Introduction to SIEM

Cybersecurity

SIEM Day 1

Class Objectives

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

Analyze logs and determine the types of data they contain, as well as the types of security events they can help identify.

Isolate, identify, and correlate fields across raw log files.

Design a correlation rule to notify when an event occurs.

Make informed decisions about which SIEM vendor is best for an organization.

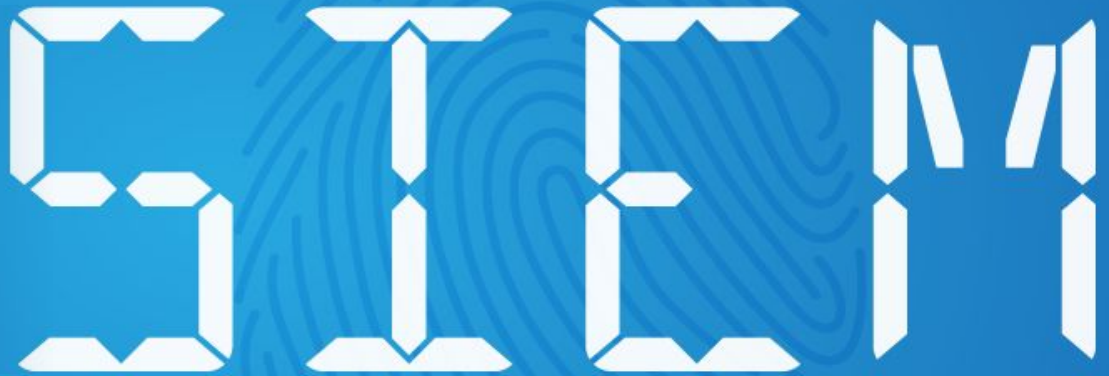
Introduction to SIEM
(Security Information and Event Management)

This week, we will move from offensive security to defensive security.

Organizations must constantly determine whether the **confidentiality**, **integrity**, and **availability** of their data are being compromised.

If an adversary were attempting to brute force their way into an online auction company's administrative website to steal privileged information, the company would need to identify the activity before sensitive data and confidentiality were breached.

Over the next two weeks, we will learn about SIEM (pronounced “sim”) technology, which organizations use to monitor and identify security incidents.



This Week...

You will play the role of a security operations center (SOC) manager at an online medical products organization called Omni Medical Products (OMP).

- OMP recently experienced several security-related events that put the organization at risk.
- As the new SOC manager, you will have to use SIEM tools and technologies to protect OMP from a variety of security events.

While the next two weeks will be very hands-on, today we'll focus on conceptual understanding and the business decisions that companies must make to maintain the **cybersecurity triad**.

Introduction to Continuous Monitoring

Continuous monitoring, also known as **information security continuous monitoring (ISCM)**, refers to the processes and technologies used to detect information security risks associated with an organization's operational environment in real time.

"In real time" means that ISCM detects issues as soon as they occur.

ISCM

ISCM provides real-time insight into:

The current state
of an organization's networked assets.

Vulnerabilities
and threats that attack an organization's networked assets.

Effectiveness
of security controls protecting an organization's networked assets.

ISCM

As we know, organizations face many threats.

For example:

- An employee can accidentally download malware onto their laptop, which can spread to an organization's network.
- A script kiddie can launch a denial of service (DOS) attack against a web server.
- A nation state can attempt a code injection attack against an application.

Limiting ISCM

Organizations cannot protect against every single potential attack, as they may have:

Financial limitations

Most modern monitoring tools and technologies are very expensive to install, deploy, and run.

Organizations often have strict budgets.

Staffing limitations

While many monitoring tools have automated features, they often require humans to monitor and respond to detected issues.


So, organizations need to make business decisions to prioritize the types of security risks they will monitor against.

Prioritizing Risks to Monitor

Prioritizing Risks

Organizations consider the following factors when determining how to prioritize security risks:

- Compliance
- Financial impact
- Reputational impact
- Likelihood of attack

Prioritizing Risk: Compliance

Depending on the business's industry, it may be required to monitor and analyze certain application and system activity.

For example:

To remain PCI-compliant, financial businesses that work with credit cards may be required to monitor their applications that manage financial data.

Prioritizing Risk: Financial Impact

How a system breach or shutdown can impact the financial performance of an organization.

For example:

A business like eBay would likely prioritize monitoring their customer-facing application.

The cost of it being compromised and taken offline would significantly affect their revenue.

eBay Sees Revenue Decline Due to Breach

Pace of Customers Returning Slower in Europe than U.S.

