







Splunk: Search, Statistics and Report

Cybersecurity
SIEMS Day 2



Class Objectives

By the end of class today, students will be able to:

-  Use SPL to create advanced searches.
-  Describe how pipes are used to chain together a series of SPL commands.
-  Use statistical methods such as frequencies, baselines, and thresholds.
-  Analyze events to develop baselines and thresholds.



Activity: Warm-Up Interview Quiz

In this activity, you will simulate answering questions in a technical interview about Splunk Enterprise.

Activities/1_interview

Suggested Time:
15 Minutes



Warm-Up Review

Execute the following searches and explain why you are conducting each investigation and what is returned in the search events.

1. **host=quiz sourcetype=access_* AND (status=500 OR status=404)**

What: This search monitors for **several internal errors** or **pages not found errors** on all servers.

Why: To check website performance issues.

New Search Save As Close

sourcetype=access_* AND (status=500 OR status=404) All time

✓ 1,423 events (before 3/5/19 12:51:20.000 PM) No Event Sampling Job

Events (1,423) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 Next

< Hide Fields All Fields

SELECTED FIELDS
a action 5
a categoryId 1
a host 3

i	Time	Event
>	2/28/19 6:18:59.000 PM	198.35.1.75 - - [28/Feb/2019:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645

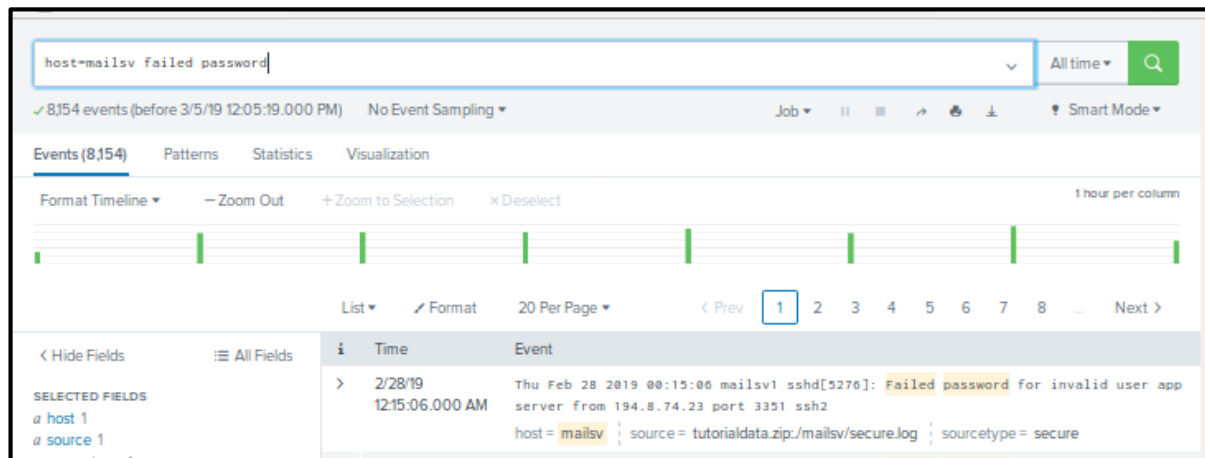
Warm-Up Review

Execute the following searches and explain why you are conducting each investigation and what is returned in the search events.

2. `host=quiz source=*mailsv/secure.log failed password`

What: This search looks for password attempts on the mail server host in secure.log file.

Why: To investigate possible password cracking.



