Endpoint Detection and Response (EDR)Tools

1 . CrowdStrike

Purpose :

In a SOC, CrowdStrike Falcon acts as an **Endpoint Detection and Response (EDR) + Threat Intelligence tool**, enabling analysts to:

- **Detect**: Identify malicious activity on endpoints in real time.
- **Investigate**: Provide forensic details for SOC analysts to understand attack vectors.
- **Respond**: Allow rapid isolation and remediation of compromised machines.
- **Hunt**: Enable proactive threat hunting using Falcon OverWatch.

Key Features :

- **EDR Telemetry** – Continuous endpoint monitoring for all processes, connections, and file activities.
- **Real-Time Alerting** – Instant alerts for suspicious or confirmed threats in the SOC dashboard.
- **Threat Hunting Tools** – Falcon's Query Language (FQL) to find hidden threats.
- **Integration with SIEM/SOAR** – Sends logs to tools like Splunk, QRadar, or Azure Sentinel.
- **Automated Response Playbooks** – SOC can execute predefined actions (isolate host, kill process) automatically.

Advantages :

- **Reduces Detection Time** – Speeds up the SOC's MTTD (Mean Time to Detect).
- **Accelerates Response** – Remote isolation prevents lateral movement during attacks.
- **Comprehensive Visibility** – Full endpoint activity timeline for investigations.
- **Global Threat Intel** – Access to CrowdStrike's intelligence database for faster IOC verification.
- **Cloud Scalability** – SOC can monitor thousands of devices without managing on-prem infrastructure.

Usage :

- **Incident Detection** – SOC Level 1 analysts receive alerts from Falcon in real time.
- **Incident Investigation** – Level 2/3 analysts use Falcon data for root cause analysis.
- **Threat Hunting** – SOC threat hunters use Falcon to proactively look for APTs and insider threats.
- **Automated Response** – SOC can trigger Falcon to block malicious processes instantly.
- **Integration with SOC Tools** – Sends EDR data to SIEM for centralized correlation and dashboards.

Architecture :

SOC-centric Falcon Architecture:

- **Endpoints (Workstations, Servers, Cloud Workloads)**
  - Falcon sensor installed, collecting telemetry.
- **CrowdStrike Cloud**
  - Processes EDR data using AI/ML.
  - Enriches alerts with global threat intel.
- **Falcon Console**
  - SOC analysts log in to view, investigate, and respond.
- **SIEM/SOAR Integration**
  - Falcon sends logs to SOC's SIEM for correlation with firewall, IDS/IPS, and network data.
  - SOAR platforms can trigger automated Falcon responses.

Workflow :

Step 1 – Data Collection

- Falcon sensors record endpoint activity continuously.
- Data sent to CrowdStrike cloud in near real time.

Step 2 – Detection

- Falcon's analytics detect suspicious behavior.
- Alerts are generated in Falcon Console and optionally pushed to SOC SIEM.

Step 3 – Triage

- L1 SOC analysts review alerts and escalate confirmed threats.

Step 4 – Investigation

- L2 SOC analysts investigate endpoint activity via Falcon's EDR timeline.
- Search for IOCs, suspicious processes, and attack patterns.

Step 5 – Response

- Analysts isolate infected hosts remotely.
- Kill malicious processes, delete malware, apply patches.

Step 6 – Threat Hunting & Intelligence

- Threat hunters proactively search for hidden threats using Falcon data.
- New intel is shared across the SOC team.

2 . Cybereason

Purpose :

Cybereason is an **Endpoint Detection and Response (EDR) + Extended Detection and Response (XDR) platform** designed to help SOC teams **detect, investigate, and respond** to advanced cyber threats in real time.
Its main purpose in a SOC is to provide **complete visibility across endpoints, networks, and cloud workloads** while **automating investigation** so analysts can respond faster and more accurately.

Key SOC goals:

- Reduce **MTTD** (Mean Time to Detect) and **MTTR** (Mean Time to Respond).
- Correlate events from multiple sources into a single, attack-centric view.
- Provide deep investigation capabilities without overwhelming analysts.

Key Features :

- **MalOp™ Detection** – Unique "Malicious Operations" view that correlates all related events (processes, users, network activity) into a single visual story for faster investigations.
- **Behavioral EDR** – Detects file-based and fileless attacks using behavioral analysis rather than just signatures.
- **XDR Integration** – Extends visibility beyond endpoints to include cloud, identity, and network telemetry.
- **Automated Investigation** – AI automatically maps attack chains, reducing manual work for SOC analysts.
- **Incident Response Tools** – Remote isolation, process termination, and remediation capabilities.

Advantages :

- **Attack-Centric View** – Groups related events into a single MalOp, reducing alert fatigue.
- **High Context Visibility** – Shows the full kill chain of an attack, helping analysts understand root cause quickly.
- **Rapid Response** – Remote containment and remediation without visiting the endpoint.
- **Scalability** – Can protect thousands of endpoints without significant resource usage.
- **Cloud or On-Prem Flexibility** – Supports both deployment models for SOC environments.

Usage :

- **24/7 Endpoint Monitoring** – Continuous telemetry collection for threat detection.
- **Incident Triage** – L1 SOC analysts can quickly identify high-priority MalOps.
- **Advanced Investigation** – L2/L3 analysts can dig deep into process trees and network activity.
- **Threat Hunting** – Use Cybereason Query Language (CRQL) to proactively search for hidden threats.
- **Integration with SIEM/SOAR** – Send enriched incident data to tools like Splunk, QRadar, or Cortex XSOAR for automation.

Architecture :

Cybereason's SOC architecture typically has four layers:

1. **Endpoint Sensors**
   - Lightweight agents on Windows, macOS, Linux devices.
   - Collect telemetry: process execution, file changes, registry edits, network connections.
2. **Cybereason Data Platform**
   - Central server (cloud or on-prem).
   - Correlates endpoint telemetry with global threat intelligence.
   - Runs AI/ML detection models.
3. **MalOp Detection Engine**
   - Groups related suspicious activities into a single MalOp (reducing the number of separate alerts).
   - Provides visual attack chain mapping.
4. **SOC Analyst Interface (Cybereason Console)**
   - Web-based dashboard for detection, investigation, and remediation.
   - Integrated with SIEM/SOAR tools for automation.

Workflow :

Step 1 – Data Collection

- Endpoint sensors collect telemetry in real time.
- Data sent to Cybereason platform for analysis.

Step 2 – MalOp Detection

- AI/ML models detect suspicious behaviors.
- Events are correlated into a single MalOp with full attack chain details.

Step 3 – Alerting & Triage

- MalOps appear in the SOC dashboard.
- L1 analysts review and decide on escalation.

Step 4 – Investigation

- L2/L3 analysts use process trees, timeline views, and forensic data to identify root cause.

Step 5 – Response & Containment

- SOC can remotely isolate the endpoint, kill malicious processes, remove files, and patch vulnerabilities.

Step 6 – Threat Hunting

- Analysts use CRQL to search for additional signs of compromise across the environment.

Step 7 – Continuous Feedback

- Threat intel from new incidents is fed back into Cybereason's detection models and shared globally.

3 . SentinelOne

Purpose :

SentinelOne is an **AI-powered Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) platform**.
Its primary purpose in a SOC is to:

- **Prevent** threats using behavioral AI.
- **Detect** attacks (including fileless, zero-day, and ransomware).
- **Respond** automatically or manually.
- **Hunt** for hidden threats across endpoints, cloud workloads, and IoT devices.

In a SOC, SentinelOne helps analysts **reduce detection time (MTTD)** and **accelerate response time (MTTR)** by providing **real-time visibility and autonomous remediation**.

Key Features :

- **Behavioral AI Detection** – Identifies malicious behavior patterns rather than relying on signatures.
- **ActiveEDR** – Links all related events into a storyline for faster investigations.
- **Automated Remediation & Rollback** – Can kill malicious processes, quarantine files, and roll back Windows devices to a pre-attack state.
- **XDR Capabilities** – Correlates data from endpoints, network, and cloud for cross-environment threat detection.
- **Threat Hunting Console** – Provides a query language (Deep Visibility) for proactive threat hunting.

Advantages :

- **Autonomous Response** – Can respond to threats without human intervention, reducing analyst workload.
- **Reduced Alert Fatigue** – Storyline technology groups related alerts into a single view.
- **High Detection Accuracy** – AI models minimize false positives.
- **Fast Forensic Investigation** – Timeline-based attack visualization helps in quick root cause analysis.
- **Ransomware Rollback** – Unique ability to restore encrypted files automatically (Windows).

Usage :

- **Endpoint Protection** – Prevent malware, ransomware, and zero-day exploits.

- **Incident Investigation** – SOC analysts can review the complete attack storyline for context.
- **Threat Hunting** – Use Deep Visibility queries to search for suspicious activity across all endpoints.
- **Automated Remediation** – Roll back systems, quarantine malware, and isolate devices remotely.
- **Integration with SIEM/SOAR** – Send enriched incident data to Splunk, QRadar, or Cortex XSOAR for orchestration.

Architecture :

SentinelOne's architecture in SOC operations typically includes:

- **Endpoint Agents (Sensors)**
  - Installed on Windows, macOS, Linux, and Kubernetes workloads.
  - Monitors processes, network traffic, file changes, and registry activity.
- **SentinelOne Management Console**
  - Cloud-based or on-premises.
  - Hosts detection AI, policy management, and alert handling.
- **ActiveEDR Storyline Engine**
  - Correlates related events into a single "story" to reduce complexity.
- **Integration Layer**
  - Connects SentinelOne with SIEM, SOAR, and ticketing tools for SOC workflows.

Workflow :

Step 1 – Data Collection

- Endpoint agent collects telemetry and analyzes activity locally in real time.

Step 2 – Local AI Analysis

- Behavioral AI detects suspicious activity instantly without relying solely on cloud lookups.

Step 3 – Threat Detection

- Detected threats are grouped into an attack storyline and sent to the management console.

Step 4 – SOC Alert Review

- L1 analysts receive the alert in SentinelOne dashboard or via SIEM.
- Alerts already include full context, process tree, and MITRE ATT&CK mapping.

Step 5 – Investigation

- L2/L3 SOC analysts analyze the storyline, determine scope, and identify affected assets.

Step 6 – Response

- SOC can quarantine files, kill processes, isolate endpoints, and roll back to pre-attack state.

