

Using ES 4.5 Class Lab Exercises

Lab typographical conventions

{student ID} indicates you should replace this with your student number.

{server-name} indicates you should substitute the server name assigned to this class.

Lab Exercise 1 – Overview of Splunk Enterprise Security

Description

In this exercise, you'll get familiar with your lab environment and access the ES user interface.

Steps

Task: Log into your Splunk classroom server, configure your user account, and navigate to the ES home page.

1. Write down your ES server's web URL: _____
Note that your server is running on HTTP on port 80.
2. Write down your ES Analyst user name and password: _____
3. Log in to your Splunk server.
4. In the top menu, select **analyst > Account Settings** to modify your user preferences.
5. Enter your name in the **Full name** field and click **Save**.
6. Navigate to the Enterprise Security home page. Note that besides links for the security posture, incident review, and app configuration pages, there are also links to ES documentation, the Splunk Answers community site, and product information.

Task: Examine the source events ES is using to monitor the security environment and notable events.

In your lab environment, a testing tool called SA-Eventgen is generating artificial source events. In a production environment, these events would be generated by Splunk forwarders, which would be gathering data from your network's servers, routers, and applications. Your lab event data only goes back as far as the time the lab server was set up—probably only a day or so.

7. In ES, select **Search > Search** to run a search using Splunk Search Processing Language (SPL). This page is very similar to the **Search and Reporting** app you have used before.
8. Begin a search for all events (*) over the **last 15 minutes**. If the search runs for more than about 30 seconds, you can stop it before it completes.
9. Examine the results. You will probably have many events. From the result count of this search you can extrapolate the daily indexing volume. Also, look at the sources and source types—this will give you a feel for the type of systems being monitored.
10. Examine the variety of source (src) and destination (dest) IP addresses and host names. Some of the other fields you may see are the host, source country and city, and the event types being assigned to the events. (Open the link for all fields and enter a field name. For example, country and city.)
11. Run a new search for all events in the notable index over the **last 24 hours**.
Note the number of results and compare this to the total number of indexed events in the main index over the last 15 minutes. This shows you how useful the notable events are; you don't need to search through all the data to find the events that need attention.
12. Examine the source field values. These are the correlation search names that created the notable events.
13. Examine some of the other discovered fields. Note that they are extracted from the source events, so they will be similar to what you saw in the **main** index.

Lab Exercise 2 – Monitoring and Investigating

Description

In this exercise, you'll use the Security Posture dashboard to monitor the overall security status of your organization and the Incident Review dashboard to work an incident. You'll also experiment with manual notable event creation and notable event suppression. For an extended example of the use of these tools, see docs.splunk.com/Documentation/ES/latest/Usecases/MalwareDetection.

Steps

Scenario: You are investigating reports of unauthorized access to your network resources.

Task: Use the Security Posture dashboard.

1. Navigate to the Security Posture dashboard.
2. Review the values in the key indicators. Note the totals, as well as the net change for each in the last 24 hours.
3. Examine the displays in the 4 panels.
4. Hover over the bars in the **Notable Events by Urgency** panel and note the values.
5. In the Notable Events By Urgency panel, click the red (critical) bar.
The Incident Review dashboard opens to display only the critical notable events.
6. Navigate back to the Security Posture dashboard.
7. Examine the Top Notable Events panel. Click the **Activity from Expired User Identity** row. Note that this time the Incident Review dashboard shows only the notable events from the Activity from Expired User Identity correlation search.
8. Note that the user account **Hax0r** has been accessing resources even though the account is expired.
9. Reset the Incident Review dashboard by clicking **Incident Review**.

Note: This re-opens the Incident Review dashboard with all fields set to default—a fast way to clear all applied filters and reset the dashboard. You will use this technique frequently throughout the lab exercises.

Task: Continue researching unauthorized network access.

10. In the Incident Review dashboard, search for the user name **Hax0r** for the last 24 hours. You should find one or more notable events for this user.

Hint: Use the **Search** field to enter the user ID.

Note: Unless otherwise indicated, execute all subsequent searches using a time range of Last 24 hours.

11. In the results, view the details for one of the notable events.
12. Examine the details of the original event. Some of this data may be useful to determine the seriousness of this vulnerability.
13. Click the **View activity from Hax0r** link to see raw events associated with this user name. This opens a new search window that uses a custom 10-minute time range which references the creation time of the notable event (5 minutes before and 5 minutes after). This allows you to see raw events that occurred immediately before and after the notable event.

Note the host names being accessed, the source characteristics (IP address, city, owner name, etc.), the application, and the action. In this case, action=failure indicates failed logon attempts. So, Hax0r is not actually authenticating, but the fact that someone is attempting to use this expired account is an issue.


14. Close the search window and return to the Incident Review dashboard.

Task: Begin working the issue.

15. In the Incident Review dashboard, make sure the search results are still filtered to the user **Hax0r**.
16. Click **Edit all XX matching events**.
17. Set the status to **In Progress** and the owner to yourself. Save the changes.
18. Note the change in status and ownership.
Note: Now you begin working with network analysts and others to research and resolve the issue. While this takes place, you will still need to review new incidents.
19. Click in the **Status** field and select **New**. **Hax0r** is still in the **Search** field. Click **Submit**—you're looking for incidents in status = new that contain the text **Hax0r**
 Notice that you no longer see your in-progress **Hax0r** incidents. You would do this to see only new incidents requiring attention. They would normally then be assigned to an owner and their status changed to show they are In Progress or Resolved.
20. Reset the Incident Review dashboard by clicking the **Incident Review** menu option.
21. In the **Owner** field, select yourself and run the search again.
 Now you only see your incidents. This is a typical way to view your queue of assigned incidents.

