



# **Splunk® Enterprise Security**

## **Use Cases 7.0.2**

Generated: 10/05/2022 4:47 pm

# Table of Contents

<b>Introduction.....</b>	<b>1</b>
Overview.....	1
<b>Detect malware.....</b>	<b>2</b>
Using Enterprise Security to find Malware.....	2
Use DNS data to identify malware patient zero.....	13
Investigating potential zero-day activity.....	15
<b>Identify suspicious activity.....</b>	<b>19</b>
Using Enterprise Security to find data exfiltration.....	19
Monitor privileged accounts for suspicious activity.....	22
<b>Isolate threats.....</b>	<b>26</b>
Isolate threats with risk alerting.....	26
Assign risk scores to assets and identities.....	27
Generate risk notables using correlation searches.....	27
Add annotations to enrich correlation search results.....	29
Classify risk objects based on annotations.....	29
Add a risk message and a risk score to a notable.....	31
Adjust risk scores for specific objects.....	31
<b>Reduce alert volume.....</b>	<b>33</b>
Reduce alert volumes by triaging notables.....	33
Add dispositions to risk notables.....	33
Sort notables by disposition.....	35
Investigate risk notables that represent a threat.....	35
<b>Isolate user behaviors.....</b>	<b>38</b>
Isolate User Behaviors That Pose Threats.....	38
Use Dashboards to track user behavior.....	38
Classify accounts based on privileged access.....	39
Use correlation searches to monitor accounts.....	39
Increase risk factors to identify unauthorized usage.....	40

# Introduction

## Overview

These use cases walk you through monitoring, investigation, and detection scenarios for security incidents using Splunk Enterprise Security. Use the available dashboards, alerts, correlation searches, as well as custom searches, to assess and remediate threats in your environment.

The following use cases explain real-world ways you can use Splunk Enterprise Security.

### Detect malware

- [Using Enterprise Security to find Malware](#)
- [Use DNS data to identify malware patient zero](#)
- [Investigating potential zero-day activity](#)

### Identify suspicious activity

- [Using Enterprise Security to find Data Exfiltration](#)
- [Monitor privileged accounts for suspicious activity](#)

### Isolate threats

- [Isolate threats with risk alerting](#)
- [Assign risk scores to assets and identities](#)
- [Generate risk notables using correlation searches](#)
- [Add annotations to enrich correlation search results](#)
- [Classify risk objects based on annotations](#)
- [Add a risk message and a risk score to a notable](#)
- [Adjust risk scores for specific objects](#)

### Reduce alert volume

- [Reduce alert volumes by triaging notables](#)
- [Add dispositions to risk notables](#)
- [Sort notables by disposition](#)
- [Investigate risk notables that represent a threat](#)

### Isolate user behaviors

- [Isolate user behaviors that pose threats](#)
- [Use dashboards to track user behavior](#)
- [Classify accounts based on privileged access](#)
- [Use correlation searches to monitor accounts](#)
- [Increase risk factors to identify unauthorized usage](#)

# Detect malware

## Using Enterprise Security to find Malware

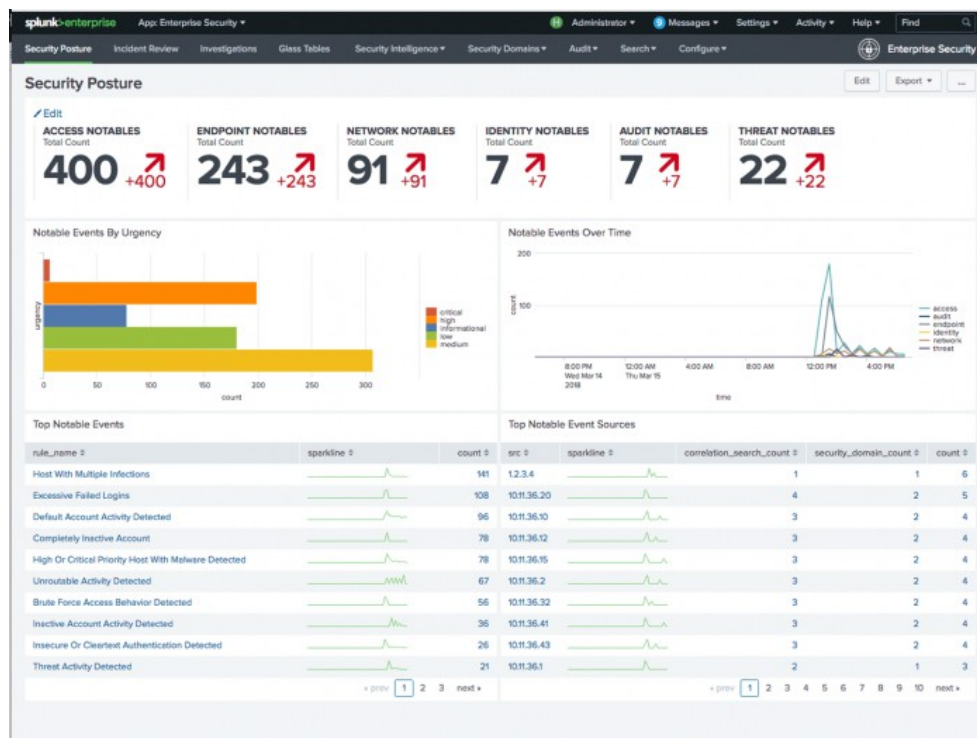
Enterprise Security provides statistics and interesting events on security domain specific dashboards. Using the dashboards together, you can build a workflow for investigating threats by reviewing the results, isolating the events that require attention, and using the contextual information provided to drill down into the issue.

### Prerequisites

- Verify that a Splunk platform instance with Splunk Enterprise Security is installed and configured.
- Verify that logs from an IDS/IPS tool, web proxy software or hardware, and/or an endpoint security product are indexed on a Splunk platform instance.

### The Security Posture dashboard

Begin by reviewing the Security Posture dashboard. The dashboard represents a summary of all notable event activity over the last 24 hours. A notable event is the result of a security-oriented correlation search that scans the indexed logs until a match is found. When a notable event is created, it represents a potential issue or threat requiring a review and, depending upon the outcome of the review, an investigation.



In the **Top Notable Events** panel, you see the count of notable events sorted by the correlation search name. The panel shows that the number of **High Or Critical Priority Host With Malware Detected** notable events had a sudden spike. To drill down into those numbers, select the peak count on the sparkline to open another browser window and drill down to the Incident Review dashboard.

## Working in Incident Review

Use the Incident Review dashboard to find, assign, analyze, and update notable events.

### ***Prioritize the task***

[illegible]

The search for **High Or Critical Priority Host With Malware Detected** ranges over several **Urgency** levels. The event urgency is calculated based on the priority assigned to a host or asset and the severity assigned to the correlation search.

All urgency levels are selected by default, and the Correlation Search Name is populated with the value "High Or Critical Priority Host With Malware Detected." The bottom portion of the image shows a table listing all the incidents. The table columns, from left to right, are Time, Security Domain, Title, Urgency, Status, Owner, and Actions.

1. Start the investigation by looking at the notable event labeled **Critical**.
2. Remove other notable events from the view by deselecting all other **Urgency** levels until only **Critical** remains. In a list of urgencies, only Critical remains selected. All other urgencies (High, Medium, Low, Info) are deselected. The cursor is shown hovering over the **Submit** button, indicating that this should be clicked after the desired urgencies are selected.
3. Click **Submit**.

The Incident Review dashboard displays only the **Critical** notable event that was created for a **High Or Critical Priority Host With Malware Detected**.

## Task assignment

Assigning notable events begins a record of activity that you can use for notes and time tracking, and lets other analysts know that an issue is being investigated.

To assign the notable event to your user account:

1. Use the check box to select the first notable event.
2. Click the **Edit all matching events** link on the top left of the table view.
3. Change the **Status** field to **In Progress**, and assign your user as the **Owner**.
4. Update the **Comment** field as required by your company security policy.
5. Click **Save changes** to return to the Incident Review dashboard.

## Notable event review

The **Description** field is a summary of the conditions a correlation search must find for you to create a notable event.

1. Click the arrow next to a notable event to expand the view and display the details of the notable event.
2. Review the information provided with the notable event.

**Notable Event Review Interface:**

**Table Headers:** Time, Security Domain, Title, Urgency, Status, Owner, Actions

**Selected Event:** 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:**

Field	Value
Destination	10.11.36.20
Destination Business Unit	americas
Destination Category	pod
Destination City	splunk
Destination Country	usa
Destination IP Address	10.11.36.20
Destination Expected	true
Destination Latitude	37.694452
Destination Longitude	-122.094461
Destination Owner	BS_williams
Destination PO Domain	trust
Destination Requires Antivirus	false
Destination Should Time Synchronize	true [should_time_sync]
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:**

```
raw_type=502 raw_type_simple="FILELOG MALWARE EVENT" event_id=1522219096 sensor=xxx.yyyz  
rs.com connection_instance=8 connection_counter=52948 connection_time=1522219096 src_ip=1  
0.123.144.101 dest_ip=10.11.36.20 disposition=Neutral action="Malware Cloud Lookup" detec  
tion=Unknown sha256=94c9b9f8a0f34430b517e3a1e5f7e3442e78f85232f754d93d9f3c6a file  
_type=PDF file_name=22919023_1357521438864_e4_de2012_728x95_52.pdf file_size=41073 direc  
tion=Download app_proto=HTTP user=user18 url=http://www.aaaaaa.com/22919023_135752143886  
4_e4_de2012_728x95_52.pdf signature="" src_port=55764 dest_port=80 ip_proto=TCP policy=4  
5427b86-3f81-11e3-bafe-909b235fe4b3 src_ip_country=unknown dest_ip_country="united state  
s" web_app=blackwave_client_app=chrome
```

**Adaptive Responses:**

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

Each notable event has a selection of fields that provide contextual information about the issue. The fields are populated with data correlated from the logs of one or more data sources and asset and identities collections.

3. Review several fields for history about the host or hints of activity. The **Urgency** assigned to this notable event was partially calculated from the priority assigned to the host.
4. Begin the investigation into the host by investigating the **Destination IP Address**. Click the arrow next to the **Destination IP Address** field to initiate a field action. A field action initiates a new search on another dashboard in Enterprise Security, using the selected field as a filter. This technique helps you to maintain context while opening multiple dashboards or using views during an investigation.
5. In the field action menu, select **Asset Investigator**.

Edit Selected | Edit All 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**

Field	Value	Action	Correlation Set
Destination	10.11.36.20	▼	Endpoint - High
Destination Business Unit	americas	▼	History:
Destination Category	pci	▼	View all review
Destination City	Pleasanton	▼	Contributing Events
Destination Country	USA	▼	View infections
Destination IP Address	10.11.36.20	▼	Original Event
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		

**Edit Tags**

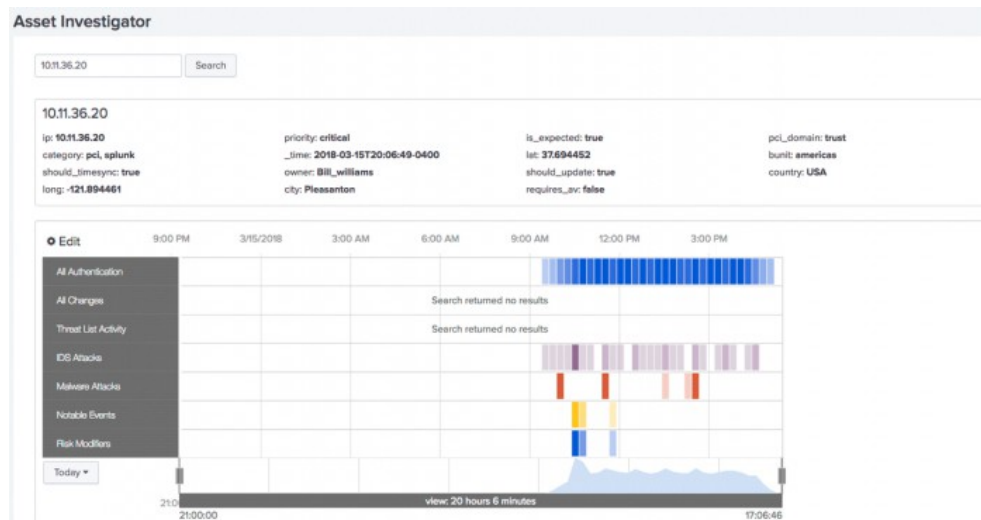
- Access Search (as destination)
- Access Search (as source)
- Asset Center
- Asset Investigator
- Domain Dossier
- Facebook Threat Exchange lookup
- Google 10.11.36.20
- Intrusion Search (as destination)

Notable

A new browser window opens to the **Asset Investigator** dashboard and begins a search on the selected **Destination IP Address**.

