Security Operations Center (SOC)

The core function of a SOC (Security Operations Center) is to investigate, monitor, prevent, and respond to threats in the cyber realm 24/7 or around the clock. Per McAfee's definition of a SOC, "Security operations teams are charged with monitoring and protecting many assets, such as intellectual property, personnel data, business systems, and brand integrity. As the implementation component of an organisation's overall cyber security framework, security operations teams act as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks". The number of people working in the SOC can vary depending on the organisation's size.

What is included in the responsibilities of the SOC?

Preparation and Prevention

As a Junior Security Analyst, you should stay informed of the current cyber security threats (Twitter and Feedly can be great resources to keep up with the news related to Cybersecurity). It's crucial to detect and hunt threats, work on a security roadmap to protect the organisation, and be ready for the worst-case scenario.

Prevention methods include gathering intelligence data on the latest threats, threat actors, and their TTPs (Tactics, Techniques, and Procedures). It also includes the maintenance procedures like updating the firewall signatures, patching the vulnerabilities in the existing systems, block-listing and safe-listing applications, email addresses, and IPs.

To better understand the TTPs, you should look into one of the CISA's (Cybersecurity & Infrastructure Security Agency) alerts on APT40 (Chinese Advanced Persistent Threat). Refer to the following link for more information, https://us-cert.cisa.gov/ncas/alerts/aa21-200a.

Monitoring and Investigation

A SOC team proactively uses SIEM (Security information and event management) and EDR (Endpoint Detection and Response) tools to monitor suspicious and malicious network activities. Imagine being a firefighter and having a multi-alarm fire - one-alarm fires, two-alarm fires, three-alarm fires; the categories classify the seriousness of the fire, which is a threat in our case. As a Security Analyst, you will learn how to prioritise the alerts based on their level: Low, Medium, High, and Critical. Of course, it is an easy guess that you will need to start from the highest level (Critical) and work towards the bottom - Low-level alert. Having properly configured security monitoring tools in place will give you the best chance to mitigate the threat.

Junior Security Analysts play a crucial role in the investigation procedure. They perform triaging on the ongoing alerts by exploring and understanding how a certain attack works and preventing bad things from happening if they can. During the investigation, it's important to raise the question "How? When, and why?". Security Analysts find the answers by drilling down on the data logs and alerts in combination with using open-source tools, which we will have a chance to explore later in this path.

Response

After the investigation, the SOC team coordinates and takes action on the compromised hosts, which involves isolating the hosts from the network, terminating the malicious processes, deleting files, and more.

Revision #1
Created 19 January 2024 20:54:07 by naruzkurai
Updated 19 January 2024 20:59:40 by naruzkurai