Scenario: Several false positives have been generated and are coming from a set of servers named **PROD-MFS-XXX**, which are a set of QA lab workstations used to test production security configurations. You want to first determine the workstation's status—are these workstations still online? You'll ping them to see.

Task: Test workstation status.

22. In the ES menu bar, select **Incident Review**.
23. Search for notable events in the **Endpoint** domain associated with the server **PROD-MFS-***.
24. You should see several notable events for malware infections. Expand the details of one of these events.
25. Click the link in the **Contributing Events** section to see the original events that triggered this notable event.
 A new search window opens and shows you events from the **Malware** data model. Note that this information comes from the **Malware_Attacks** object. You can see the affected system (**Malware_Attacks.dest**), the type of attack (**Malware_Attacks.category**), and other information about the incident.
26. Close the contributing events search window. Check the status of the affected system.
27. In incident review, open the notable event's **Actions** menu and select **Run Adaptive Response Actions**.
28. Select **Add New Response Action**, and select **Ping**.
29. In the **Ping** form, enter **dest** for the **Host Field**, and **4** in the **Max Results** field.
30. Click **Run**. The ping action is dispatched.
31. Close the **Adaptive Response Actions** modal.
32. In the incident's details, click the refresh () icon above the **Adaptive Responses** list. Your ping action should be listed with a **Success** status.
33. Click the **Ping** action to see the results. A new search window opens and displays the results of your ping action. This verifies that the server is online. (Note that all the **prod-mfs*** host names resolve to 127.0.0.1—this is intentional for our lab environment.)
34. Close the search window.

Scenario: Now that we know the status of the test systems, we'll close out the affected false positive notable events.

Task: Remove the false positives from the list of incidents.

35. In **Incident Review**, make sure you are still displaying all of the events in the **Endpoint** domain for **PROD-MFS-*** workstations.
36. Click **Edit All XX Matching Events**.
37. Change the status to **Closed** and in the comments, enter **False positive generated by testing process**. Save the changes.

Task: You have resolved the Hax0r issue by hardening a firewall asset. You can now resolve your incident.

38. Reset the Incident Review dashboard and search for all **Hax0r** incidents.
 39. Click **Edit all XX matching events**.
 40. Change the status to **Resolved** and save the changes.
 41. In the future, you probably want to see only unresolved, open incidents.
 42. Clear the dashboard and search for open incidents by selecting all status values except Resolved and Closed from the Status field.
 43. Your Hax0r events should not appear in the search results.
- Tip:** Remember that the event status field name is `status`, lower case, and that the status values are integers, with 0 being "unassigned" and 5 being "closed." You can filter out all resolved (4) or closed (5) events by adding `status<4` to the **Search** field.

Scenario: You've closed the **PROD-MFS-XXX** false positives, but new notable events will still occur. You'd like to suppress them for the rest of the testing project.

Task: Suppress notable events

44. Search for **PROD-MFS-*** events in the Incident Review dashboard.
 45. On the first result, click the Actions menu and select **Suppress Notable Events**.

Note: We are suppressing only one of several servers for the purpose of this exercise. If this many servers were identified as false positives in a production environment, your ES administrator would likely make a permanent adjustment to the correlation search to prevent future false positives from occurring.
 46. In the **Suppress From ... To** fields, select a range from now until a date 6 months in the future.
 47. Select **Save** and close the new browser window to return to ES.
- Note:** No new notable events will be generated for this server for the next 6 months.

Lab Exercise 3 – Investigation Timelines

Description

In this lab exercise, you'll use an investigation timeline to document an investigation into the use of Snort in your network.

Steps

Scenario: During routine network auditing, you notice network traffic indicating Snort is in use in your environment. Since this is not on your list of approved network tools, you want to investigate.

Task: Start an investigation

1. In ES, navigate to **My Investigations**.
2. Click **Create New Investigation**. A new investigation is created with a generic name.
3. Change the name to **Snort Activity**.
4. Add a note by clicking **Create New Entry > Note**, fill in values below, and then click **Add to Investigation**:
 - Title:** Start investigation
 - Body:** Examining use of Snort in our network.

Task: Find Snort events

5. Navigate to **Search > Search** and run the search `index=main snort` for the last 60 minutes.
6. Navigate to **My Investigations** and open the **Snort Activity** investigation.
7. Select **Create New Entry > Action History**.
8. Select the `index=main snort` search to add it to your investigation.
9. Add another note:
 - Title:** Search shows Snort activity for last 60 minutes
 - Body:** Snort is not approved.

Task: Create a notable event to track our status.

10. In your investigation timeline, select the **Search executed** entry.
11. Click the `search index=main snort` link to display the search results.
12. Expand one of the snort events.
13. From the **Event Actions** menu, choose **Create notable event**.
14. Enter field values as follows:
 - **Title:** Snort activity example
 - **Domain:** Network
 - **Urgency:** High
 - **Owner:** {you}
 - **Status:** In Progress
 - **Description:** No authorized use of snort in our network—investigating.
15. Save the new notable event.

