Cybersecurity

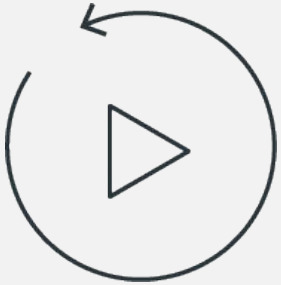
Splunk Reports and Alerts

SIEM Day 3

Class Objectives

By the end of class, you will be able to:

1. Use the SPL commands stats and eval to create new fields in Splunk.
2. Schedule statistical reports in Splunk.
3. Determine baselines of normal activity in order to trigger alerts.
4. Design and schedule alerts to notify if an attack is occurring.



Let’s **recap**

Today, we will continue to learn about Splunk's capabilities.

First, let's review what was covered in the last class.

Splunk Review

Splunk provides software utilities that search, analyze, and monitor big data with a straightforward interface. We can add additional functionality to Splunk with apps and add-ons for specific vendors and industries.

(splunk.com)

Splunk Review

Splunk has three primary methods for accessing data:

Monitoring

Splunk monitors logs from a system, device, or application to which it has direct access.

Businesses commonly use this method to monitor their production environment.

Forwarding

Install a program called a forwarder on the system from which logs are collected.

Forwarders forward logs from a device into the Splunk system.

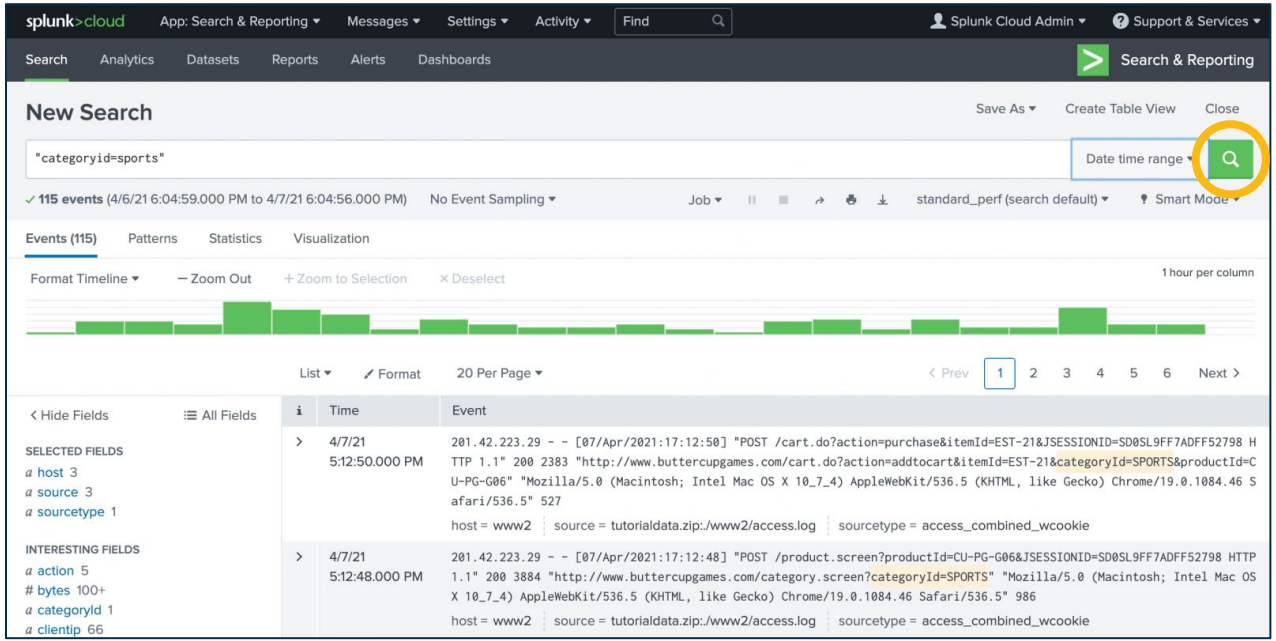
Uploading

Manually upload logs directly into your Splunk repository.