Step 7 – Threat Hunting

- Analysts use Deep Visibility to search for IOCs across all endpoints.

Step 8 – Continuous Feedback

- Threat data is added to SentinelOne's global AI models for improved detection.

4 . Cortex XDR

Purpose :

Cortex XDR (Extended Detection and Response) is Palo Alto Networks' unified security platform designed to **detect, investigate, and respond to threats** across **endpoints, networks, cloud workloads, and identities**.
In a SOC, its purpose is to:

- **Correlate** telemetry from multiple data sources (endpoint, firewall, cloud, identity) into a single view.
- **Detect** both known and unknown threats using AI/ML and behavioral analytics.
- **Investigate** incidents with complete attack timelines.
- **Respond** through integrated response actions or via SOAR automation.

Key Features :

- **Unified Data Correlation** – Combines data from endpoints, network traffic, cloud logs, and threat intelligence for holistic visibility.
- **Behavioral Analytics** – Detects anomalies using ML models and UEBA (User and Entity Behavior Analytics).
- **Endpoint Protection** – Built-in EDR capabilities to protect endpoints from malware, ransomware, and exploits.
- **Incident Visualization** – Timeline-based incident views mapping the full kill chain.
- **Native Integration with Palo Alto Ecosystem** – Works seamlessly with NGFW, Prisma Cloud, and Cortex Data Lake.

Advantages :

- **Holistic Visibility** – See threats across endpoints, networks, cloud, and identity in one dashboard.
- **Fewer False Positives** – AI-driven correlation reduces redundant alerts.
- **Faster Investigation** – Complete timeline views help analysts understand the entire attack scope.
- **Tight Integration with SOAR** – Enables automated playbook execution for faster response.

- **Scalability** – Handles enterprise-scale data ingestion without impacting SOC performance.

Usage :

- **Advanced Threat Detection** – Identify threats using combined endpoint + network + cloud data.
- **Incident Investigation** – SOC analysts can visualize and analyze full attack paths.
- **Threat Hunting** – Use query-based searches across historical telemetry data.
- **Automated Response** – Isolate endpoints, block IPs, or disable user accounts via integrated actions.
- **Compliance Reporting** – Generate detailed incident reports for audits (PCI-DSS, HIPAA, ISO 27001).

Architecture :

Cortex XDR's SOC architecture typically includes:

1. **Data Sources**
   - **Endpoints:** Telemetry from Cortex XDR agents (Windows, macOS, Linux).
   - **Network:** Logs and traffic metadata from Palo Alto firewalls, routers, and switches.
   - **Cloud & Identity:** Data from Prisma Cloud, Office 365, Okta, etc.
   - **Third-party tools:** Data ingestion from SIEM and other security platforms.
2. **Cortex Data Lake**
   - Central repository for storing all collected telemetry and logs.
   - Scalable cloud storage for historical and real-time data.
3. **Analytics Engine**
   - Machine learning and behavioral models analyze aggregated data.
   - UEBA detects insider threats and compromised accounts.
4. **Cortex XDR Console**
   - SOC analyst dashboard for detection, investigation, and response.
   - Integrates with Cortex XSOAR for automation.

Workflow :

Step 1 – Data Collection

- Endpoint agents, firewalls, and cloud integrations send telemetry to the Cortex Data Lake.

Step 2 – Data Correlation & Analysis

- Analytics engine correlates logs and events from multiple sources.
- Machine learning models flag anomalies and suspicious behaviors.

Step 3 – Alert Generation

- Threats are detected and consolidated into incidents.
- Alerts sent to SOC console (and optionally SIEM).

Step 4 – Triage

- L1 analysts review the alert's context and severity.
- Incident escalated to L2/L3 for deeper investigation.

Step 5 – Investigation

- Analysts view attack timelines showing every step of the intrusion.
- MITRE ATT&CK mapping aids understanding of adversary techniques.

Step 6 – Response

- Actions: isolate hosts, block malicious IPs, disable accounts, or trigger SOAR playbooks.

Step 7 – Threat Hunting

- SOC hunters run proactive searches using historical telemetry for IOCs or suspicious patterns.

Step 8 – Feedback Loop

- Lessons learned and new IOCs are fed into detection rules to prevent recurrence.

5 . Cynet 360 AutoXDR :

Purpose :

Cynet 360 AutoXDR is an **Extended Detection and Response (XDR)** platform with built-in **endpoint protection, network analytics, user behavior monitoring, deception technology, and automated response** capabilities.

In a SOC, its purpose is to:

- **Detect** advanced threats across endpoints, networks, and user accounts in real time.
- **Correlate** events into a single attack story to reduce alert fatigue.
- **Respond** automatically with predefined playbooks.
- **Provide 24/7 monitoring** via its MDR service (Cynet CyOps team) if needed.

It is designed for SOCs that want **one integrated security platform** instead of managing multiple separate tools.

Key Features :

- **AutoXDR Correlation Engine** – Merges endpoint, network, and user activity data into a unified incident view.
- **NGAV + EDR** – Next-Gen Antivirus and Endpoint Detection and Response for blocking known and unknown malware.

- **User Behavior Analytics (UBA)** – Detects insider threats and compromised accounts via behavioral anomalies.
- **Deception Technology** – Deploys decoy files, credentials, and systems to detect lateral movement.
- **Automated Response Orchestration** – Quarantines hosts, blocks IPs, disables accounts automatically.

Advantages :

- **All-in-One Security Platform** – Eliminates the need to manage multiple separate tools.
- **Lower Analyst Workload** – Correlation and automation reduce manual triage.
- **Built-in MDR (CyOps)** – 24/7 SOC support included at no extra cost.
- **Fast Deployment** – Cloud-managed, lightweight agents, minimal infrastructure setup.
- **Deception Layer** – Detects threats early before they impact critical assets.

Usage :

- **Endpoint Threat Detection & Response** – Monitor and block malicious activity on endpoints.
- **Network Threat Visibility** – Detect malicious communications, C2 traffic, and lateral movement.
- **Insider Threat Detection** – Identify risky user behavior or compromised credentials.
- **Automated Incident Response** – SOC can trigger playbooks to contain threats instantly.
- **Threat Hunting** – Search across historical and live data for IOCs.

Architecture :

Cynet 360's SOC-oriented architecture typically includes:

- **Endpoint Agents**
  - Installed on Windows, macOS, Linux devices.
  - Collect process, file, network, and user activity telemetry.
- **Network Sensors**
  - Monitor network traffic to detect suspicious flows, C2 activity, and lateral movement.
- **Central Correlation Engine (Cloud)**
  - AI/ML-based analytics merge endpoint, network, and identity data.
  - Applies detection rules and behavioral models.
- **Deception Layer**
  - Decoy files, accounts, and servers placed strategically to lure attackers.
- **Cynet Management Console**
  - Web-based SOC dashboard for detection, investigation, and orchestration.
- **CyOps MDR Team (Optional)**
  - 24/7 SOC experts monitoring and responding to threats.

Workflow :

Step 1 – Data Collection

- Endpoint agents and network sensors gather telemetry.
- User activity logs (logins, privilege changes) are collected.

Step 2 – Data Correlation & Analysis

- AI/ML models analyze combined endpoint, network, and user behavior data.
- Deception triggers (fake files, credentials) detect active attacks early.

Step 3 – Threat Detection

- Alerts are generated and grouped into a single incident view.
- SOC receives the context: affected assets, timeline, and attack path.

Step 4 – Triage

- L1 SOC analysts review severity, scope, and potential impact.
- Escalated to L2/L3 if further investigation is needed.

Step 5 – Investigation

- Analysts use the incident timeline to trace the root cause.
- MITRE ATT&CK mapping helps identify attacker TTPs.

Step 6 – Response

- Automated playbooks can:
  - Isolate endpoints
  - Block malicious IPs/domains
  - Disable compromised accounts
  - Remove malicious files

Step 7 – Continuous Monitoring & Threat Hunting

- SOC hunters use search queries to find hidden threats across historical telemetry.

Step 8 – Feedback & Improvement

- Detected IOCs and TTPs are added to detection rules for future prevention.

6 . Sophos

Purpose in SOC

Sophos Intercept X with XDR (Extended Detection and Response) is a **unified endpoint and network security solution** that helps SOC teams detect, investigate, and respond to threats across **endpoints, servers, email, and firewalls**.

In a SOC environment, its main purposes are:

- **Prevent** attacks with deep learning AI-based malware detection and exploit prevention.
- **Detect** threats across multiple security layers (endpoint, firewall, email).
- **Investigate** incidents quickly with root cause analysis.
- **Respond** automatically or manually to contain and remediate threats.
- **Integrate** with SIEM/SOAR for centralized SOC operations.

Key Features :

- **Deep Learning AI** – Identifies both known and unknown malware without relying solely on signatures.
- **Exploit Prevention** – Blocks techniques attackers use to exploit vulnerabilities.
- **EDR/XDR Capabilities** – Correlates data from endpoints, firewalls, and email gateways for wider visibility.
- **CryptoGuard Ransomware Protection** – Detects and stops ransomware encryption in real time.
- **Root Cause Analysis (RCA)** – Visual maps of attack chains for easier SOC investigations.

Advantages :

- **Layered Security** – Combines endpoint, firewall, email, and cloud protection in one ecosystem.
- **Fewer False Positives** – AI and behavioral analysis reduce noise for SOC analysts.
- **Rapid Deployment** – Cloud-managed with lightweight agents.
- **Seamless Integration** – Works with Sophos Central for unified management and with SIEM/SOAR tools.
- **Ransomware Rollback** – Restores encrypted files and halts active ransomware processes.

Usage :

- **Endpoint Threat Prevention** – Block malware, ransomware, and zero-day attacks.
- **Incident Investigation** – Use RCA visualizations to find the origin and spread of an attack.
- **Threat Hunting** – Query historical and live data for suspicious indicators.
- **Automated Response** – Isolate hosts, block IPs, and remove malicious files instantly.
- **Cross-Product Correlation** – Link endpoint events with firewall and email gateway alerts for complete attack context.

