Splunk® Enterprise Security Use Cases 6.3.0

Generated: 8/19/2020 8:10 am

Table of Contents

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 with Splunk Enterprise Security

Identify suspicious activity

- Using Enterprise Security to find Data Exfiltration
- Monitor privileged accounts for suspicious activity
- Monitor threat activity in your environment with a glass table

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.
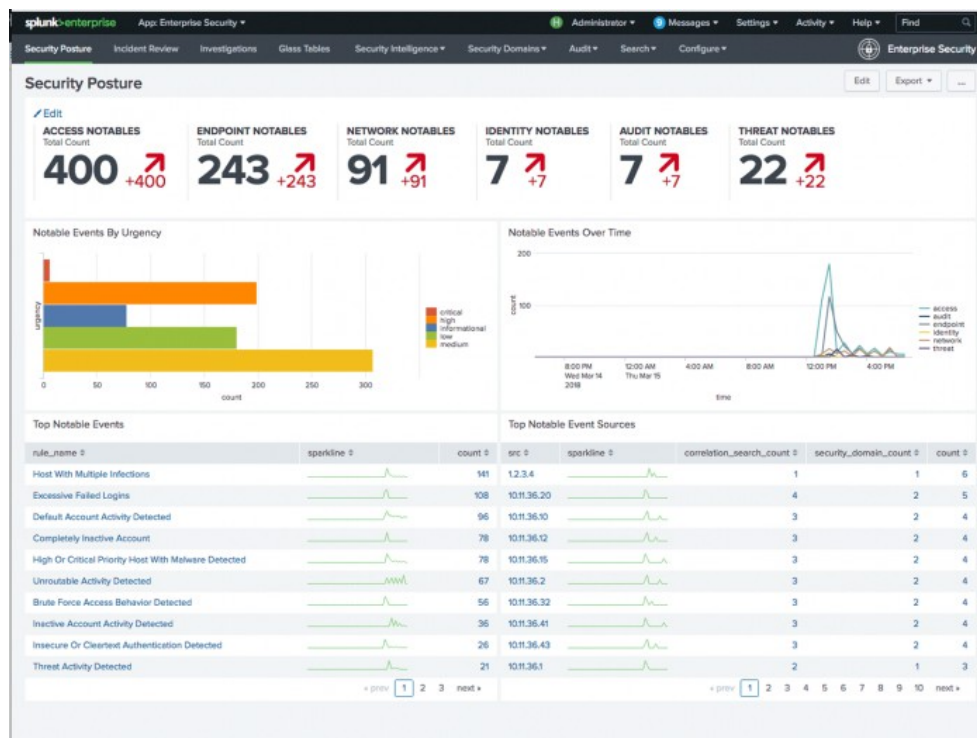
On any given day, there might be tens or hundreds of notable events represented on the Security Posture dashboard. Use the **Notable Events By Urgency** panel to determine which issue needs your immediate attention.