Eric Chabrow (GovInfoSecurity) • July 17, 2014

Twitter Facebook LinkedIn Credit Eligible Get Permission

Online retailer eBay is feeling the impact of its early 2014 **breach** where it hurts the most: in its coffers.

See Also: The Holistic Approach to Preventing Zero Day Attacks

The breach is the primary reason company officials say they lowered eBay's annual revenue target by $200 million to between $18 billion and $18.3 billion.

(Source)

Prioritizing Risk: Reputational Impact

How an incident would affect the business's reputation among customers.

For example:

An online banking provider would monitor their security controls of their customer financial data.

If their customer data were breached, their reputation could be significantly affected.

(Source)

Prioritizing Risk: Likelihood of Attack

While many types of security risk can occur, some are more likely than others.

For example:

Politically associated businesses that have public-facing websites are particularly at risk of DOS attacks.

Given this higher likelihood, these organizations should prioritize monitoring for DOS attacks.

TECHNOLOGY NEWS NOVEMBER 12, 2019 / 5:21 AM / 6 MONTHS AGO

Hackers hit UK political parties with back-to-back cyberattacks

Jack Stubbs 3 MIN READ

LONDON (Reuters) - Hackers hit Britain's two main political parties with back-to-back cyberattacks on Tuesday, sources told Reuters, attempting to force political websites offline with a flood of malicious traffic just weeks ahead of a national election.

(Source)

Organizations must decide for themselves which factors to consider when prioritizing risks.

Activity: Monitoring Your Assets

In this activity, you will analyze the types of security events and rank them based on risk to the organization.

Suggested Time:

7 Minutes

Time's Up! Let's Review.

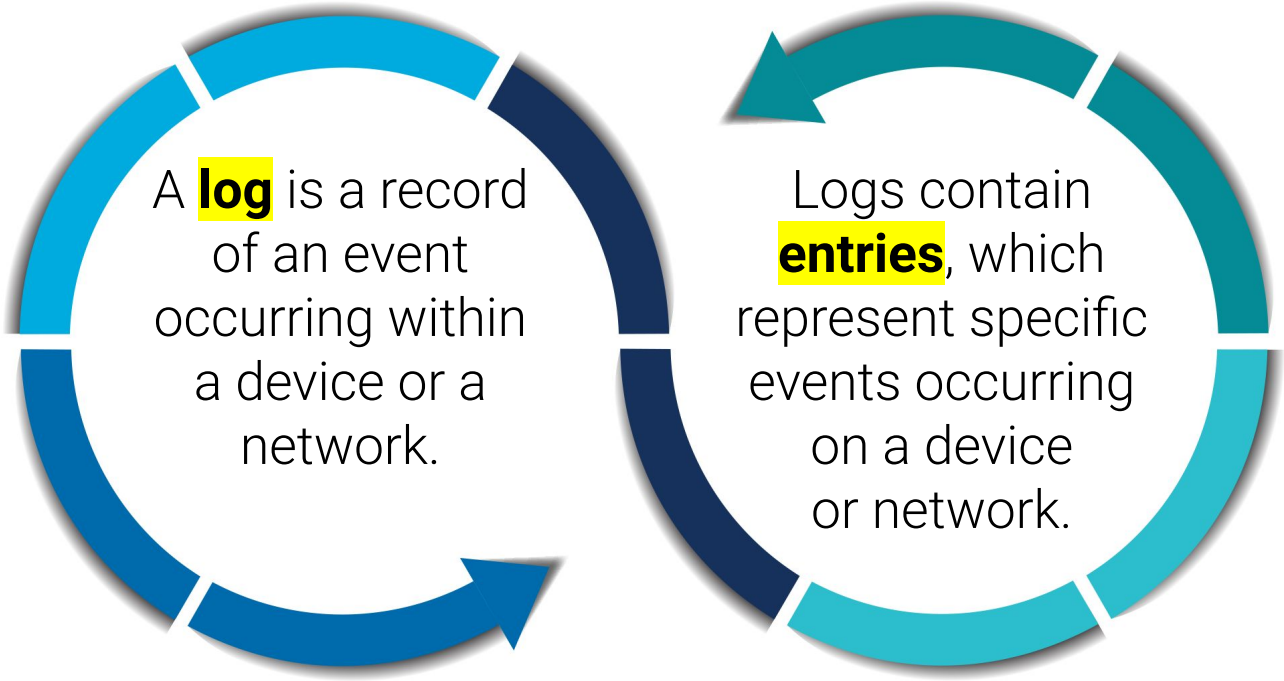
Questions?