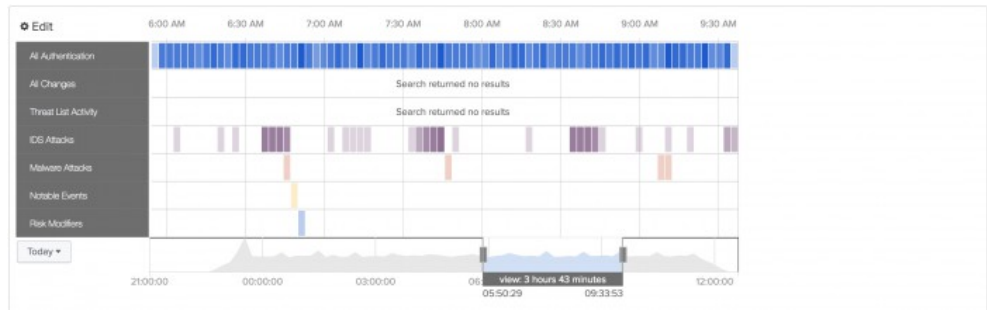
## Working in Asset Investigator

The **Asset Investigator** dashboard displays data about one asset or host collected and grouped by a common threat category. Each category is represented as a named row of data called a swim lane.



Each swim lane has a collection of data points called candlesticks. The event count within a candlestick is represented through a heat map. The brighter the color, the higher the event count.

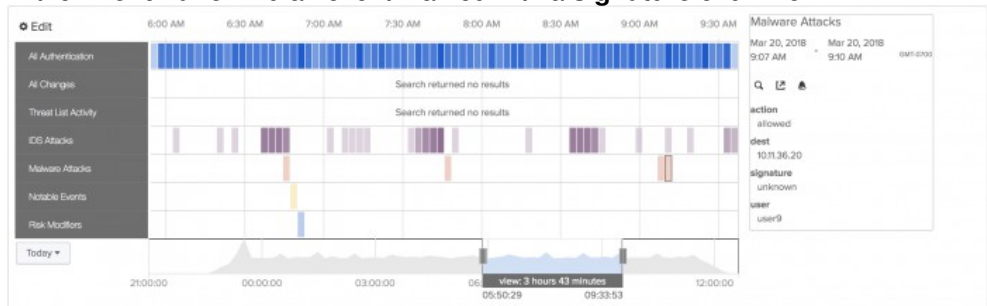
If you see too many events in one category, use the time sliders to focus the view down to the time frame where the notable event was triggered. In this example, the time sliders are moved to focus on a group of **Malware Attacks**.



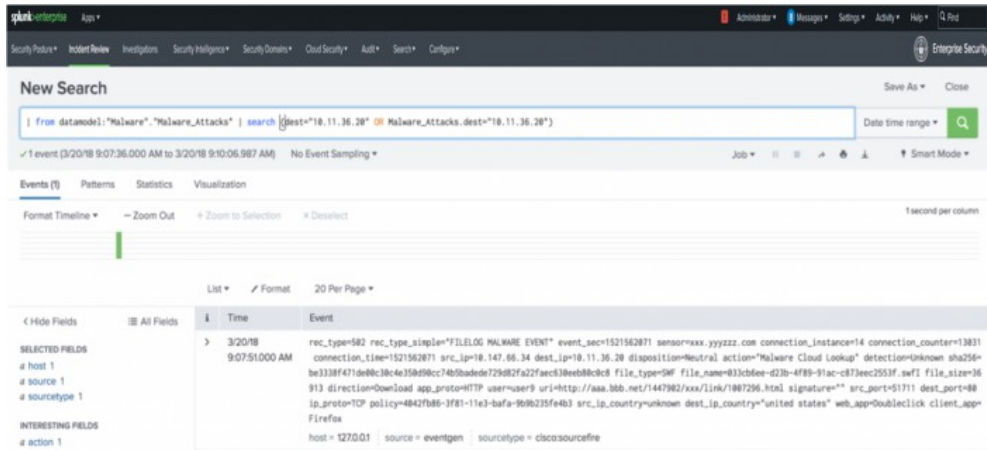
### Find the event

At this point, you can follow any number of malware events related to this host. Use the **Malware Attacks** swim lane to select a candlestick and review the common fields using the **Event Panel**.

1. In the **Malware Attacks** swim lane, select a candle stick.
2. In the **Event Panel** find an event marked with a **signature** of unknown.



3. Click the **Go to Search** icon to open another browser window to drill down and search on the selected **Destination IP Address**.





## Drill down to log events

Review the **New Search** dashboard. The search dashboard is still in Enterprise Security context, as marked by **App: Enterprise Security** in the top left corner. This mode ensures that the field values, aliases, and other field categories supplied with ES will apply when raw log events are searched from this dashboard.

Examine the drilldown search in the search bar. The process begins by identifying the `datamodel | datamodel ("Malware", "Malware_Attacks")` before calling the normalized host value for the Malware data model `| search (dest="x.x.x.x" OR "Malware_Attacks.dest="x.x.x.x")`. A `datamodel` search command searches the indexed data over the time frame, filters the results through the malware data model constraints, and returns any matches.

Enterprise Security does not use accelerated data models for drilldown searches, so it is important to set a time range for faster results. The `Malware_Attacks.dest` represents the `dest_ip` field reference in the malware data model.

## Identify relevant fields

You can see that the raw event has a lot of information to process. Let's begin by looking at common fields, such as `dest_ip`, `source`, and `sourcetype`. Reviewing these fields, you see that the `dest_ip` references an internal IP address range. Searching your network device inventory system might tell you what that `host` or `dest_ip` represents.

The source and `sourcetype` identify the events as `sourcefire` data. After confirming the `dest_ip` represents a proxy server device, you know that the `src_ip` field represents other hosts on the internal network accessing data through the proxy.

```
Time      Event
> 3/20/18  rec_type=582 rec_type_simple="FILELOG MALWARE EVENT" event_sec=1521562071 sensor=xxx.yyyzzz.com connection_instance=14 connection_counter=13831 connection_time=1521562071
9:07:51.000 AM  src_ip=18.147.66.34 dest_ip=18.11.36.28 disposition=Neutral action="Malware Cloud Lookup" detection=Unknown sha256=ba3338f471de48c38c4e358d9ec74b5badde72682fa22fawec33be
eb88cd8 file_type=SW file_name=83c6ee-d3b-4f89-91ac-c873ec253f.swf file_size=36913 direction=Download app_proto=HTTP user=user9 uri=http://aaa.bbb.net/1447982/xxx/
link/1887296.html signature="" src_port=51711 dest_port=88 ip_proto=TCP policy=4842fb86-3f81-11e3-bafa-9b96235fe4b3 src_ip.country=unknown dest_ip.country="united states"
web_app=DoubleClick client_app=Firefox
host = 127.0.0.1 source = eventgen sourcetype = cisco:sourcefire
```

This event also contains `client_app` and `uri` fields. These fields represent traffic from a web browser to a site requesting a download. Let's review which fields in the source logs are relevant, and why.

Field	Description
<code>src_ip</code>	Represents internal network hosts.
<code>dest_ip</code>	Another internal host that was discovered to be a proxy.
<code>uri</code>	A record of what is being requested by the hosts.
<code>client_app</code>	The browser used.

You know that the **Critical** notable event represents an unknown malware signature being passed through the proxy server into your network. As you progress through the investigation and followed data flows and requests, you created a list of the key fields relevant to the threat. Because a number of malware downloads are reported by the proxy, expand the search to find the internal hosts that are responsible.

## Review a broader timespan of events

Broaden the search by widening the time range and search again.

1. Select the **Date time range** button.
2. Lower the **Earliest** time field to an earlier time (for example, 02:00:00.000).
3. Raise the **Latest** field to a later time (for example, 10:00:00.000).

4. Click **Apply** to keep the changes.
5. Click Search.

The search page now shows multiple similar events that passed through the proxy.

# New Search

| from datamodel:"Malware"."Malware\_Attacks" | search [Malware\_Attacks.des

✓ 6 events (3/26/18 2:00:00.000 AM to 3/26/18 10:00:00.000 AM) No Event Sampling

Events (6) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect



List ▾ ✎ Format 20 Per Page ▾

< Hide Fields

☰ All Fields

## SELECTED FIELDS

a host 1  
a source 1  
a sourcetype 1

## INTERESTING FIELDS

a action 1  
a category 1  
a date 1  
a dest 1  
a dest\_bunit 1  
a dest\_category 2  
a dest\_nt\_domain 1  
a dest\_priority 1  
a dest\_requires su 1

i	Time	Event
>	3/26/18 7:07:12.000 AM	rec_type=502 r _ip=10.98.200. 46aab94b8db7b7 signature="SEN known web_app= host = 127.0.0.1
>	3/26/18 4:44:53.000 AM	rec_type=502 r _ip=10.11.36.2 98 file_type=S alicious_300x2 untry="united host = 127.0.0.1
>	3/26/18	rec_type=502 r

The search view displays many more events, but may be impractical for summarizing the data by important fields. Changing the search to a table view lets you retain the important fields and reduce the visual clutter. A table can also provide a reference because the results can be exported for reporting.

To view a table of the events sorted by relevant fields, use the search bar to add `| table dest src url` to the end of the existing search string and click search again.

**New Search**

Save As Close

From details: "Malware", "Malware\_Attacks" | search (Malware\_Attacks.dest\*"10.11.36.28" OR dest\*"10.11.36.28") | table dest src url

5 events (3/26/18 2:00:00:000 AM to 3/26/18 10:00:00:000 AM) No Event Sampling

Events Patterns Statistics (5) Visualization

20 Per Page Format Preview

dest	src	url
10.11.36.20	10.98.200.43	http://www.malicious-domain3.ru/victim/malicious_8.exe
10.11.36.20	10.11.36.24	http://www.2ndm.net/4152576/ATT_Top_malicious_360x250_vt_richload.swf
10.11.36.20	10.11.36.36	http://www.assassins.com/033c0f5ee-423b-4899-9fac-c873ee2553f.swf
10.11.36.20	10.98.200.43	http://www.malicious-domain1.com/v1/Zombac.exe
10.11.36.20	10.11.36.17	http://www.usuuu.com/web/en-US/content/show/220105050794224_030222587644953_malicious_728x90.swf
10.11.36.20	10.159.199.89	http://subscription-assets.fticons/yyyyy/n/1016434.htm?pa_id=333333

On the page of results, you see a number of common download requests. The `.swf` file represents shockwave flash content. Because shockwave is a commonly exploited framework used to run malicious code or exploits, review the relevant fields that describe a shockwave download.

## Find an exploited host

On the table of results, select a `src` field in an event referencing a downloaded shockwave file.

1. Click the `src` field.
2. Select **New search**.

A new browser window opens to a search dashboard and begins to search on the selected `src` field over the time range.