Architecture :

Sophos architecture in a SOC typically includes:

- **Endpoint & Server Agents**
  - Installed on Windows, macOS, Linux, and server workloads.
  - Capture telemetry: process activity, file changes, and network connections.
- **Sophos Central (Cloud Management Console)**
  - Cloud-hosted dashboard for policy management, detection alerts, and incident response.
  - Manages all Sophos products (endpoint, firewall, email, cloud).
- **Sophos Data Lake**

    - Stores telemetry data for XDR queries and historical investigation.
- **Detection & Analytics Engine**
    - Uses deep learning, exploit prevention, and behavioral analysis for detection.
- **SOC Integration Layer**
    - Sends alerts to SIEM/SOAR platforms for correlation with other SOC tools.

Workflow :

Step 1 – Data Collection

- Endpoint and server agents capture live telemetry.
- Firewall and email gateway logs are also sent to Sophos Central.

Step 2 – Threat Detection

- AI and exploit prevention modules detect malicious activity.
- Behavioral analysis identifies abnormal patterns.

Step 3 – Alert Correlation

- XDR correlates endpoint, firewall, and email alerts into a single incident.

Step 4 – SOC Triage

- L1 analysts review alerts in Sophos Central or via SIEM integration.
- Escalated to L2/L3 if deeper investigation is needed.

Step 5 – Investigation

- RCA visualizations show the attack's entry point, techniques used, and impacted assets.
- Analysts check for related indicators in the Sophos Data Lake.

Step 6 – Response

- SOC can isolate hosts, block malicious IPs, disable user accounts, or restore encrypted files.

Step 7 – Threat Hunting

- Analysts run custom XDR queries to find hidden threats across the environment.

Step 8 – Continuous Improvement

- New IOCs and patterns are fed into Sophos detection rules for better prevention.

7 . Carbon Black :

Purpose :

VMware Carbon Black is an **Endpoint Detection and Response (EDR) and Next-Generation Antivirus (NGAV)** platform designed to **detect, prevent, and respond to advanced cyber threats**.

In a SOC, it is primarily used to:

- **Continuously monitor** endpoint activity for malicious behavior.
- **Detect and analyze** suspicious events using behavioral heuristics.
- **Respond quickly** to contain and remediate attacks.
- **Enable proactive threat hunting** for hidden or dormant threats.
- **Integrate with SIEM/SOAR** platforms for centralized SOC operations.

Key Features :

- **Streaming Prevention & Detection** – Real-time behavioral analysis to detect threats as they occur.
- **Next-Generation Antivirus (NGAV)** – Blocks both signature-based and fileless malware.
- **EDR Telemetry** – Collects and stores endpoint activity for deep forensic analysis.
- **Threat Hunting Tools** – Advanced query capabilities for proactive investigations.
- **Cloud-Based Management** – Centralized management console for policy, alerts, and response.

Advantages :

- **Real-Time Visibility** – Continuous endpoint telemetry gives SOC full situational awareness.
- **Strong Behavioral Detection** – Identifies unknown and fileless attacks missed by signature-based AV.
- **Cloud-Native Scalability** – Supports large enterprise environments without heavy on-prem infrastructure.
- **Integration Friendly** – Works with SIEM, SOAR, and threat intelligence platforms.
- **Proactive Threat Hunting** – Allows analysts to search historical data for hidden compromise indicators.

Usage :

- **Threat Detection** – Identify malware, ransomware, and suspicious process activity.
- **Incident Response** – Isolate endpoints, kill malicious processes, and remove infected files.
- **Forensics & RCA** – Investigate attacks in detail using historical endpoint data.
- **Threat Hunting** – Proactively search for attacker activity across all endpoints.
- **Compliance & Reporting** – Provide audit trails and compliance evidence.

Architecture :

a. Endpoint Sensors

Installed on endpoints and servers (Windows, macOS, Linux).

Continuously collect telemetry (processes, registry changes, file writes, network activity).

b. Carbon Black Cloud

Cloud-based analytics platform for processing, storing, and analyzing telemetry.

Runs detection logic using AI, heuristics, and threat intelligence.

c. Management Console

Web interface for SOC teams to view alerts, run queries, manage policies, and initiate responses.

d. SOC Integration Layer

APIs and connectors for SIEM/SOAR tools to receive Carbon Black alerts and enrich investigations.

Workflow :

Step 1 – Data Collection

- Endpoint sensors stream real-time telemetry to Carbon Black Cloud.

Step 2 – Threat Detection

- AI and behavioral analysis detect malicious processes, fileless activity, or exploitation attempts.

Step 3 – Alert Generation

- Alerts are generated and prioritized in the Carbon Black console or sent to the SIEM.

Step 4 – SOC Triage

- L1 analysts verify alerts, check IOCs, and escalate confirmed incidents.

Step 5 – Investigation

- Analysts use the EDR data to reconstruct attack timelines and find root causes.

Step 6 – Response

- SOC can remotely isolate endpoints, terminate processes, or remove files.

Step 7 – Threat Hunting

- Analysts proactively query all endpoints for related attacker activity.

Step 8 – Continuous Feedback

- Detection logic and hunting queries are refined based on incident learnings.

8 . Microsoft Defender :

Purpose :

Microsoft Defender for Endpoint (MDE) is an **enterprise-grade Endpoint Detection and Response (EDR) and Endpoint Protection Platform (EPP)** from Microsoft.
In a SOC environment, its primary purpose is to:

- **Detect and prevent** known, unknown, and fileless threats.
- **Provide real-time endpoint visibility** for threat hunting and investigation.
- **Enable rapid incident response** via remote isolation and remediation.
- **Leverage Microsoft Threat Intelligence** for proactive protection.
- **Integrate deeply with SIEM/SOAR** for centralized monitoring and automation.

Key Features :

1. **Next-Generation Antivirus (NGAV)** – Machine learning and cloud-based protection against malware and ransomware.
2. **Endpoint Detection and Response (EDR)** – Advanced detection, investigation, and response capabilities.
3. **Attack Surface Reduction (ASR)** – Policies to block exploits, script-based attacks, and malicious macros.
4. **Threat & Vulnerability Management (TVM)** – Real-time endpoint risk assessment and remediation guidance.
5. **Automated Investigation & Remediation (AIR)** – AI-driven threat response to reduce SOC workload.

Advantages :

- **Native Microsoft 365 Integration** – Works seamlessly with Azure Sentinel, Microsoft 365 Defender, and Intune.
- **Strong Cloud AI Detection** – Leverages Microsoft's global telemetry for highly accurate threat detection.
- **Centralized Management** – Single console for monitoring, policy management, and incident handling.
- **Automated Threat Response** – Reduces SOC analyst workload by auto-remediating common threats.
- **Cross-Platform Support** – Works on Windows, macOS, Linux, Android, and iOS.

Usage :

- **Threat Detection** – Identify suspicious processes, scripts, and malicious files.
- **Incident Response** – Isolate endpoints, kill processes, and run remediation scripts remotely.

- **Threat Hunting** – Use advanced hunting queries in Kusto Query Language (KQL) for proactive detection.
- **Vulnerability Management** – Identify and prioritize patching of vulnerable software.
- **Integration with SIEM** – Forward alerts and telemetry to Azure Sentinel or other SIEM tools.

Architecture :

a. Endpoint Sensors

- Defender agents run on endpoints, monitoring files, processes, registry, and network connections.

b. Microsoft Defender Security Graph (Cloud)

- Processes telemetry from millions of devices globally, applying AI/ML models for detection.

c. Management & Investigation Console

- Web-based interface for SOC teams to view alerts, run hunting queries, and trigger responses.

d. Integration Layer

- APIs and connectors for SIEM/SOAR integration (especially Azure Sentinel).

Workflow :

Step 1 – Data Collection

- Endpoint sensors send telemetry to Microsoft Defender Cloud in real time.

Step 2 – Threat Detection

- AI, behavior analytics, and threat intelligence detect malicious activity.

Step 3 – Alert Generation

- Alerts are prioritized and correlated into incidents within the Defender console.

Step 4 – SOC Triage

- Analysts validate alerts, check IoCs, and escalate confirmed incidents.

Step 5 – Investigation

- Analysts reconstruct the attack timeline, review affected assets, and assess lateral movement.

Step 6 – Response

- Remotely isolate endpoints, block hashes/URLs, and remove malicious artifacts.

Step 7 – Automated Remediation

- AIR executes predefined playbooks to resolve common threats without human intervention.

Step 8 – Threat Hunting

- SOC uses KQL-based queries to proactively search for undetected threats.

Step 9 – Feedback Loop

- Updated detection rules and threat intelligence are applied for stronger future prevention.

9 . Bitdefender

Purpose :

Bitdefender GravityZone is an **Endpoint Detection and Response (EDR) + Endpoint Protection Platform (EPP)** designed for enterprises.
In a SOC, its purpose is to:

- **Detect, prevent, and respond** to known and unknown threats across endpoints, servers, and cloud workloads.
- Provide **real-time telemetry and threat intelligence** for SOC investigation.
- Reduce SOC analyst workload with **automated remediation and risk-based prioritization**.
- Integrate with **SIEM/SOAR platforms** for centralized security operations.
- Protect **hybrid and multi-cloud environments** alongside on-premise assets.

Key Features :

1. **Machine Learning Threat Detection** – AI-driven behavioral and signature-based analysis for malware and zero-day attacks.
2. **Integrated EDR & EPP** – Combines advanced detection with prevention in a single agent.
3. **Network Attack Defense** – Detects and blocks brute-force, ARP spoofing, and exploit attempts.
4. **Risk Analytics** – Continuous endpoint risk assessment with security posture recommendations.
5. **Sandbox Analyzer** – Suspicious files are detonated in an isolated cloud sandbox for deeper inspection.

Advantages :

- **Unified Agent** – Single lightweight agent for antivirus, EDR, and patch management reduces complexity.

- **Strong Behavioral Detection** – Effective against fileless and script-based attacks.
- **Automated Remediation** – Automatically kills malicious processes, quarantines files, and rolls back changes.
- **Granular Policy Control** – Allows per-group and per-endpoint security policy tuning.
- **Cross-Environment Coverage** – Works across Windows, macOS, Linux, virtualized, and cloud workloads.

Usage :

- **Threat Hunting** – Analysts search for IoCs using Bitdefender's cloud console and endpoint telemetry.
- **Incident Response** – Isolate compromised endpoints remotely and execute remediation scripts.
- **Vulnerability Management** – Identify and patch missing security updates.
- **Integration with SIEM** – Export logs and alerts to Splunk, QRadar, Azure Sentinel, etc.
- **Forensic Investigation** – Analyze attack chains, processes, and network connections involved in incidents.