Logs, Logs, and More Logs

After organizations decide what kind of events to monitor, they must decide how to monitor them.

Logs

Logs are the most common organizational method for monitoring.



Logs

While log entries were originally designed to assist with troubleshooting system issues, they later proved useful to security professionals as a source of insight into:

- The state of a device or a network.
- Who has access to a device or a network.
- User activities on a device or a network.

Types of Logs

There are four main log types used by information security professionals:

01 Operating system logs

02 Application logs

03 Networking device logs

04 Security device logs

Types of Logs: Operating System Logs

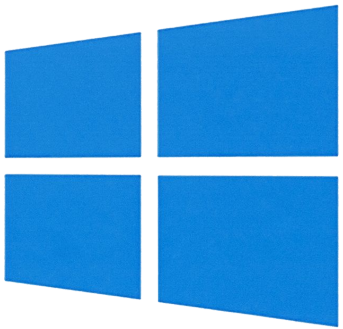
Operating system logs are created on devices such as Linux and Windows systems. Security events that can be identified by these logs include:

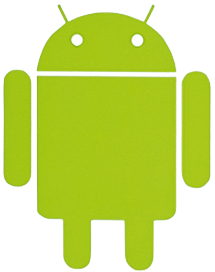
Security access events

For example, an unauthorized user attempts to view privileged data, such as a company payroll file.

Security permissions events

For example, a user attempts to give themselves permissions to view and edit a privileged file.





Types of Logs: Application Logs

Application logs are created by devices such as Apache and IIS (internet information services) servers. Security events that can be identified by these logs include:

Application access events

For example, a brute force attempt to log into an administrative account on a web application.

Fraud events

For example, a user on a financial application attempts to transfer a large sum of funds to a suspicious external account.

Types of Logs: Networking Device Logs

Networking device logs are created on devices such as routers, switches, and DHCP/DNS servers. Security events that can be identified by these logs include:

Administrative events

For example, a network administrator accidentally opens a port allowing unauthorized traffic into a network.

Network security events

For example, a DHCP starvation attack occurs in which the DHCP server receives thousands of requests in a short period of time, consuming all available IP addresses.

Types of Logs: Security device logs

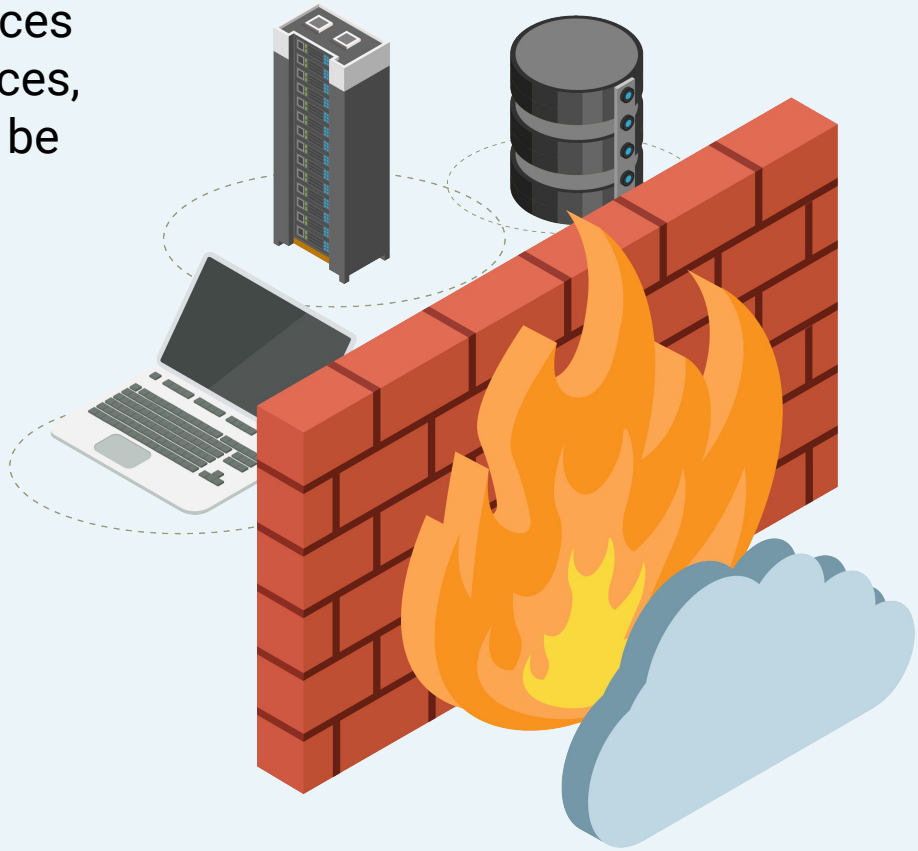
Security device logs are created on devices such as IDS/IPS, firewalls, endpoint devices, and honeypots. Security events that can be identified by these logs include:

Endpoint events

For example, a user accidentally downloads malware onto their laptop from a phishing email.

