Explore incident response

- Use a playbook to respond to threats, risks, or vulnerabilities
- Erin: The importance of diversity of perspective on a security team
- Playbooks, SIEM tools, and SOAR tools
- Wrap-up

Use a playbook to respond to threats, risks, or vulnerabilities

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.

Erin: The importance of diversity of perspective on a security team

Hi everyone. My name is Erin and I am a privacy engineer at Google. I work on speculative and emerging technology. So think of things that don't exist in the world, and that are coming within the next two to five years. My role is basically to take a look at all of the things that we are creating in terms of technology, and making sure that privacy is embedded in that. I am thinking for users before they even touch the product, making sure that when they utilize them, they'll have some form of trust in the engagement with that product. As well as knowing that we are protecting their privacy, things that they don't want to share or broadcast, and making sure that they're informed before they even touch the product. I always talk about soft skills being the most important thing over the technical skills. Because we can teach you anything but we can't teach you how to relate to people. That is something that you bring to the table. Diversity of thought and diversity of perspectives are very useful in understanding the world that we exist in. Because if we are designing products for everyday people, we need everyday people to basically help us understand those perspectives. Because I may look at something one way, but my colleague may see it another way based on their own experiences. And so, when you work together and come from different environments, you actually bring more equity and more depth to the things that you're looking at. And the perspective that you bring is the essential voice that is required in order to make a product better. When you look at people who work in journalism, or people who, like myself, worked in entertainment, they are bringing a different perspective for how they would tackle something. Or if we have a product where we are trying to convince a product team that maybe we shouldn't do this, it's always helpful to say, from someone who worked in journalism, do we really want this to end up in The Times? Probably not, right? And that is a way to come at people that, on the ground floor, they understand what that looks like. All of the experiences that you have had from the time you were born to now, they have been your experience. And you have to think about that in terms of where we're going with technology. When we're developing for a wide array of people, your experience may be someone else's experience. And so if we don't have you in the room, then we are missing the opportunity to actually bring something beautiful, I would say, to the equation. Which is why I encourage people, please come work with us in terms of technology. Get involved in STEM because the equity across product security, privacy, you name it, whether it be software engineering, everything requires a different voice. And it actually requires your voice.

Playbooks, SIEM tools, and SOAR tools

Playbooks and SIEM tools

Previously, you learned that security teams encounter threats, risks, vulnerabilities, and incidents on a regular basis and that they follow playbooks to address security-related issues. In this reading, you will learn more about playbooks, including how they are used in security information and event management (SIEM) and security orchestration, automation, and response (SOAR).

Playbooks and SIEM tools

Playbooks are used by cybersecurity teams in the event of an incident. Playbooks help security teams respond to incidents by ensuring that a consistent list of actions are followed in a prescribed way, regardless of who is working on the case. Playbooks can be very detailed and may include flow charts and tables to clarify what actions to take and in which order. Playbooks are also used for recovery procedures in the event of a ransomware attack. Different types of security incidents have their own playbooks that detail who should take what action and when.

Playbooks are generally used alongside SIEM tools. If, for example, unusual user behavior is flagged by a SIEM tool, a playbook provides analysts with instructions about how to address the issue.

Playbooks and SOAR tools

Playbooks are also used with SOAR tools. SOAR tools are similar to SIEM tools in that they are used for threat monitoring. SOAR is a piece of software used to automate repetitive tasks generated by tools such as a SIEM or managed detection and response (MDR). For example, if a user attempts to log into their computer too many times with the wrong password, a SOAR would automatically block their account to stop a possible intrusion. Then, analysts would refer to a playbook to take steps to resolve the issue.

Key takeaways

What is most important to know is that playbooks, also sometimes referred to as runbooks, provide detailed actions for security teams to take in the event of an incident. Knowing exactly who needs to do what and when can help reduce the impact of an incident and reduce the risk of damage to an organization’s critical assets

Wrap-up

Let's review what we covered in this section. We began by discussing the purpose of playbooks.

Then, we examined the six phases of an incident response playbook, including an example of how a playbook might be used to address an incident.

Playbooks are just one of the essential tools you'll use as a security analyst. They provide a structured, consistent approach to handling security incidents and can help you respond to security incidents quickly.

Knowing how and when to use a playbook, will allow you to make informed decisions about how to respond to a security incident when it occurs and help to minimize the impact and damage it may cause your organization and the people it serves.

Following the steps of the playbook and communicating appropriately with your team, will ensure your effectiveness as a security professional.