Security Terminology Related to a SOC

Cybersecurity literacy is crucial for practicing proper security hygiene.

As business leaders develop fluency in the language of information security (infosec), they become better suited to making decisions that will improve their organization's security culture.

The following glossary serves as a primer for security novices, and as a reference guide for managers who are in the process of familiarizing themselves and their workforces with infosec terminology.

Specifically, this document covers infosec terms as they relate to security operations centers, which for an increasing number of small-to medium-sized enterprises are the foundational component of strong cybersecurity.

General infosec terminology

APT: An advanced persistent threat is defined by an intruder's ability to remain persistent within the network. A criminal hacker will attempt to maintain network access for as long as possible, without detection. This requires advanced evasive hacking measures, which make APTs difficult to detect.

DDoS: Distributed denial of service, or DDoS, refers to the flooding of bandwidth with traffic from multiple sources and IP addresses (computers, internet connected devices, etc.) to render a web service unusable. Hackers may request a ransom with the promise of lifting the attack, or they may use DDoS as a diversion.

IOC: An indicator of compromise is any piece of forensic data that indicates a network intrusion. IOCs are usually uncovered through ongoing log data analysis. Typical IOCs include virus signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command-and-control servers.

NOC: A network operations center is a central location from where network administrators manage and control to one or more networks and a primary server across geographically distributed sites. NOC engineers deal with DDoS attacks, power outages, network failures and routing black holes.

SOC: A security operations center is the combination of cybersecurity personnel, threat detection and incident response processes, and supporting security technologies that make up an organization's security operations. Larger enterprises typically build and manage a SOC in house. SMEs may outsource their SOC to a SOC-as-a-service that provides continuous threat detection and response services.

MSP: A managed service provider refers to any IT vendor who provides a service, software or technology on a monthly subscription basis. The MSP is held responsible for meeting certain service-level agreements (SLAs) for the duration of a contract. Unlike technology or services that are entirely managed in-house or on-premises, ongoing maintenance of the managed service is shouldered by the MSP, typically off-site. As a result, MSPs can usually provide services with less overhead and predictable, pay-per-user pricing.

MSSP: A managed security service provider is a type of MSP that provides 24/7 management, monitoring and maintenance of security services at a fixed monthly cost. This may include configuring and monitoring firewalls, intrusion detection, endpoint protection and other cybersecurity products.

MDR: Managed detection and response providers deliver services that focus on threat detection, incident response and continuous monitoring capabilities. These services are delivered by providers that do not fit the traditional managed security service providers model.

MDR providers typically use their own cloud-based technology stack that includes a proprietary security information and event management (SIEM), and consumes log data from customers' existing cybersecurity tools (NG firewall, web app firewall, endpoint detection and response, anti-virus, etc.). In addition to technology, MDR providers include best-of-breed processes and cybersecurity experts to hunt down and triage advanced threats, and recommend remediation/response actions.

People: Roles and responsibilities

Every SOC employs security engineers capable of filling one or more of the following roles:

Forensics analyst: A computer forensics analyst performs in-depth investigation of user, network and system activity to identify compromised systems and determine if any sensitive data has been breached or stolen.

Incident responder: An incident responder is an infosec professional who determines which systems and data are impacted, and subsequently orchestrates response actions to neutralize the threat or remediate a confirmed compromise. Incident responders typically work onsite, unless response actions are automated.

Security analyst: A security analyst continuously monitors log data, network activity and security controls in to identify potential vulnerabilities in an organization's security posture. A security analyst is crucial to a successful threat detection and response strategy.

Processes: Standards and compliance guidelines

Infosec regulations and standards are crucial to the development of an adequate security posture. A compliance breach may result in penalties and legal damages, while negligence of recommended standards will undermine security efforts.

FISMA: The United States' Federal Information Security Management Act (FISMA) was signed into law in 2002 with the purpose of creating a framework to protect federal government information, operations and assets against natural or man-made threats. FISMA also assigns certain agencies with the responsibility of ensuring the security of federal government data.

