DOI: 10.2478/ias-2026-0004 • JIAS • 21(2) • 2026 • 52–88

Review

An Overview of EDR Serviceability for Security Information and Event Management (SIEM)

Padma Lochan Pradhan

Dept of Computer Engineering, MIT Academy of Engineering, Alandi, Pune, PIN-412105, India;
padma.pradhan@mitaoe.ac.in

Abstract: This review paper focuses on and addresses Endpoint Detection and Response (EDR) tools, providing an overview of their purpose, functions, operations, services, and benefits within the cybersecurity landscape. Specifically, EDR solutions are designed to detect, prevent, investigate, and respond to advanced cyber threats that often bypass traditional antivirus programs. To achieve this, these tools continuously collect and analyze data in real time using behavioral analytics, artificial intelligence (AI), and machine learning (ML). This enables the identification of anomalous activities and sophisticated attack patterns, such as zero-day exploits and fileless malware. Furthermore, the integration of open-source tools strengthens an organization's security posture by enhancing service capabilities, scalability, reliability, and availability. The paper also discusses the evolution of EDR from standalone tools to integrated, interoperable, automated, and intelligence-driven platforms that utilize behavioral and predictive analysis to counter increasingly sophisticated threats. Such integration, in turn, enables faster decision-making while reducing code complexity, operational costs, and response times. Ultimately, the sustainability of open-source tools contributes to higher quality, improved performance, effective cost management, better decision-making, and reduced risk. In summary, this review synthesizes key developments and innovations in the EDR-SIEM domain, drawing from academic research, industry analysis, and real-world applications.

Keywords: Security Information and Event Management, Extended Detection and Response, Antivirus, Machine Learning, Open-Source, Integration, Cybersecurity, Incident, Zero Trust Architecture. Threat Intelligence. Log Analysis, Open Cybersecurity Schema Framework (OCSF).

1. Introduction

Endpoint Detection and Response is an advanced security solution that continuously monitors endpoint activity to proactively detect, investigate, and respond to cyber threats that bypass traditional defences. By deploying lightweight agents, the EDR [1] system collects comprehensive remote data on process execution, network connections, and file activities from devices like EPP devices [2]. It enables automated and manual response actions, such as isolating compromised endpoints and terminating malicious processes, to rapidly contain and neutralize threats. The tool also provides deep forensic insights, allowing security teams to perform root-cause analysis and improve their security posture. Through its powerful combination of non-stop monitoring, advanced analytics, and automated response, EDR-SIEM significantly enhances an organization's ability to protect against modern cyberattacks and streamline incident response processes [3].

EDR-SIEM serviceability refers to the operational aspects and practical challenges of deploying, integrating, and maintaining advanced security [4] solutions. While powerful together, their integration involves managing data, tuning systems, and combating alert fatigue, which significantly impacts the efficiency [5] of security teams. Serviceability that requires upfront [6] planning and ongoing maintenance to configure connectors, normalize log data, and validate that all relevant endpoint telemetry is flowing into the SIEM [7]. Serviceability involves a resilient process of fine-tuning correlation rules, establishing baselines for normal behaviour, and enriching alerts with contextual data to help [8] prioritize and weed out low-priority notifications.

Open-source tools for EDR-SIEM offer distinct serviceability benefits, primarily centered on cost savings, transparency, and customization. However, they also introduce unique operational challenges that require internal expertise and dedicated resources for management, support, and maintenance in a continuous process [9].

