Security Operations Center (SOC)

Specialize in business intelligence using both Cyber capabilities and HUMINT, helping solve litigation issues, helped the Government in an investigation that involved leaks from the Central Bank, provided evidence gathering.

Penetration testing and security audits specialize in mobile carriers and mobile devices, provides forensics investigation for mobile devices and computers, checking for eavesdropping devices.

"Virtual" body guards for HNWI (High net worth individuals), Celebrities, Ex govt. officials and many more, providing encrypted channels for secret and safe communications, setting up private VPN infrastructure with many different location for totally private, safe and secure browsing online.

Designing and building tailored-maid security products for specific usages, for example special Wi-Fi router to identify unauthorized devices in secured environment.

Hardening mobile devices for more private, safe and secure usage.

Designing and building SOC centers for governments and enterprises, providing SOC as service solutions, a Security Operations Center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.

Security Operations Centers are typically staffed with security analysts and engineers as well as managers who oversee security operations.

SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery.

Security Operations Centers monitor and analyze activity on networks, servers, endpoints, mobile device, IoT devices, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise.

The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

Forensic investigations and establishment of a forensic laboratory.

How A Security Operations Center works

Rather than being focused on developing security strategy, designing security architecture, or implementing protective measures, the SOC team is responsible for the ongoing, operational component of enterprise information security. Security operations center staff is comprised primarily of security analysts who work together to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Additional capabilities of some SOCs can include advanced forensic analysis, cryptanalysis, and malware reverse engineering to analyze incidents.

The first step in establishing an organization's SOC is to clearly define a strategy that incorporates business-specific goals from various departments as well as input and support from executives. Once the strategy has been developed, the infrastructure required to support that strategy must be implemented.

Typical SOC infrastructure includes firewalls, IPS/IDS, breach detection solutions, probes, and a security information and event management (SIEM) system.

Technology should be in place to collect data via data flows, telemetry, packet capture, syslog, and other methods so that data activity can be correlated and analyzed by SOC staff.

The Security Operations Center also monitors networks and endpoints for vulnerabilities in order to protect sensitive data and comply with industry or government regulations.

Benefits of Having a Security Operations Center

The key benefit of having a Security Operations Center is the improvement of security incident detection through continuous monitoring and analysis of data activity. By analyzing this activity across an organization's networks, endpoints, servers, and databases around the clock, SOC teams are critical to ensure timely detection and response of security incidents. The 24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type. The gap between attackers' time to compromise and enterprises' time to detection is well documented in annual Data Breach Investigations Reports, and having a security operations center helps organizations close that gap and stay on top of the threats facing their environments.

Truly successful SOCs utilize security automation to become effective and efficient. By combining highly skilled security analysts with security automation, organizations increase their analytics power to enhance security measures and better defend against data breaches and cyber-attacks. Many organizations that don't have the in-house resources to accomplish this turn to managed security service providers that offer SOC services.