IDS signature events

For example, a packet with an illegal TCP flag combination is identified by an IDS.




While this is not a complete list of all the possible logs that security professionals use, you should be familiar with these types of logs and the types of security events they can help identify.

Activity: What Is This Log?

In this activity, you will analyze and categorize various log types.

Suggested Time:

7 Minutes

Time's Up! Let's Review.

Questions?

Countdown timer

15:00

(with alarm)

Log Aggregation and Normalization

The amount of incoming logs from various sources can be overwhelming.

For example, if a business wants to monitor suspicious logins on their Linux servers, they may have to monitor a variety of Linux servers and distributions. Therefore, they will want to identify all the Linux server logs available and collect them in a single destination.

Log aggregation is the identification and collection of logs from multiple computing sources.

Log Aggregation

Logs from different sources, even if they are logging similar data, are often created in different formats. The following are two ways a system may log server access:

Log 1:

```
User TJones Successfully Authenticated to 10.182.12.35 from client 43.10.8.22
```

Log 2:

```
43.182.12.35 New Client Connection 84.10.8.22 on account: PSmith: Success
```

Log Parsing

Log parsing is the process of converting the single string of data and into structured data.

Log 1:

```
User | TJones | Successfully Authenticated | to | 10.182.12.35 | from client | 43.10.8.22
```

Log 2:

```
43.182.12.35 | New Client Connection | 84.10.8.22 | on account: | PSmith | : Success
```

By separating the values, each field can be categorized and rearranged to match a uniform structure.

Log Normalization

Log normalization is the process of standardizing fields in data from different sources and formats so it can be analyzed together.

Key:	User	Destination IP	Source IP

Log 1:

```
User TJones Successfully Authenticated to 10.182.12.35 from client 43.10.8.22
```

Log 2:

```
43.182.12.35 New Client Connection 84.10.8.22 on account: PSmith: Success
```

Activity: Log Aggregation and Normalization

In this activity, you will aggregate and normalize various logs by identifying the fields contained within the log files.

Suggested Time:

7 Minutes

Time's Up! Let's Review.

Questions?

Log Correlation

Log Correlation

We can use **log correlation** to detect security events.

Individual log entries often do not indicate security events alone.

Analyzing multiple log entries **together** can help us detect security events and patterns of suspicious behavior.

Log correlation connects multiple log entries to make raw data into useful information.

Different log entries can come from the same source or different sources.

Log Correlation

While this single entry may not seem suspicious...

```
[10/12/2019 04:32:03 PM]   41.34.54.233  user=testerA "Login Failed"
```