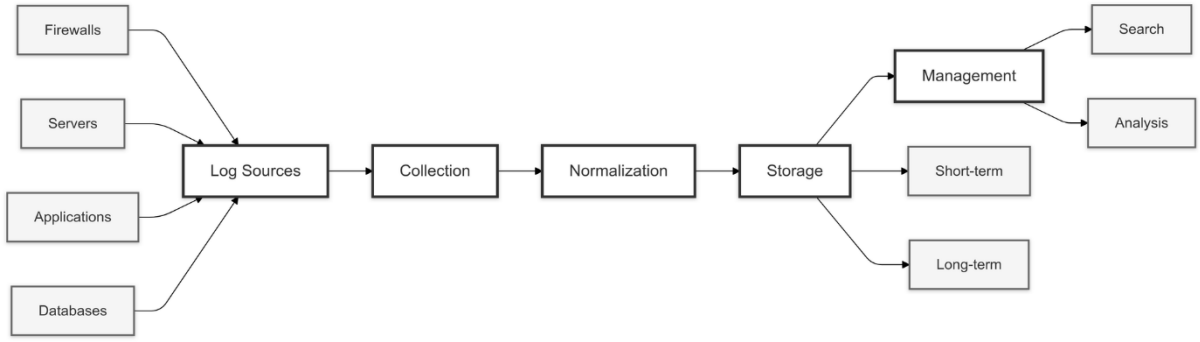
EDR-to-SIEM data ingestion is crucial for providing a holistic view of an organization's security posture by combining granular endpoint telemetry with broader network and cloud data. This integration enables better correlation, advanced threat hunting, and compliance reporting [10].

Methods of Data Ingestion: Data is typically transferred from the EDR platform to the SIEM using the following methods [11]:

a) Syslog (System Logging Protocol): EDR solutions can be configured to push logs [12] and alerts to the SIEM server using standard network protocols like TCP or UDP . (Ref to API Integration).
b) Log File Transfer: In some cases, EDR agents may write log data [13] to local files that the SIEM or an intermediary agent then retrieves and forwards for central analysis.

Log Normalization is the process of transforming raw, unstructured log data from various sources into a standardized, consistent format or schema [14]. This critical step in log management, particularly within Security Information and Event Management (SIEM) and EDR systems, makes data easier to analyse, correlate, and manage for security operations [15].

Implementing effective event correlation in EDR-to-SIEM environments is challenging due to the inherent complexities of modern IT systems and the nature of cyber threats. Key challenges include managing massive data volumes, ensuring data consistency, and balancing detection accuracy [16]. Analysis and Correlation: The normalized EDR data is correlated with other log sources (Figure. 1) (firewalls, identity providers, cloud logs) to detect complex, multi-stage attacks that might otherwise be missed [17].



Input/Domain Output/Range

Figure 1. Integrated Data Collection and Analysis

1.1 EDR Serviceability

With complex, distributed IT environments and sophisticated threats, EDR-SIEM serviceability is an evolving and critical function. It moves beyond simple deployment to include [18]:

1) Managing diverse endpoints: Many organizations now have a mix of on-premises, mobile, and cloud-based endpoints, all of which must be properly serviced and protected.
2) Integrating advanced analytics: These solutions leverage AI and machine learning, and serviceability ensures these tools are properly tuned to balance accuracy with false positives [19].
3) Leveraging managed services: Many organizations use managed detection and response (MDR) services from third-party experts to handle the complexities of this serviceability and monitoring.

Key Serviceability Challenges

While beneficial, open-source solutions shift the burden of operational maintenance and support internally, creating specific serviceability challenges:

a. Requires In-House Expertise: The greatest challenge is the need for highly skilled in-house personnel (DevOps, security engineers, data analysts). The team is responsible for deployment, configuration, integration, and maintenance. If expertise is lacking, operational costs can exceed those of commercial solutions.
b. Support Model (Community vs. Vendor): Support is primarily community-driven. While often helpful, community support lacks Service Level Agreements (SLAs) or guaranteed response times. Critical issues might require the team to debug the actual source code, a task beyond many IT departments' capabilities.

c. Maintenance and Updates: Organizations must manage the entire lifecycle, including monitoring for new vulnerabilities in the tools themselves, patching, testing updates for compatibility with existing integrations, and performing upgrades. This requires a structured maintenance schedule.
d. Scalability Management: As data volumes grow, managing the scalability of open-source SIEMs like Elasticsearch or OpenSearch requires significant expertise in distributed systems and performance tuning to prevent data loss or analysis bottlenecks [20].
e. Lack of Unified UI/UX: Often, open-source solutions are modular (e.g., using Osquery for data collection and the Elastic Stack for analysis). Analysts may need to navigate multiple interfaces and dashboards, which can slow down incident response times compared to unified commercial platforms [21].
f. Documentation Gaps: Documentation can sometimes be inconsistent, outdated, or less comprehensive than commercial offerings, making initial setup and training for new analysts challenging.