While monitoring and forwarding are important to understand conceptually, we will primarily use the upload process for the remainder of this class.

Splunk Review

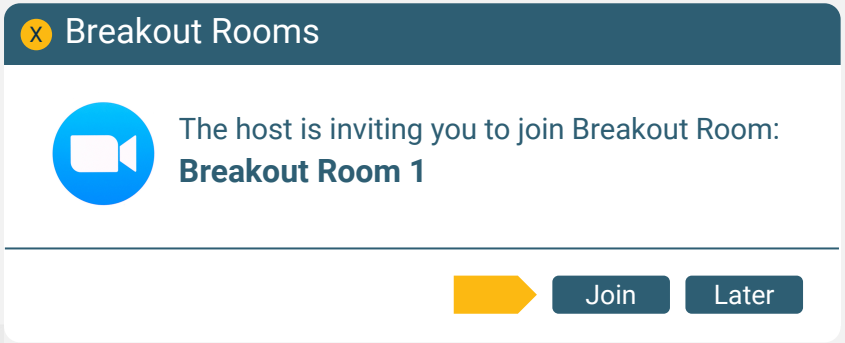
Splunk's primary feature is **searching**, which uses a coding language native to Splunk called SPL.



Splunk uses **time-based search**, in which each event or log has a time associated with it.

Activity:
Splunk Warm Up

In this activity, you will analyze logs from a Fortinet IPS system, determine the security issue, and provide mitigation strategies.



Suggested Time:
15 Minutes

Time’s up!

Let’s review

Questions?

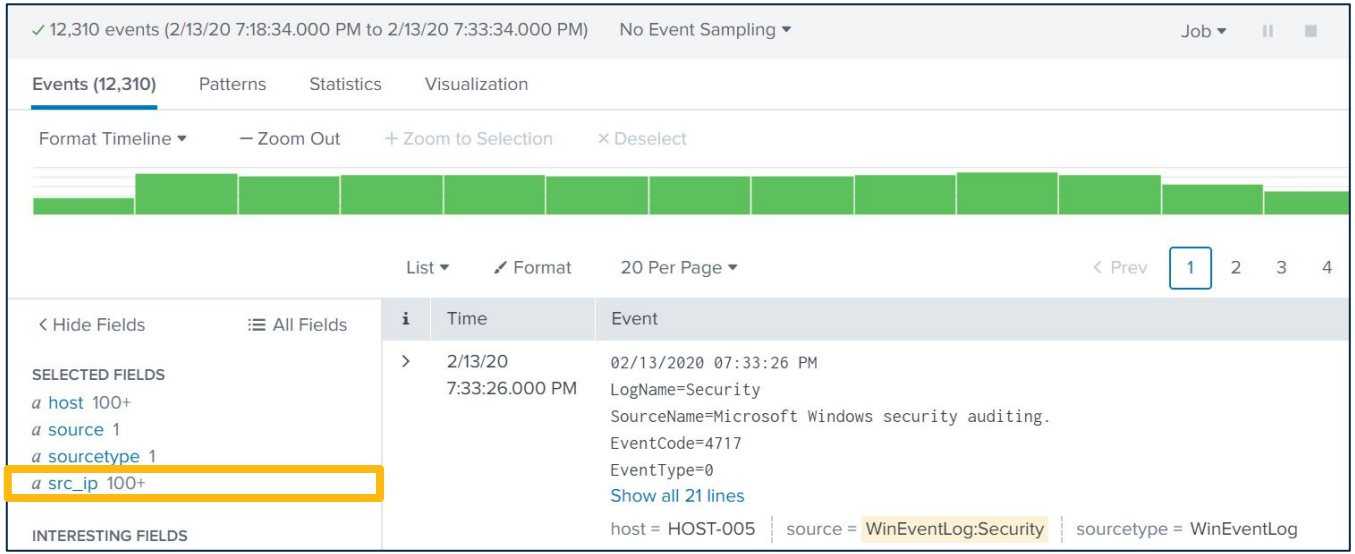
Splunk Statistics

Splunk Statistics

Security professionals often need to present Splunk search results to non-technical audiences using simple formats.