**New Search**

Save As Close

src="10.179.288.152"

10 of 2,042,053 events matched. No Event Sampling

Events (5) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Download

1 hour per column

Ver 28, 1918 5:00 AM

List Format 20 Per Page

Time	Event
3/28/18 6:59:18.000 AM	Mar 28 06:59:18 smart-actetch.com Mar 28 06:59:18 itsec smart[18774]: [1-882:6] WEB-CGI calendar access [Classification: Attempted Information Leak] [Priority: 22: (TOP) 18 179.288.152:2882 -> 192.168.1.191:80 host = 1270.01 source = evergreen sourcetype = smart
3/28/18 9:40:53.000 AM	Mar 28 09:40:53 smart-actetch.com Mar 28 09:40:53 itsec smart[18774]: [1-3486:3] WEB-MSVC SSLv3 invalid data version attempt [Classification: Attempted Denial of Service] [Priority: 23: (TOP) 18, 179.288.152:5573 -> 192.168.1.12:443 host = 1270.01 source = evergreen sourcetype = smart
3/28/18 9:32:46.000 AM	rec_type=582 rec_type_sip=7F10.00 MALWARE EVENT event_sec=1622043866 session=xxx.yyyzzz.com connection_instance=11 connection_counter=1413 connection_time=1622043866 sr c_ip=10.179.288.152 dest_ip=10.11.36.4 disposition=Neutral action="Malware Cloud Lookup" detection=Unknown sha256=abce158b1bd328289f9f31afdb83f35cab8d72f3a79d79e1d4b 72737 file_type=SW file_name=ATT_Top_malicious_360x250_v1_base.swf file_size=8796 direction=Download app_protocol=HTTP user=usr4 uri=http://au16b/cc/688/new signature="" s rc_port=6172 dest_port=88 ip_protocol=TCP policy=48407686-3f81-11e3-bdfe-9b8b233fe4b3 src_ip.country=unknown dest_ip.country="united states" web_app=Shockwave client_app=ief as host = 1270.01 source = evergreen sourcetype = ciscooutbase
3/28/18	date="2018-03-28" time="06:34:37" time-taken="1" c-ip="10.179.288.152" cs-username="" cs-auth-group="" s-exception-id="dns_unresolved_hostname" src-filer-result="DENIED" c

Examine the `url` and `file_name` fields for the host.

- 
- The screenshot shows the Splunk Search interface. At the top, the search bar contains the query `url="18.179.200.152" | table url file_name`. Below the search bar, the results are displayed in a table with columns `url` and `file_name`. The first result is `http://10.175.163.15/en-US/api/unix/_raw/services/ssh/ssh/sample_aml_examples/statistics/logs_2k.png` with `file_name` `ATT_Top_malicious_300x250_v1_base.swf`. The second result is `http://swabb.cc/ccdd/tee` with `file_name` `ATT_Top_malicious_300x250_v1_base.swf`. The third result is `http://psw-netsec-01.internal.cacheflow.com/CentErros?url=200Con%20Systems%20Internal.crl` with `file_name` `ATT_Top_malicious_300x250_v1_base.swf`. The fourth result is `http://psw-netsec-01.internal.cacheflow.com/CentErros?url=200Con%20Systems%20Internal.crl` with `file_name` `ATT_Top_malicious_300x250_v1_base.swf`. The fifth result is `http://psw-netsec-01.internal.cacheflow.com/CentErros?url=200Con%20Systems%20Internal.crl` with `file_name` `ATT_Top_malicious_300x250_v1_base.swf`. The sixth result is `http://www.pool.fnyw/ATT_Top_malicious_300x250_v1_base.swf` with `file_name` `ATT_Top_malicious_300x250_v1_base.swf`.

- As you review the results, you can see that a number of executable files were downloaded from the same domains.

### ***Find additional affected hosts***

1. Click the `url` field.
2. Click the icon next to **New search**.

**New Search**

url="http://aa/bbb/cc/c/cc/ddd/eee/"

19 events 3/28/18 2:00:00:000 AM to 3/28/18 10:00:00:000 AM No Event Sampling

Events (19) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Disabled 1 hour per column

List Format 20 Per Page

	Time	Event
SELECTED FIELDS	3/28/18 9:32:40:000 AM	rec_type=982 rec_type_similar="731E103 MALWARE EVENT" event_seq=1522432996 sensor=xxx.yyyzzz.com connection_instance=1 connection_counter=14413 connection_time=1522432996 s_ip=18.179.200.152 dest_ip=11.36.4 disposition=Neutral action="Malware Cloud Lookup" detection=known sha256=a8e15b012dc383816f931afdc034751c4d98d72f7a1b44673731 File_type=64 File_name=IT_16g_malware_386x386_v1_Java.swf File_size=6766 direction=Outbound app_proto=HTTP user-agent=ur-http://aa/bbb/cc/c/cc/ddd/eee/ signature="a_rn_gert71722 dest_port=80 ip_proto=TCP policy=46427386-381-1cd3bf-8a9230f4e43 src_ip.country=usname=dest_ip.country="United States" web_app=showware client_app=leaf os=
INTERESTING FIELDS	3/28/18 9:32:07:000 AM	rec_type=982 rec_type_similar="731E103 MALWARE EVENT" event_seq=1522432987 sensor=xxx.yyyzzz.com connection_instance=14 connection_counter=13608 connection_time=1522432987 s_ip=18.11.36.46 dest_ip=11.36.4 disposition=Neutral action="Malware Cloud Lookup" detection=unknown sha256=abe1581dc5383816f931afdc034751c4d98d72f7a1b44673731 File_type=64 File_name=Java2008811_281380x408647281_malware_386x386_v1.mfx File_size=6766 direction=Outbound app_proto=HTTP user-agent=ur-http://aa/bbb/cc/c/cc/ddd/eee/ signature="a_rn_gert71722 dest_port=80 ip_proto=TCP policy=46427386-381-1cd3bf-8a9230f4e43 src_ip.country="United States" dest_ip.country="United States" web_app=showware client_app=leaf os=
	3/28/18	rec_type=982 rec_type_similar="731E103 MALWARE EVENT" event_seq=152233972 sensor=xxx.yyyzzz.com connection_instance=1 connection_counter=14413 connection_time=152233972

## Widen the time range to broaden the search

1. Click **Date time range**.
2. Select the **Last 24 hours** option and click **Search**.

You can see that the total count of events reaching out to this domain over the last 24 hours is high.

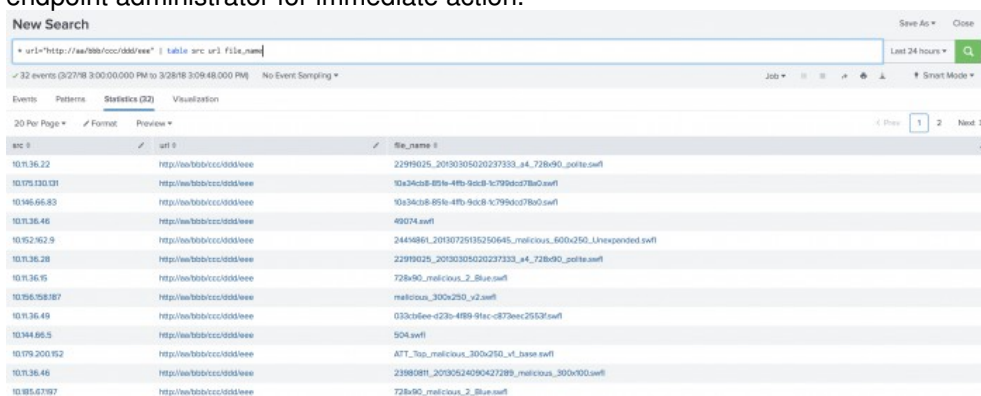
3. Review the `src` field on the field picker to identify a count of the unique hosts attempting a connection to this domain. A number of hosts will require active scanning for malware. A report of all hosts receiving downloads from this domain is a useful resource.

## Create reports of the results

Review the data in a table format.

1. Use the search bar to add `| table src url file_name` to the end of the existing search string.
2. Click **Search**.

The results show a list of potentially infected hosts including suspicious file names that can be delivered to the endpoint administrator for immediate action.

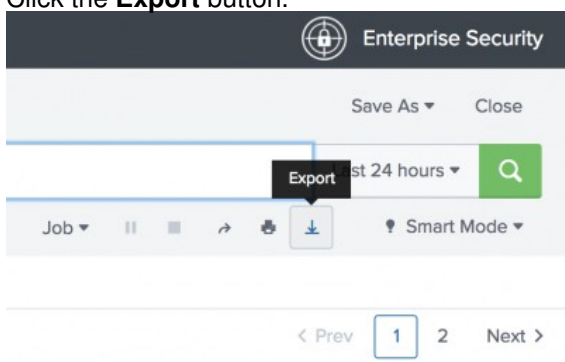


The screenshot shows the 'New Search' interface with the search string `* url="http://ea/bb/cc/dd/eee" | table src url file_name`. The results are displayed in a table with columns: `src`, `url`, and `file_name`. The table contains 10 rows of data, including IP addresses and file names like `229f9025_20130305020237333_s4_72b90_pofile.swf`.

src	url	file_name
10.11.36.22	http://ea/bb/cc/dd/eee	229f9025_20130305020237333_s4_72b90_pofile.swf
10.175.130.131	http://ea/bb/cc/dd/eee	10c34c8-85fe-4fb-9dc8-1c79bdc078a0.swf
10.146.66.83	http://ea/bb/cc/dd/eee	10c34c8-85fe-4fb-9dc8-1c79bdc078a0.swf
10.11.36.46	http://ea/bb/cc/dd/eee	49074.swf
10.152.162.9	http://ea/bb/cc/dd/eee	244f86f1_20130725135250645_malicious_600x250_Unexpected.swf
10.11.36.38	http://ea/bb/cc/dd/eee	229f9025_20130305020237333_s4_72b90_pofile.swf
10.11.36.15	http://ea/bb/cc/dd/eee	72b90_malicious_2_blue.swf
10.156.158.187	http://ea/bb/cc/dd/eee	malicious_300x250_v2.swf
10.11.36.49	http://ea/bb/cc/dd/eee	033cb6ee-c23b-4b89-9fec-c873ec2553f.swf
10.344.66.5	http://ea/bb/cc/dd/eee	504.swf
10.179.200.152	http://ea/bb/cc/dd/eee	ATT_Top_malicious_300x250_v1_base.swf
10.11.36.46	http://ea/bb/cc/dd/eee	229f9025_20130524090427289_malicious_300x100.swf
10.185.67.197	http://ea/bb/cc/dd/eee	72b90_malicious_2_blue.swf

You can export the results to place into a report or an email attachment.

3. Click the **Export** button.



4. Update the **File Name** field and save the results in a `.csv` format.
5. Click **Export** to download the results.
6. (Optional) Click **Save As** and select **Report** to save the report.
7. Fill in the required fields, and write a summary of the report for the **Description** field.
8. Click **Save** to write the report to the search head. The report is private, and available only to the creator by default.

## Update the notable event

Before you perform any additional analysis, update the notable event on the **Incident Review** dashboard. Record any objects or reports that are created, and other actions required to process and close the notable event.

Use the report results for reference and investigation. You can deliver the `.csv` of hosts and file names to the team monitoring the endpoints.

## Malware discovery summary

Using the data provided by the proxy server, Splunk Enterprise Security created notable events when hosts requested downloads from a suspicious domain. The notable events provided a starting point for investigation and included the most relevant fields to examine. By sorting the data and pivoting on those fields, an analyst generated a collection of reports that exposed the internal hosts involved, domains that might be blocked, and common file names that the malware runs as. As the remediation begins, the investigator has all of the critical information to act on the threat.

## Use DNS data to identify malware patient zero

Malware outbreaks can cripple an organization's computer systems. Quickly identifying "patient zero" allows you to readily contain a malware outbreak, eliminate the malware from that machine while preventing reinfection, and learn more about the application and/or files that delivered the malware. This use case walks you through using Splunk Enterprise Security and DNS (domain name system) data to identify patient zero in a malware outbreak in your environment.

## Prerequisites

This use case relies on the following data sources, ingested into the Splunk platform in compliance with the Splunk Common Information Model:

- Asset information in the asset lookup. See Add asset and identity data to Splunk Enterprise Security in *Administer Splunk Enterprise Security*.
- Endpoint anti-malware logs normalized to the Malware CIM data model. For example, Trend Micro OfficeScan server data, which can be added to Splunk Enterprise Security using TA-trendmicro, included with ES. See Install and deploy add-ons in the *Installation and Upgrade Manual*.
- DNS lookup data normalized to the Network Resolution CIM data model. For example, DNS queries collected by Splunk Stream. See Install and deploy add-ons in the *Installation and Upgrade Manual* for details on integrating Enterprise Security with Splunk Stream.
- Web surfing activity logs normalized to the Proxy object of the Web CIM data model.

## Assess the current state of security incidents

Review notable events identified by Splunk Enterprise Security to see the current state of threats in your environment.

