Phases of incident response playbooks

- Welcome to Week 4
- Phases of an incident response playbook
- More about playbooks
- Zack: Incident response and the value of playbooks

Welcome to Week 4

Hello and welcome back.
You've reached the final section of this course!
Previously, we discussed security information and
event management, or SIEM tools, and
how they can be used to help organizations improve their security posture.

Let's continue our security journey by exploring another tool
security professionals use: playbooks.
In this section, we'll explore how playbooks help security teams respond
to threats, risks, or vulnerabilities identified by SIEM tools.

Then, we'll discuss the six phases of incident response.
Let's get started!

Phases of an incident response playbook

Previously, we discussed how SIEM tools are used to help protect an organization's critical assets and data. In this video, we'll introduce another important tool for maintaining an organization's security, known as a playbook.

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.

The sixth and final phase in an incident response playbook is coordination. Coordination involves reporting incidents and sharing information, throughout the incident response process, based on the organization's established standards. Coordination is important for many reasons. It ensures that organizations meet compliance requirements and it allows for coordinated response and 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.

More about playbooks

Previously, you learned that playbooks are tools used by cybersecurity professionals to identify and respond to security issues. In this reading, you'll learn more about playbooks and their purpose in the field of cybersecurity.

Playbook overview

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.

An analyst using a playbook.

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.

Resources for more information

Incident and vulnerability response playbooks are only two examples of the many playbooks that an organization uses. If you plan to work as a cybersecurity professional outside of the U.S., you may want to explore the following resources:

- United Kingdom, National Cyber Security Center (NCSC) - Incident Management
- Australian Government - Cyber Incident Response Plan
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) - Vulnerability Handling and related guidelines
- Government of Canada - Ransomware Playbook
- Scottish Government - Playbook Templates

Zack: Incident response and the value of playbooks

My name is Zack. I'm a Software Engineer on the security team in Google Workspace. I have non-traditional background. When I graduated college, I originally thought that I would pursue law, but I was accepted and I decided not to go. Instead, I joined Google in recruiting. Through that work, I did a little bit of strategy work where I taught myself web scraping and I really liked it, so I took one of Google's internal training courses that helped me move from recruiting to software engineering. Processes and playbooks are documentation that software engineers and other people at Google use to determine how we can respond to things that happen. Whether that's a security or privacy incident, whether that's an active attack, we have sets of guidelines or algorithms that we use to determine the best course of action to make sure that we manage people's data and security well. I'm relatively new to cybersecurity. I've been a software engineer here for about two years, and I don't have enough knowledge to be able to respond to every single thing that could possibly come my way when I'm on call or when I'm helping resolve a vulnerability. The playbooks are super important to people like me and other folks who are joining the industry new because they allow you to solve the problem with the experience of a much more experienced person, basically decades of experience in your own resolution because you can rely on this playbook and other people's advice. The kind of things that we use playbooks for our open attacks, privacy incidents, data leaks, denial of service attacks, service alerts, and others. When I first started out at Google, my first task on the security team was to fix an externally reported vulnerability. That means some security researcher out in the wild was playing with our app and found something that could potentially leak our user's data. When I received that, it was my first task on the team. Looking back on it, it's a relatively easy thing to solve, but it felt really overwhelming at the time. But when we receive a vulnerability report, it comes with remediation guidance. There were steps in the bug that was sent toe saying this is the things that we think that you should do. The things that I would say to somebody who's interested in starting out in cybersecurity is talk to as many people in the industry as you can. You'll learn about what the job is like. You'll learn about the skills that you need to get yourself there. If that's something that you're interested in, you'll learn about open jobs and roles, what it's like to work at different companies. I wish people had told me when I graduated college that what these jobs are really like. I thought that coding would be heads down, typing away at a computer and a dark office for 12 hours a day. But it's not like that at all. 50% is communicating with other people and reviewing designs and talking about ideas. That's really compelling and I think if somebody had said that to me at the beginning of my career would have been totally different. Some teams come in and out of fashion, but security is ever-present. It's really important now it's only getting more important. There's a certain amount of security that comes with being in a security team. Definitely, a good place to be.