SOC (Security operation centre)

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.

Core Responsibilities

Preparation and Prevention

As a junior security analyst, you should keep up with the most recent cyber security concerns. Twitter and Feedly are excellent sites for doing this. It's critical to identify and investigate threats, develop a security plan to safeguard the organization, and prepare for the worst. The gathering of

intelligence information regarding the most recent dangers, threat actors, and their TTPs (Tactics, Techniques, and Procedures) is one technique of prevention. It also covers routine maintenance tasks including updating firewall signatures, fixing security holes in current systems, and blocking and safe-listing programs, email addresses, and IP addresses.

Monitoring and Investigation

To proactively track suspicious network activity, a SOC team employs SIEM (Security information and event management) and EDR (Endpoint Detection and Response) tools. As a fireman, visualize dealing with a multi-alarm fire. One-alarm, two-alarm, three-alarm fires are classified according to their seriousness, which in our situation poses a threat. You will learn how to prioritize the warnings based on their degree as a security analyst: Low, Medium, High, and Critical. It should go without saying that you should start with the highest level (Critical) and work your way down to the lowest level, which is Low-level alert. Your chances of successfully reducing the threat will be greatest if you have correctly configured security monitoring tools in place.

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 take action on the compromised hosts, Which involves isolating the hosts from the network, Terminating the malicious process, deleting files and more.