Architecture :

a. Endpoint Agent

- Installed on workstations, servers, and virtual machines.
- Monitors processes, network traffic, file changes, and memory behavior.

b. GravityZone Control Center (On-Prem or Cloud)

- Centralized web-based management for policies, monitoring, and incident response.

c. Cloud Sandbox

- Executes suspicious files in a controlled environment to detect advanced malware.

d. Threat Intelligence Network

- Feeds from global telemetry and research labs for updated threat detection rules.

e. SIEM/SOAR Connectors

- APIs and connectors to send data to SOC monitoring systems.

Workflow :

Step 1 – Endpoint Monitoring

- The agent continuously monitors processes, file changes, scripts, and network events.

Step 2 – Threat Detection

- AI/ML models and behavioral analysis detect anomalies.

- Unknown files are sent to the cloud sandbox.

Step 3 – Alert Correlation

- Alerts are aggregated in the GravityZone Control Center, often enriched with IoC details.

Step 4 – SOC Triage

- Analysts validate alerts, check threat severity, and identify compromised assets.

Step 5 – Containment & Response

- Endpoints can be isolated; malicious processes are terminated; files quarantined.

Step 6 – Automated Remediation

- The system can roll back registry and file system changes made by malware.

Step 7 – Threat Hunting

- SOC analysts run advanced queries to search for similar IoCs across the environment.

Step 8 – Reporting & SIEM Integration

- Incident details are exported to SIEM/SOAR for compliance, reporting, and automation.

10 . Broadcom's Symantec Endpoint Security Complete (SES-C)

Purpose :

Symantec Endpoint Security Complete (SES-C), now part of Broadcom's enterprise security suite, serves as a **comprehensive EDR/EPP/XDR** solution. In a SOC environment, its key purposes are to:

- **Prevent, detect, and respond** to sophisticated threats (including living-off-the-land, fileless, and zero-day attacks).
- **Predict and disrupt malicious activity proactively** before it fully unfolds using AI-powered capabilities.
- **Reduce SOC burden** by delivering rich context and automated mitigation, helping analysts focus on highest priorities.
- **Provide layered endpoint defenses**, combining signature, behavior, and machine-learning powered detection.

Key Features :

- **Incident Prediction** – AI-driven forecasting of attacker's next steps based on over 500,000 real-world attack chains, enabling pre-emptive disruption.

- **Adaptive Protection** – ML-powered, environment-aware endpoint hardening that auto-configures detection/prevention without impacting productivity.
- **Machine Learning & Behavior-based Detection** – Comprehensive detection of malware, fileless attacks, and suspicious behaviors.
- **Unified Endpoint Protection Suite** – Integrates NGAV, EDR, threat hunting, application control, and mobile threat defense under a single agent.
- **Cloud-based or On-Prem Management** – Flexible deployment options with central visibility and controls for SOC teams.

Advantages :

- **Predictive Defense** – Incident Prediction shifts response from reactive to proactive, disrupting threats before escalation.
- **Reduced Alert Fatigue** – Adaptive Protection customizes policies to reduce false positives and unnecessary SOC triage.
- **Comprehensive Coverage** – SES-C combines endpoint, mobile, and application control—eliminating the need for multiple agents and consoles.
- **Rapid Deployment & Management** – Single agent upgrade from prior Symantec products simplifies rollout and minimizes disruption.
- **Context-Rich Analytics** – AI models infused with threat hunter intelligence enable SOC analysts to make faster, better decisions.

Usage :

- **Pre-emptive Threat Disruption** – Automatically predict and block likely next moves of attackers (e.g., LOLT attacks), preventing escalation.
- **Unified Alert & Investigation Platform** – SOC analysts receive alerts with rich context and can perform investigations within a single console.
- **Threat Hunting** – SOC teams can hunt for threats using behavior-based rules and threat intel, with deep visibility into endpoint activity.
- **Endpoint Hardening** – Automatically tune protection based on each environment's baseline to proactively reduce attack surface.
- **Flexible Integration** – Send alerts, logs, and telemetry into broader SOC workflows and SIEM systems via cloud or on-prem deployment.

Architecture :

- **Single Agent Deployment**
  - One agent delivers NGAV, EDR, mobile defense, app control, and threat hunting across endpoints.
- **AI-Powered Detection Engines**
  - Adaptive Protection and Incident Prediction run AI/ML models, trained on extensive threat intelligence and attack-chain data.
- **Central Management Console**
  - SES-C console (cloud-managed or on-prem) offers visibility, alerting, investigation, and response orchestration.
- **Threat Intelligence Backbone**

    - Leverages Symantec's global intelligence for predictive modeling and contextual detection.
- **SOC Integration Layer**
    - Supports integration with SIEM and SOAR tools to embed within existing SOC workflows.

Workflow :

- **Deployment & Configuration**
    - SOC deploys SES-C agent across endpoints or upgrades from existing Symantec deployments. Adaptive Protection learns and configures policies.
- **Monitoring & Detection**
    - Agent monitors endpoint activity; AI models detect anomalies and predict attacker moves before execution.
- **Alert & Incident Creation**
    - Alerts appear in console with rich attack-chain context; predictions trigger pre-emptive mitigation.
- **SOC Triage & Investigation**
    - Analysts review alerts, investigate using contextual timelines and AI insights, optionally using natural-language summaries (powered by LLM) integrated via Broadcom–Google Cloud partnership.
- **Automated Response**
    - System auto-applies mitigation (e.g., blocking, rolling back, quarantining) based on threat prediction, with minimal business disruption.
- **Threat Hunting & Feedback Loop**
    - SOC hunters search for related behavior patterns; findings feed back to AI models, improving detection precision over time.

11 . Cisco Secure Endpoint

Purpose :

Cisco Secure Endpoint is an advanced endpoint security solution designed to **detect, prevent, and respond** to cyber threats in real-time. It combines antivirus, EDR (Endpoint Detection and Response), threat hunting, and machine learning to protect endpoints against malware, ransomware, fileless attacks, and zero-day exploits. In a SOC, it is used to **monitor, analyze, and respond to endpoint-based threats** as part of the organization's security monitoring framework.

Key Features :

- **Advanced Malware Protection (AMP)** – Uses behavior-based detection and file reputation to stop known and unknown threats.
- **Endpoint Detection and Response (EDR)** – Continuous endpoint activity monitoring with threat investigation and remediation capabilities.

- **File Trajectory & Retrospection** – Tracks file movement across the network and detects if a previously clean file turns malicious later.
- **Threat Intelligence Integration** – Leverages Cisco Talos threat intelligence for up-to-date global threat data.
- **Cloud-Delivered Management** – Centralized cloud console for unified endpoint management and policy enforcement.

Advantages :

- **Proactive Threat Detection** – Uses AI/ML to catch threats before they execute.
- **Retrospective Analysis** – Can detect past compromises when a threat is newly discovered.
- **Seamless Integration** – Works well with Cisco SecureX, firewalls, and network security solutions.
- **Low Performance Impact** – Lightweight agent minimizes system slowdown.
- **Scalable Architecture** – Supports large enterprise environments with thousands of endpoints.

Usage :

- **Incident Detection & Alerting** – SOC analysts get real-time alerts on malicious activities.
- **Threat Investigation** – Analysts use EDR features to investigate suspicious processes, network connections, and file behavior.
- **Incident Response** – Analysts can isolate compromised endpoints remotely to stop lateral movement.
- **Forensic Analysis** – Review historical endpoint activities to identify attack vectors and root causes.
- **Threat Hunting** – Proactively search for indicators of compromise (IOCs) across endpoints.

Architecture :

Cisco Secure Endpoint's architecture typically consists of:

- **Endpoint Agent** – Installed on Windows, macOS, Linux, or mobile devices to monitor activities and enforce policies.
- **Cloud Console (AMP Console)** – Web-based dashboard for policy management, threat investigation, and reporting.
- **Threat Intelligence (Cisco Talos)** – Global database of threat signatures, behavior patterns, and malware analysis.
- **Integration Layer (Cisco SecureX)** – Links with other Cisco security tools and third-party solutions for unified threat response.
- **Retrospective Analysis Engine** – Allows re-evaluation of historical endpoint activity against new threat intel.

Workflow :

Step 1: Endpoint Monitoring

- The endpoint agent continuously monitors file execution, process creation, and network traffic.

Step 2: Threat Detection

- Behavioral analysis, file reputation checks, and AI/ML models detect malicious activity.

Step 3: Alert Generation

- Alerts are sent to the SOC dashboard with threat details, affected hosts, and recommended actions.

Step 4: Incident Investigation

- SOC analysts use file trajectory, process trees, and forensic data to understand the attack scope.

Step 5: Containment & Response

- Compromised endpoints are quarantined or isolated remotely via the console.

Step 6: Remediation & Recovery

- Malware is removed, vulnerabilities patched, and normal operations restored.

Step 7: Threat Intelligence Sharing

- New threat indicators are sent to Cisco Talos and shared across the network for prevention.

12 . Trend Micro

Purpose :

Trend Micro Apex One (and its extended XDR platform Vision One) is designed to **protect endpoints, email, cloud workloads, and networks** against malware, ransomware, phishing, and advanced persistent threats (APTs).
In a **Security Operations Center (SOC)**, it acts as a **central threat detection and response platform**, combining antivirus, endpoint detection and response (EDR), cross-layer detection, and threat intelligence to help analysts detect, investigate, and remediate attacks quickly.

Key Features :

- **Cross-Layer Detection & Response (XDR)** – Correlates data from endpoints, email, servers, and cloud workloads for unified threat detection.
- **Behavior Monitoring & Machine Learning** – Detects unknown malware by analyzing suspicious behavior, not just signatures.

- **Web Reputation Services (WRS)** – Blocks access to malicious domains based on Trend Micro's global threat intelligence network.
- **Automatic Endpoint Isolation** – Instantly isolates compromised machines to prevent lateral spread of threats.
- **Vulnerability Protection** – Virtual patching for unpatched software vulnerabilities to block exploitation.

Advantages :

- **Proactive Threat Prevention** – Uses AI/ML and global threat intelligence to detect threats before they execute.
- **Integrated XDR Capabilities** – Offers deeper correlation across multiple attack vectors.
- **Low System Impact** – Optimized agent with minimal performance degradation.
- **Global Threat Intelligence** – Powered by Trend Micro Smart Protection Network for up-to-date data.
- **Cloud, On-Premise, and Hybrid Deployment** – Flexible architecture for different enterprise needs.

