What is a SOC (Security Operations Center) Service?

Small businesses are under constant attack by cyber criminals. Traditional IT (Information Technology) cybersecurity protections like antivirus, firewalls, and software patching are still necessary but no longer sufficient. Enter the SOC. SOC stands for Security Operations Center and it is a group of trained cybersecurity experts utilizing state of the art monitoring systems and platforms to detect and respond to indications of compromise (IoC) around the clock, 24/7.

A modern SOC constantly monitors telemetry from a wide range of systems and platforms. Monitors are wide ranging but typically include the following types:

- Network sensors that constantly monitoring and analyzing the traffic traversing a network.
- Software applications (agents) installed on servers and endpoints to detect behavior and potentially malicious activity.
- SaaS (Software as a Service) application logs and activity.
- Antivirus application logs, activity, and changes.
- Firewall logs, activity, and changes.
- Dark web activity related to authorized users.

Detections & Incidents

The analysis of alerts and activity gathered from the various monitors is accomplished through a combination of artificial intelligence and review by trained cybersecurity experts who know how to recognize and deal with indications of compromise. The artificial intelligence analyzes the information gathered from the monitors for the purpose of identifying a detection. A detection might result from a wide range of indicators such as comparing activity against known threat activity databases, the combination of activity from multiple monitors, or the observation of suspicious behavior. When a detection is identified, the cybersecurity experts investigate to determine if it constitutes an indication of compromise or if it might be a false positive. If a detection is determined to be valid, it is declared an incident and the managed service provider (MSP) and/or customer is notified. The SOC, MSP, and the customer then work together to provide additional context for the incident and to determine the proper incident response.

A detection will arise from a wide range of alerts and detected behavior. The monitors rely on vast databases of threat detection definitions and up to the minute feeds from Information Sharing and Analysis Centers (ISACs) that provide the monitors current threat detection signatures. SOC services and tools vary in the methods and algorithms used to produce detections.

Following is a list of some behavior and alerts that might result in a detection:

- Unusual login activity
  - Repeated unsuccessful login attempts to a monitored SaaS platform, network devices, or authentication authority like Active Directory.
  - Login from an abnormal location or IP (Internet Protocol) address known to be a source of malicious attacks.
  - Login location timing is not physically possible (i.e., login from Denver, CO, and subsequent login Turkey within a short timeframe)
- Detection of connections to a known terrorist network
- Deletion of system or application logs that might be an indicator that a threat actor is attempting to cover their tracks.
- Detection of suspicious tools or programs (i.e., network scanners, password crackers, keyloggers, remote connection software…) that while not malicious in nature, might be used by a threat actor.

There are three key platforms used by SOC service providers for the purpose of making detections:

1. Detections from a software agent installed on a server or workstations.
2. SaaS application monitors that typically require an API (application programing interface) developed by the SOC service for a specific SaaS platform. One of the most common types of SaaS application monitors in use by SOC services are Microsoft 365 and Google SaaS platforms.
3. Network sensors that are installed on a network to monitor all the traffic that traverses the network both locally and across the gateway to the public Internet.

The current cybersecurity threat landscape for small and medium sized businesses is extremely broad and in many cases a business may need to leverage more than one SOC service provider to make sure all attack vectors are covered. A business might use a SOC service that specializes in on-network detection for a corporate network and another SOC service that takes and agent-based approach to detecting threats on remote user devices (laptops).

Pricing for SOC services varies widely depending on the method of threat detection, the expertise of the SOC service personnel, and the committed service level agreement (SLA) or response times. SOC services might be priced on a per user, per device, or per IP basis. When shopping for a SOC service provider it is important to understand the covered attack surface (network only, agent based, SaaS, or a combination) and it is important to understand how the SOC service provider will work with the business or managed service provider to achieve the desired result which is to become aware of and respond to active threats as quickly as possible.

IT support personnel have long known that it is not possible to mitigate 100% of cyber risks. Rather, prevention is an exercise in deploying layers of defense to reduce the risk of the most likely types of attacks. The evolution of SOC services is a clear acknowledgement of the fact that even the best defended networks and platforms are still at risk and the best method to mitigate remaining risk is to deploy systems that alert the business of a potential issue as quickly possible. The faster an attack is recognized and thwarted, the less likely the attack will result in significant financial harm.

Summary

SOC services play a significant role in cyber defense for small and medium sized businesses by providing early detection of Indications of Compromise so that attacks can be thwarted as quickly as possible. SOC services are a logical next step for businesses that have already implemented good preventative layers of security to help reduce the risk and cost of a late reaction to a cyber-attack.