seim.png

0:20 NIST CSF focuses on five core functions: identify, protect, detect, respond, and recover. These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Basically, when it comes to security operations, NIST CSF functions are key for making sure an organization is protected against potential threats, risks, and vulnerabilities. So let's take a little time to explore how each function can be used to improve an organization's security.

1:03 The first core function is identify, which is related to the management of cybersecurity risk and its effect on an organization's people and assets. For example, as a security analyst, you may be asked to monitor systems and devices in your organization's internal network to identify potential security issues

1:26 The second core function is protect, which is the strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats.

1:41 For example, as a security analyst, you and your team might encounter new and unfamiliar threats and attacks. For this reason, studying historical data and making improvements to policies and procedures is essential.

1:57 The third core function is detect, which means identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections. For example, as an analyst, you might be asked to review a new security tool's setup to make sure it's flagging low, medium, or high risk, and then alerting the security team about any potential threats or incidents. The fourth function is respond, which means making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.

2:41 As an analyst, you could be working with a team to collect and organize data to document an incident and suggest improvements to processes to prevent the incident from happening again.

2:54 The fifth core function is recover, which is the process of returning affected systems back to normal operation.

3:03 For example, as an entry-level security analyst, you might work with your security team to restore systems, data, and assets, such as financial or legal files, that have been affected by an incident like a breach.

3:20 We've covered a lot of information in this video. Hopefully, it helped you understand the value of learning about the NIST CSF and its five core functions.

3:31 From proactive to reactive measures, all five functions are essential for making sure that an organization has effective security strategies in place.

3:41 Security incidents are going to happen, but an organization must have the ability to quickly recover from any damage caused by an incident to minimize their level of risk.

3:53 Coming up, we'll discuss security principles that work hand-in-hand with NIST frameworks and the CIA triad to help protect critical data and assets.

ssary terms from module 2

Attack vectors: The pathways attackers use to penetrate security defenses

Authentication: The process of verifying who someone is

Authorization: The concept of granting access to specific resources in a system

Availability: The idea that data is accessible to those who are authorized to access it

Biometrics: The unique physical characteristics that can be used to verify a person's identity

Confidentiality: The idea that only authorized users can access specific assets or data

Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies

Detect: A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections

Encryption: The process of converting data from a readable format to an encoded format

Identify: A NIST core function related to management of cybersecurity risk and its effect on an organization's people and assets

Integrity: The idea that the data is correct, authentic, and reliable

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

National Institute of Standards and Technology (NIST) Special Publication (S.P.) 800-53: A unified framework for protecting the security of information systems within the U.S. federal government

Open Web Application Security Project/Open Worldwide Application Security Project (OWASP): A non-profit organization focused on improving software security

Protect: A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

Recover: A NIST core function related to returning affected systems back to normal operation

Respond: A NIST core function related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process

Risk: Anything that can impact the confidentiality, integrity, or availability of an asset

Security audit: A review of an organization's security controls, policies, and procedures against a set of expectations

Security controls: Safeguards designed to reduce specific security risks

Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy

Security posture: An organization's ability to manage its defense of critical assets and data and react to change

Threat: Any circumstance or event that can negatively impact assets

As a security analyst, one of your responsibilities might include analyzing log data to mitigate and manage threats, risks, and vulnerabilities. As a reminder, a log is a record of events that occur within an organization's systems and networks. Security analysts access a variety of logs from different sources. Three common log sources include firewall logs, network logs, and server logs. Let's explore each of these log sources in more detail.

A firewall log is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.

A network log is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.

Finally, a server log is a record of events related to services such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

By monitoring logs, like the one shown here, security teams can identify vulnerabilities and potential data breaches. Understanding logs is important because SIEM tools rely on logs to monitor systems and detect security threats.

A security information and event management, or SIEM, tool is an application that collects and analyzes log data to monitor critical activities in an organization. It provides real-time visibility, event monitoring and analysis, and automated alerts. It also stores all log data in a centralized location.

Because SIEM tools index and minimize the number of logs a security professional must manually review and analyze, they increase efficiency and save time.

But, SIEM tools must be configured and customized to meet each organization's unique security needs. As new threats and vulnerabilities emerge, organizations must continually customize their SIEM tools to ensure that threats are detected and quickly addressed.

Later in the certificate program, you'll have a chance to practice using different SIEM tools to identify potential security incidents.

Coming up, we'll explore SIEM dashboards and how cybersecurity professionals use them to monitor for threats, risks, and vulnerabilities.

We've explored how SIEM tools are used to collect and analyze log data. However, this is just one of the many ways SIEM tools are used in cybersecurity.

SIEM tools can also be used to create dashboards. You might have encountered dashboards in an app on your phone or other device. They present information about your account or location in a format that's easy to understand.

