and on Incident Review.
Threat Activity Filter	Per-panel filter lookup	Per-panel filtering for the Threat Activity dashboard.
Traffic Size Analysis	Per-panel filter lookup	Per-panel filtering for the Traffic Size Analysis dashboard.
Urgency Levels	List	Urgency Levels contains the combinations of priority and severity that dictate the urgency of notable events.
URL Length Analysis	Per-panel filter lookup	Per-panel filtering for the URL Length Analysis dashboard.

View the link below for "**Manageinternallookups**" for a sortable list of the table above. You don't need to know the individual fields in these lookups, but you should understand their general purpose. For example, consider how urgency levels might be relevant in the context of asset & identity priorities and event severity. There are also 6 separate lookups involving assets and identities. Understand how these relate to the Assets & Identities framework.

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Verifyassetandidentitydata

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Manageinternallookups

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Assetandidentitylookups

11.2 Understand and configure lookup lists

From a real-word perspective, asset identification is necessary for performing risk assessments and Business Impact Analysis. The process for managing Asset and Identity lookups is described below.

1. You collect asset and identity data from data sources using an add-on and a custom search, or manually with a CSV file.
2. The Splunk ES **identity manager modular input** updates settings in the **transforms.conf** stanza **identity_lookup_expanded**.
3. You format the data as a lookup, using a search or manually with a CSV file.
4. You configure the list as a lookup table, definition, and input.
5. You create an identity lookup configuration.
6. The Splunk ES identity manager modular input detects two things:
    1. Changed size of the CSV source file.
    2. Changed update time of the CSV source file.

7. The Splunk ES identity manager modular input updates the **macros** used to identify the input sources based on the currently **enabled** stanzas in **inputs.conf**.
8. The Splunk ES identity manager modular input dispatches **custom dynamic searches** if it identifies changes that require the asset and identity lists to be merged.
9. The custom search dispatches a merge process to merge all configured and enabled asset and identity lists.
10. The custom searches **concatenate the lookup tables** referenced by the identity manager input, generate new fields, and **output** the concatenated asset and identity lists into **target lookup table files**: ***asset_lookup_by_str***, ***asset_lookup_by_cidr***, ***identity_lookup_expanded***.
11. You verify that the data looks as expected.

From the Splunk ES menu bar, click **Configure** → **Data Enrichment** → **Asset and Identity Management**.

To add an **asset** input stanza for the lookup source, click the **Asset Lookup Configuration** tab, then click **New**.

In the **New Asset Manager**, select the corresponding CSV for the lookup **Source**, ensuring that you **DO NOT** use a default lookup like ***asset_lookup_default_fields*** for onboarding ***custom*** data. Add a name and description, and **check** the Blacklist check box to exclude the lookup file from **bundle replication**.

Leave the **Lookup List Type** set to ***asset***, and use the **Lookup Field Exclusion List** to select fields that the merge process should ignore, then click **Save**.

From the **Asset Lookup Configuration** tab, drag and drop the rows of the table into a preferred order for ranking of the asset sources. Optionally **Enable** or **Disable** inputs as appropriate.

Manually add static asset data from the Splunk ES menu bar under **Configure** → **Content** → **Content Management** and click on **Assets**. Provided that you have access, double click in a cell to add, change or remove content and save your changes. The lookup will then be registered as ***static_assets*** or ***static_identities*** under **Configure** → **Data Enrichment** → **Asset and Identity Management**.

A similar process can be followed for identities. See the links on **How asset and identity data is processed** for additional procedural information on collecting, extracting, formatting and configuring asset and identity lists.

Examples of each of the response formats, particularly for REST API responses, can be found in the last link below:

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Howassetandidentitydataprocessed

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Manageassetsandidentities

https://docs.splunk.com/Documentation/Splunk/8.0.2/RESTUM/RESTusing#Example_A:_CSV_response_format_examp le

12.0 Threat Intelligence Framework (5%)

12.1 Understand and configure threat intelligence

There are three main steps for adding threat intelligence to Splunk ES:

1. Configure the threat intelligence sources included with Splunk Enterprise Security.
2. For each additional threat intelligence source not already included with Splunk Enterprise Security, follow the procedure to add threat intelligence that matches the source and format of the intelligence that you want to add.
    1. Upload a STIX or OpenIOC structured threat intelligence file
    2. Upload a custom CSV file of threat intelligence
    3. Add threat intelligence from Splunk events in Splunk Enterprise Security
    4. Add and maintain threat intelligence locally in Splunk Enterprise Security
    5. Add threat intelligence with a custom lookup file in Splunk Enterprise Security
    6. Upload threat intelligence using REST API
3. Verify that you have added threat intelligence successfully in Splunk Enterprise Security.