The Incident Review dashboard opens. Your ad hoc notable event should be the first notable event in the results list.
16. Select the event and click **Add Selected to Investigation**.
17. Make sure your Snort Activity investigation is selected and click **Save**.

Task: Analyze Snort activity.

At the bottom of the Splunk Web window is the investigation bar, and at the right side, you'll see icons for running a Quick Search (🔍), adding a note (📝), and adding an action history item (🕒).

18. At the lower left corner of the Incident Review dashboard, click the All Investigations icon (☰).
19. Select the **Snort Activity** investigation.
20. Click the Quick Search icon to open the Quick Search window.
21. In the search bar, execute the following search over the last 60 minutes:

```
index=main snort | stats count by category | sort -count
```

You see an overview of the types of attempted Snort activity.
22. Use the **Add to Investigation** button to log this search to your timeline.
23. Click the **Note** icon and add a note documenting the top two types of attacks (from the quick search results).
24. Update the quick search to include the destination IP addresses:

```
index=main snort | stats count by dest, category | sort -count
```
25. Add a note to document the top two destination (host) IP addresses.

Now you see which endpoints in your network are being targeted, and what types of attacks are being used by system.
26. Update the quick search to determine where the Snort attempts are originating:

```
index=main snort | stats count by src | sort -count
```
27. Add a note to document the most frequent source IPs.

Task: Investigate source systems.

28. In your Quick Search window, run this search for the last 60 minutes:

```
index=main snort src={most.common.src.ip}
```

Insert the most common src IP address from the previous search results.
29. Expand the details of one of the result events, and scroll down to the **src** field.
30. Open the field action menu for the **src** field.

There are many investigative tools here—you'll look at a couple.
31. Select the **Nslookup** option.

A new search window opens and shows the results of the **nslookup** command.
32. After examining this information, close the new search window, and add an action history item for the **nslookup** search to your investigation.
33. From the Quick Search window, open the **src** field's action menu again, and select the **Domain Dossier** option.

Domain Dossier is operated by centralops.net and provides basic **whois** information about IP addresses. Because this is an external web page, it will not appear in your action history. But you want to record this information in your investigation.
34. Use your browser's Print dialog window to save the Domain Dossier web page as a PDF document to your workstation.
35. Close the Domain Dossier web page.
36. Add a note to your investigation called **Domain Dossier Report** and use the file attachment option to add the saved PDF document.
37. Close the Quick Search window.
38. Click **My Investigations** and open the Snort Activity investigation.
39. Use the **Timeline** and **List** views to review all of the entries you created during the investigation.

With the above information, you can work with your network administrators to eliminate the snooping attacks. Any physical actions can also be logged in the timeline, as well as scans of any pertinent documents, copies of files, etc.

Lab Exercise 4 – Forensic Investigation

Description

In this lab exercise, you'll use some of the forensics dashboards to investigate some activity in your environment. First you'll dive into some more of Hax0r's activities in the Access domain. Then you'll do an investigation into some network traffic anomalies. Finally, you'll look into some malware issues in the endpoint domain.

Steps

Scenario: Follow up on the Hax0r incident.

Task: Use the Access Domain.

1. Navigate to Incident Review and search for **Hax0r**.
2. Open the details of one of Hax0r's incidents.
3. Open the field action menu for the **User** field. Note some of the options available.
4. Select **Access Search**. A new window opens, showing Hax0r's login attempts.
Note that all login attempts are on the same system (HOST-001), and are all failures.
5. All the attempts are using the **win:local** app. These login attempts are not coming across the network—they're originating at HOST-001.
Let's see how these Hax0r events fit into the overall access profile of your organization.
6. Navigate to **Security Domains > Access > Access Center**.
Notice that failed logins are very common (AUTH. ATTEMPTS key indicator), and that there are many login apps being used.
7. Change the **Action** filter dropdown to **failure**, and the **app** filter dropdown to **win:local**.
8. Submit the search.
9. Observe the access pattern in the top two panels—it's very repetitive, indicative of an automated script, and it's happening throughout most of the day.
10. In the **Access Over Time By App** panel, click one of the high peaks to drilldown into the activity at that point. You'll probably see a lot of activity from Hax0r, but there are others.
Based on this, you initiate an investigation into how the Hax0r account information might have been exfiltrated from your organization, and who might be using it.

Scenario: Examine the target server of the Hax0r attack to identify malicious software.

Task: Use the Malware Search and Center dashboards.

11. In ES, navigate to **Security Domains > Endpoint > Malware Search**.
12. Search for **HOST-001** using the **Destination** filter field over the last 60 minutes.
In the upper panel, you'll see a summary of the activity on the server that has been detected by a Sophos antivirus scanner, including the malware file name, the user ID associated with the file, and the signature, or type of virus software.
The lower panel contains the original events, including details like the virus type and action taken.
Note that if you expand the Mal/Packer raw events, several viruses have status = "Not cleanable", indicating they are still active on the system. Pick **Mal/Packer** to examine. Mal/Packer is a common virus in the wild, often associated with email-based phishing.
13. Navigate to **Security Domains > Endpoint > Malware Center**.
14. Examine the overall pattern of malware activity. Note that there are many infected systems, and several systems (like HOST-001) with multiple infections.
15. Note that Mal/Packer appears in the Top Infections panel. Click the Mal/Packer bar to see all systems affected by this malware.