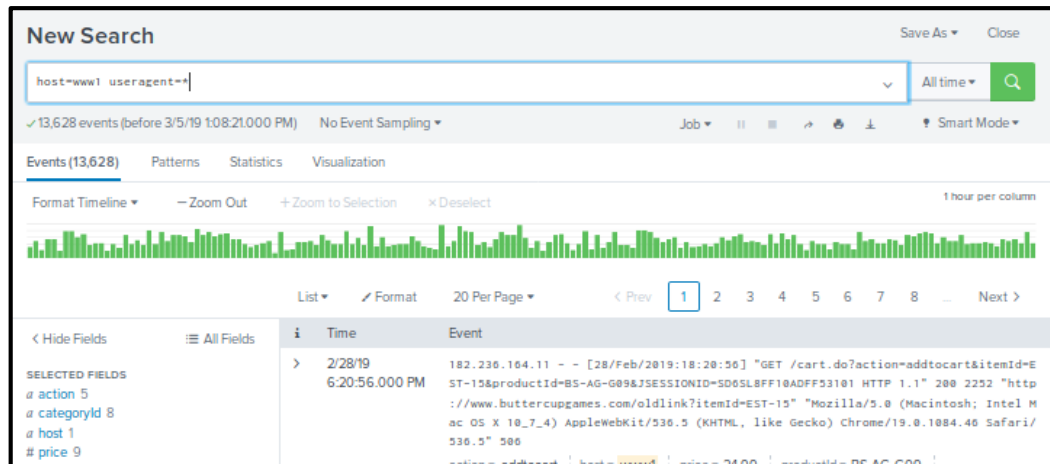
Warm-Up Review

Execute the following searches and explain why you are conducting each investigation and what is returned in the search events.

3. `host=quiz source=*www1* useragent=*`

What: This search can be used to analyze a request header.

Why: To track down specific information for requests made to the buttercupgames site.



Warm-Up Review

Execute the following searches and explain why you are conducting each investigation and what is returned in the search events.

4. “?msg=Credit*” AND file=“error.do” AND source!=*www2*

What: This search returns the purchase date, purchase item ID, user agent and client IP address for transactions on all hosts except www2.

Why: To Investigate possible credit card fraud.

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `"?msg=Credit*" AND file="error.do" AND host!=www2`. Below the search bar, it indicates 101 events were found. The interface is set to 'Smart Mode' and shows a timeline visualization of the search results. The timeline shows several green bars representing events over time. Below the timeline, there is a table of search results. The table has columns for 'Time' and 'Event'. The first event is dated 2/28/19 at 5:57:58.000 PM. The event details show a POST request to `/cart/error.do?msg=CreditDoesNotMatch` with a session ID and a user agent string.

Time	Event
2/28/19 5:57:58.000 PM	12.130.60.5 - - [28/Feb/2019:17:57:58] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD5SL6FF7ADFF53801 HTTP 1.1" 200 1167 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 232

Baselining



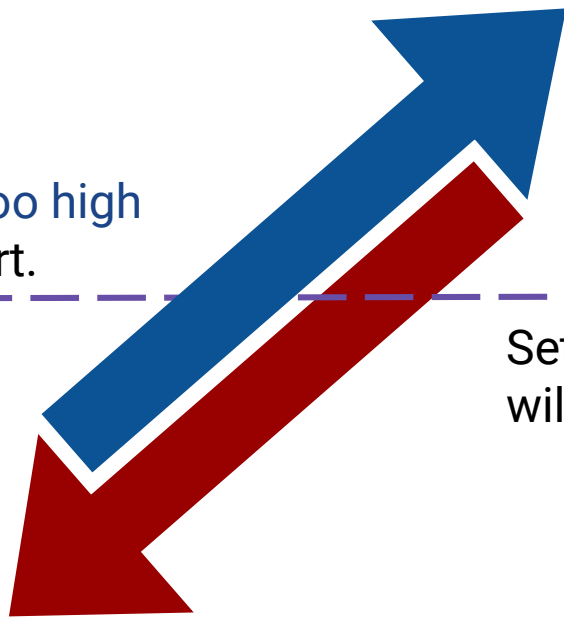
Baselining is the process of analyzing historical data in order to establish a metric of normal activity.

Setting a **Baseline** threshold

After analyzing historical data to establish a normal volume of activity, we need to establish an *abnormal* volume **threshold** that will trigger an alert if crossed.

Setting the threshold **too high**
will risk missing an alert.

Setting the threshold **too low**
will create too many false positives.



Using the SPL Search Pipeline



We have already used the Pipe Operator “|” to send the standard output of one command to the standard input of another command.

