SOC-AS-A-SERVICE

WITH QUANTUM SAFE SOLUTIONS

Background:

Cybersecurity threats are becoming more common, more dangerous, and more difficult to detect and mitigate. On average, organizations take 287 days to detect a breach, and more than a month to contain it. Therefore, it is critical for organizations of all sizes to establish effective processes for detecting, mitigating and preventing such breaches. Security Operation Centers (SOCs) focusing exclusively on cybersecurity (CSOCs) are a proven way to improve threat detection, decrease the likelihood of security breaches, and ensure an appropriate organizational response when cyber incidents do occur.

SOC-as-a-Service additionally offers an alternative model for achieving an organization's cybersecurity objectives while reducing security-related costs. Until recently, it was believed that SOCs were only suitable for large enterprises. Today, organizations of all sizes avail SOC services in different forms.

What is a Cyber SOC?

A Cyber SOC (CSOC) is a physical facility which houses an information security team. This team analyzes and monitors the organization's security systems. The CSOC's mission is to protect the organization from security breaches by identifying, analyzing, and reacting to cybersecurity threats. CSOC teams are composed of management, security analysts, and security engineers.

CSOC teams isolate unusual activity on servers, databases, networks, endpoints, applications, etc., identify security threats, investigate them, and react to security incidents as they occur.

How do Cyber SOCs work?

A Cyber SOC team has two core responsibilities: Maintaining Security Monitoring Tools and Investigating Suspicious Activities.

Below are some of the core processes CSOC teams carry out:

- Alert Triage

  The Cyber SOC collects and correlates log data, and provides tools that allow analysts to review it and detect relevant security events.

- Alert Prioritization

  Cyber SOC analysts leverage their knowledge of the business environment and the threat landscape to prioritize alerts and decide which events represent real security incidents.

- Remediation & Recovery

  Once an incident is discovered, Cyber SOC personnel are responsible for mitigating the threat, cleaning affected systems, and recovering them to their normal working conditions.

Innovation ◦ Integration ◦ Security

- **Postmortem & Reporting**

  An important function of the Cyber SOC is to document the organization's response to an incident, perform additional forensic analyses to ensure that the threat has been fully contained, and learn from the incident to improve the SOC's processes.

Benefits of SOC-as-a-SERVICE

- **24/7/365 Rapid Incident Response**

  SOC-as-a-Service operates around the clock year-round to detect and respond to incidents.

- **Threat Intelligence & Rapid Analysis**

  CSOCs use threat intelligence feeds and security tools to quickly identify threats and fully understand incidents, in order to enable appropriate responses.

- **Reduced Cybersecurity Costs**

  SOC-as-a-Service provides significant cost reductions to our customers in the long run, as well as preventing extra costs associated with ad hoc cybersecurity measures, and the damage caused by cybersecurity breaches.

- **Reduced Complexity of Investigations**

  CSOC teams can streamline their investigative efforts. The Cyber SOC can coordinate data and information from various sources such as network activity, security events, endpoint activity, threat intelligence, and authorizations. CSOC teams have visibility into the network environment, so the Cyber SOC can simplify the tasks of drilling into logs and forensic information, for example.

The Future of the SOC

The traditional physical Security Operations Center is undergoing an exciting transformation. The new Cyber SOC is empowered by powerful new technologies to identify and respond to critical cybersecurity incidents, while retaining the original and well-established SOC command structure and roles.

Planet Defense and its partners are integrating Quantum Safe Solutions with SOC-as-a-Service for clients. This evolving approach will be a game changer and will provide clients with the defense-in-depth they crucially need for effective cybersecurity.

Planet Defense LLC
10640 Main Street, Suite 300
Fairfax, VA 22030
www.planetdefensellc.com

POC: Dr. Michael G. Oehler
Director of Operations
Phone: 702-497-8882
Email: moehler@planetdefensellc.com

Innovation ◦ Integration ◦ Security