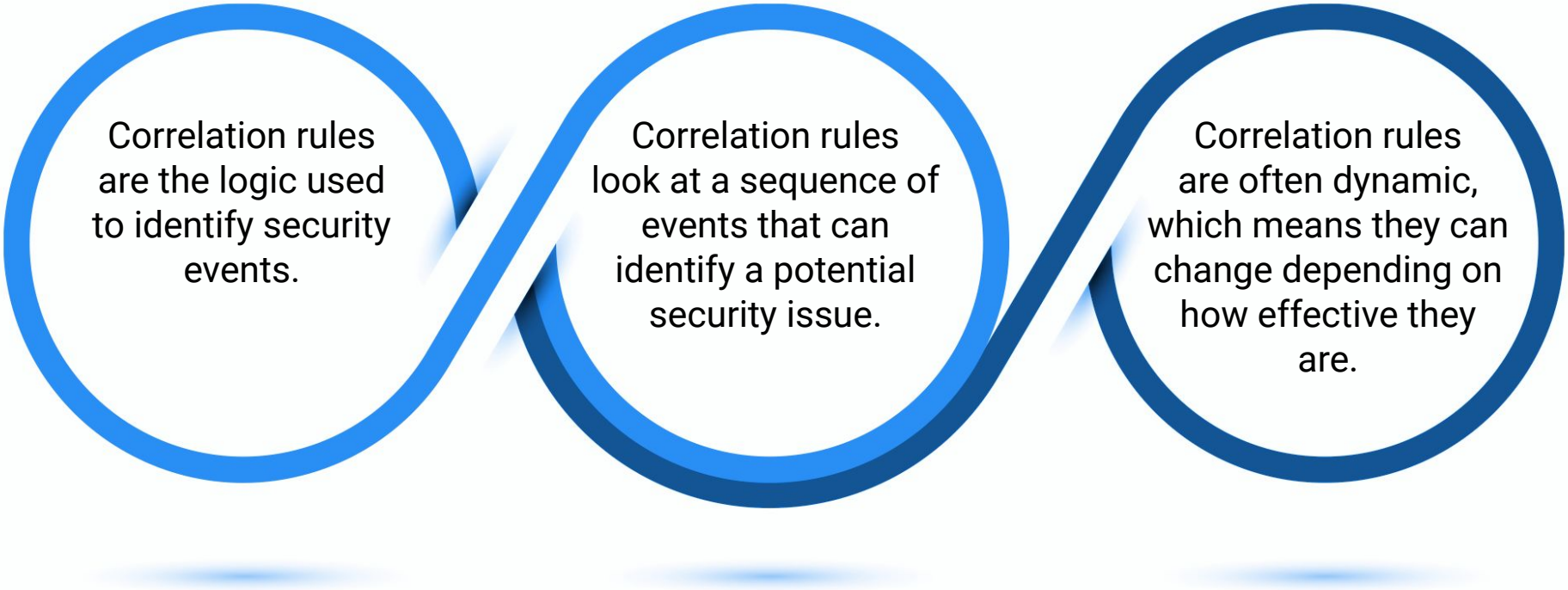
Log Correlation

Together, the following log entries indicate a potentially suspicious security event, such as a brute force attack:

```
[10/12/2019 04:32:03 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:04 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:05 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:07 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:08 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:09 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:10 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:11 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:12 PM]   41.34.54.233  user=testerA "Login Failed"
[10/12/2019 04:32:13 PM]   41.34.54.233  user=testerA "Login Failed"`
```

Correlation Rules

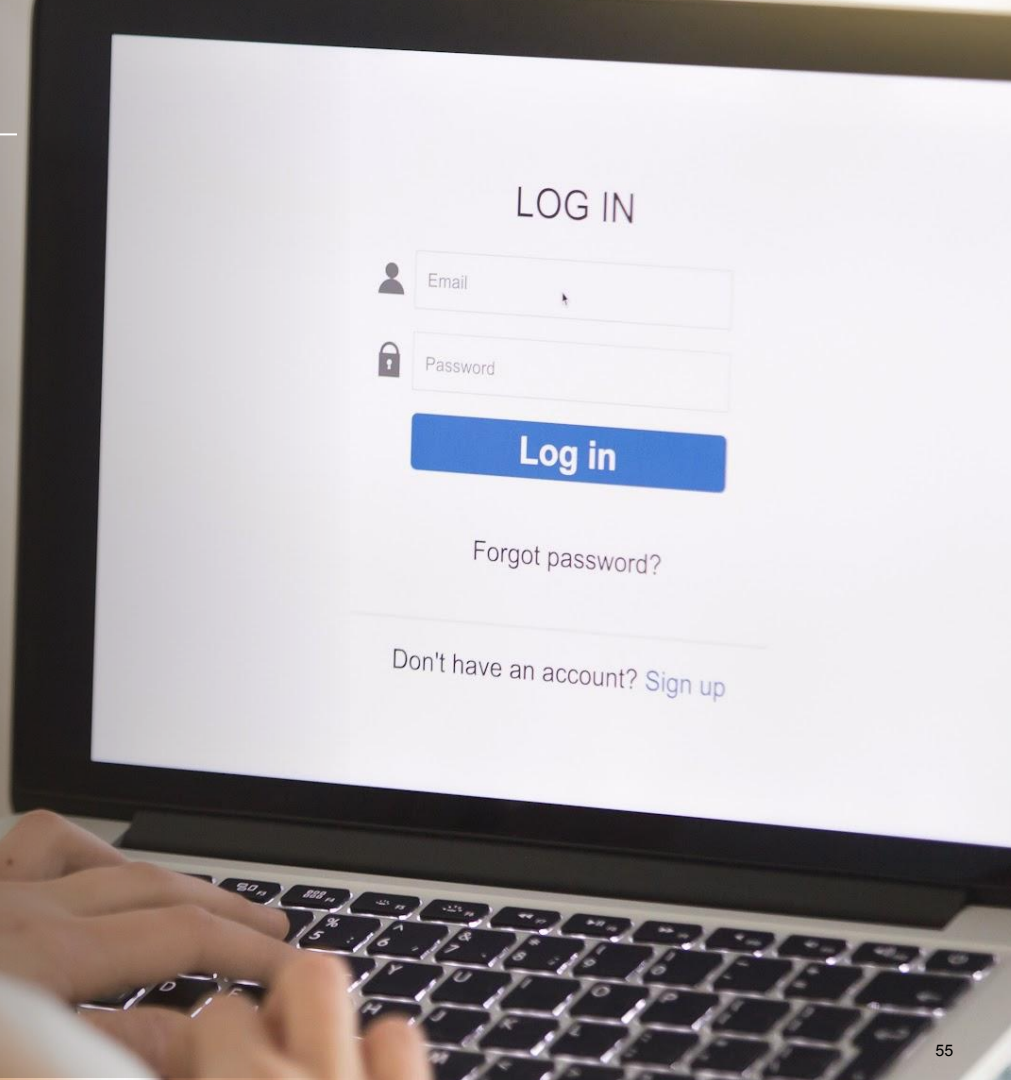
Log correlation identifies security events by using **correlation rules**.