1. Log in to Splunk Enterprise Security and view the **Incident Review** dashboard.
2. Filter the notable events by urgency, viewing only the **High** and **Critical** events in the **Endpoint** security domain.
3. Choose one of the **High or Critical Priority Host With Malware Detected** events to investigate.
4. Open the event details. The malware **Signature** is **TSPY\_FAKEMS.C**, a virus definition from TrendMicro.
5. Perform a **Notable Event Search** on the signature using the field actions.  
The notable event search opens **Incident Review** scoped to events with the **TSPY\_FAKEMS.C** malware signature. One of the events notes an **Outbreak Detected Of TSPY\_FAKEMS.C**. That event is created when more than 10 hosts have a malware infection from that signature.
6. After identifying the outbreak, open an investigation to share with other analysts. Select the relevant notable events and click **Add to Investigation**.
7. Name the investigation something like **Malware outbreak of TSPY\_FAKEMS.C** and add other analysts as collaborators so they can see your investigation progress.
8. The tier one analysts begin cleaning up the malware outbreak.
  1. Assign the notable event for an infected host to a tier one analyst.
  2. The tier one analyst takes a forensic image of the hard drive, then has the machine reimaged.
  3. As the cleanup progresses, the tier one analyst updates the notable event statuses accordingly.
9. The tier two analyst continues investigating the malware outbreak in depth.

## Perform external research on the malware signature

External research can help you determine additional indicators of compromise specific to this malware signature, or learn about aliases and threat groups associated with the malware.

1. The tier two analyst investigates and discovers that the malware signature **TSPY\_FAKEMS.C** is an alias for another malware signature that Microsoft identifies as **Trojan:Win32/Foosace.J!dha**.
2. Further research on the **Win32/Foosace** malware shows that it is associated with an advanced adversary identified by Microsoft as **STRONTIUM**.
3. You determine that the **STRONTIUM** group is known to use the `malwarecheck.info` and `softupdates.info` domains for command and control operations.
4. Investigate those domains to see if they appear in your environment.

## Investigate the outbreak further with DNS data

Look for DNS requests to the command and control domains. Hunters often use the DNS dashboards included in Enterprise Security "Protocol Intelligence" for this purpose.

1. Select **Security Intelligence > Protocol Intelligence > DNS Search**.
2. Type the wildcard domain `*malwarecheck.info` in the **Query** filter.
3. Select a time range of **Last 30 days**.
4. Click **Submit** to search.
5. The search results show DNS requests for the domain `malwarecheck.info`.
6. Open **Search** and run the following search to determine if DNS queries for `malwarecheck.info` are correlated with the malware outbreak.

```
tag=dns query=malwarecheck.info [search tag=malware tag=attack signature="TSPY_FAKEMS.C" | eval src=dest | fields src]
```

The search results confirm that endpoint hosts associated with the malware outbreak are infected with malware and also performing queries to the `malwarecheck.info` domain that operates as a command and control server.

7. Use the **Investigation Bar** to add the search to your investigation from your **Action History** in the **Investigator Journal**. This will allow other analysts to perform the same search in the future.



## Locate patient zero with DNS data

Endpoint antivirus products can fail to identify malware infections, but now you know that a DNS query to the `malwarecheck.info` domain is an indicator of compromise. Report on DNS queries to this domain to determine the earliest signs of infection in your environment, even for hosts where the antivirus product did not identify an infection.

1. In the **Search** dashboard, run a new search to determine which machines, other than those with the endpoint antivirus alerts, are performing DNS queries for the `malwarecheck.info` domain.

```
tag=dns query=malwarecheck.info NOT [search tag=malware tag=attack signature="TSPY_FAKEMS.C" | eval src=dest | fields src] | stats count by src]
```

The search results show activity from a single host performing a DNS lookup to the `malwarecheck.info` domain hours before the first antivirus alert.

2. Add the event that shows this activity from the single host to your investigation using the event actions of the event.
3. Add the search to your investigation from your **Action History**.
4. Add a note to the investigation that the infected machine performed DNS queries for the `malwarecheck.info` domain.

## Complete your investigation and remediate the malware outbreak

Identify patient zero and take remediation steps. After you identify DNS queries to the `malwarecheck.info` domain as an indicator of compromise, you know that the first machine to make contact with that domain was the originator of the malware outbreak: Patient Zero.

1. Add a note to your investigation with your findings.
2. Advise the tier one analysts to take a forensic image of the machine and wipe it to remove the malware infection.

## Summary

To identify patient zero in the malware outbreak in your environment, you started by reviewing current notable events for malware. After identifying a troublesome malware signature, you performed additional research to determine additional indicators of compromise to help identify further infected hosts. Then you used DNS data to search for DNS queries that indicated command and control activity and located a host that made a query to the command and control host before any other hosts were infected. To contain the outbreak you took action to contain that host and the malware, and completed your investigation.

## Investigating potential zero-day activity

Detect possible zero-day malware activity in your organization's network with Splunk Enterprise Security. This scenario walks you through detecting malware activity that could indicate a zero-day exploit, and using the investigation results to improve your threat detection.

A sophisticated attack using zero-day malware could begin when a spearphishing email containing malware is sent to a target recipient within an organization.

1. The target opens the email and the malicious contents compromise their computer with malware.
2. After infecting the computer, the malware signals the attacker that it is ready for command and control.

3. Splunk Enterprise Security identifies malware on the computer, and security analysts begin to investigate.
4. Security analysts perform host-based forensics on the machine and identify malware that uses a zero-day exploit.
5. Security analysts use the forensic results to identify common indicators of the threat, such as malware hashes and malicious domain lists.
6. Security analysts add the malware threat indicators to Splunk Enterprise Security.

## Required data sources

This use case relies on the following data sources that have been properly ingested into the Splunk platform in compliance with the Splunk Common Information Model.

- Asset information in the asset lookup. See Add asset and identity data to Splunk Enterprise Security in *Administer Splunk Enterprise Security*.
- One or more threat intelligence feeds. Splunk Enterprise Security has several threat intelligence feeds included. See Configure the threat intelligence sources included with Splunk Enterprise Security in *Administer Splunk Enterprise Security*.
- DNS (domain name system) data normalized to the Network Resolution CIM data model. For example, DNS queries collected by Splunk Stream. See Install and deploy add-ons in the *Installation and Upgrade Manual* for details on integrating Enterprise Security with Splunk Stream.
- Web surfing or Proxy logs normalized to the Proxy object of the Web CIM data model.
- Firewall activity logs normalized to the Network Traffic CIM data model.
- Active Directory (AD) logs normalized to the Authentication data model.
- Audit and system logs from database servers normalized to any of the relevant CIM data models, such as Databases, Change Analysis, or Authentication.

## Review risk behavior of hosts in your environment

Assess the risk posture of your environment to determine if hosts are displaying risky behavior that could pose a higher threat to your network than others.

1. Select **Security Intelligence > Risk Analysis** to open the **Risk Analysis** dashboard.
2. Review the **Risk Score By Object** to identify hosts with high risk scores.  
You notice the host `10.11.20.87` with a risk score of 800 and count of 16 events associated with it is one of the highest risk systems in your environment.
3. To see what types of sources are contributing to the increased risk for this host, review the **Recent Risk Modifiers**. You see a source of **Threat - Threat Activity Detected - Rule** which means that threat intelligence correlated with this host caused the host's high risk score.
4. To get a clearer picture of the overall risk posture for this system, filter the **Risk Analysis** dashboard on the `risk_object` host `10.11.20.87` over the **Last 30 days**.
5. A visual analysis of the **Risk Modifiers Over Time** in your environment shows a large number of risk modifiers for this host from several weeks ago and a resurgence of risk modifiers over the past couple days. You decide to investigate this pattern on the **Incident Review** dashboard to see what types of notable events are being generated for this host.

## Investigate the threat risk of a high-risk host

Investigate past notable events associated with the high-risk host to further assess the risk to your environment.

1. Open **Incident Review** and search for the `src=10.11.20.87` over the **Last 30 Days** to see what types of notable events are associated with this high-risk host.

2. You see multiple notable events associated with this host that were created and closed in the past, but no new notable events.
3. Expand the event details for a notable event for **High or Critical Priority Host With Malware Detected**. This host is tagged as a high or critical asset in your environment, indicating that it could hold sensitive data or is used by administrators.
  1. Review the **History** and click **View all review activity for this Notable Event** to see what actions analysts took when the machine was infected.
  2. If necessary, review your ticketing system to determine which malware-remediation steps desktop support took at the time of infection.
4. Expand the event details for another notable event, **Threat Activity Detected**. You see a **Destination** domain of micro\$oft[.]com, which seems suspiciously similar to Microsoft.com.
  1. You review the **Threat Description** and **Threat Group** to understand more about the domain and the threat it poses.
  2. Determine what others on the web are sharing about the domain. From the **Destination** field actions, select **Google micro\$oft[.]com**. Review the search results for reputable sources discussing activity associated with the domain.
  3. Return to the notable event and investigate the whois records for the domain. From the **Destination** field actions, select **Domain Dossier**. Review the domain owner, registrar, and registration date for suspicious values.
5. Return to Splunk Enterprise Security to continue investigating the domain. Select **Security Intelligence > Web Intelligence > New Domain Analysis** and search for the micro\$oft[.]com domain as a type of **Newly Seen**.
6. Based on the details you collect, because the domain is newly seen in your environment, the whois details indicate that it is newly registered, and threat activity is associated with the domain, you can conclude that the domain is likely malicious.

### ***Using Google searches to investigate threat risk***

Google may track searches using cookies and have data sharing policies that cannot be moderated by Splunk. Using Google search may expose sensitive information like IDs, internal adaptive directory names, and so on to third parties. Therefore, the option to use Google search in Enterprise Security is disabled by default.

However, you may choose to enable the Google search functionality by creating a workflow action using Splunk Web and navigating to **Settings > Fields > Workflow actions**. For more information on setting up workflow actions, see *Create workflow actions in Splunk Web*.

### **Open an investigation to track your work**

1. From the **Incident Review** dashboard, select the notable events that are relevant to your investigation and select **Add Selected to Investigation**.
2. Start a new investigation and name it **Malicious domain activity on host 10.11.20.87**.
3. Using the Investigation Bar, add your action history from the **Risk Analysis**, **Incident Review**, and **New Domain Activity** dashboards to the investigation from your Investigator Journal.
4. Add notes about the results of your Google search and **Domain Dossier** investigation steps, including links to relevant articles and a screenshot of the whois record.

### **Perform a forensic investigation on the host**

You determine that micro\$oft[.]com is a malicious domain. Perform a forensic investigation on the host to identify the zero-day malware that evaded the endpoint detection software. A forensic investigation can include steps for finding malicious dropper programs, similar malware, and mentions of command and control servers embedded in the files. After the forensic investigation is complete, collect information about the malware that can be used to identify it in the future.

Common criteria for identifying malware include queried IP addresses, domains, and MD5 file hashes of the malware files.

## Detect future threats from this zero day

Set up Splunk Enterprise Security to detect threats related to this malicious compromise in the future. Add the malware file hash and IP addresses to an existing local threat source in Splunk Enterprise Security in order to detect compromised hosts.

1. On the Enterprise Security menu bar, select **Configure > Content > Content Management**.
2. Find the **Local IP Intel** lookup and click the name of the lookup to open it.
3. Type a description of "Potential zero day malware IP addresses."
4. Add the IP address indicators to the lookup. Right-click and select **Insert Row Below** to add new rows as needed.
5. (Optional) Type a numeric **Weight** to change the risk score for objects associated with indicators on this threat intelligence source.
6. Click Save.

Repeat these steps for the **Local File Intel** lookup to add the malware file hashes.

## Identify additional zero-day compromises

Use the newly-added threat indicators to identify previous compromises related to this zero-day attack.

1. Open the **Threat Activity** dashboard.
2. Filter the dashboard to show only threats with a **Threat Group** of **local\_ip\_intel** or **local\_file\_intel**.
3. Choose a time range to search over and click **Submit**.
4. Review the results in the **Threat Activity Over Time** panel. Investigate threat results further in the **Threat Activity Details** panel.
5. Use the `threat_match_value` to identify which indicator of compromise is associated with the host.

Continue your investigation with the new host information, or look for additional hosts associated with more **Threat Group** sources that you created.