In the **Notable Events Over Time** panel, you see a spike in activity labeled "endpoint." The endpoint domain represents host based security, so you know there was a large spike in suspicious activity on the network hosts.
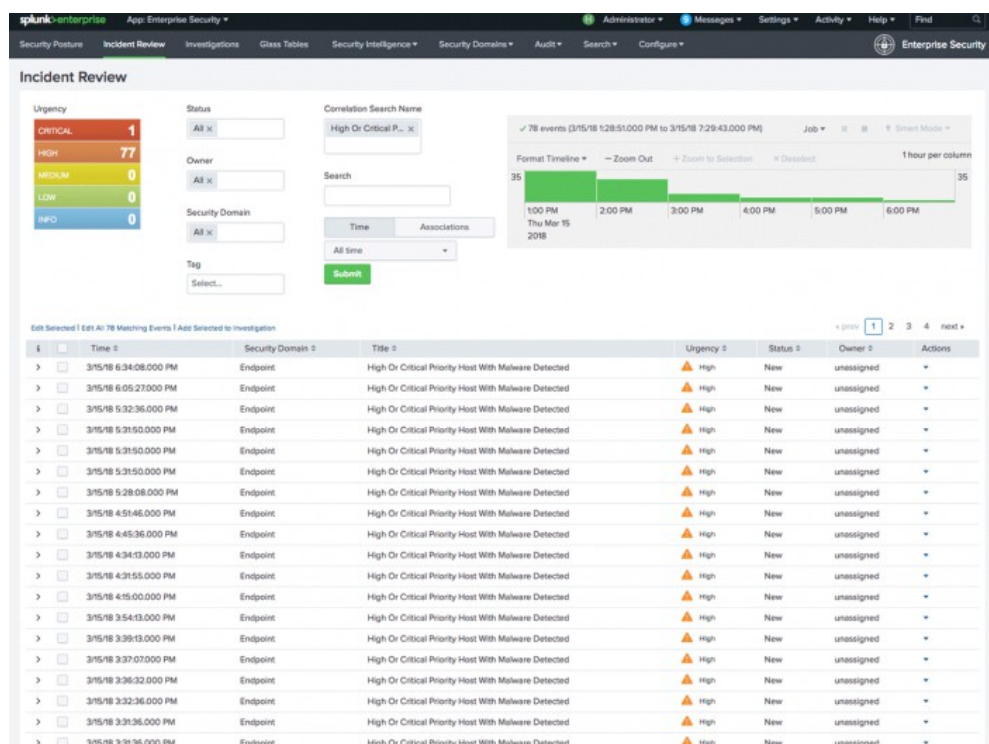
In the **Top Notable Events** panel, you see the count of notable events sorted by the correlation search name. The panel shows that the number of **High Or Critical Priority Host With Malware Detected** notable events had a sudden spike. To drill down into those numbers, select the peak count on the 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. Because the link to Incident Review was initiated from another dashboard panel, the Incident Review dashboard opens with a search for **High Or Critical Priority Host With Malware Detected** notable events and scoped to a narrow timeframe.

Prioritize the task

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.

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.

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.

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**.

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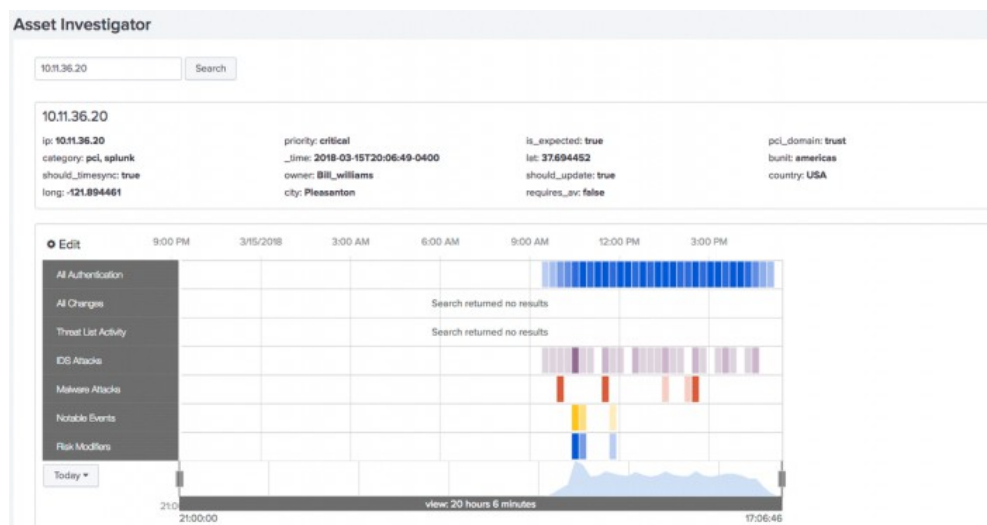
Each swim lane has a collection of data points called candlesticks. The event count within a candlestick is represented through a heat map. The brighter the color, the higher the event count.

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**.
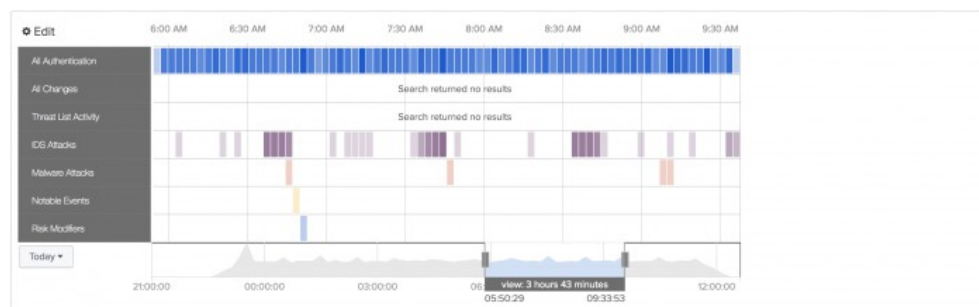
Find the event

