Security Scorecard | The Hartford

Cybersecurity Acronyms Guide

Executive Summary

This document serves as a quick reference guide cybersecurity acronyms, providing a brief definition for each. It's designed to help understand common terminology used in the field of cybersecurity.

Top 10 List

1. **MFA (Multi-Factor Authentication)**: Essential for securing access by requiring multiple forms of verification.
2. **VPN (Virtual Private Network):** Critical for secure remote access and protecting internet traffic.
3. **Firewall (FW):** Fundamental network security device that controls and monitors traffic.
4. **DDoS (Distributed Denial-of-Service):** A common and impactful attack that disrupts service availability.
5. **Ransomware:** A prevalent and damaging type of malware that encrypts data and demands payment.
6. **Phishing:** A widely used social engineering tactic to steal sensitive information.
7. **SIEM (Security Information and Event Management):** Centralized system for log management and security analysis.
8. **EDR (Endpoint Detection and Response):** Crucial for monitoring and responding to threats on individual devices.
9. **SSL/TLS (Secure Sockets Layer/Transport Layer Security):** Vital for securing communication over the internet.
10. **CIA Triad (Confidentiality, Integrity, Availability):** The core principles that guide information security.

Authentication and Access Control

- **MFA (Multi-Factor Authentication):** Verifying identity with multiple factors.
- **IAM (Identity and Access Management):** Controlling user access to resources.
- **RBAC (Role-Based Access Control):** Controlling access based on user roles.
- **ACL (Access Control List):** A list of permissions attached to an object.
- **NAC (Network Access Control):** Controlling access to a network based on device and user.

Network Security

- **VPN (Virtual Private Network):** Encrypting internet traffic for secure connections.
- **IDS (Intrusion Detection System):** Monitoring networks for malicious activity.
- **IPS (Intrusion Prevention System):** Actively blocking malicious network activity.
- **FW (Firewall):** A network security system that monitors and controls traffic.
- **NIDS (Network-based Intrusion Detection System):** Monitoring network traffic for malicious activity.

Threats and Attacks

- **DDoS (Distributed Denial-of-Service):** Overwhelming a system with traffic to disrupt service.
- **Ransomware:** Malicious software that encrypts data and demands payment.
- **Phishing:** Deceptive attempts to obtain sensitive information via email or other means.
- **Malware (Malicious Software):** Software designed to harm or disrupt systems.
- **APT (Advanced Persistent Threat):** Long-term, targeted cyberattacks.
- **Zero-Day:** A vulnerability unknown to the vendor and actively exploited.
- **MITM (Man-in-the-Middle):** An attack where an attacker intercepts communication.
- **RAT (Remote Access Trojan):** Malware that allows remote control of a system.
- **DoS (Denial of Service):** Disrupting access to a system or network.

Security Management and Operations

- **SIEM (Security Information and Event Management):** Centralized log management and security analysis.
- **SOC (Security Operations Center):** A centralized team for security monitoring and response.
- **EDR (Endpoint Detection and Response):** Monitoring and responding to threats on endpoints.
- **XDR (Extended Detection and Response):** Unifying security tools into a cohesive whole for threat detection.
- **IR (Incident Response):** The process of responding to a security incident.
- **SOAR (Security Orchestration, Automation, and Response):** Automating security tasks and incident response.

Email Security

- **SPF (Sender Policy Framework):** An email authentication method.
- **DKIM (DomainKeys Identified Mail):** An email authentication method.
- **DMARC (Domain-based Message Authentication, Reporting & Conformance):** An email authentication protocol.

Web Application Security

- **API (Application Programming Interface):** A set of rules for software interaction.
- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):** Protocols for secure communication over a network.
- **OWASP (Open Web Application Security Project):** An organization focused on web application security.
- **WAF (Web Application Firewall):** Protecting web applications from attacks.
- **SAST (Static Application Security Testing):** Testing application source code for vulnerabilities.

Vulnerabilities and Standards

- **CVE (Common Vulnerabilities and Exposures):** A list of publicly known information security vulnerabilities.
- **PCI DSS (Payment Card Industry Data Security Standard):** Security standard for organizations handling credit card information.
- **GDPR (General Data Protection Regulation):** EU regulation on data protection and privacy.
- **ISO (International Organization for Standardization):** Organization that develops and publishes international standards.

Other Security Concepts

- **BYOD (Bring Your Own Device):** Allowing employees to use personal devices for work.
- **RDP (Remote Desktop Protocol):** Protocol for remote access to computers.
- **UEBA (User and Entity Behavior Analytics):** Monitoring user and entity behavior for anomalies.
- **AES (Advanced Encryption Standard):** A symmetric-key encryption algorithm.
- **CIA Triad (Confidentiality, Integrity, Availability):** Core principles of information security.
- **DRP (Disaster Recovery Plan):** A plan for recovering from a disaster.
- **HIDS (Host-based Intrusion Detection System):** Monitoring a single host for malicious activity.
- **HIPS (Host-based Intrusion Prevention System):** Actively blocking malicious activity on a single host.
- **PKI (Public Key Infrastructure):** System for managing digital certificates and public-key encryption.
- **PoC (Proof of Concept):** Demonstration that a concept or idea is feasible.
- **SaaS (Software as a Service):** Software delivered over the internet.

About SecurityScorecard

SecurityScorecard helps security professionals work collaboratively to solve mission-critical, cybersecurity issues in a transparent way. The SecurityScorecard platform provides continuous, non-intrusive cyber risk monitoring of any organization and its ecosystem.

Ready to get started? Schedule a demo today: **https://securityscorecard.com/the-hartford/**

SecurityScorecard.com
info@securityscorecard.com

SecurityScorecard