Usage :

- **Threat Monitoring** – Real-time alerting for malware, ransomware, and suspicious behaviors.
- **Incident Investigation** – SOC analysts can pivot from endpoint logs to email and server activity for attack tracing.
- **Proactive Threat Hunting** – Search for Indicators of Compromise (IOCs) across multiple data sources.
- **Incident Response** – Remote isolation, malware cleanup, and vulnerability patching.
- **Reporting & Compliance** – Generate reports for security audits and compliance checks (PCI DSS, HIPAA, etc.).

Architecture :

Trend Micro Apex One / Vision One typically consists of:

- **Endpoint Agent** – Installed on Windows, macOS, and Linux devices to enforce security policies.
- **Management Server / Cloud Console** – Centralized control panel for policy deployment, alert monitoring, and investigations.
- **Trend Micro Smart Protection Network** – Cloud-based threat intelligence with real-time updates on global threat activity.
- **XDR Analytics Platform** – Correlates logs from multiple vectors (email, endpoints, servers, cloud) to identify complex attacks.
- **Integration APIs** – Allows SOC teams to integrate with SIEM, SOAR, and ticketing tools.

Workflow :

Step 1: Endpoint & Network Monitoring

- The Apex One agent and network sensors continuously monitor file execution, email attachments, URLs, and processes.

Step 2: Threat Detection

- AI/ML models, behavioral monitoring, and reputation analysis detect suspicious or malicious activities.

Step 3: Alert & Log Generation

- The system sends alerts to the SOC dashboard, along with correlated data from XDR sources.

Step 4: Investigation

- Analysts trace attack paths, pivot between logs, and check indicators of compromise.

Step 5: Containment

- Compromised endpoints are isolated remotely. Malicious files or URLs are blocked.

Step 6: Remediation

- Malware removal, vulnerability patching, and system recovery are performed.

Step 7: Threat Intel Update

- New indicators are fed back to Trend Micro's threat network for global protection.

13 . McAfee MVISION EDR

Purpose :

McAfee MVISION EDR is designed to **detect, investigate, and respond to advanced endpoint threats in real time**.
In a **Security Operations Center (SOC)**, it helps analysts **uncover stealthy attacks, investigate suspicious behavior, and respond to incidents faster** by leveraging machine learning, behavioral analytics, and cloud-based threat intelligence.

Key Features :

- **Automated Threat Detection** – Uses AI-driven analytics to identify suspicious patterns on endpoints.
- **Real-Time Endpoint Visibility** – Monitors all processes, file changes, registry edits, and network connections.
- **Guided Investigations** – Provides SOC analysts with contextual data and step-by-step investigation workflows.

- **Threat Intelligence Integration** – Leverages McAfee Global Threat Intelligence (GTI) for updated Indicators of Compromise (IoCs).
- **Cloud-Native Architecture** – Centralized management via the MVISION platform for global security visibility.

Advantages :

- **Rapid Incident Response** – SOC teams can isolate, quarantine, or remediate endpoints in seconds.
- **Reduced Analyst Fatigue** – Guided investigations help prioritize critical alerts and reduce noise.
- **Proactive Threat Hunting** – Built-in hunting tools enable analysts to search for hidden threats.
- **Scalable Cloud Platform** – Easy to deploy across thousands of endpoints without heavy infrastructure.
- **Integration with McAfee & Third-Party Tools** – Works with SIEM, SOAR, and other SOC security products.

Usage :

- **Endpoint Threat Detection** – Identifying malware, ransomware, and fileless attacks.
- **Incident Investigation** – SOC analysts can replay the attack chain to find root causes.
- **Threat Containment** – Isolating infected endpoints to prevent lateral movement.
- **Proactive Threat Hunting** – Searching across endpoints for suspicious behaviors or IoCs.
- **Compliance Reporting** – Generating audit-ready reports for regulatory compliance.

Architecture :

Core Components:

- **MVISION EDR Cloud Console** – Centralized dashboard for monitoring, investigation, and response.
- **Endpoint Agents** – Installed on Windows, macOS, or Linux devices to collect telemetry and enforce policies.
- **McAfee Global Threat Intelligence (GTI)** – Provides up-to-date threat data and IoCs.
- **Data Lake** – Stores historical endpoint activity for forensic analysis.
- **Integration Layer** – Connects to SIEM/SOAR platforms like Splunk, IBM QRadar, or Azure Sentinel.

Workflow :

Step 1: Data Collection

- Endpoint agents continuously record process executions, file changes, registry edits, and network connections.

Step 2: Analysis & Detection

- Data is sent to the MVISION EDR cloud for machine learning and behavioral analysis to detect anomalies.

Step 3: Alert Generation

- Threats are prioritized based on risk score and displayed in the SOC console.

Step 4: Investigation

- Analysts use guided investigation tools to review attack chains, timelines, and related IoCs.

Step 5: Response & Containment

- Compromised endpoints can be remotely isolated, processes killed, or files quarantined.

Step 6: Threat Hunting

- SOC teams run IoC searches across all endpoints to ensure no further compromise.

Step 7: Reporting & Continuous Improvement

- Generate detailed post-incident reports and feed learnings into the threat intelligence database.

14 . ESET Enterprise inspector

Purpose :

ESET Enterprise Inspector is designed to **detect, investigate, and respond to advanced endpoint threats** in real time.
In a **Security Operations Center (SOC)**, it helps security teams **gain deep visibility into endpoint activity, identify suspicious behaviors, hunt for threats, and perform forensic analysis**, all while integrating with ESET's endpoint protection platform for a layered defense.

Key Features :

- **Real-Time Endpoint Monitoring** – Continuous telemetry collection from endpoints for live threat detection.
- **Custom Detection Rules** – Analysts can define organization-specific detection logic and alerts.
- **Incident Investigation Tools** – Attack timeline view, file/process analysis, and relationship mapping.
- **Threat Hunting Capabilities** – Query endpoints for IoCs, suspicious processes, or unusual behaviors.
- **Integration with ESET Security Products** – Works seamlessly with ESET Endpoint Security and Threat Intelligence.

Advantages :

- **Deep Endpoint Visibility** – Tracks processes, scripts, network activity, and registry changes in detail.
- **Low System Impact** – Lightweight agents reduce endpoint performance overhead.
- **Customizable Detection Logic** – SOC teams can tune rules to match specific business risks.
- **Efficient Response Actions** – Quarantine files, kill processes, or isolate devices instantly.
- **Integration-Friendly** – Supports APIs for integration with SIEM, SOAR, and threat intel platforms.

Usage :

- **Advanced Threat Detection** – Identifying fileless malware, ransomware, and insider threats.
- **Incident Forensics** – Reconstructing attack chains to understand root causes.
- **Threat Hunting** – Proactively searching for indicators of compromise across endpoints.
- **Incident Containment** – Rapidly isolating compromised devices from the network.
- **Security Policy Enforcement** – Monitoring compliance with organizational security standards.

Architecture :

Core Components:

- **ESET Enterprise Inspector Server** – Centralized system that collects and processes endpoint data.
- **Endpoint Agents** – Installed on endpoints (Windows/macOS) to monitor activity and enforce security policies.
- **Database Storage** – Stores collected telemetry and investigation data for historical analysis.
- **Management Console** – Web-based interface for SOC analysts to view alerts, investigations, and reports.
- **Integration Layer** – APIs and connectors for SIEM, SOAR, and other SOC tools.

Workflow :

Step 1: Data Collection

- Endpoint agents gather telemetry on processes, files, network traffic, scripts, and registry activity.

Step 2: Detection & Alerting

- Rules and behavior analytics flag suspicious events; alerts appear in the EEI console.

Step 3: Triage & Investigation

- Analysts review alerts, analyze timelines, and investigate related processes and IoCs.

Step 4: Response Actions

- Analysts can isolate endpoints, quarantine files, kill malicious processes, or block network connections.

Step 5: Threat Hunting

- Proactive searches are run for suspicious patterns or known IoCs across all monitored endpoints.

Step 6: Reporting & Knowledge Sharing

- SOC generates incident reports, feeds findings into detection rules, and improves future response times.

15 . Kaspersky EDR Optimum

Purpose :

Kaspersky EDR Optimum is built to **detect, analyze, and respond to endpoint threats** that bypass traditional antivirus.
In a **Security Operations Center (SOC)**, it helps analysts **monitor endpoint activity, investigate incidents, hunt for threats, and take immediate containment actions** while maintaining centralized control and visibility over the security posture.

Key Features :

- **Centralized Threat Visibility** – Unified console to monitor endpoint security events across the organization.
- **Advanced Threat Detection** – Uses behavioral analysis, machine learning, and threat intelligence to detect sophisticated attacks.
- **Automated Response Actions** – Quarantine files, isolate endpoints, and terminate malicious processes instantly.
- **Integrated Threat Intelligence** – Real-time global threat feeds to enhance detection accuracy.
- **Incident Visualization** – Graph-based attack chain mapping for faster root cause analysis.

Advantages :

- **Low Complexity** – Easy to deploy and operate compared to full enterprise-grade EDR tools.
- **Strong Threat Intelligence** – Backed by Kaspersky's global research and malware database.
- **Fast Incident Response** – Reduces Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
- **Scalability** – Supports medium and large environments without heavy resource demands.

- **Regulatory Compliance** – Helps meet security audit and compliance requirements (GDPR, ISO 27001, etc.).

Usage :

- **Detecting Advanced Malware** – Including fileless attacks and zero-day exploits.
- **Investigating Security Incidents** – Using attack timeline visualization and root cause tracing.
- **Threat Hunting** – Searching across endpoints for IoCs and suspicious patterns.
- **Automated Incident Containment** – Isolating infected systems before the threat spreads.
- **Integration with SIEM/SOAR** – Feeding alerts into larger SOC monitoring ecosystems.

Architecture :

Core Components:

- **Kaspersky Security Center (KSC)** – Centralized management and monitoring console for SOC teams.
- **EDR Agent** – Installed on each endpoint to collect telemetry and enforce security actions.
- **EDR Server** – Processes collected data, correlates events, and generates alerts.
- **Threat Intelligence Cloud** – Provides updated global threat indicators and detection rules.
- **Integration Layer** – APIs and connectors to share data with SIEM, SOAR, and other SOC tools.