HOST-001 is not the only system affected by Mal/Packer. Seeing this, you initiate a ticket with your IT team to begin removing the malware.

Scenario: As a network analyst, one of your daily tasks is to monitor the network for vulnerabilities. You will begin by checking on the ES Vulnerability Center to see if any new vulnerabilities have appeared since your last check.

Task: Use the Vulnerability Center and Search dashboards.

16. Navigate to **Security Domains > Network > Vulnerability Center**.
17. Make sure the dashboard is searching over the last 24 hours.
18. Note the values in the key indicators—especially total vulnerabilities. They’ve gone up quite a bit.
19. Examine the panel results. Note the relative number of vulnerabilities by signature (top vulnerabilities), and the list of most vulnerable hosts.
20. In the **Top Vulnerabilities** panel, locate the **USN 19-1: squid vulnerabilities** bar.
Note that depending on your browser, the longer vulnerability names may be compressed—hover your mouse over them to read them.
21. Click the **squid vulnerabilities** bar to drill down into the issues for this vulnerability type. There are potential issues with a Squid proxy server.
The Vulnerability Search dashboard opens and displays the events for this vulnerability. (Note: If for some reason squid vulnerabilities is not in the **Top Vulnerabilities** panel, navigate to the **Vulnerabilities Search** and search for ***squid*** in the **Signature** field over the last 24 hours.)
The top table in the search dashboard lists vulnerabilities by destination server (**dest**) in order of decreasing count of vulnerability issues.
22. Click the **dest** IP value in the top row of the table to drill down into issues for the most active server.
This opens a search page with events for the **dest** IP you selected. Note that the search uses the **Vulnerabilities** data model.
23. Expand one of the events and locate the event’s **dest** field.
24. Open the **dest** field’s **Actions** menu (at the right end of the field’s row) and review the selection of available tools to continue your investigation. Scroll to see all options.
25. Select **Intrusion Search (as destination)**.
This dashboard shows the types of IDS events that have been generated for this server (upper panel) and the source events (lower panel). Note the various **signature** values—these are the types of attacks happening on this server. FTP:AUDIT:REP-INVALID-REPLY is probably one of the most common types of intrusions.
The **src** values identify the origin of the attacks.
26. In the **signature** column, click **FTP:AUDIT:REP-INVALID-REPLY** to drill down to the source event(s).
In the new search page, you’ll see the detailed events detected by your vulnerability scanner. You can expand the time range of this search to see more events.

Scenario: The vulnerabilities you’ve identified so far have made you wonder what other intrusion activity might be happening.

Task: Use the Intrusion Center dashboard.

27. Navigate to **Security Domains > Network > Intrusion Center**.
28. For **IDS Type**, select **network**.
29. Make sure the time range is **Last 24 hours**, and click **Submit**.
30. Examine the values for the key indicator fields. High severity network attacks are on the rise.

31. Examine the summary panels. Note the pattern of attacks over time by severity and also the list of top attacks. Note the FTP vulnerability you saw before is listed here.
32. In the **Scanning Activity (Many Attacks)** panel, click the top IP bar to drill down to the Intrusion Search dashboard.

Once again, you see that FTP invalid replies are a large percentage of the overall intrusion issues. Based on the above, the vulnerability is significant. You initiate a ticket with IT to reconfigure your FTP servers to reduce the vulnerability.

Lab Exercise 5 – Risk Analysis

Description

In this lab exercise, you'll use the Risk Analysis dashboard to examine how risk is allocated to objects and users in your environment.

Steps

Scenario: Hax0r is a high-risk user—use the Risk Analysis dashboard to examine where this risk comes from.

Task: Examine user risk.

1. Navigate to the Incident Review dashboard and search for Hax0r.
2. Open the details of one of Hax0r's incidents. Note the number in the red box next to Hax0r's user ID. This is Hax0r's current risk score.
3. Click Hax0r's risk score to open the Risk Analysis dashboard (automatically filtered to Hax0r).
Based on this, you can see that Hax0r's risk comes from the **Identity - Activity from Expired User Identity** correlation search.
4. Clear Hax0r from the **Risk Object** filter field and re-run the search. Now you see all risk activity for the last 24 hours.
5. Examine the **Risk Modifiers over Time** graph. This shows you a diagram over time (default: previous 24 hours) that indicates points in time when risk scores on assets in your enterprise increased. Events where the risk score increased rapidly are cause for concern.
6. Click on the largest risk score column in the timechart. This drills down into the source events that triggered the increase in risk.
7. Examine the fields available for your use. The data in these fields can help you understand what threats, systems, processes, and users could be involved in the increased risk assessment.
8. Navigate back to the **Risk Analysis** dashboard (**Security Intelligence > Risk Analysis**).
9. Examine the panels showing risk scores by object, source, and most recent risk modifiers. Note that you can also drill down by object or risk source.
10. You see Hax0r in the risk score by object panel, but there are other risk objects and users too.
11. Re-sort the **Risk Score By Object** panel by **source_count**—this will show how many different sources of risk there are for each risk object, and put the ones with the most sources of risk at the top.
12. The top item is probably an IP address, and probably has 3 to 6 different sources of risk. Click this row to drill down.
Note that the drilldown search uses the **Risk** data model. Also notice that the events are stored in the **risk** index. Each event in risk is an association to a user or device and a risk score. This is where all risk scoring is stored.
All the risk sources are correlation searches. Individually, each correlation search severity may not be very high, but taken together, they are causing the risk score of this object to increase more than other objects. An investigation into why this object has so many sources of risk may be indicated.
13. Navigate back to the **Risk Analysis** dashboard and examine the **Most Active Sources** panel. You can re-sort this by risk score, risk_objects, or source to identify the most common sources of risk in your environment. This could help you prioritize your risk mitigation effort.

