Cybersecurity Glossary

This page is a glossary of various cybersecurity acronyms. Some of these definitions may be powered by ChatGPT.

Glossary

Term	Definition
EDR (Endpoint Detection & Response)	EDR focuses on monitoring and responding to threats on endpoints like computers, laptops, mobile devices, or servers. It involves installing lightweight agents on these devices to collect and analyze data, allowing for the detection of suspicious activities or threats. EDR solutions offer real-time visibility into endpoint activities and enable rapid response to potential threats.
Framework	A framework guidance for organizations to better understand, assess, prioritize, and communicate their cybersecurity efforts. It is a set of best practices and does not prescribe how outcomes should be achieved.
MDR (Managed Detection & Response)	MDR is a service-based approach to cybersecurity that typically includes EDR functionalities but goes beyond by providing continuous monitoring, threat hunting, and incident response capabilities. MDR services are often outsourced to third-party providers who manage and monitor an organization's security infrastructure, offering expertise and round-the-clock monitoring to detect, analyze, and respond to security incidents.
NDR (Network detection & Response)	NDR focuses on monitoring and analyzing network traffic to detect and respond to threats within a network. It involves capturing and inspecting network traffic to identify abnormal behaviors, potential threats, or malicious activities that might bypass traditional perimeter security measures like firewalls. NDR solutions often use advanced analytics and machine learning to detect anomalies in network traffic.
XDR (Extended Detection & Response)	XDR is an evolution of traditional cybersecurity approaches, aiming to integrate and correlate data from multiple security components (such as EDR, MDR, NDR, and others) across different environments (endpoints, networks, cloud services, etc.). XDR provides a more holistic view of security threats by aggregating and analyzing data from various sources, enabling better detection and response capabilities across the entire IT infrastructure.

What is the Difference Between SIEM and SOAR?

SIEM (Security Information and Event Management)

- **Functionality**: SIEM systems aggregate and analyze log data from various sources within an organization's IT infrastructure. They collect, normalize, and correlate logs to identify potential security incidents by detecting patterns or anomalies in the data.
- **Use Cases**: SIEM is primarily used for real-time monitoring, threat detection, incident response, and compliance reporting. It helps security teams gain visibility into their environment, enabling them to respond promptly to security events.
- **Features**: SIEM tools often include capabilities like log management, correlation of events, real-time monitoring, and reporting.

SOAR (Security Orchestration, Automation, and Response)

- **Functionality**: SOAR platforms focus on automating and orchestrating security operations and incident response tasks. They integrate with various security tools, allowing for the automation of repetitive tasks and the orchestration of complex workflows.
- **Use Cases**: SOAR is used to streamline incident response, improve efficiency by automating routine tasks (like alert triaging, enrichment, and response), and facilitate collaboration among security teams.
- **Features**: SOAR tools typically include automation capabilities, playbook creation for incident response, integration with different security tools via APIs, and case management.

Comparison:

- **Focus**: SIEM primarily focuses on log management, correlation, and real-time monitoring for threat detection, while SOAR concentrates on automating and orchestrating incident response processes.
- **Function**: SIEM identifies and alerts about security events, while SOAR automates incident response actions and orchestrates workflows to remediate security incidents.
- **Usage**: SIEM is more about monitoring, detection, and compliance, while SOAR emphasizes response automation and operational efficiency.
- **Integration**: Both can integrate with various security tools, but SOAR's focus is on creating seamless workflows and automating responses across these tools.

Integration:

In practice, organizations often use SIEM and SOAR together. SIEM identifies potential threats, and when an incident occurs, SOAR can automatically trigger response actions based on predefined playbooks, leveraging the data and insights from SIEM, thus enhancing the efficiency and effectiveness of incident response.

Ultimately, SIEM and SOAR complement each other by providing visibility, detection, and automated response capabilities, contributing to a more robust cybersecurity posture.