## Summary of zero-day investigation

To identify zero-day malware activity, start by reviewing the high-risk hosts in your environment on the Risk Analysis dashboard. Review the past malware and threat activity associated with those hosts on the Incident Review dashboard and investigate suspicious domains with the field actions and the New Domain Analysis dashboard. Track your work in an investigation and perform a forensic investigation on the host to gather valuable file hashes and determine if the malware activity and suspicious domain are associated with a zero-day vulnerability. Finally, use the results of the forensic investigation to add intelligence to the Threat Intelligence framework in Splunk Enterprise Security and track down future and past compromises associated with this zero-day activity.

# Identify suspicious activity

## Using Enterprise Security to find data exfiltration

Enterprise Security provides statistics and interesting events on security domain specific dashboards. Using the dashboards together, you can build a workflow for investigating threats by reviewing the results, isolating the events that require attention, and using the contextual information provided to drill down into the issue.

This scenario provides an example of detecting potential data exfiltration involving the domain `dataker.ch`. Use this scenario as an example of how to perform a similar investigation in your own environment.

### Prerequisites

- Verify that a Splunk platform instance with Splunk Enterprise Security is installed and configured.
- Verify that these CIM data models contain data: Network Traffic, Network Resolution, Email, and Web. Data sources include web proxy or next-gen firewall (NGFW) logs, Splunk Stream, Bro, Exchange, Sendmail, and DNS logs.
- Verify that the Splunk App for Stream is installed and the Splunk Stream add-on is configured.

### Start with Incident Review

Enterprise Security includes correlation searches that report on suspicious activity across security domains. Some common paths for data exfiltration are tracked by the correlation searches.

Correlation search	Description	Data Models : Sources
Prohibited Port Activity Detected	Detects the use of ports that are not approved. Unapproved port detection is useful for detecting the installation of new software (potentially unapproved) or a successful compromise of a host (such as the presence of a backdoor or a system communicating with a botnet).	Sources that populate the Network Traffic Data Model: Splunk Stream, firewall traffic, Bro, etc.
High Volume Email Activity to Non-corporate Domains by User	Alerts on high volume email activity by a user to non-corporate domains.	Sources that populate the Email data model: Splunk Stream, Bro, Exchange, Sendmail, etc.
Host Sending Excessive Email	Alerts when a host not designated as an e-mail server sends excessive e-mail to one or more target hosts.	Sources that populate the Email data model: Splunk Stream, Bro, Exchange, Sendmail, etc.
Excessive DNS Queries	Alerts when a host starts sending excessive DNS queries	Sources that populate the Network resolution data model: Splunk Stream, Bro, Microsoft DNS, bind, Infoblox, etc.
Substantial Increase In Port Activity	Alerts when a statistically significant increase in events on a given port is observed.	Sources that populate the Network Traffic Data Model: Splunk Stream, firewall traffic, Bro, etc.
Web Uploads to Non-corporate Sites by Users	Alerts on high volume web uploads by a user to non-corporate domains.	Sources that populate the Web data model: web proxy, next-gen firewall (NGFW) logs, etc.
Personally Identifiable Information Detected	Detects personally identifiable information (PII) in the form of payment card data in machine-generated data. Some systems or applications inadvertently include sensitive information in logs thus exposing it in unexpected ways.	No specific data model: system log files, application log files, network traffic payloads, etc.

Correlation search	Description	Data Models : Sources

### ***Assign notable events for investigation***

1. From the Enterprise Security menu bar select **Incident Review**.
2. Use the **Search** option on the Incident Review dashboard to look for a specific notable event.
3. (Optional) Reprioritize the notable event by changing the **Urgency** before assigning it.
4. Assign a notable event to an analyst for review and investigation.

While analysts review any notable events representing possible data exfiltration attempts, you can investigate other dashboard panels for signs of anomalous behavior.

## **Review the User Activity dashboard**

The User Activity dashboard displays panels representing common risk-generating user activities.

1. On the Enterprise Security menu bar, select **Security Intelligence > User Intelligence > User Activity**.
2. View the key indicators NonCorp Web Volume and NonCorp Email Volume for evidence of suspicious changes over the last 24 hours.

### ***Non-corporate Web Uploads***

Examine the **Non-corporate Web Uploads** panel to identify suspicious activity involving data being uploaded to external locations. Also look for unknown users or credentials, **Watchlisted** identities, and large data transfers indicated in the **size** column.

### ***Non-corporate Email Activity***

Review the **Non-corporate Email Activity** panel to look for suspiciously large email messages to addresses outside the organization. Also look for uncommon user names, **Watchlisted** identities, and large messages or a large number of smaller messages.

If suspicious activity is found, create a notable event and assign it to an analyst for investigation. Continue to look at other dashboards for indications of compromise.

## **Review the Email Activity dashboard**

The Email Activity dashboard displays metrics relevant to the email infrastructure.

1. On the Enterprise Security menu bar, select **Security Intelligence > Protocol Intelligence > Email Activity**.

### ***Top Email Sources***

Examine the **Top Email Sources** panel to find surges in email counts by IP address. Look for unfamiliar addresses sending a large numbers of messages. Use the sparklines to identify consistent spikes of activity from a host, as it can be an indicator of automated or scripted activity.

On a panel with dense search results and many fields, use the **Open in Search** icon in the lower right corner to open the results in a separate search view.

## Large Emails

Review the **Large Emails** panel and look for emails larger than 2MB that were sent to internal or external addresses.

Selecting a record on either panel will drill down into the **Email Search** dashboard, where you can continue to investigate the email traffic. If suspicious activity is found, create a notable event and assign it to an analyst for investigation.

## Review the DNS Activity dashboard

The DNS Activity dashboard displays metrics relevant to the DNS infrastructure.

1. On the Enterprise Security menu bar, select **Security Intelligence > Protocol Intelligence > DNS Activity**.

### Queries Per Domain

Examine the **Queries Per Domain** panel to find unfamiliar domains receiving a large number of queries from internal hosts. You see there are a large number of DNS queries for subdomains of "dataker.ch", and choose to examine the DNS traffic as a first step. Selecting a record on the **Queries Per Domain** panel will drill down to the DNS Search page.

## Follow the drilldown to the DNS Search dashboard

A new browser window opens to the DNS Search dashboard and begins to search on the selected domain over the time range. You determine that the `src_ip` of all of the queries is in the corporate desktop range. Use the *Source* filter to restrict the search to one subnet. Looking at the events, you see a large amount of traffic that includes base64 encoded subdomains.

Utilizing DNS queries with encoded information is a known method to exfiltrate data. But you do not know if the work is being initiated by malware on the asset of an innocent user, or as an insider threat. Reviewing the asset might provide some clarity.

1. Select a raw event in the **DNS Search** dashboard,
2. Use the arrow on the left to expand the field results.
3. Find the `src` field and open the **Actions** menu.
4. Select **Asset Center**.

## Examine the asset in Asset Center

The Asset Center dashboard reports on known values for a specified asset. The asset responsible for sending the encoded DNS queries is reported as a standard user desktop. As the asset details did not provide any additional clues, you choose to continue the investigation as an insider threat. You expect to find malware running on the asset as the tool used to exfiltrate data, but tracking the user's activity is an appropriate preemptive step. Let's create a new notable event to track our investigation.

## Create a new notable event

On the Enterprise Security menu bar, open **Configure > Incident Management** and select **New Notable Event**.

Field	Details
Title	Possible data exfiltration: <Asset>, <User>, <Date>

Field	Details
Security Domain	Threat
Urgency	Critical. This investigation is a top priority.
Owner	<ANALYST>
Status	In Progress
Description	There might be data exfiltration via DNS. Begin enhanced monitoring of <User>, their access controls, and the <Asset>. Notify the SecOps Manager and HR regarding possible insider threat.

After updating and assigning the notable event, monitor the network for encoded DNS data.

## Use Splunk Stream to capture DNS

Monitoring the network traffic to determine if DNS queries include encoded data requires a tool to monitor and sort the data before feeding the results into Enterprise Security.

Splunk offers About Splunk Stream as the preferred method of capturing encoded DNS traffic on the network.

Build a search that utilizes Stream results. Begin by using the Deployment Server to install the Stream Add-on onto the asset. The add-on monitors the network traffic and sends the DNS data to Enterprise Security for evaluation.

### *DNS search for encoded data*

On the Enterprise Security menu bar, open **Search** and select **Search**.

Now that the Stream add-on is capturing the DNS data, we need a search to find Base64 encoded content in DNS queries. The goal is to examine the DNS query field of the data stream to find subdomain streams that contain only Base64 valid characters.

```
sourcetype="stream:dns" (message_type=RESPONSE OR message_type=TXT) | rex field=query "(?<subdomain>.*?)\..*"
| regex
subdomain="^(([A-Za-z0-9+]/]{4})+)$|^([A-Za-z0-9+]/]{4})+((([A-Za-z0-9+]/]{2}[AEIMQUYcgkosw048]=)|([A-Za-z0-9+]/[AQgw]=)))*$"
| stats count by subdomain
```

The query can result in false positive matches if the subdomain contains a number of characters divisible by 4, and contains only alphanumeric characters. A visual inspection of the search results by an analyst will be required.

## Data exfiltration summary

The notable events generated by Splunk Enterprise Security provided a starting point for the investigation by detecting common sources of suspicious behavior. The User and Email Activity dashboards expose recurring or large data transfers to known and unknown domains. The Stream add-on allows the capture and filtering of network data from internal hosts. By using the tools and searches provided with ES, an investigator can check common data exfiltration paths and establish active monitoring of compromised machines.

## Monitor privileged accounts for suspicious activity

Use Splunk Enterprise Security to identify, search, and report on the activities of users with privileged accounts and help protect your environment from malicious attackers. Privileged accounts are user or system accounts with elevated



privileges, such as users with Domain Administrator rights or root privileges. An attacker that gains access to privileged user credentials can take control of an organization's infrastructure to modify security settings, exfiltrate data, create user accounts, and more. If an attacker gains privileged account access credentials, their activities appear more legitimate and become harder to detect. Attackers attempt to gain access to privileged accounts by using social engineering techniques, sending spear-phishing messages, using malware, or "passing the hash" attacks.

## Prerequisites

- A Splunk platform instance with Splunk Enterprise Security installed and configured.
- An identity lookup that contains user accounts with a category field of `category=privileged`. Use this search to view the user accounts:

```
| datamodel "Identity_Management" High_Critical_Identities search |stats count by All_Identities.identity
```

## Identify privileged user accounts

In order to monitor privileged account activity and identify suspicious actions that could indicate an adversary moving around in the network, define privileged accounts in your identity lookup using the **Category** field. You can use a search with the `ldapsearch` command to populate the `identity.csv` with privileged users.

1. Create an identity lookup that includes users who have **Domain Admin** privileges or who are in the **VIP** group.
2. Modify the example search below for your specific environment, or create your own.

This example search takes users with a group membership of **Domain Admins** or **VIPs** and adds them to the privileged category. Depending on your environment, you can modify the search to focus on specific organizational units (OUs) rather than group membership.

```
| ldapsearch domain=Acme search="(&(objectclass=user)(!(objectClass=computer)))" | eval suffix="" | eval priority="medium" | eval category="normal" | eval watchlist="false" | eval endDate="" | eval category=case(match(memberOf, "(?i)^.*?Domain\sAdmins?.+"), "privileged", match(memberOf, "(?i)^.*?VIP?.+"), "privileged") | table sAMAccountName, personalTitle, displayName, givenName, sn, suffix, mail, telephoneNumber, mobile, manager, priority, department, category, watchlist, whenCreated, endDate | rename sAMAccountName as identity, personalTitle as prefix, displayName as nick, givenName as first, sn as last, mail as email, telephoneNumber as phone, mobile as phone2, manager as managedBy, department as bunit, whenCreated as startDate |outputlookup my_identity_lookup
```

See more about the **Category** lookup field in [Format an asset or identity list as a lookup in Splunk Enterprise Security in Administer Splunk Enterprise Security](#). To add a new identity lookup, see [Configure the new asset or identity list in Splunk Enterprise Security in Administer Splunk Enterprise Security](#).

## Review current privileged account activity

Splunk Enterprise Security includes two reports that depict privileged user activity. Review them to determine the current state of privileged account usage in your environment.

