nuspire

A Guide to Key Cybersecurity Acronyms

What They Are and What's in It for You

> **Cybersecurity acronyms are tossed around as if everyone knows what they mean and how they improve security. This handy guide covers the key acronyms you need to know to make the right cybersecurity decisions for your business. You'll learn what they mean and the benefits they can bring to your security posture.**

Managed Security Services (MSS)

MSS are delivered by a managed security services provider (MSSP) that monitors and manages security devices and systems for organizations. Technologies include firewall, intrusion detection, security information and event management (SIEM), vulnerability scanning and endpoint protection services such as anti-virus and endpoint detection and response (EDR).

Reasons to use MSS:

- Use the latest security technologies without capital expense.
- Reduce security costs because you don't need to maintain an in-house team.
- Centralize visibility of what's being monitored to address threats faster.
- Access additional services such as threat hunting.
- Tap the expertise of security experts who can help reduce risk.
- Enable 24x7x365 protection and monitoring of the enterprise security posture.

Endpoint Detection and Response (EDR)

An EDR solution uses software such as anti-virus and anti-malware to detect threats on fixed and mobile endpoints such as smartphones, tablets, laptops, desktops and servers. Alerts are sent to a security team, which investigates events and initiates action against perceived threats.

Reasons to use EDR:

- Centralize endpoint monitoring and management functions.
- Isolate compromised devices.
- Customize threat watchlists.
- Store logs to support digital forensics.
- Remediate threats using multiple techniques.
- Hunt for new "zero-day" threats.

Managed Detection and Response (MDR)

MDR is a service, provided by an MDR-specific provider or a MSSP, covers endpoints, cloud and networks on-premises and in hybrid environments. Capabilities include 24x7 threat monitoring, threat detection, threat intelligence, threat hunting, advanced analytics and human experts (housed in a security operations center (SOC).

Reasons to use MDR:

- Customize security services and runbooks.
- Implement around-the-clock monitoring.
- Validate incidents in real time to minimize false positives and alert fatigue.
- Obtain advanced analytics with the use of machine learning (ML).
- Receive expert human security expertise in incident investigations.

Extended Detection and Response (XDR)

XDR is a platform that collects the greatest number and types of telemetry from cloud, network and endpoint sources, thus extending threat visibility. Integration, automation and orchestration unify and speed activities including data collection and correlation, data enrichment via threat intelligence, analysis, detection and real-time response.

Reasons to use XDR:

- Broaden visibility across an organization's entire attack surface 24x7x365.
- Integrate multiple security products and domains into a single view.
- Manage detection and response using a single interface.
- Lower overall costs associated with detection and response.
- Increase security efficiency with automated response actions.
- Identify complex and sophisticated attacks.

Security Information and Event Management (SIEM)

A SIEM solution is software that collects, aggregates and analyzes log data from multiple sources to identify abnormal behavior and potential threats. Findings are communicated via alerts to a security team that analyzes the data to determine if a threat exists and what to do about it.

Reasons to use SIEM:

- Simplify the security view with visual dashboards.
- Detect security events as they occur.
- Manage logs and retain data for investigative and/or compliance purposes.
- Enforce security policies.
- Keep up with the changing threat landscape when settings, rules and configurations are fine-tuned continually.

Security Orchestration, Automation and Response (SOAR)

Known to be complex to build and implement, SOAR platforms allow security teams to integrate disparate security tools and create custom automated runbooks. SOAR automates data analysis, recommendations and response actions; manages workflow; and provides a single access point to threat intelligence and reports.

Reasons to use SOAR:

- Automate manual processes and repetitive tasks.
- Connect SIEMs, firewalls, threat intelligence sources and other security tools.
- Reduce alert fatigue.
- Leverage artificial intelligence (AI) and ML to improve context and threat analysis.
- Enable analysts to keep up with the increasing volume and sophistication of bad actors.

Security Operation Center as a Service (SOCaaS)

SOCaaS monitors and manages an organization's security technology such as endpoint, cloud and network. SOCaaS includes the human experts who specialize in areas such as threat intelligence, threat modeling, threat hunting, forensics and incident response.

Reasons to use SOCaaS:

- Reduce the cost and complexity of maintaining an in-house SOC.
- Lower risk by centralizing and unifying your security program.
- Bring in experts to run your security technology since resources are hard to find.
- Operate in compliance with minimal internal effort and expense.