For example, weather apps display data like temperature, precipitation, wind speed, and the forecast using charts, graphs, and other visual elements. This format makes it easy to quickly identify weather patterns and trends, so you can stay prepared and plan your day accordingly.

Just like weather apps help people make quick and informed decisions based on data, SIEM dashboards help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.

For example, a security analyst receives an alert about a suspicious login attempt. The analyst accesses their SIEM dashboard to gather information about this alert. Using the dashboard, the analyst discovers that there have been 500 login attempts for Ymara's account in the span of five-minutes. They also discover that the login attempts happened from geographic locations outside of Ymara's usual location and outside of her usual working hours. By using a dashboard, the security analyst was able to quickly review visual representations of the timeline of the login attempts, the location, and the exact time of the activity, then determine that the activity was suspicious.

In addition to providing a comprehensive summary of security-related data, SIEM dashboards also provide stakeholders with different metrics. Metrics are key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.

SIEM dashboards can be customized to display specific metrics or other data that are relevant to different members in an organization. For example, a security analyst may create a dashboard that displays metrics for monitoring everyday business operations, like the volume of incoming and outgoing network traffic.

We've examined how security analysts use SIEM dashboards to help organizations maintain their security posture. Well done!

Coming up, we'll discuss some common SIEM tools used in the cybersecurity industry. Meet you there.

Previously, you were introduced to security information and event management (SIEM) tools, along with a few examples of SIEM tools. In this reading, you will learn more about how SIEM tools are used to protect organizational operations. You will also gain insight into how and why SIEM tools are changing to help protect organizations and the people they serve from evolving threat actor tactics and techniques.

Current SIEM solutions

A **SIEM** tool is an application that collects and analyzes log data to monitor critical activities in an organization. SIEM tools offer real-time monitoring and tracking of security event logs. The data is then used to conduct a thorough analysis of any potential security threat, risk, or vulnerability identified. SIEM tools have many dashboard options. Each dashboard option helps cybersecurity team members manage and monitor organizational data. However, currently, SIEM tools require human interaction for analysis of security events.

The future of SIEM tools

As cybersecurity continues to evolve, the need for cloud functionality has increased. SIEM tools have and continue to evolve to function in cloud-hosted and cloud-native environments. Cloud-hosted SIEM tools are operated by vendors who are responsible for maintaining and managing the infrastructure required to use the tools. Cloud-hosted tools are simply accessed through the internet and are an ideal solution for organizations that don't want to invest in creating and maintaining their own infrastructure.

Similar to cloud-hosted SIEM tools, cloud-native SIEM tools are also fully maintained and managed by vendors and accessed through the internet. However, cloud-native tools are designed to take full advantage of cloud computing capabilities, such as availability, flexibility, and scalability.

Yet, the evolution of SIEM tools is expected to continue in order to accommodate the changing nature of technology, as well as new threat actor tactics and techniques. For example, consider the current development of interconnected devices with access to the internet, known as the Internet of Things (IoT). The more interconnected devices there are, the larger the cybersecurity attack surface and the amount of data that threat actors can exploit. The diversity of attacks and data that require special attention is expected to grow significantly. Additionally, as artificial intelligence (AI) and machine learning (ML) technology continues to progress, SIEM capabilities will be enhanced to better identify threat-related terminology, dashboard visualization, and data storage functionality.

The implementation of automation will also help security teams respond faster to possible incidents, performing many actions without waiting for a human response. **Security orchestration, automation, and response (SOAR)** is a collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention. This frees up security analysts to handle more complex and uncommon incidents that, consequently, can't be automated with a SOAR. Nevertheless, the expectation is for cybersecurity-related platforms to communicate and interact with one another. Although the technology allowing interconnected systems and devices to communicate with each other exists, it is still a work in progress.

Key takeaways

SIEM tools play a major role in monitoring an organization's data. As an entry-level security analyst, you might monitor SIEM dashboards as part of your daily tasks. Regularly researching new developments in SIEM technology will help you grow and adapt to the changes in the cybersecurity field. Cloud computing, SIEM-application integration, and automation are only some of the advancements security professionals can expect in the future evolution of SIEM tools.