Correlation Rule

For the list of logs we just looked at, we can create a correlation rule that detects an attempted brute force attack if all the following are true:

- More than three “Login Failed”
- From the same user
- From the same IP address
- Within a five-minute period



Once a rule is triggered, we need to decide what action to take.

The most common response is an alert.

A **correlation alert** is a notification that correlation rules have been met and an event was detected.

Correlation Alerts

Correlation alerts can have multiple delivery methods.

Correlation alerts can have multiple delivery methods, including:

- Displays on the screen at SOC
- Notifications sent with phone calls, text messages, or emails

Alerts are often designed to notify multiple individuals for faster response.

Alerts typically provide high-level details of the reason for the alert.

Correlation Rule and Alert

For the previous example, the alert delivery method could be added to the correlation rule, as such:

If the following is detected:

- More than three “Login Failed”
- From the same user
- From the same IP address
- Within a five-minute period

Send a(n):

- Phone call to the SOC manager
- Email message to the SOC email distro list

Activity: Rule Correlation

In this activity, you will create correlation rules that will identify an attack.

Suggested Time:

10 Minutes

Time's Up! Let's Review.

Questions?

SEM + SIM = SIEM

Security Monitoring

Organizations take the following steps to monitor against security events:

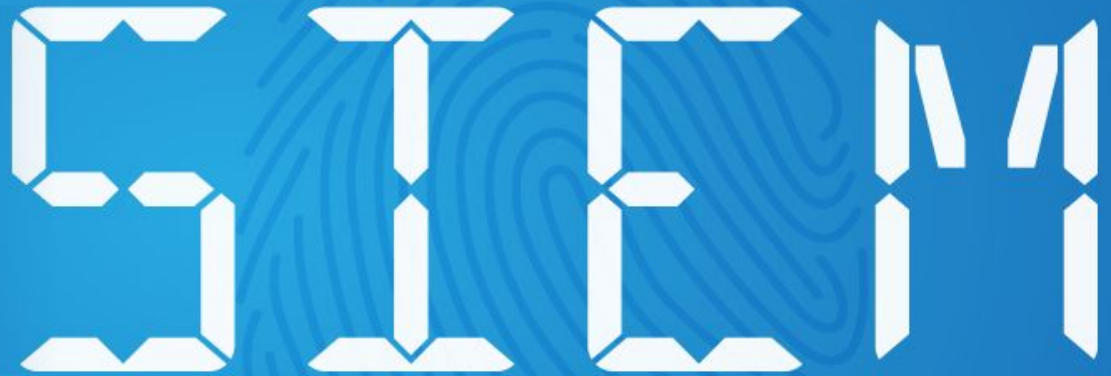
01 Decide what to monitor by prioritizing the risks to their business.

02 Decide how to monitor, which is typically accomplished by logs.

03 Aggregate, parse, and normalize logs so they can be analyzed together.

04 Correlate logs with rules to alert when a security event is detected.

Security professionals use **security information and event management (SIEM)** to simplify and manage monitoring security events.