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**.
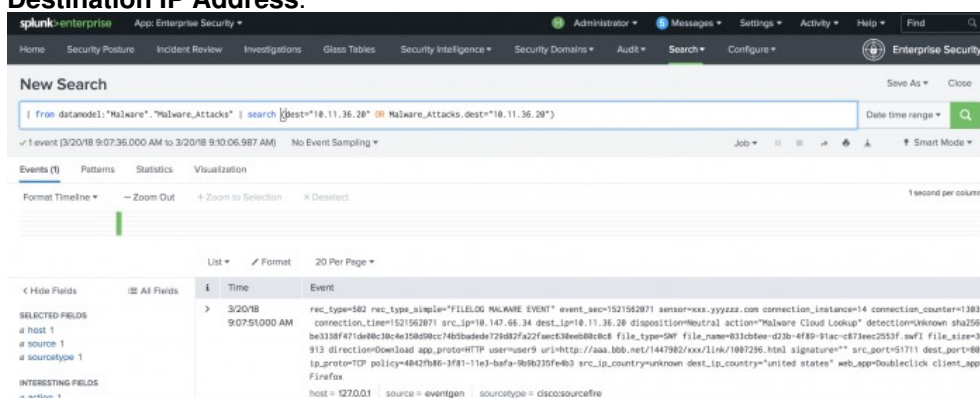
Drill down to log events

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.

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
src_ip	Represents internal network hosts.
dest_ip	Another internal host that was discovered to be a proxy.
uri	A record of what is being requested by the hosts.
client_app	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 Sampli

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

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

9

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.

On the page of results, you see a number of common download requests. The `.swfl` 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.

From the results, you can see additional alerts about this host from other log sources, implying that the specific `src` is being targeted with multiple forms of attacks. There is a chance that this host has downloaded an exploit from an Internet domain.

3. Examine the `url` and `file_name` fields for the host.
    1. Review the data in a table format to give you a view of the important events.
    2. Use the search bar to add `| table url file_name` to the end of the existing search string and select search.

    3. Sort the table by selecting the `url` field.

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

At this point, quarantine the infected host based upon the data collected. More information is contained in the proxy logs, such as the domain being used to download the suspicious files. Digging deeper into those logs can provide information to use in active remediation.

Find additional affected hosts

On the table of results, select a `url` field in an event that references a suspicious domain.

1. Click the `url` field.
2. Click the icon next to **New search**.
   A new browser window opens to a search dashboard and begins searching on the selected `url` field over the time range.
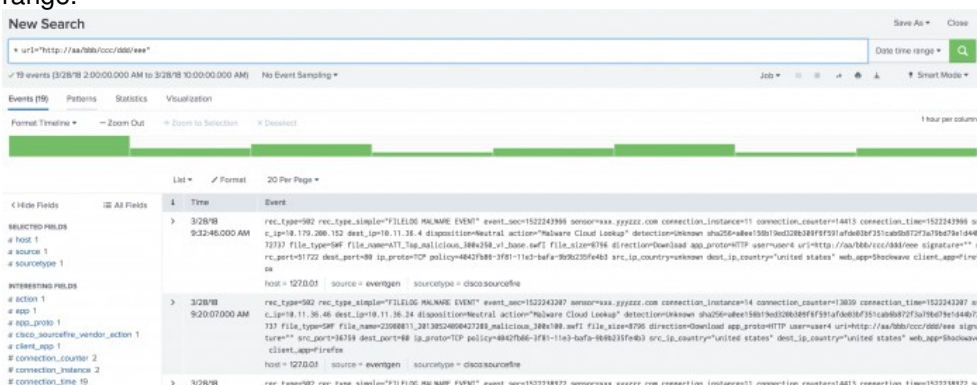
Widen the time range to broaden the search