0:00 [MUSIC] My name is Parisa and I'm a vice president of engineering and lead the Chrome Team. So as General manager of the Chrome Team, I lead a team of engineers and product managers and designers around the world who actually build Chrome and keep all of our users safe. I think accessibility is important to all aspects of technology, and when we think about its relevance for cybersecurity, you know, we ultimately want to keep everybody safe. I think of accessibility as making information, activities, or even environments meaningful, sensible, usable to as many people as possible. And when we're talking about this in a technology standpoint, it's usually about making information or services available to people with disabilities. Decisions we make based on our own abilities to enhance security can actually be ineffective. For example, you'll sometimes see the color red used for indication of a warning. Well, for somebody who's colorblind, like that is going to be ineffective. And so really thinking about accessibility when we're trying to keep people safe is super important for them to be effective. I've worked in the space of security for a really long time. And I do see some parallels between the spaces. I've really been able to see innovation driven when you're trying to solve a very specific security problem or a specific accessibility problem. Closed Captioning was originally designed and built to help people with hearing impairments, but it ends up helping everybody. For people who are new to the field of cybersecurity, it's just really important to remember that there's a range of abilities that you are wanting to serve. It's so important to get user research and feedback and a range of abilities in terms of testing the effectiveness of your security mitigations. I know it was scary for me early on. I didn't look like everybody else. I really struggled with whether I belonged. Finding people who could be mentors, having the courage to ask questions and recognize that you're rarely the only person with that question. And just sort of persevering through, sometimes hard moments can lead to breakthroughs and also just growing confidence. And one of the things I've learned is me having a different background than other people in this space was my own superpower. Instead of focusing on the delta between what I was and what the norm was in the room, I should feel a lot of pride in what made me unique and what unique skills and perspective I brought to the table.

Hello again! Previously, we discussed how SIEM tools help security analysts monitor systems and detect security threats.

In this video, we'll cover some industry leading SIEM tools that you'll likely encounter as a security analyst. First, let's discuss the different types of SIEM tools that organizations can choose from, based on their unique security needs.

Self-hosted SIEM tools require organizations to install, operate, and maintain the tool using their own physical infrastructure, such as server capacity. These applications are then managed and maintained by the organization's IT department, rather than a third party vendor. Self-hosted SIEM tools are ideal when an organization is required to maintain physical control over confidential data.

Alternatively, cloud-hosted SIEM tools are maintained and managed by the SIEM providers, making them accessible through the internet. Cloud-hosted SIEM tools are ideal for organizations that don't want to invest in creating and maintaining their own infrastructure.

Or, an organization can choose to use a combination of both self-hosted and cloud-hosted SIEM tools, known as a hybrid solution. Organizations might choose a hybrid SIEM solution to leverage the benefits of the cloud while also maintaining physical control over confidential data.

Splunk Enterprise, Splunk Cloud, and Chronicle are common SIEM tools that many organizations use to help protect their data and systems. Let's begin by discussing Splunk.

Splunk is a data analysis platform and Splunk Enterprise provides SIEM solutions. Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time. Splunk Cloud is a cloud-hosted tool used to collect, search, and monitor log data. Splunk Cloud is helpful for organizations running hybrid or cloud-only environments, where some or all of the organization's services are in the cloud.

Finally, there's Google's Chronicle. Chronicle is a cloud-native tool designed to retain, analyze, and search data. Chronicle provides log monitoring, data analysis, and data collection. Like cloud-hosted tools, cloud-native tools are also fully maintained and managed by the vendor. But cloud-native tools are specifically designed to take full advantage of cloud computing capabilities such as availability, flexibility, and scalability.

Because threat actors are frequently improving their strategies to compromise the confidentiality, integrity, and availability of their targets, it's important for organizations to use a variety of security tools to help defend against attacks. The SIEM tools we just discussed are only a few examples of the tools available for security teams to use to help defend their organizations. And later in the certificate program, you'll have the exciting opportunity to practice using Splunk Cloud and Chronicle.

Previously, you learned about several tools that are used by cybersecurity team members to monitor for and identify potential security threats, risks, and vulnerabilities. In this reading, you'll learn more about common open-source and proprietary cybersecurity tools that you may use as a cybersecurity professional.

Open-source tools

Open-source tools are often free to use and can be user friendly. The objective of open-source tools is to provide users with software that is built by the public in a collaborative way, which can result in the software being more secure. Additionally, open-source tools allow for more customization by users, resulting in a variety of new services built from the same open-source software package.

Software engineers create open-source projects to improve software and make it available for anyone to use, as long as the specified license is respected. The source code for open-source projects is readily available to users, as well as the training material that accompanies them. Having these sources readily available allows users to modify and improve project materials.

Proprietary tools

Proprietary tools are developed and owned by a person or company, and users typically pay a fee for usage and training. The owners of proprietary tools are the only ones who can access and modify the source code. This means that users generally need to wait for updates to be made to the software, and at times they might need to pay a fee for those updates. Proprietary software generally allows users to modify a limited number of features to meet individual and organizational needs. Examples of proprietary tools include Splunk® and Chronicle SIEM tools.

Common misconceptions

There is a common misconception that open-source tools are less effective and not as safe to use as proprietary tools. However, developers have been creating open-source materials for years that have become industry standards. Although it is true that threat actors have attempted to manipulate open-source tools, because these tools are open source it is actually harder for people with malicious intent to successfully cause harm. The wide exposure and immediate access to the source code by well-intentioned and informed users and professionals makes it less likely for issues to occur, because they can fix issues as soon as they're identified.