SIEM

SIEM is made up of two types of software:

01 Security information management (SIM)

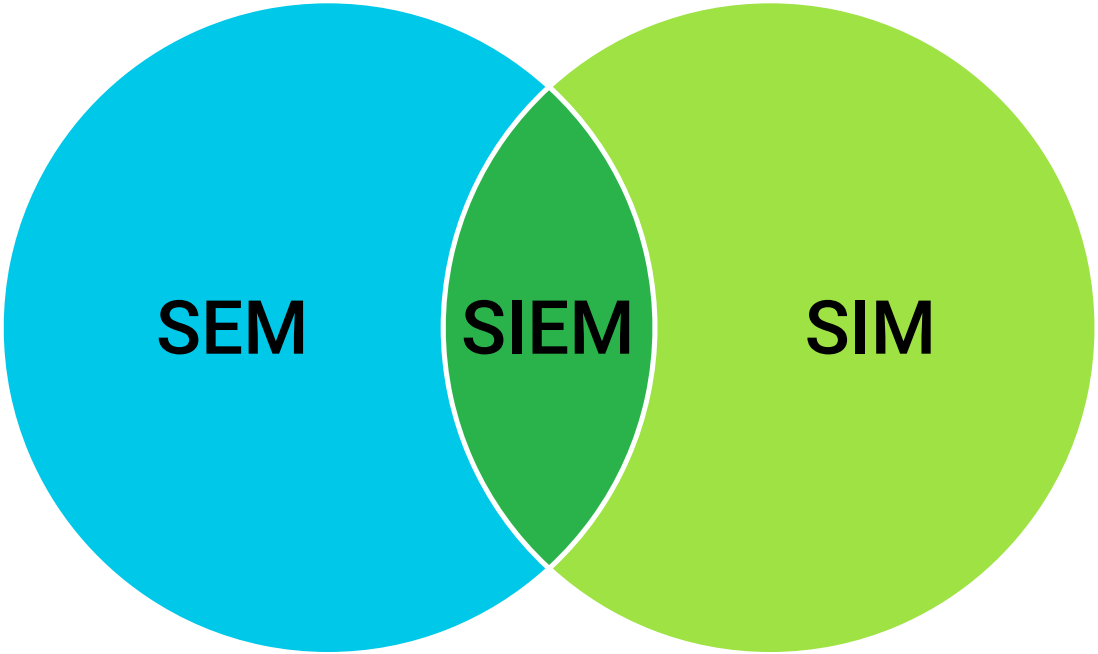
Primarily focused on log management and involves collecting logs in a central location for later analysis.

02 Security event management (SEM)

Primarily focused on event monitoring and involves identifying, evaluating, and correlating logs to determine security events and create alerts.

SEM + SIM = SIEM

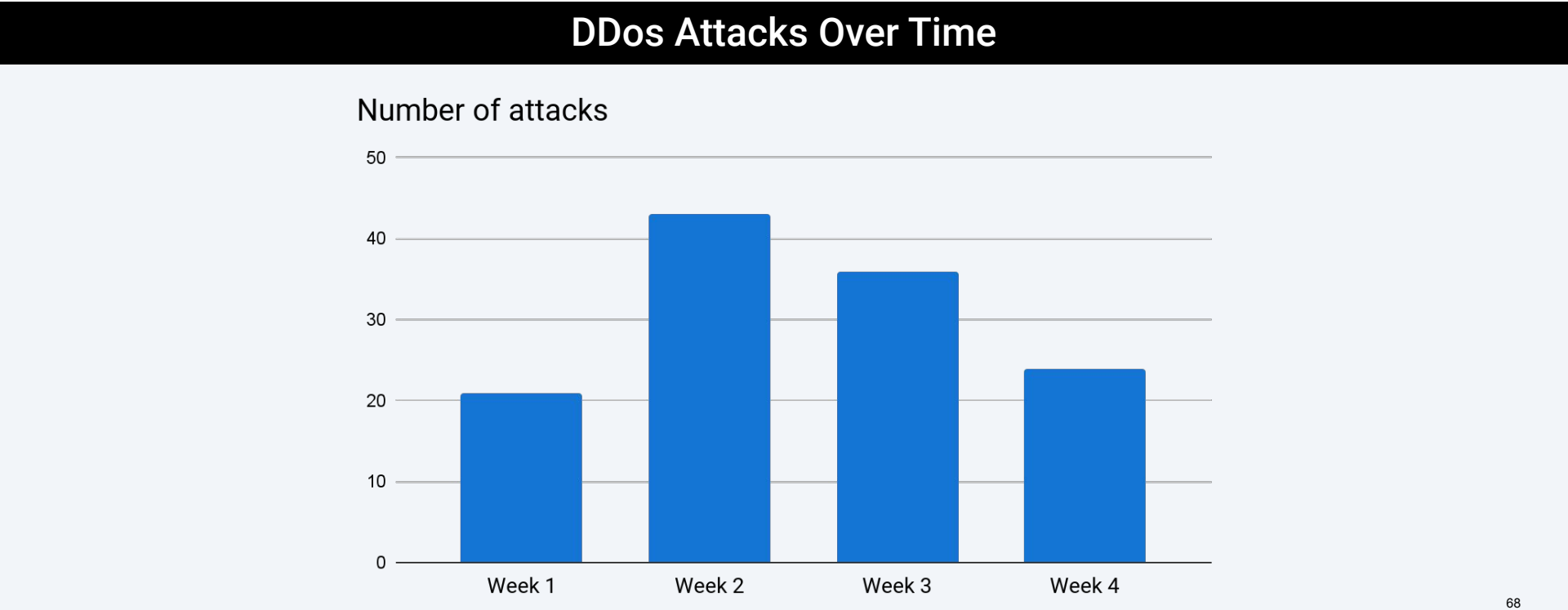
SIEM combines the technologies of SIM and SEM to collect, organize, and analyze logs to detect security-related events across an organization's technology infrastructure.