For example:

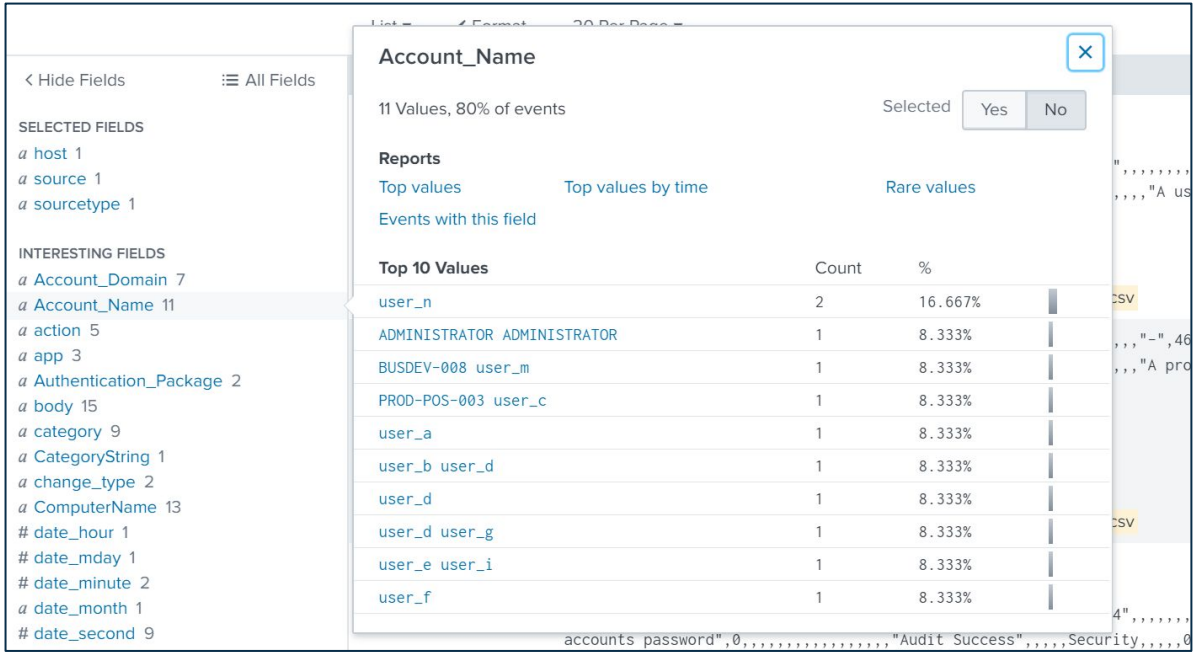
If we need to illustrate the top 10 IP addresses from a DoS attack, this results page could be confusing to a non-expert.



Splunk Statistics

Splunk uses the Statistics feature to display specific data points from search results in an easy-to-read format.

The stats command is the most basic Splunk command to create a statistics report.



We will use the stats command to create a simple statistical report of the top account names (Account_Name) being targeted in a brute-force attack.

Instructor **Demonstration**

Splunk Statistics

Creating Fields with eval

We can use Splunk to create new fields and add them to a statistical report.

For example:
Suppose we are analyzing logs for potential brute-force attempts.

Our logs have event codes (`EventCode`) that assign numerical codes to events.

`EventCode 4740` indicates a user lockout.

Since user lockouts are a potential identifier of a brute-force attack, we can create a new field to identify events that contain this event code.

If the `EventCode` field has a value of `4740`, the field value will be `Potential Brute Force`.

If the field does not have a value of `4740`, the field value will be `Not Brute Force`.

The eval Command

We can use the eval command to create fields.

1. The eval command calculates an expression (such as if then) and places the resulting values into a search field.

2. If the search field doesn't exist, it creates a new search field.

3. If the search field does exist, it overwrites the field with the new values.

```
source="statsreport.csv" | eval BruteForce = if('EventCode'="4740",
"Potential Brute Force", "Not Brute Force")
```

The eval Command

We can use the eval command expressions, such as if, and place the resulting values into a search field.