Examples of open-source tools

In security, there are many tools in use that are open-source and commonly available. Two examples are Linux and Suricata.

Linux

Linux is an open-source operating system that is widely used. It allows you to tailor the operating system to your needs using a command-line interface. An **operating system** is the interface between computer hardware and the user. It's used to communicate with the hardware of a computer and manage software applications.

There are multiple versions of Linux that exist to accomplish specific tasks. Linux and its command-line interface will be discussed in detail, later in the certificate program.

Suricata

Suricata

Suricata is an open-source network analysis and threat detection software. Network analysis and threat detection software is used to inspect network traffic to identify suspicious behavior and generate network data logs. The detection software finds activity across users, computers, or Internet Protocol (IP) addresses to help uncover potential threats, risks, or vulnerabilities.

Suricata was developed by the Open Information Security Foundation (OISF). OISF is dedicated to maintaining open-source use of the Suricata project to ensure it's free and publicly available. Suricata is widely used in the public and private sector, and it integrates with many SIEM tools and other security tools. Suricata will also be discussed in greater detail later in the program.

Key takeaways

Open-source tools are widely used in the cybersecurity profession. Throughout the certificate program, you will have multiple opportunities to learn about and explore both open-source and proprietary tools in more depth.

Previously, you were introduced to security information and event management (SIEM) tools and a few SIEM dashboards. You also learned about different threats, risks, and vulnerabilities an organization may experience. In this reading, you will learn more about SIEM dashboard data and how cybersecurity professionals use that data to identify a potential threat, risk, or vulnerability.

Splunk

Splunk offers different SIEM tool options: Splunk® Enterprise and Splunk® Cloud. Both allow you to review an organization's data on dashboards. This helps security professionals manage an organization's internal infrastructure by collecting, searching, monitoring, and analyzing log data from multiple sources to obtain full visibility into an organization's everyday operations.

Review the following Splunk dashboards and their purposes:

Security posture dashboard

The security posture dashboard is designed for security operations centers (SOCs). It displays the last 24 hours of an organization's notable security-related events and trends and allows security professionals to determine if security infrastructure and policies are performing as designed. Security analysts can use this dashboard to monitor and investigate potential threats in real time, such as suspicious network activity originating from a specific IP address.

Executive summary dashboard

The executive summary dashboard analyzes and monitors the overall health of the organization over time. This helps security teams improve security measures that reduce risk. Security analysts might use this dashboard to provide high-level insights to stakeholders, such as generating a summary of security incidents and trends over a specific period of time.

Incident review dashboard

The incident review dashboard allows analysts to identify suspicious patterns that can occur in the event of an incident. It assists by highlighting higher risk items that need immediate review by an analyst. This dashboard can be very helpful because it provides a visual timeline of the events leading up to an incident.

Risk analysis dashboard

The risk analysis dashboard helps analysts identify risk for each risk object (e.g., a specific user, a computer, or an IP address). It shows changes in risk-related activity or behavior, such as a user logging in outside of normal working hours or unusually high network traffic from a specific computer. A security analyst might use this dashboard to analyze the potential impact of vulnerabilities in critical assets, which helps analysts prioritize their risk mitigation efforts.

User sign in overview dashboard

The user sign in overview dashboard provides information about user access behavior across the organization. Security analysts can use this dashboard to access a list of all user sign-in events to identify unusual user activity, such as a user signing in from multiple locations at the same time. This information is then used to help mitigate threats, risks, and vulnerabilities to user accounts and the organization's applications.

Key takeaways

SIEM tools provide dashboards that help security professionals organize and focus their security efforts. This is important because it allows analysts to reduce risk by identifying, analyzing, and remediating the highest priority items in a timely manner. Later in the program, you'll have an opportunity to practice using various SIEM tool features and commands for search queries.

Chronicle

Chronicle is a cloud-native SIEM tool from Google that retains, analyzes, and searches log data to identify potential security threats, risks, and vulnerabilities. Chronicle allows you to collect and analyze log data according to:

- A specific asset
- A domain name
- A user
- An IP address

Chronicle provides multiple dashboards that help analysts monitor an organization's logs, create filters and alerts, and track suspicious domain names.

Review the following Chronicle dashboards and their purposes:

Enterprise insights dashboard

The enterprise insights dashboard highlights recent alerts. It identifies suspicious domain names in logs, known as indicators of compromise (IOCs). Each result is labeled with a confidence score to indicate the likelihood of a threat. It also provides a severity level that indicates the significance of each threat to the organization. A security analyst might use this dashboard to monitor login or data access attempts related to a critical asset—like an application or system—from unusual locations or devices.