SIEM can also visualize data related to security events in order to simplify data interpretation.

SIEM

For example, a SIEM can help an SOC employee develop a simple chart illustrating how often their organization experiences DDOS attacks.



SIEM can assist organizations with the steps covered in today's lesson to implement an effective monitoring solution.

Organizations need to decide **what to monitor** by prioritizing the risks to their business.

....look at historical data to determine how often a security event has occurred. This data can help an organization prioritize monitoring decisions.

Organizations decide **how to monitor**, which is typically accomplished by logs.

...made of smart devices that assist security departments with forwarding and collecting logs from various sources.

Organizations **aggregate**, **parse**, and **normalize** multiple logs so they can be analyzed together.

...is its automation of aggregation, parsing, and normalization. When logs are loaded into SIEM, they are automatically parsed and normalized, with all the field headers identified. This reduces the manual work of parsing and identifying all fields.

Organizations **correlate** these logs with correlation rules to alert when a security event or suspicious activity is detected.

...simple rule correlation designer, which helps SOC employees manage the creation, editing, and viewing of correlation rules.

There are many SIEM vendors and products available, each offering different solutions.

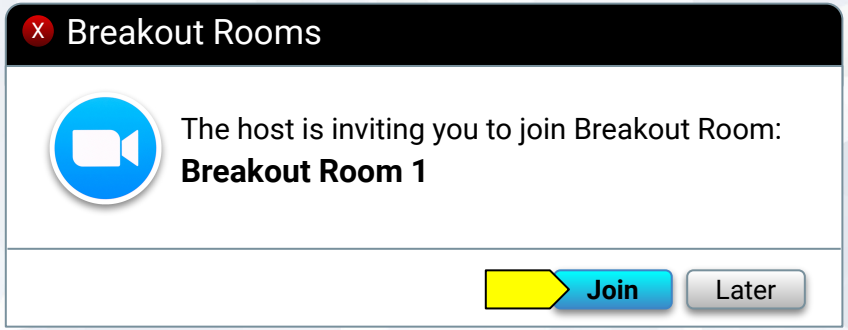
Choosing a SIEM Vendor

Organizations should consider the following when selecting a vendor:

Consideration	Reason
Cost	While cost is always a consideration when selecting a SIEM vendor, how an organization is billed can also be a consideration.
Ease of implementation and use	Organizations should research how challenging a SIEM vendor's solutions will be to set up and manage.
Log compatibility	Organizations should confirm that the SIEM vendor is able to accommodate every type of log the business is required to monitor.
SIEM features	While every SIEM vendor claims to have the most advanced and user-friendly features, organizations should review each vendor's features and assess which will best serve their business goals.

Activity: Choosing a SIEM Vendor

In this activity, you will choose the SIEM vendor that is the best fit for your organization.



Suggested Time:

15 Minutes

SIEM Tools Top 10

Time's Up! Let's Review.

Questions?

Next Class

We will use a Splunk application that resides within the Ubuntu Vagrant distribution.


The End