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.
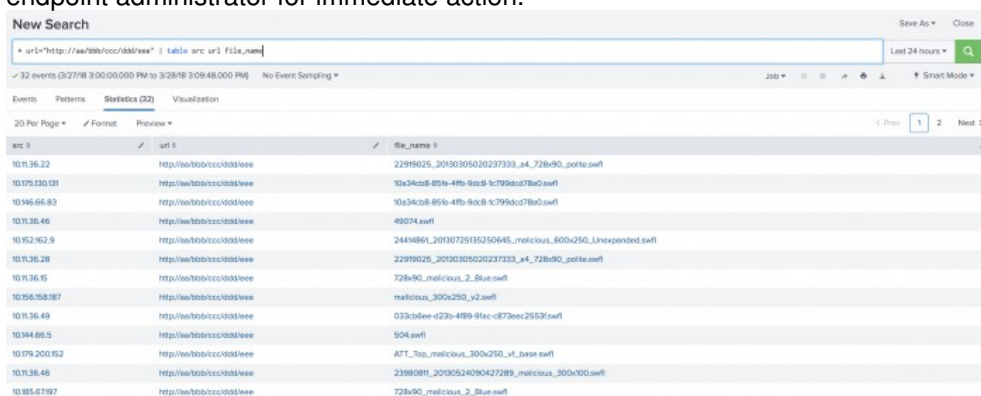
Create reports of the results

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.

You can export the results to place into a report or an email attachment.
3. Click the **Export** button.
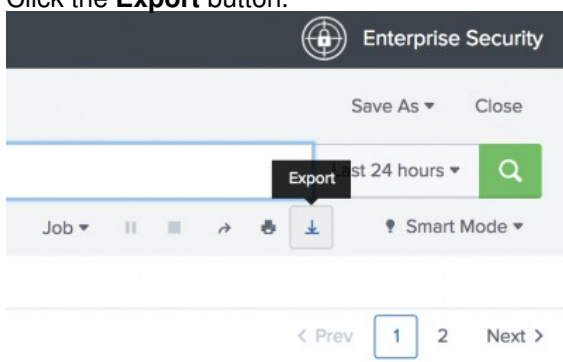
4. Update the **File Name** field and save the results in a `.csv` format.
5. Click **Export** to download the results.
6. (Optional) Click **Save As** and select **Report** to save the report.
7. Fill in the required fields, and write a summary of the report for the **Description** field.
8. Click **Save** 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 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 **Advanced Threat > 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 with Splunk Enterprise Security

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.

15

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 micros0ft[.]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 micros0ft[.]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 micros0ft[.]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.

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 micros0ft[.]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
Unapproved 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
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 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,dep artment,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.

Monitor threat activity in your environment with a glass table

In this example, monitor threat activity in your environment by creating a glass table that visualizes and tracks specific threat activity metrics.

- Create a glass table to monitor threat activity.
- Start monitoring threat activity metrics on the glass table.
- Organize the metrics visually.
- Monitor custom metrics on the glass table.
- Save and view the glass table.

Create a glass table to monitor threat activity

1. From the Splunk ES menu bar, click **Glass Tables** to open the list of existing glass tables.
2. Click **Create New Glass Table**.
3. Type a **Title** of **Monitor Threat Activity**.
4. Type a **Description** of **Monitor threat activity in the network. Displays metrics related to threat notables, threat actors, and types of intelligence.**
5. Click **Shared in App** to allow other users of Splunk Enterprise Security to view the glass table.
6. Click **Create Glass Table**.
7. Click the title of the glass table to edit it.

Start monitoring threat activity metrics on the glass table

After opening the glass table to edit, collect the relevant threat activity metrics for your glass table.

1. In the list of **Security Metrics**, click **Threat Activity**
2. Click the **Threat Activity - Total Count** metric and drag it onto the glass table.
3. In the **Configurations** panel, scroll down to **Thresholds** and select **On**.
4. Click **Edit** to set up a threshold.
5. Click **Add Threshold** and type **50** for a **Medium** number of total threat activity events.

6. Repeat to add a **High** threshold of **100** events.
7. Make sure that the threshold below medium is set to **Normal**.
8. Click **Done** to save the changes to the threshold.
9. Click **Update** to save the changes to the security metric.
10. Click and drag the **Threat Activity - Unique Categories** metric, the **Threat Activity - Unique Collections** metric, the **Threat Activity - Unique Matches** metric, and the **Threat Activity - Unique Sources** metric onto the canvas. Do not set a threshold for the categories, sources, or collections metrics, because a higher number of categories, sources, and collections indicates only that there is more intelligence available to you, rather than a security incident that needs attention.

Organize the metrics visually

Use the editing tools on the glass table canvas to upload images, draw shapes, add icons, add text, and make connections that reflect the relationships between the threat metrics.