Scenario: You determine that the Hax0r account has not been compromised, and therefore you can reduce the risk for this user.

Task: Manually adjust a risk score.

14. In the **Risk Object** field, select **user** from the drop-down, then type: Hax0r

15. Click **Submit**.
16. Make a note of Hax0r's current risk score. You'll reset it to zero.
17. Click **+Create Ad-Hoc Risk Entry**.
18. Enter the negative value of Hax0r's current risk score. In other words, if the current score is **160**, enter **-160**.
19. Populate the remaining fields as follows:
 - Description: **resetting risk**
 - Risk object: **Hax0r** (this is case sensitive)
 - Risk object type: **user**
20. Click **Save**.
21. Refresh your browser window or select **Security Intelligence > Risk Analysis** again.
22. Filter the form to user **Hax0r** and submit the search.
23. You should now see a net risk score of zero for Hax0r
24. In the **Most Active Sources** panel, click the **AdHoc Risk Score** adjustment you just created to drill down into the risk index data.

Lab Exercise 6 – Web Intelligence

Description

In this exercise, you'll use the Web Intelligence dashboards to examine the potential issues posed by internal threats.

Scenario: Periodically, you want to review the types of user agents accessing your HTTP resources. The HTTP User Agent Analysis dashboard is very useful for this purpose.

Task: Perform HTTP User Agent analysis.

1. Navigate to **Security Intelligence > Web Intelligence > HTTP User Agent Analysis**.
2. Set the Standard Deviation Index selector to **All** and make sure the search range for the dashboard is **Last 24 hours**.
3. Submit the search.
4. Examine the key indicators, showing statistics about user agent string length. Recall that very short or very long user agent strings can be a sign of malicious intent.
Note the scatter chart in the User Agent Distribution panel. This chart shows the count for each user agent. Notice that one, Shockwave Flash, is very high.
5. In the **User Agent Details** list, the sort order defaults to descending by user agent string length. Examine some of the longer user agent strings, looking for embedded SQL or shell commands. These are common signs of attacks.
6. Look for the string "**FunWebProducts**" in one of the top few Mozilla user agent strings. You may have to navigate through a few pages to find it. It usually has a 116 character length. While not technically malware, this is evidence that at least some of your desktops are running Adware on their browsers that is probably not good for your network.
7. Re-sort the **User Agent Details** panel by decreasing **count**. Note that Shockwave Flash is indeed a very common user agent.

Scenario: You've decided that Flash is not a threat and you'd like to eliminate it from the list of user agents.

Task: Use a per-panel filter.

8. Select the row in the **User Agent Details** panel for Shockwave Flash.
9. Click **Advanced Filter...**
10. Make sure **Filter them...** is selected and select **Save**.
11. Confirm Shockwave Flash is no longer displayed in the panels.

Scenario: Examine the web site categories users are accessing.

Task: Use the HTTP Category Analysis dashboard.

12. Navigate to **Security Intelligence > Web Intelligence > HTTP Category Analysis**.
The source events for this dashboard all come from one sample server and one sample user, so the bar graph shows a flat profile.
13. Examine some of the categories displayed in the lower panel. Sort this panel descending by count.
Many of these categories are uninteresting and could be excluded by filtering.
However, some categories, such as weapons, drugs, etc., may be cause for concern.
14. Locate a questionable category, such as weapons or drugs, and drill down.
You'll see that the source events are from the **Web** data model.
15. Expand the details of one of the events.

16. Examine the fields available, such as **dest**, **src**, **user**, **url**, etc. All of this data could be important if launching an investigation of inappropriate user behavior.

You can use one of these events to create an incident.

17. From the **Event Actions** menu, select **Create notable event**. Populate the form as follows:

- Title: **Inappropriate website access**
- Domain: **Audit**
- Urgency: **Medium**
- Owner: **unassigned**
- Status: **Unassigned**
- Description: **Investigate user access to this suspicious website.**

18. Click **Save**.

Your new incident displays on the Incident Review dashboard. This can be the initiation of an investigation into the user's activities.

Lab Exercise 7 – User Intelligence

Description

In this lab exercise, you'll use the dashboards in the **User Intelligence** menu to examine the potential issues posed by internal threats. For an extended example of the internal threat tools, see docs.splunk.com/Documentation/ES/latest/Usecases/DataExfiltration.

