# Endpoint Security Monitoring

## 1. Fundamentals of Endpoint Security Monitoring

### Definition

Endpoint security monitoring refers to the ongoing surveillance of endpoint devices, which include laptops, desktops, smartphones, servers, and IoT (Internet of Things) devices. This is crucial for detecting and responding to security threats targeting these devices. Since endpoints serve as gateways to broader networks, they are prime targets for cyberattacks. Effective endpoint security monitoring helps organizations stay ahead of potential breaches by providing real-time visibility into endpoint activity.

### Endpoints

An endpoint is any device that connects to a network, allowing data exchange with other systems. The most common endpoints include:

- **Computers**: Desktops, laptops, and workstations.
- **Mobile Devices**: Smartphones and tablets.
- **Servers**: Physical or virtual machines that host applications and store data.
- **IoT Devices**: Internet-connected objects like security cameras, smart home systems, medical devices, and industrial sensors.

These devices can be exploited by attackers to infiltrate networks, steal data, or cause damage. Therefore, monitoring their behavior is critical to an organization’s overall security strategy.

### Goals of Endpoint Security Monitoring

- **Threat Detection**: Identifying malicious activities, such as malware, unauthorized access, or unusual file changes, at the endpoint level.
- **Threat Mitigation**: Once a threat is detected, mitigation strategies are deployed to minimize the damage.
- **Data Protection**: Safeguarding sensitive data from breaches or unauthorized access.
- **Compliance**: Ensuring that endpoint security aligns with relevant industry standards (such as GDPR, HIPAA, or PCI-DSS), which require proper protection of data and reporting on security incidents.

### Types of Endpoint Threats

- **Malware**: Malicious software designed to damage or steal data from systems. This category includes:
  - **Viruses**: Self-replicating programs that spread from one device to another.
  - **Ransomware**: Encrypts files on a victim's device and demands payment for decryption.
  - **Spyware**: Secretly gathers user information and transmits it to third parties.
- **Phishing**: Cybercriminals use deceptive methods, such as fake emails or websites, to trick users into revealing personal or sensitive information.
- **Insider Threats**: These threats come from individuals within an organization—employees, contractors, or vendors—who misuse their access to systems.

- **Unauthorized Access**: Attackers exploit vulnerabilities (e.g., outdated software or weak passwords) to gain unauthorized entry into systems and devices.

---

## 2. Technologies for Endpoint Security

### EPP (Endpoint Protection Platform)

- **What is it?**

  EPP is a basic solution for protecting endpoints against known threats, such as viruses and malware. It provides preventive security through signature-based detection (recognition of known malware patterns).

- **Limits:** Not effective against new, unknown or advanced attacks
- **Example:** An antivirus program that blocks a known malware variant.

### EDR (Endpoint Detection and Response)

- **What is it?**

  EDR goes beyond EPP and provides real-time endpoint monitoring, suspicious activity detection, and forensic capabilities. EDR focuses on behavioral analysis to identify unusual or new threats.

- **Example:** Can detect advanced threats and respond faster to incidents.

### XDR (Extended Detection and Response)

- **What is it?**

  XDR goes beyond EDR by monitoring not only endpoints, but also networks, servers and cloud environments and correlating data from all these sources to provide broader threat analytics.

- **Example:** An XDR system that analyzes both endpoint and network data to identify a multi-vector attack (e.g. endpoint phishing and lateral movement through the network).

---

## 3. EDR Tools

### Definition of EDR

Endpoint Detection and Response (EDR) tools are security solutions specifically designed to monitor endpoint activities, detect suspicious behaviors, and respond to potential threats. EDR provides security teams with real-time visibility into what's happening on endpoints, enabling faster responses to security incidents.

### Common Features of EDR Tools

- **Real-Time Monitoring**: Continuous tracking of endpoints for suspicious activity, which allows organizations to detect potential threats before they escalate.
- **Behavioral Analysis**: Rather than just looking for known malware, behavioral analysis tracks unusual or unauthorized behavior on endpoints. For example, if a user typically accesses files during work hours

but is suddenly accessing them at midnight, it might signal a compromised account.
- **Incident Response**: EDR tools provide various mechanisms to respond to detected threats, including quarantining infected files, isolating compromised systems, or triggering alerts for security teams.
- **Threat Hunting**: EDR enables proactive searches for potential threats that haven't triggered alerts. Analysts can explore endpoint data for signs of hidden or emerging threats, allowing for preventive actions.

### Popular EDR Tools

- **CrowdStrike Falcon**: A leading cloud-based EDR tool. It uses artificial intelligence to detect threats and offers real-time responses to incidents, making it suitable for organizations of all sizes.
- **Microsoft Defender ATP**: A built-in Windows security tool, it provides endpoint protection and integrates with Microsoft's cloud infrastructure to enhance security.
- **Wazuh**: An open-source security monitoring tool, Wazuh provides intrusion detection, vulnerability analysis, and log monitoring.
- **OSSEC**: Another open-source tool, OSSEC offers host-based intrusion detection (HIDS), monitoring logs and files for signs of tampering or unauthorized changes.