Data ingestion and health dashboard

The data ingestion and health dashboard shows the number of event logs, log sources, and success rates of data being processed into Chronicle. A security analyst might use this dashboard to ensure that log sources are correctly configured and that logs are received without error. This helps ensure that log related issues are addressed so that the security team has access to the log data they need.

IOC matches dashboard

The IOC matches dashboard indicates the top threats, risks, and vulnerabilities to the organization. Security professionals use this dashboard to observe domain names, IP addresses, and device IOCs over time in order to identify trends. This information is then used to direct the security team's focus to the highest priority threats. For example, security analysts can use this dashboard to search for additional activity associated with an alert, such as a suspicious user login from an unusual geographic location.

Main dashboard

The main dashboard displays a high-level summary of information related to the organization's data ingestion, alerting, and event activity over time. Security professionals can use this dashboard to access a timeline of security events—such as a spike in failed login attempts— to identify threat trends across log sources, devices, IP addresses, and physical locations.

Splunk

Splunk offers different SIEM tool options: Splunk® Enterprise and Splunk® Cloud. Both allow you to review an organization's data on dashboards. This helps security professionals manage an organization's internal infrastructure by collecting, searching, monitoring, and analyzing log data from multiple sources to obtain full visibility into an organization's everyday operations.

Review the following Splunk dashboards and their purposes:

Security posture dashboard

The security posture dashboard is designed for security operations centers (SOCs). It displays the last 24 hours of an organization's notable security-related events and trends and allows security professionals to determine if security infrastructure and policies are performing as designed. Security analysts can use this dashboard to monitor and investigate potential threats in real time, such as suspicious network activity originating from a specific IP address.

Executive summary dashboard

The executive summary dashboard analyzes and monitors the overall health of the organization over time. This helps security teams improve security measures that reduce risk. Security analysts might use this dashboard to provide high-level insights to stakeholders, such as generating a summary of security incidents and trends over a specific period of time.

Incident review dashboard

The incident review dashboard allows analysts to identify suspicious patterns that can occur in the event of an incident. It assists by highlighting higher risk items that need immediate review by an analyst. This dashboard can be very helpful because it provides a visual timeline of the events leading up to an incident.

Risk analysis dashboard

The risk analysis dashboard helps analysts identify risk for each risk object (e.g., a specific user, a computer, or an IP address). It shows changes in risk-related activity or behavior, such as a user logging in outside of normal working hours or unusually high network traffic from a specific computer. A security analyst might use this dashboard to analyze the potential impact of vulnerabilities in critical assets, which helps analysts prioritize their risk mitigation efforts.

Chronicle

Chronicle is a cloud-native SIEM tool from Google that retains, analyzes, and searches log data to identify potential security threats, risks, and vulnerabilities. Chronicle allows you to collect and analyze log data according to:

- A specific asset
- A domain name
- A user
- An IP address

Chronicle provides multiple dashboards that help analysts monitor an organization's logs, create filters and alerts, and track suspicious domain names.

- An IP address

Chronicle provides multiple dashboards that help analysts monitor an organization's logs, create filters and alerts, and track suspicious domain names.

Review the following Chronicle dashboards and their purposes:

Enterprise insights dashboard

The enterprise insights dashboard highlights recent alerts. It identifies suspicious domain names in logs, known as indicators of compromise (IOCs). Each result is labeled with a confidence score to indicate the likelihood of a threat. It also provides a severity level that indicates the significance of each threat to the organization. A security analyst might use this dashboard to monitor login or data access attempts related to a critical asset—like an application or system—from unusual locations or devices.

Data ingestion and health dashboard

The data ingestion and health dashboard shows the number of event logs, log sources, and success rates of data being processed into Chronicle. A security analyst might use this dashboard to ensure that log sources are correctly configured and that logs are received without error. This helps ensure that log related issues are addressed so that the security team has access to the log data they need.

IOC matches dashboard

The IOC matches dashboard indicates the top threats, risks, and vulnerabilities to the organization. Security professionals use this dashboard to observe domain names, IP addresses, and device IOCs over time in order to identify trends. This information is then used to direct the security team's focus to the highest priority threats. For example, security analysts can use this dashboard to search for additional activity associated with an alert, such as a suspicious user login from an unusual geographic location.

Main dashboard

The main dashboard displays a high-level summary of information related to the organization's data ingestion, alerting, and event activity over time. Security professionals can use this dashboard to access a timeline of security events—such as a spike in failed login attempts— to identify threat trends across log sources, devices, IP addresses, and physical locations.