Unix Review: Pipes and Pipelines

What do each of these commands do?

```
$ ps -aux | wc -l
```

```
$ ls var/log/*.log | grep conf | wc -l
```

Unix Review: Pipes and Pipelines

What do each of these commands do?

```
$ ps -aux | wc -l
```

- This command displays the number of processes running in the system.

```
$ ls var/log/*.log | grep conf | wc -l
```

Unix Review: Pipes and Pipelines

What do each of these commands do?

```
$ ps -aux | wc -l
```

- This command displays the number of processes running in the system.

```
$ ls var/log/*.log | grep conf | wc -l
```

- This command gets the list of files in the **var/log** directory with the ***.log** extension.
 - The output from the **ls** command is passed to the **grep** command to look for the string **conf**.
 - The output from the **grep** command is passed to the **wc** command to count the number of lines.

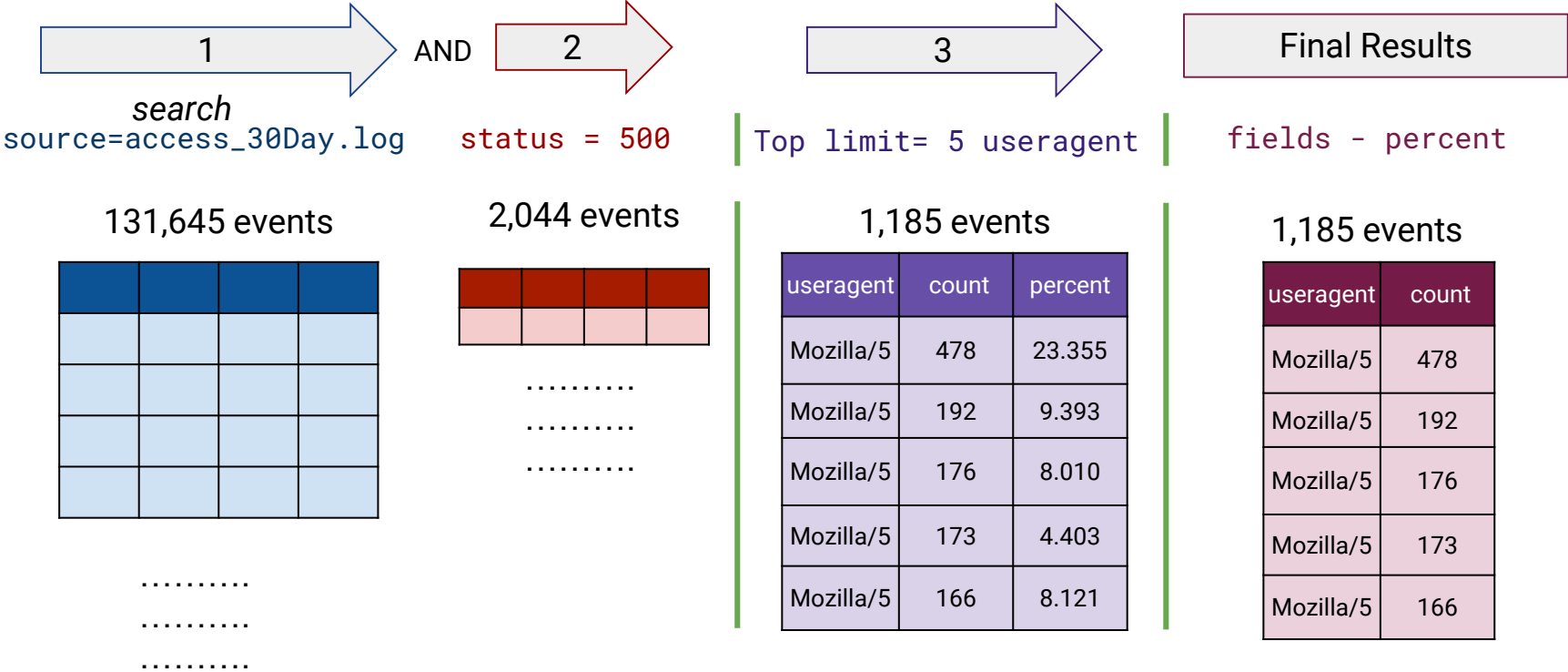
How do Pipes and Pipelines Work?

Pipes are used in Search Process Learning (SPL) to narrow down search result to specific criteria:

- Like Unix, a vertical bar | is used to chain together a series (or pipeline) of search commands.
- Commands are processed from left to right.
 - The results of the command to the left of the | operator is fed into the command to the right of the | operator.
- The intermediate command results table from each search is used (*or piped*) as input to the next command.