In summary, the serviceability of open-source tools offers high levels of control and cost savings, but demands a strong internal commitment to resources, expertise, and ongoing operational management [22].

Endpoint Protection Platform (EPP): Endpoint security is the practice of protecting endpoint devices, such as desktops, laptops, smartphones, and servers, from cyber threats. As more employees work remotely and use personal devices for work (Bring Your Own Device or BYOD), the traditional network perimeter has dissolved, making endpoint protection a vital part of an organization's cybersecurity strategy [23]. An integrated suite of endpoint protection technologies—such as antivirus, data encryption, and intrusion prevention—that detects and stops a variety of threats at the endpoint (Figure 2).

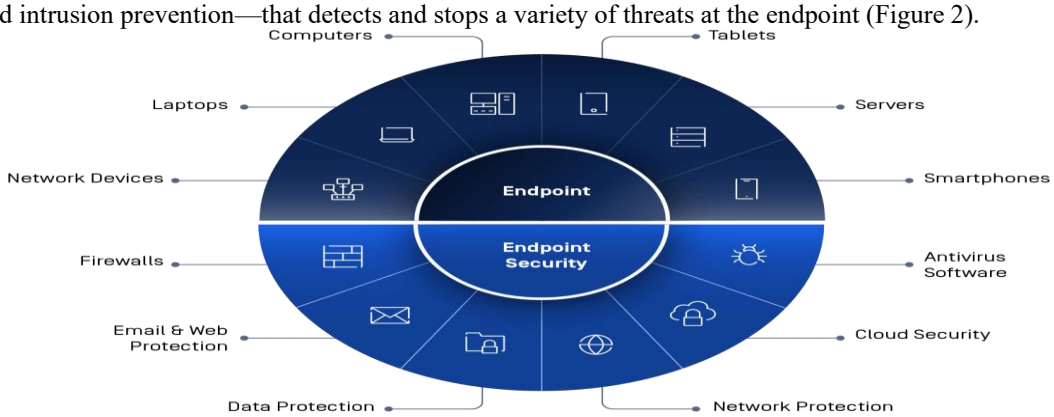


Figure 2. Overview of EPP.

A robust EDR serviceability program is crucial for maximizing the value of an EDR solution and maintaining a strong cybersecurity posture.

Key Aspects of EDR serviceability (Operational management and monitoring)

a. Monitoring: Serviceability involves continuously monitoring the EDR-SIEM solution itself to ensure its agents are active on all endpoints and are reporting data correctly [24].
b. System health checks: This includes regular checks of the system's components, such as its cloud-based console or on-premises servers, to ensure they are available and performing as expected.
c. Performance optimization: The solution should operate efficiently without significantly impacting endpoint performance. Serviceability ensures agents are lightweight and do not cause system slowdowns [25].
d. Resource management: Administrators can use serviceability tools to modify deployment settings, such as adjusting resources for specific components, to match the needs of their environment [26].

1.1.1. Key Components

Purpose: The purpose of an Endpoint Detection and Response solution is to protect an organization from advanced cyber threats by uninterrupted monitoring of endpoint devices for suspicious activity, providing deep investigative capabilities, and automating responses to contain and eliminate threats. It goes beyond traditional antivirus software by assuming that prevention can sometimes fail and focusing on the detection and remediation of threats that have successfully breached a network's defences [27].