GDPR: The General Data Protection Regulation is a regulation that requires businesses to protect the personal data and privacy of citizens of the European Union for any company that does business within the EU member states.

HIPAA: The Health Insurance Portability and Accountability Act protects the privacy of patient health records. Title II, in particular, governs the secure storage, processing, transfer and access of electronic protected health information (ePHI).

NIST: This National Institute of Standards and Technology is a non-regulatory entity under the umbrella of the United States Department of Commerce. NIST Publication Series 800 provides a comprehensive listing of information security measures and controls that have been determined through extensive research.

PCI: The Payment Card Industry Data Security Standard (PCI-DSS) was developed to protect credit, debit and cash card transactions and prevent misuse of cardholder's personal information by any companies/merchants that electronically handle payment card holder data.

SOC 2: The Service Organization Control 2 report establishes minimum security control requirements for any organization that stores customers' data in the cloud. This includes the majority of MSSPs. Its purpose is to minimize risk and exposure to cloud-based information.

SOX: The Sarbanes-Oxley Act of 2002 mandates the secure storage of all corporate records for a minimum of five years prior to erasure. The primary purpose of SOX is to deter corporate fraud.

Technology: Security products

The most commonly used tools, technologies and methodologies in any SOC may include some combination of the following:

AV: Anti-virus is a type of IT security software that scans for, detects, blocks and eliminates malware. AV programs will typically run in the background, scanning for known malware signatures and behavior patterns that may indicate the presence of malware.

CASB: Cloud access security brokers are security policy plans between cloud services users and the providers that identify and consolidate enforcement mechanisms, such as authentication, encryption, alerting and more.

EDR: Endpoint detection and response is an emerging category of tools and solutions that focus on detecting, investigating and mitigating suspicious activity on endpoints and hosts. The value of EDR is in its ability to detect advanced threats that may not have a known behavioral pattern or malware signature. EDR can also trigger an adaptive response based on the nature of detected threats.

EPP: Endpoint protection is a less advanced, centrally managed version of EDR that secures devices (laptops, tablets, smartphones) on a corporate network. This differs from other endpoint-based security features such as anti-virus, which are typically managed through the individual endpoint.

IAM: Identity access management refers to a framework and set of policies that dictate the management of users' electronic identities. Its purpose is to make sure that users receive the appropriate degrees of access and privileges for IT systems, and that proper authentication measures are put in place to enforce those privileges.

IDS/IPS: Intrusion detection systems and intrusion prevention systems, respectively, both provide real-time monitoring of network traffic and automatic alerting upon detection of IOCs. The only difference between IDS and IPS is that the latter can sometimes prescribe action upon detecting a threat.

IR: Incident response refers to the organized protocols and processes that are enacted upon detection of an IOC or confirmation of an intrusion. The purpose of IR within a SOC is to mitigate a threat such as a malware intrusion, data breach or other cyberattack swiftly, limiting further damages. Recovery of lost data and restoration of disrupted services, as well as post-incident analysis to identify lessons learned, all fall under the umbrella of IR.

NGFW: A next-generation firewall is a network security system that uses a combination of enterprise firewall, IPS technology and application control to identify and block more advanced threats. An NGFW can effectively contextualize web application traffic, improving its chances of catching and blocking suspicious subtleties. It can be managed on-premises or in the cloud.

SIEM: Security information and event management is the centralization of all security-related log data into a single point of reference. SIEM software must integrate with a wide variety of data sources including security tools (firewall, IDS, AV, etc.) in order to funnel all pertinent data into a central management console, where it can undergo continuous analysis. SIEM is an essential aspect of any SOC.

UEBA: User and entity behavior analytics perform deep analysis of user actions in an attempt to more accurately identify deviations from the norm. This helps sift out some of the noise, including false positives that may occur during log analysis.

VM: Vulnerability management is proactive scanning for potential vulnerability vectors and the subsequent verification, mitigation and patching needed to improve overall network security.

WAF: A web application firewall monitors, filters and, if necessary, blocks data packets that move to and from web-based applications and services. A WAF is effective at blocking known web-based application attacks, which typically bypass an NGFW.

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com