Threat Intelligence is managed from the ES menu bar under **Configure → Data Enrichment → Threat Intelligence Management → Sources**. Threat sources can be modified by users holding the ***edit_modinput_threatlist*** **capability**. Click on **Advanced Edit** next to the intelligence document you want to modify in order to view the **Intelligence Download Settings**. If this is a new data source, you may need to refresh the UI before the intelligence document becomes available.

To configure a **custom workload**, click on an intelligence document, then click the **General** tab and scroll down to deselect ***Threat Intelligence***. Recall that Threat Intelligence workloads are managed automatically. From the **Advanced** tab, select the desired workloads or actions for the selected document.

Threat match searches can be modified by users holding the ***administrator*** **role** with ***edit_modinput_threatmatch*** **capabilities** to edit the threat match settings.

From the ES menu bar, click on **Configure → Data Enrichment → Threat Intelligence Management → Threat Matching**. Click on the threat match source to configure settings for the following fields:

- **Source**: Type of threat match sources
- **Interval**: Cron interval when the search runs
- **Earliest Time**: When the search starts
- **Latest Time**: When the search completes
- **Match Fields**: Fields to match against to generate threats
- **Status**: Enable or disable the threat match search

Changes made here will be reflected in the **DSS Threat Intelligence** module, in the **inputs.conf** configuration file, within the **[threat match]** stanza.

Clicking **Edit Threat Match Configuration** allows you to modify the following settings:

- [Stanza] Name
- Source
- Earliest Time & Latest Time
- Interval
- Max Aggregate values
- Datasets

To add a new data set to the threat match set:

1. Click on **Add Dataset** → **Datamodel** to specify the source of the data set, such as ***Authentication***.
2. Select the [Dataset] **Object**, such as ***Failed_Authentication***.
3. Use the **Event Filter** to specify boolean matches for filtering out events for the threat match search, which corresponds to the **where** clause in the resulting search SPL.
4. Specify the **Match field** field to select fields to match on, such as sourcetype.
5. Click **Add Aggregate** to identify datasets that the search may retrieve from the datamodel
6. Specify the **alias** for the **field** to rename the aggregate. For example, ***All_Certificates.src*** as ***src***.
7. Click **Save Dataset** to build the threat match search.

Global threat list settings can be configured from **Configure** → **Data Enrichment** → **Threat Intelligence Management** → **Global Settings**. This includes **proxy settings** (***server, port, user and realm***), as well as **parse modifier settings** including Certificate Attribute Breakout, IDNA Encode Domains, and Parse Domain from URL.

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Addthreatintel

12.2 Configure user activity analysis

User activity analysis is typically associated with User & Endpoint Behavioural Analysis or UEBA, but suspicious activity can also be determined through Enterprise Security. Two examples include data exfiltration and monitoring privileged accounts for suspicious activity.

The **User Activity** dashboards provides a high level overview. From the ES menu bar, select **Security Intelligence** → **User Intelligence** → **User Activity**. Key indicators of **Web Volume** and **Email Volume** to view evidence of suspicious or atypical changes over the last 24 hours.

The **Email Activity** dashboard provides an overview of **Top Email Sources** and **Large Emails**.

The **DNS Activity** dashboard provides an overview of **Queries per Domain** and allows drilldown into the **DNS Search** dashboard. **Splunk Stream** can be used to capture DNS traffic if not available from another source.

Based on this analysis, a new **notable event** can be manually created via **Configure** → **Incident Management** → **New Notable Event**. This requires configuration of the following fields:

- Title (E.g. possible data exfiltration)
- Domain (E.g. Threat)

- Urgency (E.g. Critical)
- Owner (E.g. Analyst's name)
- Status (E.g. In Progress)
- Description

Custom dashboards can also be created for analysis of privileged accounts.

- Select **Search → Reports** and find the ***Access – Privileged Accounts in Use*** report.
- Click **Add to Dashboard → New** to set a dashboard title
- Set **Dashboard Permissions** to ***Shared in App***
- Type a **Panel Title**, then set **Panel powered By** to ***Report***, and set **Panel Content** to ***Statistics***
- **Save** and **View Dashboard** to validate the report is showing in the new dashboard as expected.
- Under **Configure → General Navigation**, locate the **Identity** security domain navigation collection.
- Click the **Add View** icon and select the new **Privileged Accounts** dashboard.
- Click **Save** to save the dashboard navigation location, then **Save** to update the menu bar.

Additional dashboards or panels can be added to this or other collections for user (or other) analysis.