Detecting and Stopping Advanced Threats

a. Catch what traditional security misses: Unlike traditional antivirus (AV) that relies on a signature database of known malware, EDR uses behavioral analysis and machine learning to find unusual activity that may indicate a new, unknown (zero-day) threat [28].
b. Thwart sophisticated attacks: It is designed to detect advanced persistent threats (APTs), fileless attacks that operate in a computer's memory, and social engineering attacks that bypass perimeter defences.
c. Fight ransomware effectively: This solution can identify ransomware behaviour early on, enabling automatic isolation of the affected endpoint and preventing the attack from spreading and encrypting an organization's critical data [29].
d. Automate responses: Upon detection, EDR can automatically take actions based on predefined rules, such as isolating a compromised device from the network or terminating a malicious process. This reduces an attacker's "dwell time" in the network and minimizes potential damage.
e. Speed up investigations: By keeping a forensic record of endpoint activities, EDR allows security analysts to trace the root cause of a security incident. This provides a complete attack timeline and helps inform future security strategies.

Mechanism: Endpoint Detection and Response (EDR) operates through a multi-layered mechanism involving advanced analytics, automated responses, and forensic capabilities. Instead of relying on static signature databases like traditional antivirus, it focuses on understanding the behaviours of processes and users to detect more sophisticated, evasive threats [30].

API hooking is a primary mechanism used by EDR (Endpoint Detection and Response) solutions to monitor and detect malicious activity on endpoints. At the same time, SIEM (Security Information and Event Management) platforms ingest the resulting data for broader correlation and analysis. Adversaries actively develop techniques to bypass EDR-SIEM API hooking mechanisms (Figure 3) to evade detection [31].

EDR workflow:

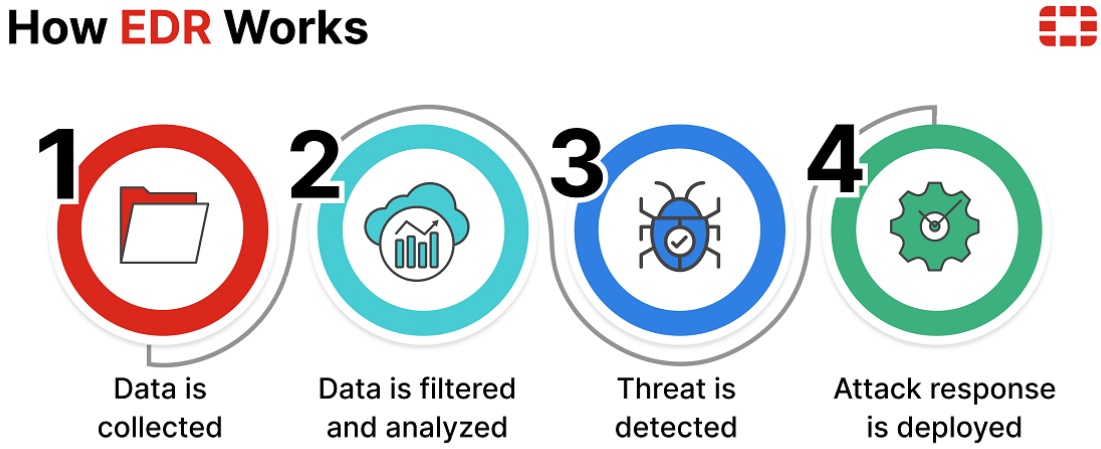


Figure 3. Working Mechanism of EDR

EDR and API Hooking: Open-source tools implement API hooks to gain visibility into system activities and stop threats in real-time (Ref to API Integration (Figure 4).

- ✓ Mechanism: When a program makes a function call (e.g., to create a process or write to memory), the EDR inserts its own code (a "hook") into the system's dynamic linked libraries (DLLs), typically ntdll.dll in user mode. This redirection forces the execution flow to the EDR's code first.
- ✓ Detection and Response: The EDR's code inspects the activity for suspicious behavior (e.g., analyzing the bytes of shellcode being written into memory). If the activity is malicious, the EDR can block it; otherwise, it allows the original function to proceed [32].
- ✓ Focus: EDR specializes in deep, granular, endpoint-level forensics and automated response for specific threats like fileless malware or process injection.