1. Click each metric and modify the width and height of each metric to make it the shape you want.
2. Draw lines between the different threat activity metrics to differentiate the types of metrics.
3. If threat activity tracking happens at the router or firewall level, add a router or firewall icon.
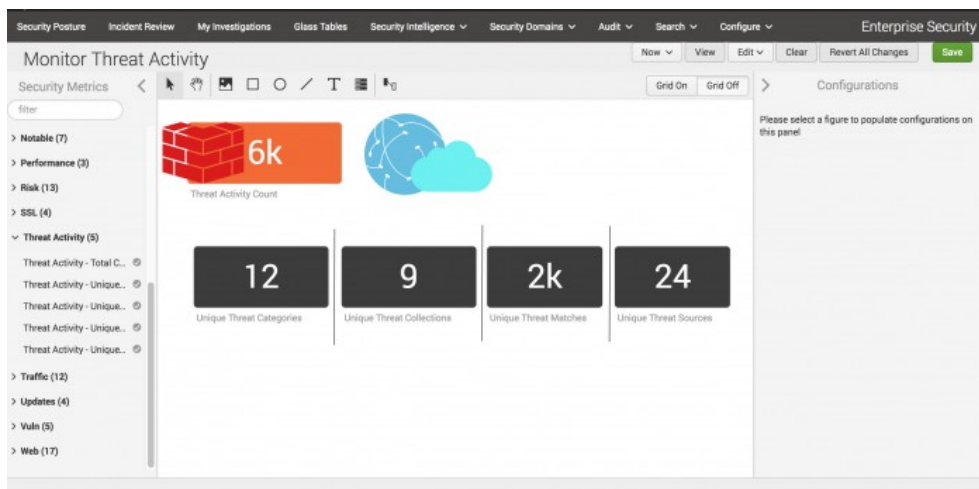
Monitor custom metrics on the glass table

Add a custom search to track custom threat activity metrics. You want to track threat activity by a specific threat group, the APT group.

1. In a new tab, open the **Search** dashboard and construct a search that looks for the APT group. This search relies on the threat list activity correlation search, and identifies notable events over time that contain threat activity from the APT threat group.

   ```
   `notable("Threat - Threat List Activity - Rule")` | search threat_category="APT" | stats count by
   threat_category
   ```
2. When you are satisfied with your search, copy it to your clipboard.
3. Return to the glass table to add an ad hoc search.
4. In the list of **Security Metrics**, click **Ad hoc search** and drag it onto the glass table.
5. In the **Configurations** editor, type a **Label** of **APT activity** for your ad hoc search.
6. Copy your previously-created search that identifies APT activity by threat category in your environment.

```
`notable("Threat - Threat List Activity - Rule")` | search threat_category="APT" | stats count by
threat_category
```
7. Click **Update** to save your changes to the ad hoc search metric.
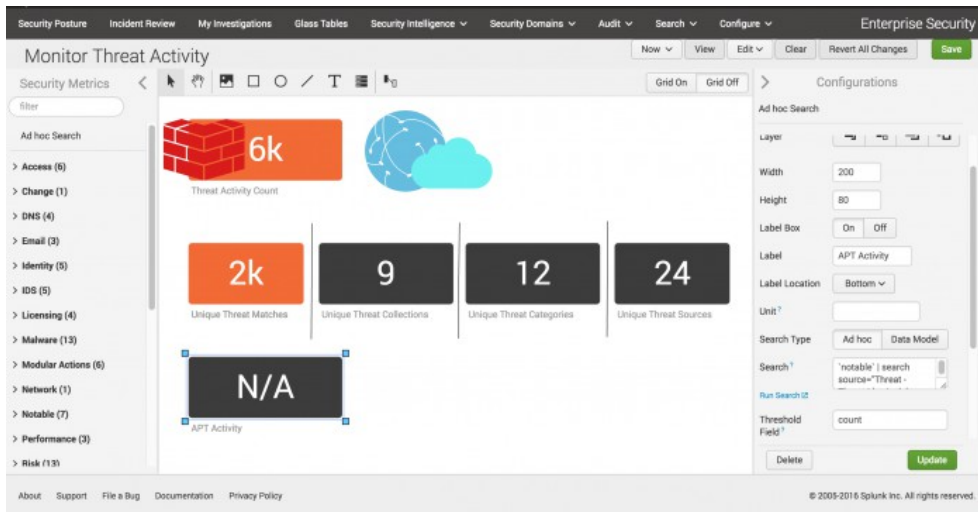
Save and view the glass table

After you finish creating the glass table, you can start monitoring threat activity.

1. Click **Save**.
2. Click **View**.

Enjoy the view.