1. On the Splunk Enterprise Security menu bar, select **Search > Reports**.
2. In the **filter**, type the word `privileged` to locate the privileged user reports.
3. Click the **Access - Privileged Account Usage Over Time** report to open it and review the total count of events over time that included a privileged user account to see the pattern of normal privileged account usage and identify unusual or unexpected activity.
4. Click the **Access - Privileged Accounts In Use** report to open it and review privileged accounts in use during the selected time frame, as well as how many times the accounts have been used to log in to identify rarely used accounts that suddenly show bursts of activity.

You notice that the domain admin account **bob** has logged in 100,000 times in the last 24 hours.

5. Select **Configure > Incident Management > New Notable Event** to create a notable event for a tier one analyst to investigate.
6. In the new notable event, type a title of **Privileged user bob has logged in 100,000 times in 24 hrs.**
7. Set the **Urgency to Critical.**
8. Assign the notable event to a tier one analyst.
9. The tier one analyst investigates **bob** and determines that it is an administrative account used to run scripts, so the authentications are legitimate.

## Set up a dashboard to monitor privileged accounts

To allow the security analysts to more easily review and monitor privileged user accounts, create a privileged account dashboard from the two reports.

1. Select **Search > Reports** and filter on **privileged** to see the privileged account reports.
2. Click the title to view the **Access - Privileged Accounts In Use** report.
3. Click **Add to Dashboard** and select a **New** dashboard.
4. Type a **Dashboard Title** of **Privileged Accounts**. The Dashboard ID is set automatically.
5. For **Dashboard Permissions** select **Shared in App**.
6. Type a **Panel Title** of **Privileged Accounts in Use**.
7. For **Panel Powered By** select **Report**.
8. For **Panel Content** select **Statistics** to view the raw data rather than a graph.
9. Click **Save** and **View Dashboard** to view your creation.
10. Add the **Access - Privileged Account Usage Over Time** report to the new dashboard using the same steps, but select an **Existing** dashboard of **Privileged Accounts** instead of creating a new dashboard.

After you create the dashboard, make it easy to find by adding it to the Splunk Enterprise Security menu bar.

1. Select **Configure > General > Navigation** to view the navigation editor.
2. Locate the **Identity** security domain navigation collection.
3. Click the **Add View** icon and select the **Privileged Accounts** dashboard.
4. Click **Save** to save the dashboard navigation location.
5. Click **Save** to update the menu bar.

## Monitor privileged accounts with notable events

In the case of **bob**, you manually created a notable event in order for a tier one analyst to investigate the account activity. By using a correlation search, you can automate privileged account activity monitoring and generate alerts as notable events. See Create correlation searches in Splunk Enterprise Security in *Administer Splunk Enterprise Security*.

You want to alert tier one analysts when a privileged user account makes concurrent access attempts to the same application from different hosts. This search creates notable events to identify potentially shared privileged credentials. This example uses a modified version of the existing correlation search, **Concurrent Login Attempts Detected**, to do this.

1. Select **Configure > Content > Content Management**.
2. Select **Create New Content > Correlation Search**.
3. Type a **Search Name** of **Shared Privileged Account Credentials**.
4. Use the following search as your **Search**:

```
| datamodel "Identity_Management" High_Critical_Identities search | rename All_Identities.identity as "user" | fields user | eval cs_key='user' | join type=inner cs_key [| tstats `summariesonly`
```

```
count from datamodel=Authentication by
_time,Authentication.app,Authentication.src,Authentication.user span=1s |
`drop_dm_object_name("Authentication")` | eventstats dc(src) as src_count by app,user | search
src_count>1 | sort 0 + _time | streamstats current=t window=2 earliest(_time) as
previous_time,earliest(src) as previous_src by app,user | where (src!=previous_src) | eval
time_diff=abs(_time-previous_time) | where time_diff<300 | eval cs_key='user']
```

5. Type a **Cron Schedule** for how often you want the search to run.
6. Select **Add New Response Action** and select a **Notable**.
7. Type a **Title**, a **Description**, and other important fields for the notable event.
8. Click **Save**.

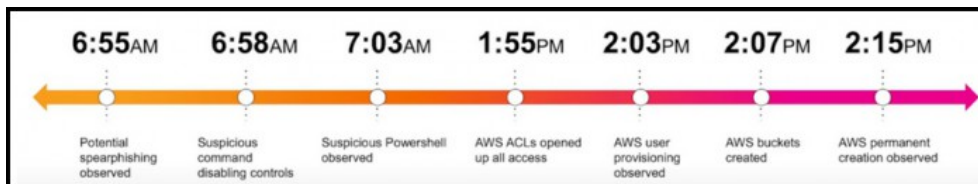
## Summary

You needed to monitor privileged account activity to identify suspicious activity indicating data exfiltration, lateral movement by an attacker, shared privileged credentials, and more. After configuring the identity data stored in Splunk Enterprise Security to categorize privileged users, you reviewed the two privileged account reports to identify any current users acting suspiciously. Then you created a dashboard to more easily review those reports in the future and keep a close eye on user accounts like **bob**. Finally, you set up a correlation search so that the tier one analysts would be notified of definitive suspicious activity such as concurrent login attempts from a privileged account.

# Isolate threats

## Isolate threats with risk alerting

Buttercup Games, a fictitious company, runs an e-commerce site to sell its products. Kay, the manager of the security operations center (SOC) at Buttercup Games, receives numerous notables during the course of a morning indicating various suspicious behaviors over a specific time period that may be a risk to his organization.



Previously, Kay requested Ram, a security analyst on his team, to use Splunk Enterprise Security to run correlation searches on all assets and identities to generate security events and create notables or risk alerts. However, correlation searches generated an excessive amount of notables and manually parsing through them to identify patterns was neither efficient nor effective for detecting security threats to Buttercup Games on time. High-fidelity notables were often suppressed and didn't get incorporated into the investigative story, creating visibility gaps.

This time, Kay asks Ram to use the risk alerting framework in Splunk Enterprise Security to dynamically adjust risk scores for assets and identities based on specific conditions. Dynamically adjusting risk scores allows Ram to automatically raise the risk scores associated with specific assets and identities by assigning these conditions as risk factors. Assigning risk factors helps to expose notables earlier for investigation. Therefore, Ram can prioritize suspicious behavior and mitigate risk by taking quick action on the risk event.

The risk alerting framework in Splunk Enterprise Security allows Kay and Ram to conduct higher value investigations through more streamlined and effective threat isolation. Ram leverages the risk alerting framework to explore the high volume and noisy endpoint data that Kay asked him to investigate. This use case describes how Kay, a SOC manager, and Ram, a security analyst, use risk scores and risk factoring to classify the notables based on risk level and map out the risk in their security environment by taking these steps.

1. [Assign risk scores to assets and identities](#)
2. [Generate notables using correlation searches](#)
3. [Add annotations to enrich correlation search results](#)
4. [Classify risk objects based on annotations](#)
5. [Add a risk message and a risk score to a notable](#)
6. [Adjust risk scores for specific objects](#)

Learn more

- Create risk objects
- Create risk factors
- Manage risk factors
- Use default risk factors

## Assign risk scores to assets and identities

Using Splunk Enterprise Security, Ram assigns risk scores to the assets and identities in his network environment. The risk scores show the relative risk of a device or user in the network environment over time and creates an extra layer of security-enriched data. The risk scores help to exponentially increase the number of detections because they let Ram calculate the risk within his environment posed by small events over time. Ram now creates more meaningful and higher fidelity alerts, called risk notables, which increase visibility and reduce overall risk. The Risk Analysis dashboard displays these risk scores and other risk-related information. Enterprise Security indexes all risks as events in the risk index.

Ram can add risk scores to a user, a system, or an object in multiple ways:

- Using a custom correlation search
- Specifying risk as an adaptive response action from the Incident Review page
- Adding an ad hoc risk entry from the Risk Analysis dashboard
- Assigning risk through a search

[Learn more](#)

[Create and adhoc risk entry.](#)

[Assign risk through a search](#)

## Generate risk notables using correlation searches

Ram configures a default correlation search in Enterprise Security to generate notables that match certain risk score thresholds or risk conditions and then, classifies them based on risk level.

Correlation searches can search for a conditional match based on the risk score assigned to the assets and identities. Assets and identities are the devices and user objects in the network environment. When the correlation search finds a match, it generates a risk alert as a notable event, a risk modifier, or both.

1. From the home page of Splunk Enterprise Security, Ram selects **Configure > Content > Content Management**.
2. Ram sorts the list of searches by Correlation Search, to view all existing correlation searches.
3. Ram clicks the default correlation search called **Risk Notable: Risk Threshold Exceeded For Risk Object Over 24 Hour Period**, which leverages the risk data model. The search opens in the **Edit Correlation Search** window. This default correlation search helps Ram to identify only those notables whose risk threshold has been exceeded within the previous 24 hours.

**Edit Correlation Search**  
[Back to Content Management](#)

**Correlation Search**

Search Name: Risk Notable: Risk Threshold Exceeded For Risk Object Over 24 Hour P

App: SA-AttributionDemo

UI Dispatch Context: None

Description: Risk Notable: Risk Threshold exceeded for an object within the previous 24 hours.

Mode: Guided Manual

Search

```

|from datamodel:"Risk.All_Risk"|search source="*- RR - *"
|lookup system_or_service_users_ignore user as risk_object|search NOT comment=*
|stats values(risk_object_type) as risk_object_type values(annotations.mitre_attack.mitre_tactic) as mitre_tactic dc(annotations.mitre_attack.mitre_tactic) as mitre_tactic_count values(annotations.mitre_attack.mitre_technique) as mitre_technique values(source) as source dc(source) as source_count sum(calculated_risk_score) as risk_score_sum values(threat_object_type) as threat_object_type min(_time) as _time by risk_object
|where risk_score_sum > 100
|rex field=source "\w+ - RR - (?<source_short>.*) - \w+ - Rule"
| eval severity=case(risk_score_sum<100,"low",
risk_score_sum<250,"medium",
risk_score_sum<500,"high",
risk_score_sum>=500,"critical")

```

- Using this correlation search, Ram classifies notables into various risk categories. If the risk score for an object exceeds 100 over the last 24 hours, the `risk_score_sum` value is greater than 100. If the risk score is less than 250, Ram classifies the notables in the medium risk category. If the risk score is less than 500, Ram classifies the notables in the high risk category. If the risk score is greater than or equal to 500, Ram classifies the notables in the critical risk category. Classifying the notables helps Ram to prioritize the investigation effort on the critical notables and minimize threat.
- Ram can also customize the Splunk Processing Language (SPL) of the correlation search to change specific conditions. For example, if Ram wants to identify risk objects that have a risk score threshold of 200 instead of 100 over the last 24 hours. Leveraging the risk data model and creating risk notables based on MITRE ATT&CK tactics and techniques allows Ram to search through risk events that created the notable.

Following is an example SPL search that Ram can customize to specify risk conditions and adjust risk scores:

```

|from datamodel:"Risk.All_Risk"|search source="*- RR - *"
|lookup system_or_service_users_ignore user as risk_object|search NOT comment=*
|stats values(risk_object_type) as risk_object_type values(annotations.mitre_attack.mitre_tactic) as mitre_tactic dc(annotations.mitre_attack.mitre_tactic) as mitre_tactic_count
values(annotations.mitre_attack.mitre_technique) as mitre_technique values(source) as source dc(source) as source_count sum(calculated_risk_score) as risk_score_sum values(threat_object_type) as threat_object_type min(_time) as _time by risk_object
|where risk_score_sum > 100
|rex field=source "\w+ - RR - (?<source_short>.*) - \w+ - Rule"
| eval severity=case(risk_score_sum<100,"low",
risk_score_sum<250,"medium",
risk_score_sum<500,"high",
risk_score_sum>=500,"critical")

```

In this SPL:

- The `lookup system_or_service_users_ignore` helps to focus the search to generate risk notables based on specific risk objects and ignore system or service accounts or users.
- The `stats` command calculates statistics based on specified fields and returns search results. This helps to identify the information that will be included in the risk notable to help the analyst.