A separate course is available for Splunk User Behaviour Analytics, so is not detailed here, but further information on the app and training are available in the second and third link below:

https://docs.splunk.com/Documentation/ES/6.6.0/Usecases/DataExfiltration

https://www.splunk.com/en_us/software/user-behavior-analytics.html

https://www.splunk.com/en_us/training/courses/user-behavior-analytics.html

Appendix A: Threat Intelligence Examples

Example STIX JSON threat intelligence

```
{
  "type": "bundle",
  "id": "bundle—56be2a3b-1534-4bef-8fe9-602926274089",
  "objects": [
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator—d81f86b9-975b-4c0b-875e-810c5ad45a4f",
      "created": "2014-06-29T13:49:37.079Z",
      "modified": "2014-06-29T13:49:37.079Z",
      "name": "Malicious site hosting downloader",
      "description": "This organized threat actor group operates to create profit from all types of crime.",
      "indicator_types": [
        "malicious-activity"
      ],
      "pattern": "[url:value = 'http://x4z9arb.cn/4712/']",
      "pattern_type": "stix",
      "valid_from": "2014-06-29T13:49:37.079Z"
    },
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware—162d917e-766f-4611-b5d6-652791454fca",
      "created": "2014-06-30T09:15:17.182Z",
      "modified": "2014-06-30T09:15:17.182Z",
      "name": "x4z9arb backdoor",
      "description": "This malware attempts to download remote files after establishing a foothold as a
backdoor.",
      "malware_types": [
        "backdoor",
        "remote-access-trojan"
      ],
      "is_family": false,
      "kill_chain_phases": [
        {
          "kill_chain_name": "mandiant-attack-lifecycle-model",
          "phase_name": "establish-foothold"
        }
      ]
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship—864af2ea-46f9-4d23-b3a2-1c2adf81c265",
      "created": "2020-02-29T18:03:58.029Z",
      "modified": "2020-02-29T18:03:58.029Z",
      "relationship_type": "indicates",
      "source_ref": "indicator—d81f86b9-975b-4c0b-875e-
810c5ad45a4f",          "target_ref": "malware—162d917e-766f-
4611-b5d6-652791454fca"
    }
  ]
}
```

Source: https://oasis-open.github.io/cti-documentation/examples/indicator-for-malicious-url

Example OpenIOC XML threat intelligence

```
<?xml version="1.0" encoding="us-ascii"?>
```

```
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="c32ab7b5-
49c8-40cc-8a12-ef5c3ba91311" last-modified="2011-10-28T19:28:20"
xmlns="http://schemas.mandiant.com/2010/ioc">
 <short_description>FIND WINDOWS</short_description>
 <description>This is a sample IOC that will hit on a number different artifacts present on a Windows
computer. This IOC is used to test or illustrate the use of an IOC.</description>
 <keywords />
 <authored_by>Mandiant</authored_by>
 <authored_date>0001-01-01T00:00:00</authored_date>
 <links />
 <definition>
  <Indicator operator="OR" id="2e693207-ae90-4f9b-8a31-67f31f1d263c">
   <IndicatorItem id="5ebfad1c-6f1a-472b-ae58-6fdfede0f4e7" condition="contains">
    <Context document="FileItem" search="FileItem/FullPath" type="mir" />
    <Content type="string">\kernel32.dll</Content>
   </IndicatorItem>
…
   <Indicator operator="AND" id="990fbe29-6af6-45cb-b07e-6d13c5a30617">
    <IndicatorItem id="de7c6347-34d8-4a16-b559-38d9f4e6aabb" condition="is">
     <Context document="FileItem" search="FileItem/FileName" type="mir" />
     <Content type="string">sens.dll</Content>
    </IndicatorItem>
    <IndicatorItem id="96b8856c-f865-4805-93ed-aa8780b87617" condition="is">
     <Context document="FileItem" search="FileItem/PEInfo/DigitalSignature/SignatureExists" type="mir" />
     <Content type="string">true</Content>
    </IndicatorItem>
   </Indicator>
  </Indicator>
 </definition>
</ioc>
```

Source: https://github.com/STIXProject/openioc-to-stix/blob/master/examples/find_windows.ioc.xml

Python SDK Search Export

```
# Set parameters of what you wish to search (e.g. splunklib in
the last hour) sys.path.insert(0,
os.path.join(os.path.dirname(__file__), "..", "lib")) import
splunklib.client as client import splunklib.results as results
```

```
# Change or acquire these values as necessary
HOST =
"localho
```

```
st" PORT
= 8089
USERNAME = "admin"
PASSWORD = "changeme"
# Use the client library to establish a connection and run a normal-
mode search, then use the results library’s ResultsReader to export
results to variable rr.
service = client.connect(     host=HOST,     port=PORT,
username=USERNAME,     password=PASSWORD) rr =
results.ResultsReader(service.jobs.export("search index=_internal
earliest=-1h | head 5"))
# Get the results and display them using the ResultsReader. Note the use
of result in the rr loop, but results.Message (plural) to verify the
instance for result in rr:     if isinstance(result, results.Message):
        # Diagnostic messages might be returned
in  the  results              print  '%s:  %s'  %
(result.type,   result.message)            elif
isinstance(result, dict):
        # Normal events are
returned as dicts
print result assert
rr.is_preview == False
```