Steps

Scenario: You are continuing your investigations into the incidents from the preceding exercise. You want to find out more about the assets and identities involved.

Task: Examine and learn more about the Hax0r user account.

1. Navigate to **Security Intelligence > User Intelligence > Identity Investigator**.
2. Enter **Hax0r** in the search field and set the time range to **last 24 hours**.
3. Click **Search**.
4. Note that **Hax0r** has been attempting to log in quite frequently. Notable events have been created by the **Activity from Expired User Identity** correlation rule.
5. Try using the pan/zoom controls at the bottom of the swim lanes to zoom in on the time just before and after the last notable event to make it easier to see the pattern of login events in the authentication swim lane.
6. Notice that the authentication events come in bursts, with many attempts in a very short time frame.
7. Click the bars in the All Authentication lane to see details, like the **src**, **dest**, **host** name, and number of events. Note that the action is failure, indicating no successful login. Make a note of the **dest** field value (HOST-001).
Note that in the details side bar there are options to drill down into the source events (the magnifying glass), share this result (as a URL), or create a notable event (the bell icon).
8. Click the notable event bar to see the details of the notable event generated.

Task: Investigate the server that Hax0r is attempting to access.

9. Navigate to **Security Intelligence > User Intelligence > Asset Investigator**. The Asset Investigator dashboard opens.
10. Enter the host name you discovered while investigating Hax0r's activities (HOST-001). Make sure the time range is **Last 24 hours** and that the pan/zoom controls at bottom are expanded to the full length of the time range.
11. You will probably see many authentications, possibly some IDS attacks, and perhaps a few changes along with the notable event you are investigating. This activity is all focused on this one server. Note that this is not a known server—there is no asset information for it—but ES is still tracking it.
12. Examine the details of some of the authentications, malware attacks, and any changes, if found.

Scenario: After working with the Hax0r incident, you want to get an overview of user activity in your environment to check for insider threats.

Task: Use the User Activity and Access Anomalies dashboards.

13. Navigate to **Security Intelligence > User Intelligence > User Activity**.
14. By default, the dashboard shows all user activity over the last 24 hours. Examine the key indicator values.
15. Note that Hax0r appears in the Users By Risk Scores panel—the correlation search results for Hax0r's activity have increased the user's risk. However, there are other users with elevated risk scores.

16. Note the users with non-corporate email and non-corporate web upload activity (external) sites. This could indicate dangerous activity by these users.
17. Select one of the users in the Non-corporate Web Uploads panel (such as **admin**). This opens the Identity Investigator dashboard for the admin user.
Initially, the default swim lane set is displayed, but there is an alternative set of lanes for investigating user activity.
18. Click the **Edit** icon above the list of swim lane names. Select the **User Activity** collection and close the modal.
19. You now see many web upload events. Click one of the darker bars, indicating a large number of events in that time period.
20. Examine the details on the right. Note the number of events indicated, the time range, and options to share the results or creating a notable event.
21. Click the (Q) icon to open the source events in a drilldown search.
22. Note that this data comes from the **Web** data model.
Some of the useful fields are `dest_ip`, `src_ip`, and `uri`.
23. Close the drilldown search window, and navigate back to the **User Activity** dashboard.
The Watchlisted Site Activity panel shows which users are accessing sites your company has added to the watch list.

Scenario: Examine the pattern of geographic access by your users.

Task: Use the Access Anomalies and Access Search dashboards.

24. Navigate to **Security Intelligence > User Intelligence > Access Anomalies**. The search executes by default over the last 60 minutes. Note the list of anomalous access incidents.
25. Try filtering the list by success vs. failure. There are likely examples of both.
26. Examine the app values, such as **sshd**. It's not surprising to see **sshd** events that happen concurrently in remote locations, but **login** or **windows:local** would be more suspicious.
27. Try clicking on a row in the top panel and note the drilldown results.
28. Return to the **Access Anomalies** dashboard and hover your mouse over the pie charts in the map. Note the summary of event statistics. Try drilling down on the pie charts to see more details.

Lab Exercise 8 – Threat Intelligence

Description

In this lab exercise, you'll use the Threat Intelligence dashboards to examine the potential issues posed by internal (user) and external threats. For an extended example of the internal threat tools, see docs.splunk.com/Documentation/ES/latest/Usecases/DataExfiltration.

Steps

Scenario: As a network security analyst, you want to be aware of any threat activity in your environment.

Task: Review threat activity.

1. Use the **Incident Review** dashboard to search for all **Threat** domain notables in the last 24 hours. There are probably many of them. Examine the details of a few.

You can run an ad-hoc search to see what types of threats we're dealing with.

2. Navigate to **Search > Search**.
3. Execute the following search over the Last 24 hours:

```
`notable` | stats count by threat_source_type
```

You're using the **notable** macro, which searches in the **notable** index and then adds all incident values such as owner, status, etc. Note there are both CSV and STIX sources. CSV sources are simple threat lists of IP numbers with no additional information—all you know is that you connected to a malicious site. The name of the list (**threat_source_id**) can tell you something about the type of threat. STIX, on the other hand, is a detailed threat information source from a TAXII server. This allows the **Threat Activity Detected** correlation search to look beyond simple IP addresses.