Workflow :

Step 1: Data Collection

- Endpoint agents continuously collect process, file, registry, and network telemetry.

Step 2: Threat Detection

- Behavioral analysis, ML models, and IoC matching flag suspicious activities.

Step 3: Alerting & Visualization

- SOC analysts receive alerts in the Kaspersky Security Center with an attack chain diagram.

Step 4: Investigation

- Analysts examine processes, files, and network connections to identify the attack's origin and scope.

Step 5: Response Actions

- Analysts can isolate endpoints, quarantine files, or kill malicious processes remotely.

Step 6: Threat Hunting & Optimization

- Proactively searching for similar attack patterns, refining rules, and updating response strategies.

16 . Blackberry CylancePROTECT + CylanceOPTICS

Purpose :

BlackBerry's CylancePROTECT + CylanceOPTICS are designed to work together to **prevent, detect, investigate, and respond to endpoint threats**.
In a **Security Operations Center (SOC)**, they help reduce **false positives**, detect **zero-day attacks**, and **automate investigation and response** using **AI-driven threat prevention** and **endpoint detection and response (EDR)**.

- **CylancePROTECT** → AI-powered prevention of malware, fileless attacks, and exploits.
- **CylanceOPTICS** → EDR module for incident investigation, threat hunting, and automated responses.

Key Features :

CylancePROTECT

1. **AI-based Malware Prevention** – Predictive AI models to block threats before execution.
2. **Memory Exploit Protection** – Stops buffer overflows and memory-based attacks.
3. **Script Control** – Detects malicious PowerShell, macros, and scripts.
4. **Device Control** – Manages USB and peripheral usage policies.
5. **Offline Protection** – AI detection works without internet connectivity.

CylanceOPTICS

1. **Automated Incident Response** – Custom playbooks to respond instantly to detections.
2. **Threat Hunting** – Search across endpoints for Indicators of Compromise (IoCs).
3. **Behavioral Threat Detection** – Detects suspicious patterns in real-time.
4. **Root Cause Analysis** – Timeline view of how an attack unfolded.
5. **Cloud and On-Prem Integration** – Works with SIEM, SOAR, and threat intelligence platforms.

Advantages :

- **Prevention-First Approach** – Stops threats before they execute, reducing incident volume.
- **Lightweight Agent** – Low CPU/RAM usage compared to traditional AV.
- **AI Without Signatures** – No need for daily signature updates.
- **Integrated EDR + AV** – Single solution for prevention and response.
- **Fast Deployment** – Cloud-managed and quick to roll out in enterprise environments.

Usage :

- **Proactive Threat Blocking** – Using CylancePROTECT to prevent ransomware, malware, and phishing payloads.
- **Incident Investigation** – Using CylanceOPTICS to trace and analyze attacks.
- **Threat Hunting** – Searching for suspicious behaviors or IoCs across all endpoints.
- **Automated Remediation** – Executing isolation, kill process, and file quarantine instantly.
- **SOC-SIEM Integration** – Feeding Cylance alerts into Splunk, QRadar, or other SOC dashboards.

Architecture :

Core Components:

- **Endpoint Agent** – Lightweight AI-driven prevention & EDR module.
- **Cylance Cloud Console** – Centralized SOC dashboard for alerts, threat intel, and policy control.
- **Threat Intelligence Engine** – AI models trained on billions of malware samples.
- **Integration Layer** – APIs to connect with SIEM/SOAR platforms.
- **On-Prem/Hybrid Support** – Flexible deployment for compliance needs.

Architecture Layers:

1. **Prevention Layer** → CylancePROTECT blocks threats before execution.
2. **Detection & Monitoring Layer** → CylanceOPTICS captures activity logs & alerts SOC analysts.
3. **Investigation Layer** → Analysts use timeline-based RCA and IoC searches.
4. **Response Layer** → Automated or manual remediation actions.

Workflow :

Step 1: Prevention

- CylancePROTECT's AI engine blocks malicious files, scripts, and exploits instantly.

Step 2: Data Collection

- CylanceOPTICS continuously records endpoint telemetry (processes, file changes, network activity).

Step 3: Detection

- Behavioral analysis and AI models detect suspicious activities missed by prevention.

Step 4: Alerting & Investigation

- Alerts sent to the SOC console (and SIEM) with detailed attack chain mapping.

Step 5: Response

- SOC team isolates endpoint, kills malicious processes, quarantines files, or rolls back changes.

Step 6: Threat Hunting & Forensics

- Analysts perform IoC searches across all endpoints, export forensic data for deeper analysis.

17 . RSA Netwitness Endpoint

Purpose :

RSA NetWitness Endpoint is designed to **detect, investigate, and respond to endpoint threats** faster than traditional antivirus or EDR solutions.
Unlike signature-based AV, it **monitors all endpoint activity continuously**, enabling the SOC to uncover stealthy attacks, insider threats, and zero-day malware that evade prevention tools.

In SOC operations, it:

- Provides **complete visibility** into endpoint behavior.
- Correlates endpoint data with **network and log intelligence**.
- Enables **fast triage** and **threat hunting**.

Key Features :

- **Continuous Endpoint Monitoring** – Records process, file, registry, and memory activity in real-time.
- **Behavioral Detection Engine** – Detects malicious activity patterns, not just known malware.
- **Threat Intelligence Integration** – Matches observed behaviors with global threat intel feeds.
- **Automated Triage & Scoring** – Assigns risk scores to suspicious endpoints for SOC prioritization.
- **Full Endpoint Forensics** – Provides a timeline of attack progression for detailed investigation.

Advantages :

- **Detects Stealthy Threats** – Finds fileless malware, memory exploits, and insider abuse.
- **Deep Visibility** – Captures data at a granular level for accurate investigation.
- **Integrated with RSA NetWitness Platform** – Combines endpoint, network, and SIEM data for richer context.
- **Faster Mean Time to Detect (MTTD)** – AI scoring and triage reduce detection delays.
- **Scalable** – Supports large enterprise environments with thousands of endpoints.

Usage :

- **Threat Hunting** – Search endpoint history for IoCs and suspicious patterns.
- **Incident Investigation** – Trace the exact sequence of attacker actions.
- **Response Actions** – Isolate infected endpoints, kill malicious processes, remove persistence mechanisms.
- **Root Cause Analysis** – Map out how the attack entered and spread.
- **Threat Correlation** – Combine endpoint alerts with network and log data for complete attack context.

Architecture :

Core Components:

- **Endpoint Agent** – Lightweight sensor installed on endpoints to collect activity telemetry.
- **RSA NetWitness Endpoint Server** – Centralized data aggregation and analysis engine.
- **NetWitness Platform Integration** – Shares endpoint data with RSA SIEM and network monitoring modules.
- **Threat Intelligence Feeds** – Enrich endpoint data with global attack indicators.
- **SOC Console (Investigation UI)** – For search, analysis, triage, and response.

Architecture Layers:

1. **Data Collection Layer** → Endpoint agents capture process, file, registry, memory activity.
2. **Analysis Layer** → Behavioral analytics and machine learning score suspicious activities.
3. **Correlation Layer** → Endpoint data is combined with network and log events in the NetWitness platform.
4. **Response Layer** → SOC analysts execute automated or manual containment actions.

Workflow :

Step 1: Endpoint Data Collection

- Agents capture every process execution, file change, registry edit, and network connection.

Step 2: Detection

- Behavioral rules and threat intel identify suspicious or malicious activity.

Step 3: Alerting

- Alerts with risk scores are sent to the SOC dashboard for prioritization.

Step 4: Investigation

- Analysts drill into endpoint timelines, process trees, and file hashes to confirm the threat.

Step 5: Response

- Endpoint is isolated, malicious files are removed, persistence entries are deleted.

Step 6: Post-Incident Analysis

- Data is archived for compliance, forensic review, and playbook improvements.

18 . Symantec Endpoint Detection and Response

Purpose :

Symantec EDR is built to **detect, investigate, and remediate endpoint threats** that bypass traditional prevention measures.
It focuses on **real-time monitoring, behavioral analytics, and threat hunting** to help Security Operations Centers (SOCs) identify and respond to advanced persistent threats (APTs), fileless malware, ransomware, and insider abuse.

In SOC operations, it's used to:

- Monitor **all endpoint activities** in real-time.
- Detect **sophisticated threats** using AI-driven analytics.
- Support **proactive threat hunting** and **incident response** workflows.

Key Features :

- **Advanced Threat Detection** – Identifies malicious activities using behavioral analysis, machine learning, and global threat intelligence.
- **Automated Incident Response** – Allows isolation of compromised endpoints, process termination, and threat removal without manual intervention.
- **Threat Hunting Console** – Enables SOC analysts to query historical endpoint activity for Indicators of Compromise (IoCs).
- **Integration with Symantec Global Intelligence Network (GIN)** – Leverages one of the largest global threat intelligence databases.
- **Attack Visualization & Timeline** – Presents a clear map of attack progression for quicker investigation.

Advantages :

- **Comprehensive Visibility** – Tracks processes, registry changes, file activity, and network connections at the endpoint level.
- **Reduced Detection Time** – AI-assisted triage helps SOCs respond faster to threats.
- **Seamless Integration** – Works with Symantec Endpoint Protection (SEP) for prevention + detection synergy.
- **Scalable Architecture** – Suitable for organizations from mid-size to large-scale enterprises.
- **Global Threat Intelligence** – Constantly updated with new IoCs from Symantec's worldwide network.

Usage :

- **Incident Detection** – Identify abnormal behavior patterns on endpoints.
- **Threat Hunting** – Search for hidden malware, command-and-control communications, and fileless threats.
- **Forensic Analysis** – Examine process trees, memory snapshots, and event histories.
- **Automated Response Actions** – Isolate infected devices and remove malicious files.
- **Post-Breach Analysis** – Determine attack vectors, lateral movement, and persistence mechanisms.

Architecture :

Core Components:

- **Endpoint Sensor** – Lightweight agent installed on each endpoint to collect and send telemetry.
- **EDR Management Server** – Central analysis engine that processes and stores endpoint data.
- **Threat Intelligence Feed (Symantec GIN)** – Provides updated IoCs and threat patterns.
- **SOC Console / Investigation UI** – Used by analysts to investigate and respond to threats.
- **Integration Layer** – Connects with SIEMs, SOAR platforms, and other SOC tools for correlation.