Searches through all the results from the `statsreport.csv` file.

```
source="statsreport.csv" | eval BruteForce =
if('EventCode'="4740", "Potential Brute Force", "Not Brute Force")
```

The eval Command

We can use the eval command expressions, such as if, and place the resulting values into a search field.

Creates a new field called `BruteForce`.

```
source="statsreport.csv" | eval BruteForce =
if('EventCode'="4740", "Potential Brute Force", "Not Brute Force")
```

The eval Command

We can use the eval command expressions, such as if, and place the resulting values into a search field.

```
source="statsreport.csv" | eval BruteForce =
if('EventCode'="4740", "Potential Brute Force", "Not Brute Force")
```

States the following expression: “If the `EventCode` field has a value of `4740`.”

The eval Command

We can use the eval command expressions, such as if, and place the resulting values into a search field.

```
source="statsreport.csv" | eval BruteForce =
if('EventCode'="4740", "Potential Brute Force", "Not Brute Force")
```

Continue the statement,
“If true, name this value
`Potential Brute Force`.”

The eval Command

We can use the eval command expressions, such as if, and place the resulting values into a search field.

```
source="statsreport.csv" | eval BruteForce =
if('EventCode'="4740", "Potential Brute Force", "Not Brute Force")
```

Continues the statement, “If false, name this value `Not Brute Force`.”

The eval Command

We can use the eval command expressions, such as if, and place the resulting values into a search field.

Searches through all the results from the `statsreport.csv` file.

Creates a new field called `BruteForce`.

```
source="statsreport.csv" | eval BruteForce =
if('EventCode'="4740", "Potential Brute Force", "Not Brute Force")
```

States the following expression: “If the `EventCode` field has a value of `4740`.”

Continue the statement, “If true, name this value `Potential Brute Force`.”

Continues the statement, “If false, name this value `Not Brute Force`.”

Activity:
Splunk Statistics

In this activity, you will create statistical reports to illustrate details about the DoS attack.

Suggested Time:
15 Minutes

Time’s up!

Let’s review

Questions?

Splunk Reports

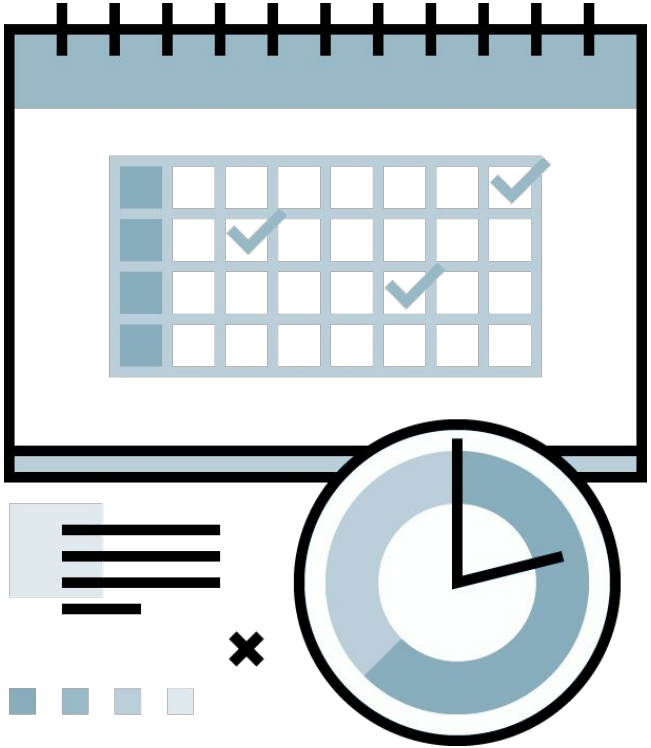
Splunk Reports

Statistical reports may need to be run at specific or recurring times.

For example:

If an organization is experiencing suspicious network attacks around 12am daily, it would want to analyze its network traffic every night at that time.

With Splunk, we can create and schedule custom reports to automate this task.