4. Execute the following search over the Last 24 hours:

```
`notable` | search threat_match_field = service | fields threat* dest
```

Note the information available in these events. This information comes from the STIX content downloaded from the TAXII server from Mandiant. This information indicates there is a possible compromised service named OSEASV.

5. In the top result event, locate the **dest** field (an IP address) and copy it to the clipboard. This is the server running the suspect service.
6. Navigate to **Security Intelligence > Threat Intelligence > Threat Activity**. This view shows you all activity associated with threat intelligence over the search period (default 24 hours), not just threat notable events. Examine some of the key indicator values and panel contents.
7. Change the **Search** filter field to **Destination** and paste the IP address you copied to the clipboard earlier.
8. Click **Submit**.

Note that the dashboard now shows the specific threat source and details for this threat.

9. Navigate to **Security Intelligence > Threat Intelligence > Threat Artifacts**.

This displays the entire content of the threat intelligence framework being managed by ES. It includes data from threat lists (block lists) as well as STIX and OpenIOC sources. The Threat Overview tab shows you a list of all the source threat intelligence, with a list of all the threat intelligence sources—i.e., threat lists (CSV) or advanced threat data (STIX, OpenIOC). The four other panels show a summary of artifacts (data from the threat intelligence) by type—Endpoint, Network, Certificate, and Email.

Each of the sub-tabs enable you to further drill down into the details contained in the threat intelligence ES has downloaded.

10. Change the **Threat Artifact** drop-down to **Service** and enter ***OSEASV*** in the Name field.
11. Click **Submit**.

The Threat Overview tab now shows you the source path to the threat intelligence (a STIX report from Mandiant), and the endpoint artifacts panel shows you a list of the known threat groups and categories.

12. Click the **Endpoint** tab and expand the row in the **Service Intelligence** panel. This is the detail in the Mandiant threat feed for this threat.

Lab Exercise 9 – Protocol Intelligence

Description

In this lab exercise, you'll work with the Protocol Intelligence dashboards.

Steps

Scenario: As a network security professional, you routinely monitor the status of network activity using Protocol Intelligence.

Task: Use Protocol Intelligence.

1. Navigate to **Security Intelligence > Protocol Intelligence > Protocol Center**.
2. Examine the panel contents.
3. In the **Connections by Protocol** panel, click the **http** segment to see a report of the HTTP connections by server.
4. Return to the Protocol Center dashboard
5. In the **Usage for Well Known Ports** panel, click the **dest_port** value in the first row to see details about the port in the **Traffic Search** dashboard, including a summary in the top panel, and individual events in the bottom panel.
6. Expand one of the events in the bottom panel and examine the fields available for analysis.
7. Navigate to the **DNS Activity** dashboard and examine the available data. Note the breakdown by query sources, DNS, and domain, as well as the most recent queries.
8. In the **Top DNS Queries** panel, locate the **Doc.exfil.ru** domain name.
This is a suspicious domain name and warrants further investigation.
9. Click **Doc.exfil.ru** to open the **DNS Search** dashboard.
10. Examine some of the systems making DNS queries for this domain—there seem to be a lot!
11. To investigate further, open a new search window and execute the following search over the Last 24 hours:

```
| datamodel Network_Resolution DNS search | search DNS.query=*exfil.ru
```


This search shows all DNS resolution queries for any servers in the exfil.ru domain. You see many happening in your network—this is a possible indicator of data exfiltration occurring. You should open an investigation immediately.
12. Navigate to the **SSL Activity** dashboard and examine the available data. Note the breakdown of connections by common DNS name, as well as recent SSL sessions showing authentication issuer, start and end time, and validity.
13. Navigate to the **Email Activity** dashboard. Here you can see at a glance the most prolific email senders, as well as rare senders and receivers. This can be useful to identify suspicious email activity.
14. Click one of the rarely seen senders to open the **Email Search** dashboard. You'll now see a report of that sender's emails and the associated raw events (from yesterday).
15. Expand one of the email events to see the details collected. Note that the body of the email is not collected, but the events do include a summary of the body contents in **content_body** and **content_transfer_encoding**, such as any embedded URLs.

Lab Exercise 10 – Glass Tables

Description

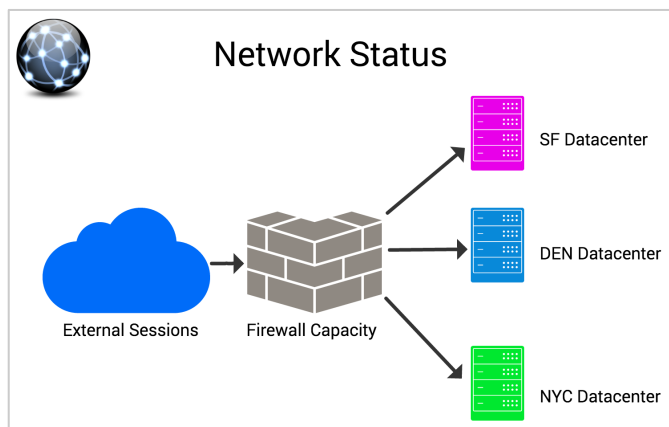
In this lab exercise, you'll create a glass table, and create a new key indicator that can be used on your glass table.

Steps

Scenario: Create a glass table to display network security indicators for display in your security operations center.

Task: Create the initial glass table.