---

## 4. Key Components of Endpoint Security Monitoring

To ensure effective endpoint security monitoring, several critical components must be in place:

- **File Integrity Monitoring (FIM)**: This involves continuously checking key system files for unauthorized changes. FIM tools can detect if critical files (such as configuration files, system binaries, or important user data) have been tampered with. This is particularly useful for detecting ransomware or other malware that alters system files.
- **Log Monitoring**: All systems and applications generate logs, which are valuable sources of information for security analysis. Endpoint monitoring tools collect these logs and analyze them for signs of suspicious activity, such as multiple failed login attempts or unexpected software installations.
- **Threat Intelligence Integration**: Many modern endpoint security tools integrate with threat intelligence feeds that provide information about the latest cyber threats. By cross-referencing endpoint activity with known threat data, these tools can quickly identify and block known threats before they can cause harm.
- **Behavioral Analytics**: This is the practice of using machine learning or other advanced algorithms to analyze user or process behavior and detect anomalies. For example, if a normally dormant process suddenly begins sending large volumes of data, this behavior could indicate a data exfiltration attempt.

---

## 5. Endpoint Security Tools and Capabilities

There are various tools available to ensure effective endpoint security. Each has unique features and capabilities designed to detect and respond to different types of threats.

### CrowdStrike Falcon

- **Cloud-native**: This tool operates entirely in the cloud, meaning it can monitor endpoints regardless of their physical location.

- **Threat Detection and Response**: CrowdStrike uses artificial intelligence (AI) and machine learning (ML) to detect both known and unknown threats.
- **Real-Time Visibility**: Offers detailed information on the processes, file activities, and network connections happening across endpoints.

### Microsoft Defender ATP

- **Advanced Threat Protection**: Defender ATP integrates with the broader Microsoft security suite, providing a holistic approach to protecting Windows systems.
- **Automated Incident Response**: Uses behavioral analysis to detect abnormal activity and can automatically isolate infected endpoints.
- **Unified Ecosystem**: Defender ATP can integrate with other Microsoft tools such as Azure, Office 365, and Intune for comprehensive endpoint protection.

### Wazuh

- **Open-Source**: As a free-to-use tool, Wazuh is accessible to organizations of all sizes. It provides real-time intrusion detection and continuous monitoring of endpoints.
- **Log Monitoring**: Wazuh collects and analyzes logs from endpoints to detect abnormal activities.
- **Vulnerability Detection**: The tool continuously scans for known vulnerabilities in software and operating systems, providing proactive protection.

### OSSEC

- **Host-Based Intrusion Detection**: OSSEC provides extensive monitoring of system logs and critical files to detect anomalies. It's widely used to secure both physical and virtual environments.
- **Alerting and Remediation**: OSSEC sends alerts for suspicious activities and can automatically trigger predefined responses (such as isolating an endpoint).

an interresting video for Wazuh: https://www.youtube.com/watch?v=3CaG2GI1kn0&t=152s

---

## 6. Techniques for Endpoint Security Monitoring

Endpoint monitoring employs a range of techniques to detect threats and safeguard devices:

- **Signature-Based Detection**: This method relies on comparing endpoint activity to a database of known threat signatures. While effective at catching known threats, it cannot detect new or unknown types of attacks.

- **Anomaly-Based Detection**: This technique looks for unusual or unexpected behaviors, which may indicate a potential threat. For instance, if a process is suddenly using more system resources than usual, this could be a sign of malicious activity.

- **User and Entity Behavior Analytics (UEBA)**: By monitoring normal user and device behavior, UEBA systems can detect deviations that suggest insider threats or advanced attacks. For example, an employee accessing a large volume of sensitive data at unusual times could trigger a security alert.

- **Automated Incident Response**: Advanced tools can take automated actions when specific threats are detected. For instance, if malware is identified, the system might quarantine the infected endpoint or

block the malicious process without requiring human intervention.

---

# 7. Threat Detection and Incident Response

Effective endpoint security monitoring enables rapid detection and response to potential security incidents.

## Threat Detection

The primary goal of endpoint monitoring is to detect various types of security threats, including:

- **Malware and Ransomware**: Detecting software that is designed to cause damage or steal information.
- **Phishing Attempts**: Identifying when users are exposed to malicious emails or websites.
- **Unauthorized Access**: Monitoring for attempts to bypass security controls, such as by exploiting vulnerabilities or using stolen credentials.
- **Abnormal Network Activity**: Detecting unexpected communication patterns that could indicate data exfiltration or a command-and-control connection to a malicious actor.

## Incident Response Phases

1. **Containment**: Once a threat is detected, the compromised endpoint is isolated to prevent the spread of malware or other harmful activities across the network.
2. **Eradication**: After containment, the malware or attacker must be removed from the endpoint, which may involve deleting malicious files or revoking access credentials.
3. **Recovery**: After eliminating the threat, the system must be restored to normal operation. This may involve reinstalling software, restoring data from backups, or applying patches.
4. **Forensics**: A detailed analysis is often performed on compromised endpoints to determine how the attack occurred, what data was affected, and how future incidents can be prevented.

---