Splunk Report Demonstration

In the following demonstration, we will create and schedule a report using the continued scenario of monitoring brute-force attacks:

1. We were notified that the most recent brute-force attacks happened around 12am.
2. Therefore, we will run a report at 1am each night to view activity for the past several hours.
3. We'll also automate an email linking to the report after it runs.

Instructor **Demonstration**

Creating and Scheduling Reports

Activity:
Splunk Reports

In this activity, you will schedule a statistical report for OMP management so they can review the current state of the attacks against a server.

Suggested Time:
15 Minutes

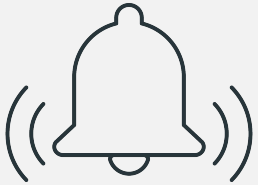
Time’s up!

Let’s review

Questions?

Break

15 mins

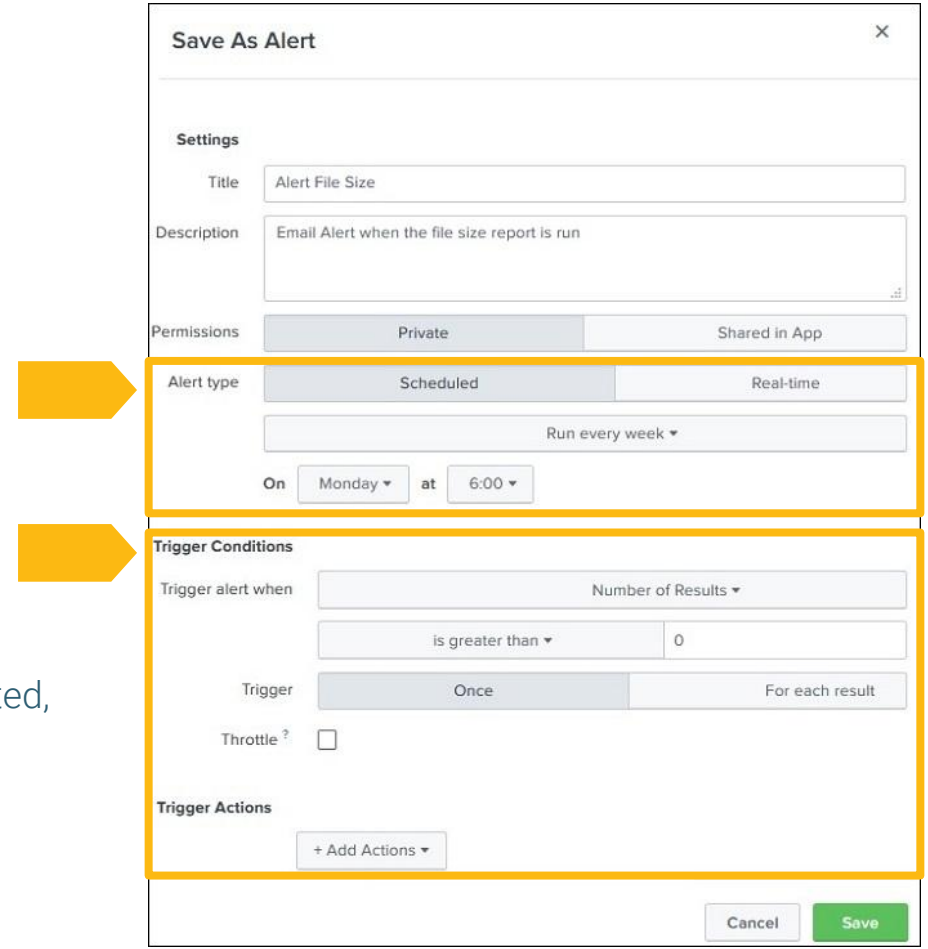


Splunk Alerts

Splunk Alerts

So far we have covered how Splunk statistics and reports can help information security professionals identify security issues.

- This process can be further improved through the use of alerts.
- Splunk alerts are designed to automatically notify one or more individuals when a specific condition, known as a trigger condition, is met.
- Splunk alerts are automatic. Once they are created, Splunk's software checks the trigger condition.