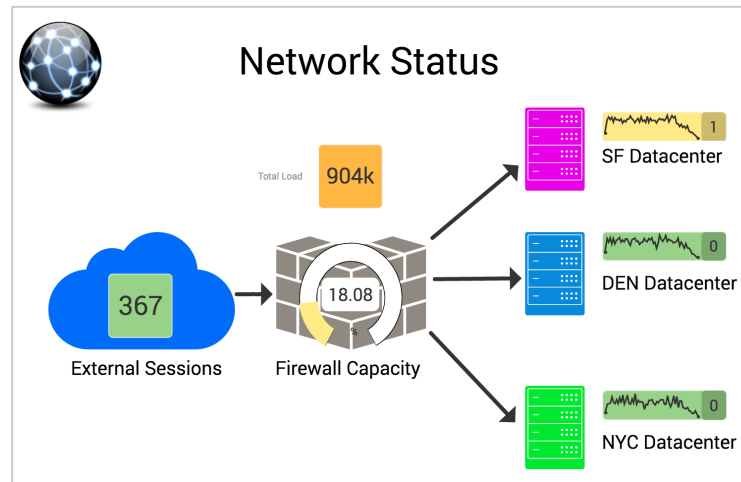
1. Navigate to **Glass Tables** and select **Create New Glass Table**.
2. Populate the dialog as follows:
 - Title: **Network Status**
 - Description: **Network security indicators**
 - Permissions: **Shared in App**
3. Click **Create Glass Table**.
4. Click **Network Status** to open the glass table in edit mode.
5. Lay out the glass table as below:



6. Use icons from the icon library.
7. Set colors as above—exact matches are not important.
8. For arrows, use the line control to draw lines, and then use the **Start** and **End Decorator** controls to configure the arrow heads.
9. Use the text control to add the text, and set the text size.
10. Your instructor will provide the background image file for the top-left icon.
11. Save your work.

Task: Add ad-hoc security metrics to your glass table.

In this task, you create four ad-hoc metrics. Leave all fields default unless specified. Make sure you click Update before moving on to the next metric. When this task is complete, your glass table should look like this:



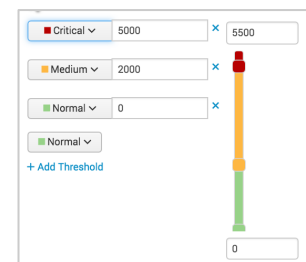
12. In the left sidebar, click **Ad hoc Search** and drag over the **External Sessions** (cloud) icon, then release.

13. Position the box in the center of the graphic.

Tip: Use the left, right, up, and down arrow keys.

14. Populate the right sidebar as follows:

- Search: `index=main sourcetype=stream:http earliest=-60m latest=now | stats dc(src_ip) as count`
- Threshold field: **count**
- Thresholds: **On**
- Threshold map: per image on right
- Viz type: **single value**



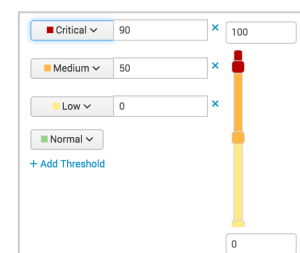
15. Click **Update**.

16. Click **Save**.

17. Repeat the above steps to create three more Ad hoc Search widgets:

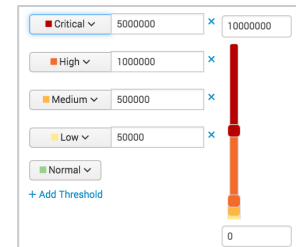
Firewall Capacity:

- Search: `index=main sourcetype=stream:http earliest=-60m latest=now | stats sum(bytes) as load | eval pct_cap = (load / 50000)`
- Threshold field: **pct_cap**
- Thresholds: **On**
- Threshold map: per image on right
- Viz type: **gauge**



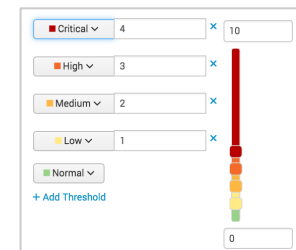
Total Load:

- Label: **Total Load**
- Label Location: **Left**
- Search: `index=main sourcetype=stream:http earliest=-60m latest=now | stats sum(bytes) as Load`
- Threshold field: **Load**
- Thresholds: **On**
- Threshold map: per image on right
- Viz type: **single value**



SF Datacenter:

- Search: `index=main host=acme-001 earliest=-60m latest=now | timechart count`
- Threshold field: **count**
- Thresholds: **On**
- Threshold map: per image on right
- Viz type: **sparkline**



- Copy and paste the **SF Datacenter** metric twice, and position the copies for the **DEN** and **NYC Datacenter** metrics.
- Edit the **DEN Datacenter** metric and replace "acme-001" with "acme-002", then click **Update**.
- Repeat with the **NYC Datacenter** and replace "acme-001" with "acme-003", then click **Update**.
- Click **Save**.
- Switch to **View** mode and examine the glass table.
- Try changing the time setting to different points in time and observe the changes.
- Click on some of the metric widgets—note the drilldown searches that are opened. If you wanted a different glass table, dashboard or external web page to open instead, each widget has a custom drilldown setting to allow you to control navigation.