How Do Pipes and Pipelines Work?

```
source=access_30DAY.log status=500 | top limit=5 useragent
```





Activity: Using Pipes in Splunk

In this activity, you will practice using the Splunk search pipeline using alert logs from SNORT IDS.

Activities/2_pipes

Suggested Time:
20 Minutes



Using Pipes in Splunk Review

Part 1: *Create a search that will find all alerts for port scanning activity. Display results for the top destination IP addresses.*

Search command:

```
host="remote-snort" | top dest_ip
```

Using Pipes in Splunk Review

Part 1: *Create a search that will find all alerts for port scanning activity. Display results for the top destination IP addresses.*

Search command:

```
source="alert_json_000015.log" | top dest_ap
```

How many search results were returned from the top command?

Using Pipes in Splunk Review

Part 1: *Create a search that will find all alerts for port scanning activity. Display results for the top destination IP addresses.*

Search command:

```
source="alert_json_000015.log" | top dest_ap
```

How many search results were returned from the top command?

The **top** command returns the first 10 search results by default.

Using Pipes in Splunk Review

Part 1: *Create a search that will find all alerts for port scanning activity. Display results for the top destination IP addresses.*

Search command:

```
source="alert_json_000015.log" | top dest_ap
```

How many search results were returned from the top command?

The **top** command returns the first 10 search results by default.

Look at the Interesting Fields down on the protocol. What were the top three scans that were performed?

Using Pipes in Splunk Review

Part 1: *Create a search that will find all alerts for port scanning activity. Display results for the top destination IP addresses.*

Search command:

```
source="alert_json_000015.log" | top dest_ip
```

How many search results were returned from the top command?

The **top** command returns the first 10 search results by default.

Look at the Interesting Fields down on the protocol. What were the top three scans that were performed?

- ICMP
- TCP
- ARP

Using Pipes in Splunk Review

Part 1: *Create a search that will find all alerts for port scanning activity. Display results for the top destination IP addresses.*

Narrow the **search** to contain only the **TCP port scans** for the **top five** source IP addresses. Show **only** the number of search results

This search command uses the logical **AND** operator and two pipes.

```
source="alert_json_000015.log" AND proto="TCP" | top limit=5 src_ip | fields - percent
```


Using Pipes in Splunk Review

Part 2: Investigate alerts that indicate remote code execution.

Sort by the destination AP in descending order.

```
source="alert_json_000015.log" | sort -dest_ap
```

Using Pipes in Splunk Review

Answer the Questions / Fill in the Blanks

1. Limiting search by _____ is key to faster results and is a best practice

Time

2. What are the three main search modes?

Fast, Verbose, and Smart

3. _____ mode has discovery OFF for event searches. No event or field data for stats searches.

Fast

4. _____ mode has all events and field data; switches to this mode after visualization.

Verbose

Using Pipes in Splunk Review

Answer the Questions / Fill in the Blanks

5. _____ mode (default-based on search string data) has field discovery ON for event searches. No event or field data for stats searches.

Smart

6. List the three booleans

NOT, AND, OR

7. When searching for exact phrases you need to use _____

Quotations

8. _____ fields that appear by default are host, sourcetype, source.

Selected Fields

9. Having only the choices of inclusion and exclusion, which is preferable?

Exclusion is better than inclusion

Take a Break!



Using Tables to Display Events in Splunk



Now, we will continue to use pipelines and demo how to use the table command to return a table with specified fields.

Using Tables to Display Events in Splunk

Next, we will use the table command to return a table with specified fields.

- By default, the columns in a table are labeled using the field name, but this may not always be the most useful labeling method.
- For example: The count field can mean different things in different searches: count of errors? count of purchases?
- Labeled Tables simplifies the process of interpreting results of searches in reports and dashboards.

Using Tables to Display Events in Splunk

The Table Command

```
source="alert_json_000015.log" proto="UDP" src_ap="192*" dst_ap="192*" | table  
proto, src_ap, dst_ap, | rename proto AS "Protocol" src_ap AS "Source IP and Port"  
dst_ap AS "Destination IP and Port"
```

- The table command is preceded by a pipe “|” character.
- The rename command is used to create the labels for the columns.
 - It is preceded by a pipe character.
 - Columns are displayed in the same order that fields are specified.
- The first AS statement sets the proto field to display the text **Protocol** in the column header.
- The next AS statements set the src_ap and dst_ap fields display the text **Source IP and Port** and **Destination IP and Port**.