Splunk Alerts

A Splunk user selects a trigger condition based on the security event they are trying to monitor. Trigger conditions contain the following:

01

Search/report results indicate which criteria to check.

For example:
300 logins have been attempted.

02

Time parameters indicate the time period to check.

For example:
Within last 24 hours

03

Schedule determines the frequency with which these criteria are checked.

For example:
Every day at 12pm

Splunk Alerts

When the condition is met, a **trigger action** is executed to alert the Splunk user.
For example:

```
"Send an email to soc_manager@acme.com."
```

In summary, the complete alert would be:

```
Every day at 12pm, check if at least 300 login attempts have
occurred within the last 24 hours. If this condition is met,
send an email to soc_manager@acme.com.
```

Baselining

Designing Strong Alerts

A required skill for designing strong alerts is avoiding **false positives** and **false negatives**.

	False positive	False negative
What occurred	Regular login activity	Brute-force attack
Alerts	Yes	No
Outcome	Alerts went off but security professionals identified a non-issue.	No alerts went off, a brute-force attack occurred, and several accounts were breached.

False Positives

False positives occur when conditions are met and an alert is triggered, but the security situation did not actually occur.

1. For example, an alert is created to detect suspicious login activity on our Linux server.
2. The chosen criteria checks activity every hour and creates an alert when 10 login attempts occur within an hour.
3. Several alerts were triggered per these conditions, but further research determined the alerts were set off by normal user activity.
4. The SOC realizes that 10 login attempts within an hour is not very suspicious.

False Negatives

False negatives occur when the condition is met and an alert is not triggered, meaning the security situation occurred undetected.

1. For example, an alert was created to detect suspicious login activity on our Linux server.

2. The chosen criteria checks activity every hour and creates an alert when 500 login attempts occur within an hour.

3. Suspicious login activity did occur on the server when an attacker tried to brute force the Linux server with 400 attempts, but no alerts were triggered.

Security professionals can avoid these false results by using **baselines** to design their alerts.

Baselining is a method of looking at historical data to determine what we should consider as normal activity.

Instructor **Demonstration**

Baselining

Setting a Baseline Threshold

Baselining is a method of looking at historical data to determine typical activity, known as a threshold. When the **threshold** is exceeded, an alert is triggered.

Setting the threshold **too high** risks missing an alert.

Setting the threshold **too low** creates too many false positives.