Architecture Layers:

- **Collection Layer** – Endpoint sensors capture events (process, registry, file, network activity).
- **Analytics Layer** – Machine learning and rule-based detection analyze behaviors.
- **Threat Intelligence Layer** – Matches behaviors against global IoCs.
- **Response Layer** – Executes remediation actions and isolation commands.

Workflow :

Step 1: Data Collection

- Endpoint agents continuously record system events and send them to the EDR server.

Step 2: Detection

- AI & behavioral analytics flag anomalies, suspicious processes, or policy violations.

Step 3: Alerting & Prioritization

- High-risk events are escalated to SOC analysts with context and severity scores.

Step 4: Investigation

- Analysts examine attack chains, process relationships, and historical endpoint activity.

Step 5: Containment & Response

- Infected endpoints are isolated; malicious files/processes are terminated.

Step 6: Post-Incident Reporting

- Root cause is documented, IoCs are added to threat intelligence, and playbooks are updated.

19 . F-Secure Elements EDR / WithSecure Elements EDR

Purpose :

WithSecure Elements EDR consolidates **primary endpoint prevention with advanced detection and response** capabilities. Designed for SOCs, its core purpose is to:

- **Detect sophisticated threats** and breaches quickly using behavioral insights.
- **Provide deep contextual visibility** across user and device activity for accurate triage.
- **Enable rapid, automated response** actions or elevate complex cases to expert analysts.
- **Support proactive threat hunting and containment**—all from a unified, cloud-native platform.

Key Features :

1. **Broad Context Detection (BCD)**
   Aggregates endpoint and identity events into contextual detection stories with risk scoring to simplify SOC analyst workflows.
2. **Event Search & Threat Hunting**
   Built-in advanced filtering enables SOC teams to query raw endpoint telemetry and hunt for indicators of compromise (IOCs).
3. **Automated Response & Outbreak Control**
   Automates remediation actions like host isolation, malware rollbacks, and elevated protections during attacks.
4. **Elevate to WithSecure (Expert Assistance)**
   SOC can escalate complex incidents to WithSecure's expert threat hunters for deeper analysis and guidance.
5. **Memory Capture for Fileless Attacks**
   Captures in-memory processes, enabling detection of fileless threats often invisible to traditional AV.

Advantages :

- **Fast Detection with Minimal Noise**
  Combines behavior, reputation, and big-data analysis to reduce false positives and accelerate breach discovery.
- **Unified Cloud-Native Platform**
  Accessible via a browser-based console—no on-prem infrastructure required—simplifying SOC operations.
- **Extended SOC Capability with Expert Support**
  Built-in "Elevate" service brings expert threat hunter assistance for difficult cases and

escalations.

- **Integrated Prevention & Response**
  Combines EPP + EDR seamlessly, backed by proactive patch and device control management.
- **Rapid Response Automation**
  Automates containment and remediation workflows, reducing Mean Time To Response (MTTR) even when SOC staff are offline.

Usage :

- **Incident Detection and Triage**
  SOC analysts identify breaches and suspicious behaviors through broad context detections and dashboards.
- **Threat Hunting and Investigation**
  Analysts use Event Search to dive into endpoint logs and IoCs for proactive threat detection.
- **Automated or Manual Host Containment**
  SOC can isolate a host or apply response actions automatically when high-risk detections occur.
- **Incident Escalation to Experts**
  When SOC runs into complex threat scenarios, they can elevate the case directly to WithSecure threat experts.
- **Fileless and Memory-Based Attack Handling**
  Memory capture enables SOC to detect and investigate stealthy attacks that bypass disk-based defenses.

Architecture :

- **Elements Agent (EDR-enabled)**
  Lightweight cloud-delivered endpoint sensor capturing process, file, registry, and memory telemetry.
- **Elements Security Center (Cloud Console)**
  Centralized browser-based management portal for detection, investigation, response, and health overview.
- **Broad Context Detection Logic**
  Cloud-based AI/ML engine that correlates endpoint and identity signals into actionable detections.
- **Automation Engine & Outbreak Control**
  Executes automatic containment flows (e.g. isolation or lockdown) based on detection severity.
- **Elevate Escalation Pathway**
  Direct connection for SOC to escalate to WithSecure's expert incident responders and threat hunters.

Workflow :

1. **Agent Deployment and Monitoring**
   Elements Agent is deployed across endpoints; continuous telemetry feeds to the cloud

console.

2. **Detection via Broad Context**
   The cloud engine analyzes behaviors and aggregates suspicious events into a detection story (BCD).
3. **Alerting & Automated Actions**
   Detections appear in the Security Center; automated response actions can trigger based on risk thresholds.
4. **Threat Investigation**
   Analysts explore the detection story, use Event Search for deeper root cause analysis, and view memory captures if needed.
5. **Containment & Remediation**
   Analysts execute manual or automated containment like host isolation or threat removal.
6. **Escalation if Needed**
   Complex cases can be elevated to WithSecure's expert analysts for further guidance.
7. **Post-Incident Review & Improvements**
   Incident insights feed into detection tuning, response playbooks, and broader threat intelligence.

20 . Malwarebytes EDR

Purpose :

Malwarebytes Endpoint Detection and Response (EDR) is designed to **detect, isolate, and remediate** advanced threats such as ransomware, fileless malware, and zero-day attacks on endpoints. It goes beyond traditional antivirus by providing **post-infection remediation, behavioral monitoring, and rollback capabilities** to restore systems to their pre-infection state.

In a **SOC environment**, Malwarebytes EDR serves as:

- A **real-time threat detection** tool for endpoints.
- An **incident response** platform with automated remediation.
- A **forensics source** for endpoint behavior analysis.

Key Features :

- **Ransomware Rollback** – Restores encrypted files and system changes to pre-attack state.
- **Cloud-Based Threat Detection** – Uses AI and threat intelligence for real-time detection.
- **Suspicious Activity Monitoring** – Tracks unusual behavior to catch fileless and zero-day attacks.
- **Endpoint Isolation** – Disconnects infected systems from the network without losing admin control.
- **Threat Hunting Dashboard** – Allows SOC teams to proactively investigate suspicious activity.

Advantages :

- **Minimal System Impact** – Lightweight agent with low resource usage.
- **Fast Incident Response** – Automated remediation reduces SOC workload.
- **Cross-Platform Support** – Works on Windows, macOS, and some Linux endpoints.
- **Strong Post-Breach Recovery** – Rollback and deep remediation ensure complete cleanup.
- **Integrates with SIEM/SOAR** – Fits into larger SOC ecosystems for unified visibility.

Usage :

- **Continuous Endpoint Monitoring** – SOC analysts use it to track endpoint activities 24/7.
- **Incident Investigation** – Provides endpoint forensics data for root cause analysis.
- **Threat Containment** – Quarantines or isolates endpoints to prevent lateral movement.
- **Automated Remediation** – Reduces manual cleanup efforts for analysts.
- **Threat Hunting** – Enables proactive searches for Indicators of Compromise (IOCs).

Architecture :

High-Level Components:

- **Endpoint Agent** – Installed on client devices for real-time monitoring.
- **Cloud Management Console** – Central dashboard for SOC teams to view alerts and manage policies.
- **Threat Intelligence Cloud** – Malwarebytes' AI-powered detection engine using global telemetry.
- **Forensics & Logging** – Stores event and behavior logs for investigation.
- **Integration Layer** – Connects with SIEM, SOAR, and ticketing systems.

Flow:
Endpoints → Agent collects data → Data sent to Cloud → Threat Analysis (AI + signatures) → SOC Console receives alerts → Analyst actions (isolation, remediation, rollback).

Workflow :

- **Deployment** – Install agents on all monitored endpoints.
- **Data Collection** – Agents continuously send telemetry and threat data to the Malwarebytes cloud.
- **Threat Detection** – AI/behavioral analytics identify malicious activity.
- **Alert Generation** – SOC analysts receive alerts via the management console or integrated SIEM.
- **Incident Response** – Analysts isolate endpoint, perform forensic analysis, and initiate remediation.
- **Rollback (if needed)** – System files and data restored to pre-infection state.
- **Reporting & Documentation** – SOC team logs incident resolution in the IR workflow.

21 . Secureworks Taegis

Purpose :

Secureworks Taegis is a **cloud-native extended detection and response (XDR) platform** designed to **detect, investigate, and respond** to advanced cyber threats across endpoints, networks, and cloud environments.
In a **SOC** context, it acts as a **centralized hub** for security data collection, automated correlation, and incident response, enabling analysts to respond faster and more effectively.

Its primary goals in SOC operations:

- Provide **360° threat visibility** across multiple attack surfaces.
- Reduce **alert fatigue** by correlating events into meaningful incidents.
- Enable **faster investigation and response** through automation and AI-driven analysis.

Key Features :

- **XDR Detection Engine** – Aggregates endpoint, network, and cloud data for advanced threat correlation.
- **Threat Intelligence Integration** – Uses Secureworks Counter Threat Unit (CTU) intel for faster identification of new attack patterns.
- **Automated Response Actions** – Isolate endpoints, block IPs, disable accounts, and stop malicious processes instantly.
- **Collaborative Investigation** – SOC analysts can chat and share context in real-time within the platform.
- **Unified Data Lake** – All security telemetry stored in a central repository for deep investigations.

Advantages :

- **Centralized Security Visibility** – Reduces the need for multiple separate tools in the SOC.
- **Lower Analyst Fatigue** – Correlated alerts cut down noise and false positives.
- **Faster Incident Response** – Automated playbooks execute containment steps instantly.
- **Threat Hunting Ready** – Built-in hunting tools for proactive investigations.
- **Integration Friendly** – Connects with SIEM, SOAR, EDR, and cloud security tools.

Usage :

- **Continuous Threat Monitoring** – SOC uses Taegis as the main detection and response hub.
- **Incident Investigation** – Provides detailed timelines, attack paths, and root cause data.
- **Automated Containment** – SOC triggers instant isolation or blocking to stop an attack.
- **Threat Hunting** – Analysts query historical data to uncover hidden threats.
- **Collaboration** – SOC members communicate and share findings directly in the platform.

Architecture :

Core Components:

- **Data Collectors** – Agents and APIs pull telemetry from endpoints, network devices, and cloud services.