Activity: Using Tables in Splunk

In this activity, you will create a search that uses a table and removes duplicates.

Activities/3_tables

Suggested Time:
10 Minutes



Using Tables in Splunk Review

Create a search that returns events for Snort rules starting with **122**.

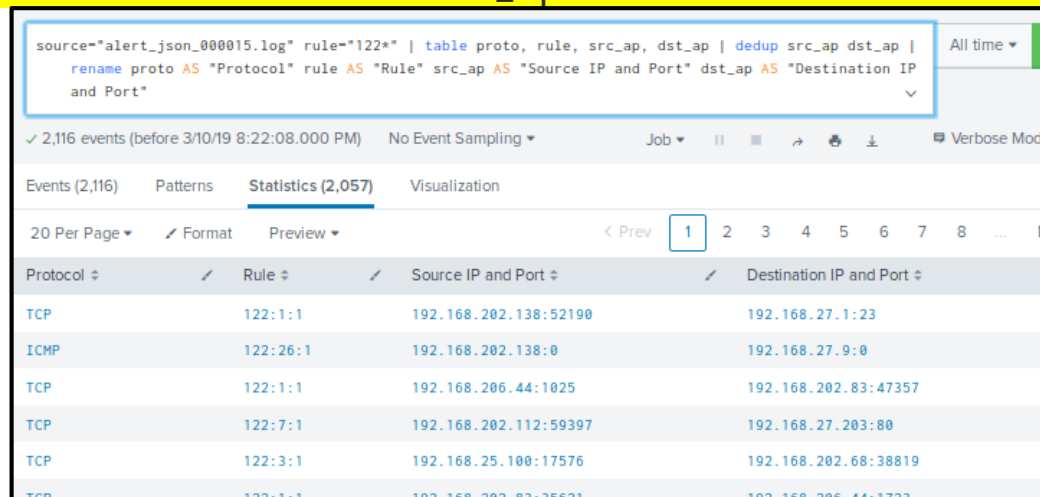
- Remove any duplicate source or destination IPs.
- Create a table with the following fields: protocol, rule, source and destination ips.
- Label the columns: Protocol, Rule, Source IP and Port and Destination IP and Port.

Using Tables in Splunk Review

Create a search that returns events for Snort rules starting with **122**.

Search command:

```
source="alert_json_000015.log" rule="122*" | table proto, rule, src_ap, dst_ap | dedup src_ap dst_ap | rename proto AS "Protocol" rule AS "Rule" src_ap AS "Source IP and Port" dst_ap AS "Destination IP and Port"
```



source="alert_json_000015.log" rule="122*" | table proto, rule, src_ap, dst_ap | dedup src_ap dst_ap | rename proto AS "Protocol" rule AS "Rule" src_ap AS "Source IP and Port" dst_ap AS "Destination IP and Port"

✓ 2,116 events (before 3/10/19 8:22:08.000 PM) No Event Sampling Job ▾ || ▢ ↻ ⚙ ⬇ 🔊 Verbose Mod

Events (2,116) Patterns **Statistics (2,057)** Visualization

20 Per Page ▾ ✎ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ...

Protocol	Rule	Source IP and Port	Destination IP and Port
TCP	122:1:1	192.168.202.138:52190	192.168.27.1:23
ICMP	122:26:1	192.168.202.138:0	192.168.27.9:0
TCP	122:1:1	192.168.206.44:1025	192.168.202.83:47357
TCP	122:7:1	192.168.202.112:59397	192.168.27.203:80
TCP	122:3:1	192.168.25.100:17576	192.168.202.68:38819
TCP	122:1:1	192.168.202.83:35631	192.168.206.44:1732

Alerts in Splunk

Understanding the Splunk Alert

Remember from last class: Monitoring and alerting is a key component in Splunk



Alerts are used to monitor for and respond to specific events



Alerts can look for events in real time or on a schedule.



Alert can be assigned a priority, such as Information or Critical.