- The `where` command specifies the constraint of the search and identify risk objects that have an aggregate risk score, which is greater than 100.
- The `rex` command extracts fields using regular expression. For example, here the `rex` command identifies the risk notable or risk rule based on its naming convention. `RR - (?<source_short>.*) - \w+ - Rule`. Example of the naming convention used by risk rules or risk notables in Splunk Enterprise Security: "RR-Access Additional Cloud Credentials in Azure-User" or "RR-Add User to Administrator Group in Azure-User".
- The `eval` command creates new fields in your events by using existing fields and an arbitrary expression. Here, the `eval` command classifies risk events based on their risk score and categorizes them by "medium", "high", or "critical" risk categories.

## Add annotations to enrich correlation search results

Ram adds annotations to enrich the results of his correlation search by adding context from industry standard cyber security mappings in Splunk Enterprise Security. Managed annotations might be based on cybersecurity frameworks such as CIS20, Kill 10, MITRE ATT&CK, and NIST. Unmanaged annotations are custom annotations that you can add to your specific use case.

1. Ram decided to add MITRE ATT&CK annotations to the correlation search by scrolling down in the Edit Correlation Search window to the Annotations panel.
2. Ram types T1078.004 in the MITRE ATT&CK field to align the security detection to a managed annotation based on a specific MITRE ATT&CK sub-technique.

3. Ram can also add custom annotations to his security detections in the SPL of the correlation search.
4. Ram uses the correlation search "Risk Notable: Risk Threshold Exceeded For Risk Object Over 24 Hour Period" that he customized to identify the alerts that are generated when a user exceeds an aggregated score of 100 in a 24-hour period. Ram now has the context provided by the annotations to investigate all the factors that contributed to generating the alert.

[Learn more](#)

Use security framework annotations in correlation searches.

## Classify risk objects based on annotations

Ram views the annotations associated with the risk objects by accessing the Embedded Risk Workbench panels in Splunk Enterprise Security and classifies the risk objects for more targeted threat investigation. Risk workbench panels provide at-a-glance risk-based insight into the severity of the events occurring in Ram's system or network, help to

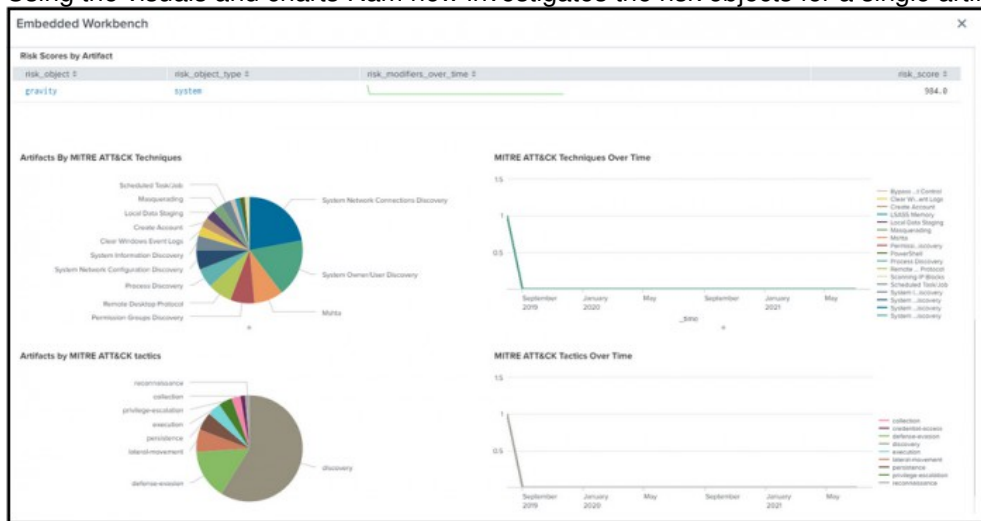
prioritize notable events, assign targeted notable events to security analysts for review, and examine specific notable annotations for investigations.

By visually classifying the risk objects based on risk modifiers, risk scores, MITRE ATT&CK techniques, and tactics, Ram can identify specific adaptive response actions and streamline his threat investigation process.

1. From the Enterprise Security menu, Ram selects Incident Review to display the Incident Review page and see a list of notable events for the security domains.
2. Ram expands a notable event by clicking on **Action** next to the **Risk Object**, **Destination**, **User**, or **Source** fields.
3. Ram selects the **Workbench-Risk (risk\_object)** as Asset action.  
This opens the **Embedded Workbench** panel that displays the following items:

- Recent risk modifiers that are applied to the risk object.
- Risk scores by artifact and trends of risk modifiers over time.
- Pie chart displaying the distribution of artifacts by MITRE ATT&CK techniques like **Driven by Compromise**, **Account Manipulation**, and so on.
- Pie chart displaying the distribution of artifacts by MITRE ATT&CK tactics like **discovery**, **persistence**, **defense evasion**, and so on.
- Time chart displaying the **MITRE ATT&CK Techniques Over Time**.
- Time chart displaying the **MITRE ATT&CK Tactics Over Time**.

Using the visuals and charts Ram now investigates the risk objects for a single artifact in the Embedded Workbench.





## Add a risk message and a risk score to a notable

Ram adds a risk message and a risk score to the notable event that represents a threat by creating an adaptive response action. Adaptive response actions can be used to gather more information, take an action in another system, send information to another system, modify a risk score, and so on. Adding a custom risk message helps Ram to build detections based on specific information, such as risk scores, instead of merely relying on the Risk Analysis data model schema.

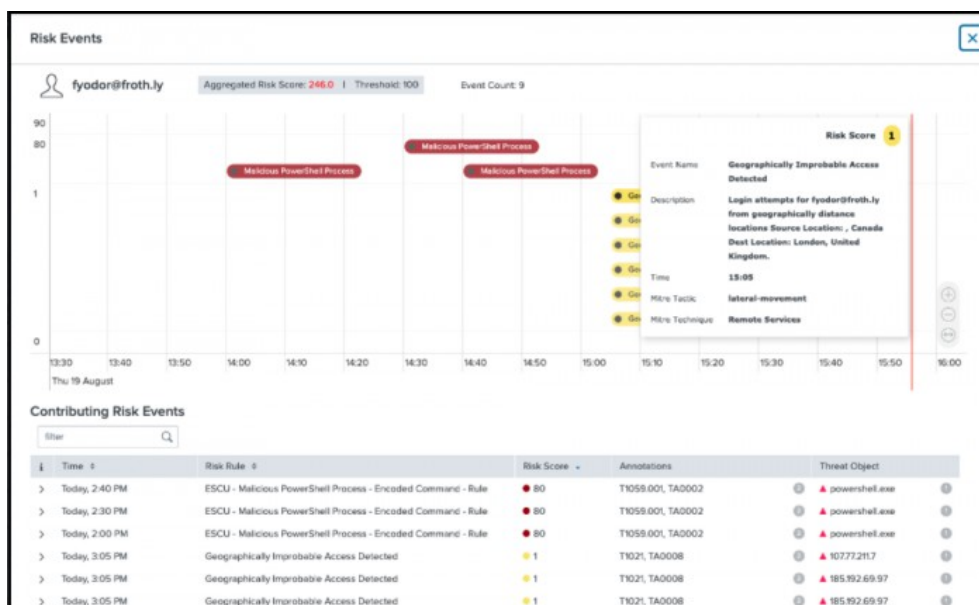
1. From a risk notable event, Ram selects the arrow to expand the Actions column and clicks **Run Adaptive Response Actions**.
2. Ram clicks **Add New Response Action** and selects the **Risk Analysis** adaptive response action from the dropdown list to create risk modifier events in the risk index.
3. Ram types a risk message, `Possible Bypass of User Account Controls`.
4. Ram also adds a risk modifier by populating the following fields:
  - ◆ **Risk Score**
  - ◆ **Risk Object Field**
  - ◆ **Risk Object Type**
5. Ram clicks **Run** to run the adaptive risk action on the notable.

## Adjust risk scores for specific objects

Ram uses risk factors to adjust risk scores for specific risk objects to more effectively map out the risk in his security environment and simplify the threat investigation process to prioritize suspicious behavior. Risk factors increase the risk scores based on specific conditions without creating new searches. For example, Ram can increase the risk score by a factor of two on a laptop that might be targeted if it belongs to a director instead of an employee. Risk factors are calculated based on a formula.

Ram can also use the default risk factors designed for specific conditions to dynamically assign risk scores to risk objects and effectively isolate threats using Splunk Enterprise Security. Splunk Enterprise Security provides seven risk factors by default, which can be further customized based on Ram's specific environment. Ram can also use these default risk factors as examples for guidance and create his own risk factors based on his environment.

1. Ram can modify the score of a risk object based on **tactic**, **user**, **src**, **dest**, and **threat object**. For more information on creating risk factors, see *Create risk factors in Splunk Enterprise Security*.
2. From the Enterprise Security menu, Ram selects **Configure > Content > Content Management**.
3. From the **Create New Content** drop-down list, Ram selects **Risk Factor**, which opens the Risk Factor Editor.
4. Ram then clicks the default risk factor, **Watchlisted User**.



This default risk factor increases the risk score for users on a watch list by a multiple of 1.5. So, if `user_watchlist` is `true`, the risk factor is increased by a multiple of 1.5. Ram can include all the directors on the watchlist. Now Ram is able to mitigate risk successfully by using risk factors that dynamically modify risk scores based on specific conditions and keep Buttercup Games safe from security threats.

[Learn more](#)

[How the risk factor scoring works](#)

[Using watchlists to your advantage](#)

# Reduce alert volume

## Reduce alert volumes by triaging notables

Buttercup Games, a fictitious company, runs an e-commerce site to sell its products. Ram, a security analyst at Buttercup Games, triages incoming notables from correlation searches and opens investigations to assess risk to his organization. He receives over 10,000 notables every day, 50% of which are false positives.

Despite Ram's best attempts to triage all notables and delegate the investigations, manually selecting notables for triage forces him to abandon certain notables that he deems less risky. Sifting through the high volume of notables causes Ram to burn out quickly. The high volume of excessive notables also results in slow threat detection and response time, which exposes Ram's organization to security threats.

Kay, the manager of the security operations center (SOC) at Buttercup Games and Ram's manager, wants to streamline the manual and monotonous triage process. Kay knows that Ram can potentially overlook the risks in the SOC and asks Ram to use dispositions and other features available in Splunk Enterprise Security to triage notables and classify them. This helps Ram to separate the false positives and focus on the notables that pose the highest threat.

This use case describes how Ram uses dispositions to separate notables that are false positives from notables that represent real threats while reducing alert fatigue and risk in the SOC of Buttercup Games by taking these steps.

1. [Add dispositions to risk notables](#)
2. [Sort notables by disposition](#)
3. [Investigate risk notables that represent a threat](#)

## Add dispositions to risk notables

Ram adds dispositions to the risk notables using the Incident Review dashboard to identify the threat level associated with the notable accurately. Adding a disposition helps to classify the notables, separate the false positives, and drill down on the notables that pose the highest threat. This helps Ram to accelerate the triage of notables during an investigation and respond to security threats faster.

1. From the Splunk Enterprise Security menu bar, Ram clicks the Incident Review page and scrolls down to the table that lists the notables.
2. Ram sorts them to bubble up only the risk notables and selects the checkbox beside the risk notables for which he wants to add a disposition.
3. Ram clicks **Edit Selected** to edit the notable that he selected.
4. For each risk notable, Ram selects one of the options from the **Disposition** drop-down list as shown in the following image and saves his changes.

## Edit Events



1 event(s) selected. You are editing selected events.

Status

Select...



Urgency

Select...



Owner

Select...



[Assign to me](#)

Disposition

Select...



Comment

True Positive - Suspicious Activity

Benign Positive - Suspicious But Expected

False Positive - Incorrect Analytic Logic

False Positive - Inaccurate Data

Other

Undetermined

Now Ram needs to investigate only risk notables that are tagged as **True Positive - Suspicious Activity**.

## Sort notables by disposition

Ram now sorts the notables by disposition in the Incident Review page so that he can drill down on the risk notables that are tagged as **True Positive - Suspicious Activity** and ignore the false positives as shown in the following image.