Rule detections dashboard

The rule detections dashboard provides statistics related to incidents with the highest occurrences, severities, and detections over time. Security analysts can use this dashboard to access a list of all the alerts triggered by a specific detection rule, such as a rule designed to alert whenever a user opens a known malicious attachment from an email. Analysts then use those statistics to help manage recurring incidents and establish mitigation tactics to reduce an organization's level of risk.

User sign in overview dashboard

The user sign in overview dashboard provides information about user access behavior across the organization. Security analysts can use this dashboard to access a list of all user sign-in events to identify unusual user activity, such as a user signing in from multiple locations at the same time. This information is then used to help mitigate threats,

User sign in overview dashboard

The user sign in overview dashboard provides information about user access behavior across the organization. Security analysts can use this dashboard to access a list of all user sign-in events to identify unusual user activity, such as a user signing in from multiple locations at the same time. This information is then used to help mitigate threats, risks, and vulnerabilities to user accounts and the organization's applications.

Key takeaways

SIEM tools provide dashboards that help security professionals organize and focus their security efforts. This is important because it allows analysts to reduce risk by identifying, analyzing, and remediating the highest priority items in a timely manner. Later in the program, you'll have an opportunity to practice using various SIEM tool features and commands for search queries.

Terms and definitions from Course 2, Module 3

Chronicle: A cloud-native tool designed to retain, analyze, and search data

Incident response: An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

Log: A record of events that occur within an organization's systems

Metrics: Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

Operating system (OS): The interface between computer hardware and the user

Playbook: A manual that provides details about any operational action

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that use automation to respond to security events

Splunk Cloud: A cloud-hosted tool used to collect, search, and monitor log data

Splunk Enterprise: A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time

module 4

A playbook is a manual that provides details about any operational action. Playbooks also clarify what tools should be used in response to a security incident. In the security field, playbooks are essential.

Urgency, efficiency, and accuracy are necessary to quickly identify and mitigate a security threat to reduce potential risk. Playbooks ensure that people follow a consistent list of actions in a prescribed way, regardless of who is working on the case.

Different types of playbooks are used. These include playbooks for incident response, security alerts, teams-specific, and product-specific purposes.

Here, we'll focus on a playbook that's commonly used in cybersecurity, called an incident response playbook. Incident response is an organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach. An incident response playbook is a guide with six phases used to help mitigate and manage security incidents from beginning to end. Let's discuss each phase.

The first phase is preparation. Organizations must prepare to mitigate the likelihood, risk, and impact of a security incident by documenting procedures, establishing staffing plans, and educating users. Preparation sets the foundation for successful incident response. For example, organizations can create incident response plans and procedures that outline the roles and responsibilities of each security team member.

The second phase is detection and analysis. The objective of this phase is to detect and analyze events using defined processes and technology. Using appropriate tools and strategies during this phase helps security analysts determine whether a breach has occurred and analyze its possible magnitude.

The third phase is containment. The goal of containment is to prevent further damage and reduce the immediate impact of a security incident. During this phase, security professionals take actions to contain an incident and minimize damage. Containment is a high priority for organizations because it helps prevent ongoing risks to critical assets and data.

The fourth phase in an incident response playbook is eradication and recovery. This phase involves the complete removal of an incident's artifacts so that an organization can return to normal operations. During this phase, security professionals eliminate artifacts of the incident by removing malicious code and mitigating vulnerabilities. Once they've exercised due diligence, they can begin to restore the affected environment to a secure state. This is also known as IT restoration.

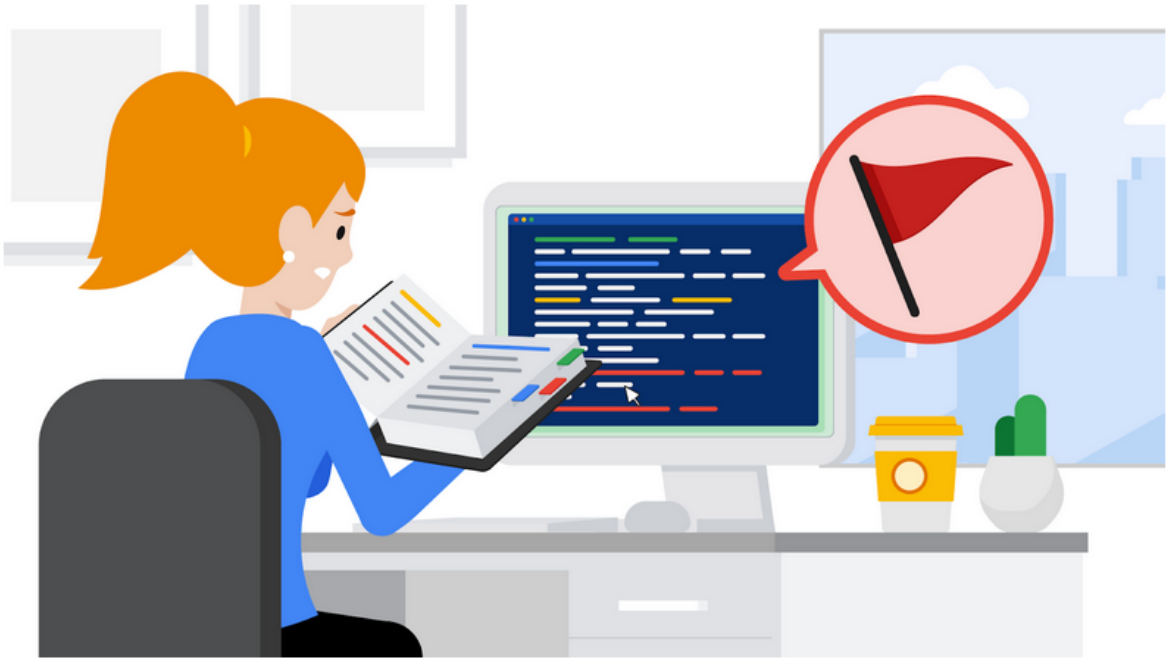
The fifth phase is post-incident activity. This phase includes documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organization is better prepared to handle future incidents. Depending on the severity of the incident, organizations can