Parts of a Splunk Alert

Splunk alerts have a structure that defines how alerts are configured and handled:

alert-type **triggering-options** **throttling-options**

Alert Type: In Splunk, there are two alert types: *scheduled* and *real-time*.

- The alert type determines when events are searched
- Timing options or cron syntax can be used.

Triggering Option specifies *how* and *the number of times* an alert is triggered.

- Dependent on the alert type.

Throttling Options specifies the *time period of suppression*.

- Dependent on the alert type.

Real-Time Alerts

Real-time alerts monitor events *continuously* and can be configured to trigger once per-result or within a rolling time window.

Example 1: Trigger an alert every time there is a password failure on the root account.

- The triggering options are set to alert every time there is a search result, a.k.a *per-result triggering*.
- A custom script is run to alert the security team.

Example 2: Triggering an alert if a service has more than three errors in a minute.

- Configure a real-time alert that searches for the service error event with a specified one minute *rolling* window.
- An email is sent to the operations team.

Scheduled Alerts

Scheduled alerts, *as it sounds*, search for events a repeated schedule.

Example : Monitoring how often a server returns a 500 error.

- Create a scheduled alert that searched for 500 errors **every half hour** and triggers an event when there are more than 50 results.
- A Notification is logged to the TRiggered alerts list.

It is important to schedule a time range that prevents data from being evaluated twice in a search.

Event s should be scheduled with a minimum of a one-minute delay.



Activity: Using Alerts to Monitor System Files

In this activity, you will create an alert that will be logged in the Triggered Alert list.

Activities/4_alerts

Suggested Time:
10 Minutes



Using Baselines to Create Effective Alerts

You are tasked with monitoring a web application where customers can purchase your company's products. You are concerned that there is a threat of an attacker attempting to brute force log in to your application.

How can we use Splunk so that we are aware if a brute force attack is occurring?

Create an alert.

Why isn't it ideal for an alert to triggered every time there are several failed attempts?

Customers may have forgotten their passwords, and have tried to log-in several times. This is known as a **false positive**.



Student Activity: Alert Fatigue

In this activity, you will read an article on a major security concern called alert fatigue and then answer the provided questions.

Activities/5_baseline

Suggested Time:
10 Minutes



Baselining Demo

We'll create a baseline demo on a sample Windows event log.

01

Load the event logs file.

02

Run a search.

03

View the search results.

04

Change Search criteria to look at failed logins.

05

Identify the spike in locked users.

06

Identify the baseline of normal activity.

07

Determine a threshold for an alert.

Alert Fatigue Review

1. Define alert fatigue.
2. Identify one concerning takeaway from this article.

Alert Fatigue Review

1. Define alert fatigue.

Alert fatigue occurs when one is exposed to such a large number of frequent alerts that they become desensitized to them.

2. Identify one concerning takeaway from this article.

Alert Fatigue Review

1. Define alert fatigue.

Alert fatigue occurs when one is exposed to such a large number of frequent alerts that they become desensitized to them.

2. Identify one concerning takeaway from this article.

There are many takeaways from this article. Arguably, the biggest is that 31.9% of security professionals ignore alerts because there are too many false positives.

Alert Fatigue Review

3. Which organization was affected by alert fatigue? What happened?

4. How can a company prevent alert fatigue?

Alert Fatigue Review

3. Which organization was affected by alert fatigue? What happened?

Target was affected by alert fatigue in a 2014 breach. The security product they were using correctly alerted them of the breach. However, due to high volume of alerts and the frequency of false alerts, Target's IT security team ignored it.

4. How can a company prevent alert fatigue?

Alert Fatigue Review

3. Which organization was affected by alert fatigue? What happened?





Target was affected by alert fatigue in a 2014 breach. The security product they were using correctly alerted them of the breach. However, due to high volume of alerts and the frequency of false alerts, Target's IT security team ignored it.

4. How can a company prevent alert fatigue?

- Create better alerts that have fewer false positives.
- Create less alerts.
- Create alerts that have severity indicators, such as Critical / High.

Class Objectives

By the end of class today, students will be able to:

-  Use SPL to create advanced searches.
-  Describe how pipes are used to chain together a series of SPL commands.
-  Use statistical methods such as frequencies , baselines, and thresholds.
-  Analyze events to develop baselines and thresholds.