Title	Risk Object	Aggregated Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
24 hour risk threshold exceeded for system-my-mac	my-mac	517500	22500	Risk Notable	Today, 7:40 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for user-hacker007	hacker007	452500	22500	Risk Notable	Today, 7:40 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for other-bernardo	bernardo	475000	22500	Risk Notable	Today, 7:40 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for system-2727271	2727271	427500	22500	Risk Notable	Today, 7:40 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for user-wonderland	wonderland	49900	1243	Risk Notable	Today, 6:15 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for system-windows desktop	windows desktop	41537	1257	Risk Notable	Today, 6:15 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for user-risky_user	risky_user	45077	1257	Risk Notable	Today, 6:15 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for system-my-mac	my-mac	48957	1259	Risk Notable	Today, 6:15 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for user-hacker007	hacker007	46091	1259	Risk Notable	Today, 6:15 PM	True Positive - Suspicious Activity	Threat	High	New	unassigned	
24 hour risk threshold exceeded for other-bernardo	bernardo	47350	1245	Risk Notable	Today, 6:15 PM	False Positive - Inconclusive Analytic Logic	Threat	High	New	unassigned	
24 hour risk threshold exceeded for system-2727271	2727271	42920	1259	Risk Notable	Today, 6:15 PM	False Positive - Inconclusive Analytic Logic	Threat	High	New	unassigned	
24 hour risk threshold exceeded for system-21212527	21212527	49023	1257	Risk Notable	Today, 6:15 PM	Undetermined	Threat	High	New	unassigned	

1. From the Enterprise Security menu, Ram selects the Incident Review page that provides a list of notable events for the security domains.
2. Ram clicks **Disposition** in the table to sort the notables tagged as **True Positive - Suspicious Activity**.

The table of notable events in the Incident Review page also lists the risk events associated with the notable.

Now Ram can focus on investigating risk notables that are grouped together as **True Positive - Suspicious Activity**.

## Investigate risk notables that represent a threat

Ram investigates the risk notables that are tagged as **True Positive - Suspicious Activity** using the timeline visualization on the Incident Review page and identifies the source of the security threat.

1. From the Splunk Enterprise Security menu bar, Ram clicks the Incident Review page.
2. From the **Type** filter drop-down list, Ram selects **Risk Notable** to display the notables that have associated risk events.
3. Ram focuses only on the risk notables that have the Disposition tagged as **True Positive - Suspicious Activity**.
4. Ram reviews the following two fields for the risk notables: **Risk Event** and **Aggregated Score**. The **Aggregated Score** is the sum of all the scores associated with each of the contributing risk events.
5. Ram clicks the value in the Risk Events field for the notable event that he wants to investigate. This opens a window that contains two panels. The top panel displays a timeline visualization of the contributing risk events that created the notable. The bottom panel includes a table with detailed information on the contributing risk events as shown in the following image:



6. Ram expands the risk notable in the **Contributing Risk Events** table for more details to further analyze the risk objects in his security environment.

This includes information on the following fields: **Risk Object Source Risk Score Risk Message Saved Search Description Threat Object Threat Object Type** These details provide Ram with further context to analyze the risk object, such as power shell, registry entries, commands, risk messages, user login information, or any other suspicious activity as shown in the following image:



7. Ram correlates the risk events with dates and the severity of the risk scores in the timeline visualization to identify threats.
8. Ram also zooms in and out to narrow down the time of occurrence since the timeline visualization plots the contributing risk events using time on the x-axis and the risk score on the y-axis. The timeline visualization also uses color codes on the icons that indicate the severity of the risk scores. Color coding risk score icons are consistent across the **Contributing Risk Events** table and the timeline visualization of the risk events. Ram knows that a lower risk score corresponds to a lighter color icon.
9. Ram now identifies the risk object type through the icons displayed in the header of the timeline visualization. Icons include:
  - ◆ **User**
  - ◆ **System**
  - ◆ **Network Artifacts**
  - ◆ **Other**

Using the filters, timeline, and other visualizations on the Incident Review page in Splunk Enterprise Security helps Ram to accelerate the triage process of notables during the investigation workflow. Ram can now quickly identify the risk events that might be a threat to the SOC of Buttercup Games.

# Isolate user behaviors

## Isolate User Behaviors That Pose Threats

Buttercup Games, a fictitious company, runs an e-commerce site to sell its products. As a best practice, Ram, a security analyst at Buttercup Games tries to track user behavior and maintain the security hygiene of his security operations center (SOC) by monitoring the accounts that are created, the purpose for which the accounts are created, and the expected usage of the accounts. However, the size of his SOC makes it impossible to maintain all the records of when an account is created, when an account is dormant, if an account is shared between individuals, or if the account is a service account. So Ram uses Splunk Enterprise Security to make the task of tracking account activity easier and to monitor user behaviors. User behaviors that represent security threats in this particular SOC include compromised user credentials, insider threats, and misuse by privileged users. Compromised user credentials represent the biggest threat for the assets and identities in Ram's SOC. Ram knows that user credentials can be compromised due to any of the following reasons:

- When phishing emails are sent to user accounts from purportedly reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.
- When passwords are shared across multiple user accounts.
- When passwords are inadvertently exposed due to insecure password sharing, and so on.

Ram also wants to identify all high-priority accounts. High-priority accounts are accounts that typically have administrative privileges and executive-level authority, which can access sensitive or confidential assets. By identifying high-priority accounts, Ram can prevent unauthorized users from misusing the accounts. Ram also knows that a valid credential might be used by an insider in an unauthorized manner. This use case describes how Ram, a security analyst, uses the various dashboards, correlation searches, risk factors, and other analytics provided by Splunk Enterprise Security to monitor user behaviors that pose a security threat to the SOC of Buttercup Games using the following steps:

1. [Use dashboards to track user behavior](#)
2. [Classify accounts based on privileged access](#)
3. [Use correlation searches to monitor accounts](#)
4. [Increase risk factors to identify unauthorized usage](#)

## Use Dashboards to track user behavior

Ram uses the following dashboards in Splunk Enterprise Security to monitor and track user account activity: Access Center Access Tracker Access Search Account Management Default Account Activity User Activity Identify Investigator

The Access Center dashboard helps Ram to automatically track account creation, updates to accounts, and deleted accounts across all data sources. Using the Access Center dashboard, Ram gets a summary of all authentication events, such as brute-force attacks, use of clear text passwords, or access to certain systems outside of work hours. This dashboard helps Ram to identify all security incidents that involve authentication attempts.

The Access Tracker dashboard provides Ram with an overview of account statuses, tracks newly active or inactive accounts, tracks accounts that have been inactive for a period of time but recently became active, and discovers accounts that are not properly de-provisioned or inactivated when a person leaves the organization. Because inactive accounts or improperly active accounts are vulnerable to attackers, Ram believes that it is a good idea to check the Access Tracker dashboard on a regular basis. Ram also uses this dashboard during investigations to identify suspicious accounts and closely examine user access activity. The Access Search dashboard helps Ram to find specific authentication events for ad-hoc searching of authentication data or to drill down on searches.



The Account Management dashboard enables Ram to identify changes to user accounts, such as account lockouts, newly created accounts, disabled accounts, and password resets. Ram knows that a sudden increase in the number of accounts created, modified, or deleted can indicate malicious behavior or a rogue system and a high number of account lockouts can indicate an attack.

The Default Account Activity dashboard helps Ram to locate any activity on "default accounts", or accounts enabled by default on various systems, such as network infrastructure devices, databases, and applications. The Default Account Activity dashboard helps Ram to identify the usage of more than 50 common default accounts from various vendors and software products. Default accounts have well-known passwords and are often not disabled properly when a system is deployed.

Occasionally, Ram wants to investigate an account from a historic or forensic perspective. Viewing an account from a historical perspective allows Ram to receive an indication from a third party that a user needs some scrutiny, like if human resources or the internal fraud department of Buttercup Games flags a user for review, and requests a complete timeline of that account's network activity and access patterns. Ram then uses the User Activity and Identity Investigator dashboards in Splunk Enterprise Security to help him investigate the accounts.

## **Classify accounts based on privileged access**

Ram first collects and extracts all assets and identity data to add it to Enterprise Security. Next, Ram formats the collected asset or identity data into a lookup file so that it can be processed by Splunk Enterprise Security. Finally, Ram uses the Assets and Identities framework in Splunk Enterprise Security to specify categories for all the accounts in his SOC, and label the privileged accounts.

For more information on how to format the asset and identity list, see [Format an asset or identity list as a lookup](#)

Specifying categories for all the accounts in his SOC allows Ram to use the default correlation searches in Splunk Enterprise Security to monitor those accounts more closely and get visibility into interesting account activity or unauthorized usage.

## **Use correlation searches to monitor accounts**

1. Ram uses the following correlation searches available by default in Splunk Enterprise Security to monitor account activity:
  - ◆ **Account Deleted:** Detects user and computer account deletion.
  - ◆ **Completely Inactive Account:** Discovers accounts that are no longer used. It's a good idea to disable unused accounts because they are often used by attackers to gain unauthorized access.
  - ◆ **Inactive Account Activity Detected:** Discovers previously inactive accounts that are now being used. Reactivated accounts might be due to an attacker that successfully gained access to an account that was no longer being used.
  - ◆ **New User Account Created on Multiple Hosts:** Alerts when a previously unseen account is created on multiple hosts.
  - ◆ **Short Lived Windows Accounts:** This search detects accounts that were created and deleted in a short time period.
2. Ram uses the following correlation searches that are available by default in Splunk Enterprise Security to identify potential risk events through compromised user credentials.
  - ◆ **Geographically Improbable Access Detected:** Alerts on access attempts that are improbable based on time and geography.

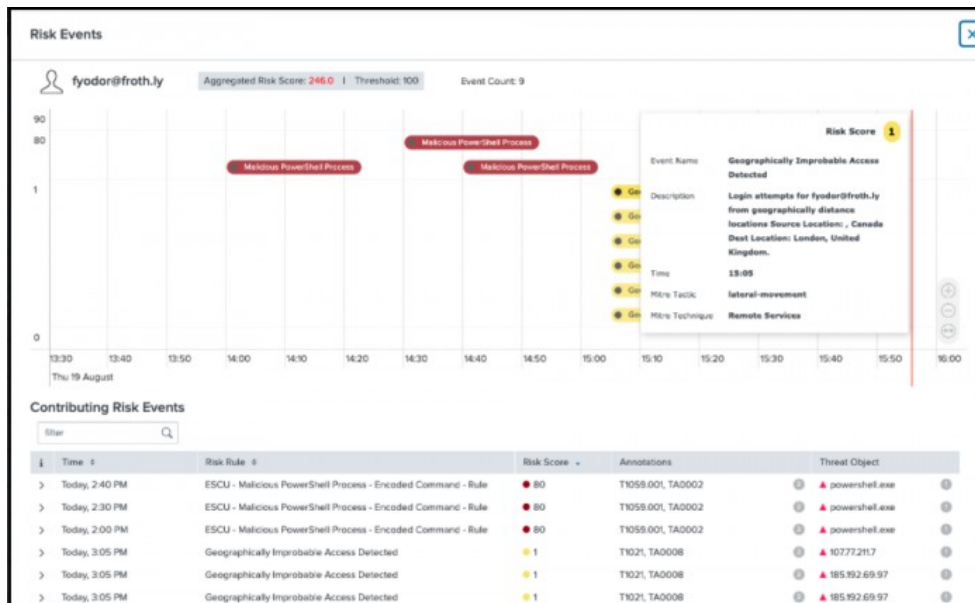
- ◆ Concurrent Login Attempts Detected: Alerts on concurrent access attempts to an app from different hosts. These access attempts are good indicators of shared passwords and potential misuse.

3. Ram uses these correlation searches to see if a password is being used in a suspicious manner, even if the authentication is successful. However, these correlation searches generate numerous notable events.
4. Ram can also create his own correlation searches to identify if there was an increase in the number of host systems that a user logged into or whether there was a new interactive login from a service account.

## Increase risk factors to identify unauthorized usage

Ram can also increase the risk factor of privileged user accounts using the risk alerting framework of Splunk Enterprise Security.

If Ram sets an increased risk factor for these accounts, the risk- based alerting framework automatically drives higher risk scores for the account and the analyst is immediately notified about the high- urgency notable event.



For more information on how risk factors work and assigning conditions to risk factors, see [Create risk factors](#).