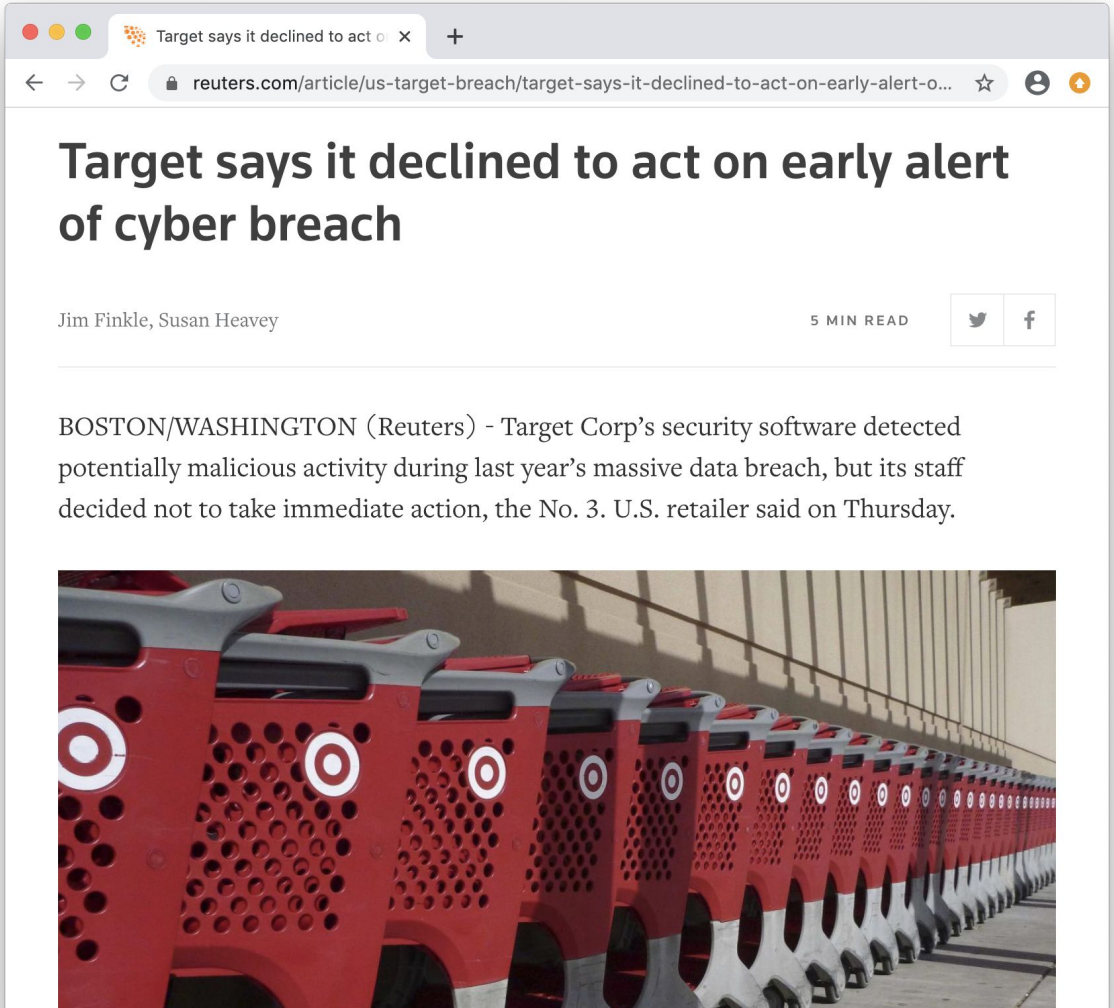
Alert fatigue occurs when security professionals receive so many alerts that they cannot adequately respond to each one.

- Even when an organization builds good alerts and an alert gets triggered, security professionals will need to research and respond to it.
- If an organization's system triggers too many alerts, even if they are good alerts, security professionals will often miss issues as they get lost in the noise.

Alert Fatigue

Alert fatigue can have a major impact on organizations:

- In 2014, a breach at Target cost the company US$252 million and led to the resignation of its CIO and CEO.
- One of the company's security products actually detected the breach.
- But due to the high quantity of alerts and the frequency of false alerts, the company's IT security team ignored it.



Target says it declined to act o

reuters.com/article/us-target-breach/target-says-it-declined-to-act-on-early-alert-o...

Target says it declined to act on early alert of cyber breach

Jim Finkle, Susan Heavey

5 MIN READ

BOSTON/WASHINGTON (Reuters) - Target Corp's security software detected potentially malicious activity during last year's massive data breach, but its staff decided not to take immediate action, the No. 3. U.S. retailer said on Thursday.

Alert Fatigue

To prevent alert fatigue:

Activity:
Baselining

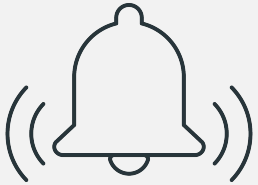
In this activity, you will review logs and create a baseline of typical hourly login counts.

Suggested Time:
15 Minutes

Time’s up!

Let’s review

Questions?