conduct a full-scale incident analysis to determine the root cause of the incident and implement various updates or improvements to enhance its overall security posture.
resolution.

There are many ways security professionals may be alerted to an incident. You recently learned about SIEM tools and how they collect and analyze data. They use this data to detect threats and generate alerts, which can inform the security team of a potential incident. Then, when a security analyst receives a SIEM alert, they can use the appropriate playbook to guide the response process. SIEM tools and playbooks work together to provide a structured and efficient way of responding to potential security incidents.

Throughout the program, you'll have opportunities to continue to build your understanding of these important concepts.

A **playbook** is a manual that provides details about any operational action. Essentially, a playbook provides a predefined and up-to-date list of steps to perform when responding to an incident.



Playbooks are accompanied by a strategy. The strategy outlines expectations of team members who are assigned a task, and some playbooks also list the individuals responsible. The outlined expectations are accompanied by a plan. The plan dictates how the specific task outlined in the playbook must be completed.

Playbooks should be treated as living documents, which means that they are frequently updated by security team members to address industry changes and new threats. Playbooks are generally managed as a collaborative effort, since security team members have different levels of expertise.

Updates are often made if:

- A failure is identified, such as an oversight in the outlined policies and procedures, or in the playbook itself.
- There is a change in industry standards, such as changes in laws or regulatory compliance.
- The cybersecurity landscape changes due to evolving threat actor tactics and techniques.

Types of playbooks

Playbooks sometimes cover specific incidents and vulnerabilities. These might include ransomware, vishing, business email compromise (BEC), and other attacks previously discussed. Incident and vulnerability response playbooks are very common, but they are not the only types of playbooks organizations develop.

Each organization has a different set of playbook tools, methodologies, protocols, and procedures that they adhere to, and different individuals are involved at each step of the response process, depending on the country they are in. For example, incident notification requirements from government-imposed laws and regulations, along with compliance standards, affect the content in the playbooks. These requirements are subject to change based on where the incident originated and the type of data affected.

Incident and vulnerability response playbooks

Incident and vulnerability response playbooks are commonly used by entry-level cybersecurity professionals. They are developed based on the goals outlined in an organization's business continuity plan. A business continuity plan is an established path forward allowing a business to recover and continue to operate as normal, despite a disruption like a security breach.

These two types of playbooks are similar in that they both contain predefined and up-to-date lists of steps to perform when responding to an incident. Following these steps is necessary to ensure that you, as a security professional, are adhering to legal and organizational standards and protocols. These playbooks also help minimize errors and ensure that important actions are performed within a specific timeframe.

When an incident, threat, or vulnerability occurs or is identified, the level of risk to the organization depends on the potential damage to its assets. A basic formula for determining the level of risk is that risk equals the likelihood of a threat. For this reason, a sense of urgency is essential. Following the steps outlined in playbooks is also important if any forensic task is being carried out. Mishandling data can easily compromise forensic data, rendering it unusable.

Common steps included in incident and vulnerability playbooks include:

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery from an incident

Additional steps include performing post-incident activities, and a coordination of efforts throughout the investigation and incident and vulnerability response stages.

Key takeaways

It is essential to refine processes and procedures outlined in a playbook. With every documented incident, cybersecurity teams need to consider what was learned from the incident and what improvements should be made to handle incidents more effectively in the future. Playbooks create structure and ensure compliance with the law.

Welcome back! In this video, we're going to revisit SIEM tools and how they're used alongside playbooks to reduce organizational threats, risks, and vulnerabilities.