- **Secureworks Data Lake** – Stores raw and processed security data.
- **Detection & Analytics Layer** – AI + machine learning + CTU threat intel.
- **SOC Analyst Console** – Web-based dashboard for investigation, hunting, and response.
- **Integration APIs** – Connect to SIEMs, firewalls, IAM systems, and third-party EDR.

Flow:

1. Data from multiple sources is ingested into Taegis.
2. AI-driven analytics and CTU intel detect suspicious patterns.
3. Alerts are correlated into incidents.
4. SOC analysts investigate via the console.
5. Automated or manual containment actions are triggered.

Workflow :

- **Data Ingestion** – Taegis collects telemetry from endpoints, firewalls, cloud logs, and EDR tools.
- **Detection** – Analytics engine identifies potential threats using AI, rules, and threat intel.
- **Incident Correlation** – Multiple related alerts are grouped into a single incident.
- **Investigation** – SOC analyst reviews attack chain, indicators, and impacted assets.
- **Response** – Execute playbooks (e.g., isolate device, block IP, disable account).
- **Threat Hunting** – Search historical data for IOCs to detect hidden or dormant threats.
- **Reporting** – Incident is documented for compliance and post-mortem analysis.

22 . ReaQta EDR

Purpose :

ReaQta EDR (by IBM) is an **AI-driven endpoint detection and response platform** designed to automatically detect, investigate, and respond to cyber threats without overwhelming SOC teams.
It is widely used in SOC operations for:

- **Continuous endpoint monitoring** to detect suspicious behaviors in real time.
- **AI-based threat detection** to minimize false positives.
- **Automated remediation** to stop attacks before they spread.
- **Memory-level analysis** to catch fileless and stealthy threats.

Key Features :

- **NanoOS Technology** – Runs outside the OS kernel, invisible to attackers, preventing tampering.
- **Behavioral AI Detection** – Identifies threats based on behavior patterns instead of just signatures.
- **Real-Time Response Actions** – Isolate endpoints, kill processes, block IPs instantly.

- **Visual Attack Storyline** – Displays an interactive timeline of an attack for easier investigation.
- **Automated Playbooks** – Predefined remediation workflows to speed up SOC incident response.

Advantages :

- **Stealth Deployment** – NanoOS makes it extremely difficult for attackers to bypass detection.
- **Low False Positive Rate** – AI behavior analysis reduces unnecessary alerts.
- **Fast Incident Containment** – Automation shortens dwell time.
- **Strong Memory Forensics** – Detects advanced threats like in-memory malware.
- **Easy SOC Integration** – Works with SIEM/SOAR platforms for centralized security.

Usage :

- **24/7 Endpoint Monitoring** – Ensures continuous visibility for SOC analysts.
- **Incident Investigation** – Provides deep visibility into process trees and attack chains.
- **Threat Hunting** – Analysts search for indicators of compromise (IOCs) across historical data.
- **Automated Remediation** – SOC triggers predefined playbooks to respond to incidents.
- **Compliance & Reporting** – Generates detailed security reports for audits.

Architecture :

Core Components:

- **ReaQta Agent with NanoOS** – Installed on endpoints for invisible monitoring.
- **AI Detection Engine** – Processes behavioral telemetry in real time.
- **Data Lake** – Stores endpoint activity logs for threat hunting.
- **SOC Analyst Console** – Web-based dashboard for alerts, investigations, and responses.
- **Integration Layer** – APIs to connect with SIEM, SOAR, and threat intel feeds.

Flow:

1. Endpoint agent (NanoOS) captures behavioral events in real time.
2. Data is sent to the ReaQta AI detection engine.
3. Suspicious patterns are flagged and enriched with threat intel.
4. Alerts are sent to the SOC console for review.
5. Automated or manual response actions are executed.

Workflow :

- **Telemetry Collection** – NanoOS agent collects behavioral and memory data without being detected.
- **Detection & Analysis** – AI correlates events to detect known and unknown threats.
- **Incident Creation** – Related alerts are grouped into a single case.
- **SOC Investigation** – Analysts review the attack timeline and affected systems.

- **Response Execution** – Playbooks or manual actions are triggered (isolate endpoint, kill process).
- **Post-Incident Review** – SOC documents findings and implements prevention measures.

23 . FireEye Endpoint Security

Purpose :

FireEye Endpoint Security (formerly FireEye HX) is an **advanced Endpoint Detection and Response (EDR) platform** designed to protect endpoints from **known, unknown, and advanced persistent threats (APTs)**.
In a SOC environment, it's used for:

- **Real-time endpoint threat detection** using signature-based and behavioral analysis.
- **Forensic investigations** on compromised machines.
- **Rapid incident response** to contain breaches.
- **Malware prevention and remediation** without affecting business continuity.

Key Features :

- **Multi-Engine Protection** – Combines signature-based, behavioral, and machine learning detection.
- **Exploit Guard** – Identifies and blocks exploit attempts before they execute.
- **Endpoint Visibility** – Full process and file tracking for threat hunting.
- **Integrated Threat Intelligence** – Enriches alerts with FireEye's Mandiant threat intel data.
- **On-Host Containment** – Isolates compromised endpoints to prevent lateral movement.

Advantages :

- **Advanced Threat Coverage** – Detects both known malware and sophisticated zero-day attacks.
- **Mandiant Integration** – Access to industry-leading incident response expertise and intel.
- **Granular Forensics** – Detailed logs for deep SOC investigations.
- **Low Dwell Time** – Quickly identifies and stops active attacks.
- **Scalable for Large SOCs** – Handles thousands of endpoints efficiently.

Usage :

- **Continuous Endpoint Monitoring** – SOC gets real-time visibility into all endpoint activity.
- **Incident Response** – SOC analysts use isolation and process-kill features to stop attacks.
- **Threat Hunting** – Search for IoCs across historical and live data.
- **Malware Analysis** – Execute suspicious files in a sandbox for safe inspection.
- **Reporting & Compliance** – Generate incident reports for audits and compliance requirements.

Architecture :

Core Components:

- **Endpoint Agent (HX Agent)** – Installed on each endpoint to monitor and block threats.
- **Detection Engines** – Signature-based, behavioral, and ML models for threat detection.
- **Management Console** – Centralized dashboard for SOC teams to investigate and respond.
- **Threat Intelligence Module** – Feeds real-time Mandiant intel to enrich detections.
- **Forensic Storage** – Stores endpoint event data for later analysis.

Architecture Flow:

- Endpoint agent continuously monitors processes, file changes, and memory activity.
- Detection engines analyze events and identify suspicious patterns.
- Alerts are enriched with threat intel before being sent to the SOC console.
- SOC analysts investigate and decide on remediation steps.
- Remediation commands (isolation, process kill) are pushed to endpoints.

Workflow :

- **Telemetry Collection** – HX Agent logs endpoint activity in real time.
- **Detection Phase** – Multi-engine detection (signatures, behavior, ML) scans data.
- **Alert Generation** – Alerts are enriched with Mandiant threat intel.
- **SOC Triage** – Analysts verify the alert's legitimacy and assess impact.
- **Response Actions** – Isolate endpoint, kill malicious processes, or remove malware.
- **Forensic Investigation** – SOC retrieves historical logs and artifacts for analysis.
- **Reporting & Lessons Learned** – Findings are documented for compliance and prevention.

24 . Microsoft Advanced Threat Analysis

Purpose :

Advanced Threat Analytics (ATA) is designed to **detect, investigate, and respond to advanced persistent threats (APTs), insider threats, and compromised credentials** in enterprise networks.

In a **Security Operations Center (SOC)**, it works by **continuously monitoring network traffic and authentication logs**, identifying suspicious patterns such as credential theft, lateral movement, and reconnaissance, and then providing actionable alerts for incident response.

Key Features :

- **Behavioral Analytics** – Learns normal user and entity behavior over time to detect anomalies.
- **Credential Theft Detection** – Identifies Pass-the-Hash, Pass-the-Ticket, and other credential-based attacks.
- **Suspicious Activity Timeline** – Provides a clear investigation timeline for SOC analysts.

- **Integration with Active Directory** – Monitors and analyzes all domain authentication events.
- **Real-Time Alerts** – Sends prioritized alerts for rapid SOC response.

Advantages :

- **Proactive Threat Detection** – Identifies threats before they cause significant damage.
- **Reduces False Positives** – Behavioral profiling minimizes irrelevant alerts.
- **Fast Deployment** – Integrates easily with existing Active Directory and network monitoring infrastructure.
- **Clear Forensics** – Timeline-based investigation makes SOC response faster and more accurate.
- **Insider Threat Visibility** – Detects unusual activities from legitimate accounts.

Usage :

- **Credential Attack Detection** – Identifying attacks like Golden Ticket or Brute Force against AD accounts.
- **User Behavior Analysis** – Spotting unusual access times, locations, or data usage.
- **Threat Hunting** – Searching for patterns of lateral movement within the network.
- **Incident Investigation** – Using timelines to understand the full scope of an attack.
- **SOC Workflow Automation** – Integrating with SIEM/SOAR platforms for automated incident response.

Architecture :

Components:

- **ATA Center** – The main server that processes and analyzes data, applies detection algorithms, and stores events.
- **ATA Gateway / Lightweight Gateway** – Installed on domain controllers or as standalone sensors to capture and analyze traffic.
- **Active Directory Integration** – Pulls authentication and directory data for analysis.
- **Threat Intelligence Database** – Stores known attack patterns and IoCs.
- **SOC Integration Layer** – Connects with SIEM and incident management systems.

Workflow :

Step 1: Data Collection

- ATA Gateways capture network traffic (Kerberos, DNS, NTLM) and authentication logs from domain controllers.

Step 2: Behavioral Profiling

- Machine learning models create a baseline of normal activity for each user and device.

Step 3: Threat Detection

- Deviations from the baseline (e.g., a user logging in from a new country or accessing unusual servers) trigger alerts.

Step 4: Alert Prioritization

- ATA assigns severity levels and sends alerts to the SOC dashboard or SIEM.

Step 5: Investigation

- SOC analysts review the suspicious activity timeline, correlate events, and identify root cause.

Step 6: Response & Containment

- Malicious accounts are disabled, compromised endpoints are isolated, and attack vectors are blocked.

Step 7: Feedback & Learning

- Detected indicators are fed into threat intelligence to improve detection accuracy.