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.

Revision #2
Created 15 June 2023 12:54:44 by naruzkurai
Updated 15 June 2023 12:55:44 by naruzkurai