An incident response playbook is a guide that helps security professionals mitigate issues with a heightened sense of urgency, while maintaining accuracy. Playbooks create structure, ensure compliance, and outline processes for communication and documentation. Organizations may use different types of incident response playbooks depending on the situation. For example, an organization may have specific playbooks for addressing different types of attacks, such as ransomware, malware, distributed denial of service, and more.

To start, let's discuss how a security analyst might use a playbook to address a SIEM alert, like a potential malware attack. In this situation, a playbook is invaluable for guiding an analyst through the necessary actions to properly address the alert.

The first action in the playbook is to assess the alert. This means determining if the alert is actually valid by identifying why the alert was generated by the SIEM. This can be done by analyzing log data and related metrics.

Next, the playbook outlines the actions and tools to use to contain the malware and reduce further damage. For example, this playbook instructs the analyst to isolate, or disconnect, the infected network system to prevent the malware from spreading into other parts of the network.

After containing the incident, step three of the playbook describes ways to eliminate all traces of the incident and restore the affected systems back to normal operations. For example, the playbook might instruct the analyst to restore the impacted operating system, then restore the affected data using a clean backup, created before the malware outbreak.

Finally, once the incident has been resolved, step four of the playbook instructs the analyst to perform various post-incident activities and coordination efforts with the security team. Some actions include creating a final report to communicate the security incident to stakeholders, or reporting the incident to the appropriate authorities, like the U.S. Federal Bureau of Investigations or other agencies that investigate cyber crimes.

This is just one example of how you might follow the steps in a playbook, since organizations develop their own internal procedures for addressing security incidents. What's most important to understand is that playbooks provide a consistent process for security professionals to follow.

Note that playbooks are living documents, meaning the security team will make frequent changes, updates, and improvements to address new threats and vulnerabilities. In addition, organizations learn from past security incidents to improve their security posture, refine policies and procedures, and reduce the likelihood and impact of future incidents. Then, they update their playbooks accordingly.

As an entry-level security analyst, you may be required to use playbooks frequently, especially when monitoring networks and responding to incidents. Having an understanding of why

playbooks are important and how they can help you achieve your working objectives will help ensure your success within this field.

Course 2 glossary

Glossary

Cybersecurity

Terms and definitions from Course 2

A

Assess: The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

Asset: An item perceived as having value to an organization

Attack vectors: The pathways attackers use to penetrate security defenses

Authentication: The process of verifying who someone is

Authorization: The concept of granting access to specific resources in a system

Authorize: The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that might exist in an organization

Availability: The idea that data is accessible to those who are authorized to access it

B

Biometrics: The unique physical characteristics that can be used to verify a person's identity

Business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

C

Categorize: The second step of the NIST RMF that is used to develop risk management processes and tasks

Chronicle: A cloud-native tool designed to retain, analyze, and search data

Confidentiality: The idea that only authorized users can access specific assets or data

Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies

D

Detect: A NIST core function related to identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections

E

Encryption: The process of converting data from a readable format to an encoded format

External threat: Anything outside the organization that has the potential to harm organizational assets

I

Identify: A NIST core function related to management of cybersecurity risk and its effect on an organization's people and assets

Implement: The fourth step of the NIST RMF that means to implement security and privacy plans for an organization

Incident response: An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach

Integrity: The idea that the data is correct, authentic, and reliable

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

L

Log: A record of events that occur within an organization's systems

M

Metrics: Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application

Monitor: The seventh step of the NIST RMF that means be aware of how systems are operating

N

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

National Institute of Standards and Technology (NIST) Special Publication (S.P.) 800-53: A unified framework for protecting the security of information systems within the U.S. federal government

O

Open Web Application Security Project/Open Worldwide Application Security Project (OWASP): A non-profit organization focused on improving software security

Operating system (OS): The interface between computer hardware and the user

P

Playbook: A manual that provides details about any operational action

Prepare: The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

Protect: A NIST core function used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats

R

Ransomware: A malicious attack where threat actors encrypt an organization's data and demand payment to restore access

Recover: A NIST core function related to returning affected systems back to normal operation

Respond: A NIST core function related to making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process

Risk: Anything that can impact the confidentiality, integrity, or availability of an asset

Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

S

Security audit: A review of an organization's security controls, policies, and procedures against a set of expectations

Security controls: Safeguards designed to reduce specific security risks

Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that use automation to respond to security events

Security posture: An organization's ability to manage its defense of critical assets and data and react to change

Select: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization

Shared responsibility: The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Splunk Cloud: A cloud-hosted tool used to collect, search, and monitor log data

Splunk Enterprise: A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time

T

Threat: Any circumstance or event that can negatively impact assets

V

Vulnerability: A weakness that can be exploited by a threat

---

class 3 Cybersecurity google.