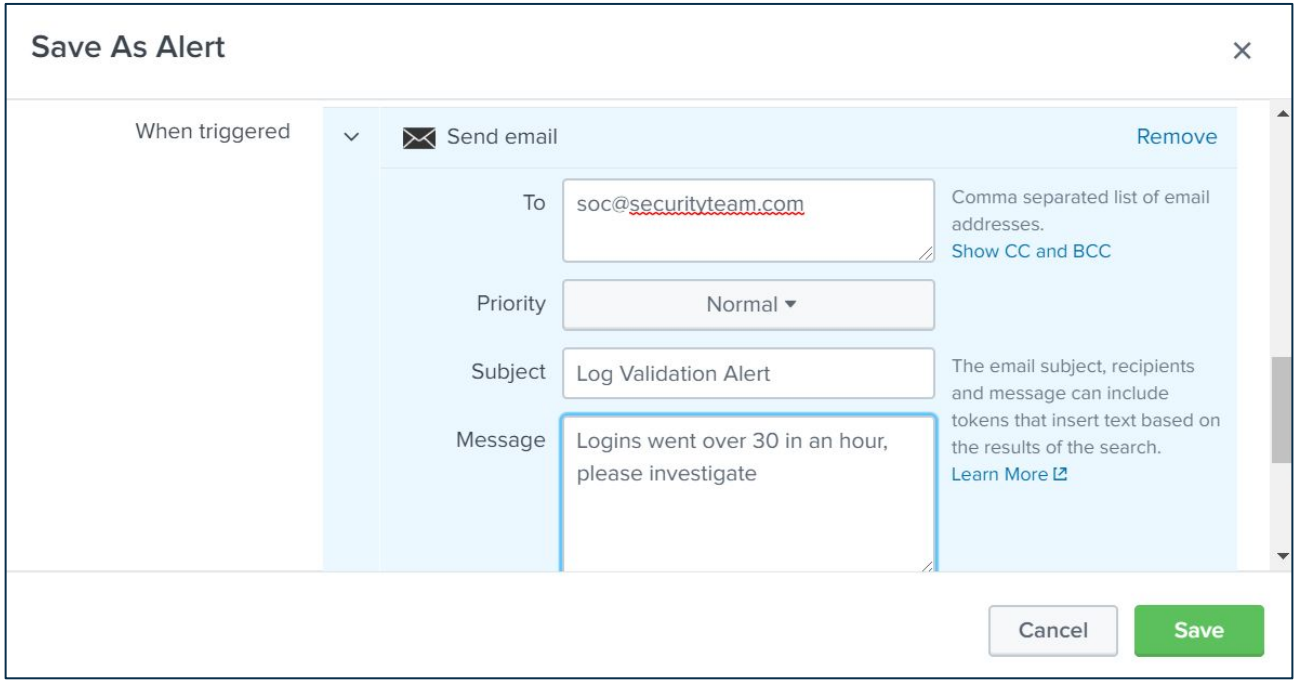


Creating and **Scheduling** Alerts

Creating and Scheduling Alerts

Now that we can determine accurate baselines, we can continue with our scenario and design the alerts.

- We will design an alert to trigger when 30 login attempts occur in an hour.
- We will run this alert to check the count every hour.
- Once the alert is triggered, an email will be sent.

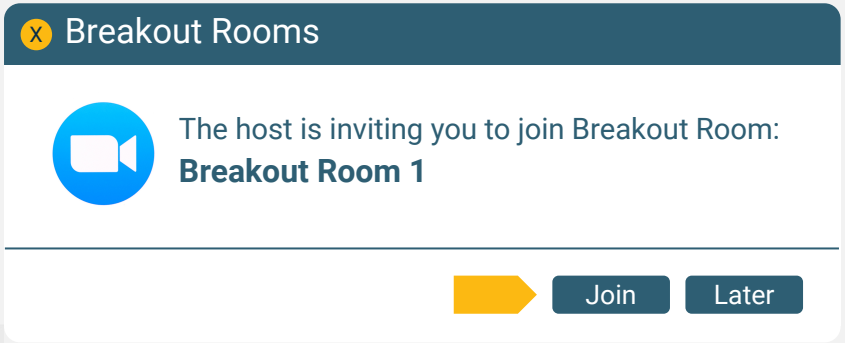


Instructor **Demonstration**

Creating and Scheduling Alerts

Activity:
Creating and Scheduling Alerts

In this activity, you will design and schedule an alert to notify your team if a brute-force attack is occurring.



Suggested Time:
15 Minutes

Time’s up!

Let’s review

Questions?

The End