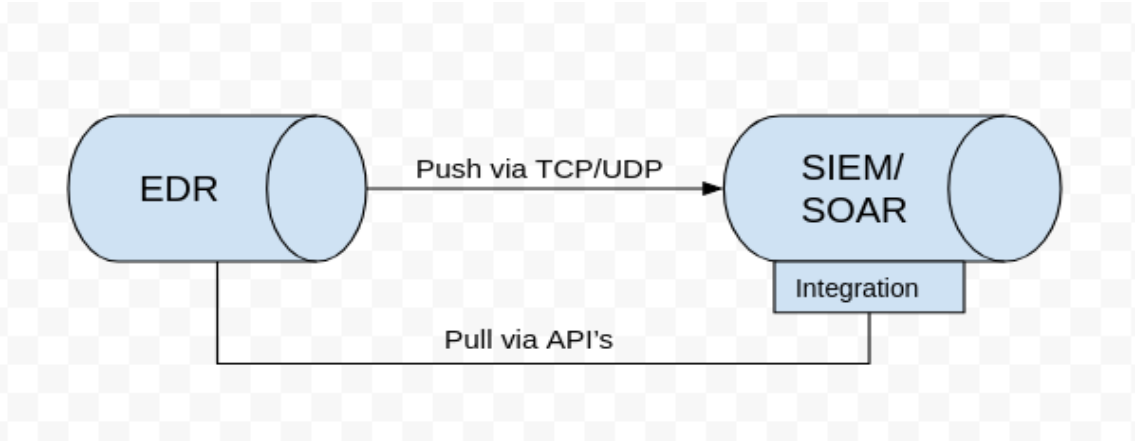


Figure 4. API Integration

1.1.2. SIEM and Data Ingestion

SIEM platforms do not typically use API hooking themselves but act as a central hub for security data from various sources, including EDRs (Figure 5).

a) Mechanism: EDR solutions feed detailed endpoint telemetry (logs and alerts) into the SIEM [33].
b) Correlation & Context: The SIEM correlates this endpoint data with other events across the network (firewall logs, identity provider logs, cloud service APIs, etc.) to provide a holistic view of the organization's security posture (Figures 1, 5, and 6) [33].
c) Focus: SIEM excels at detecting broad anomalies and generating alerts for compliance and large-scale threat hunting, using the EDR data to enrich context and speed up investigations.

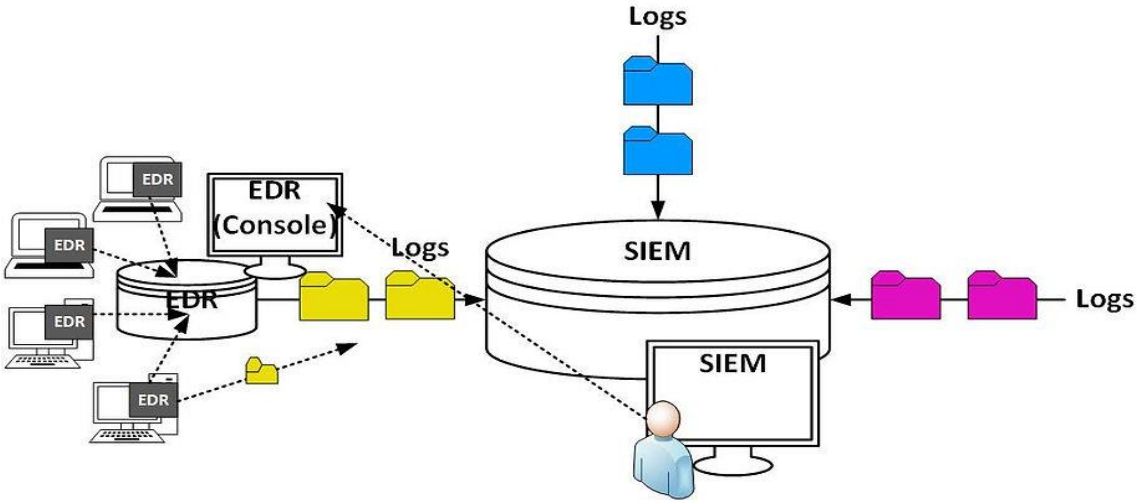


Figure 5. Integrated Log Management

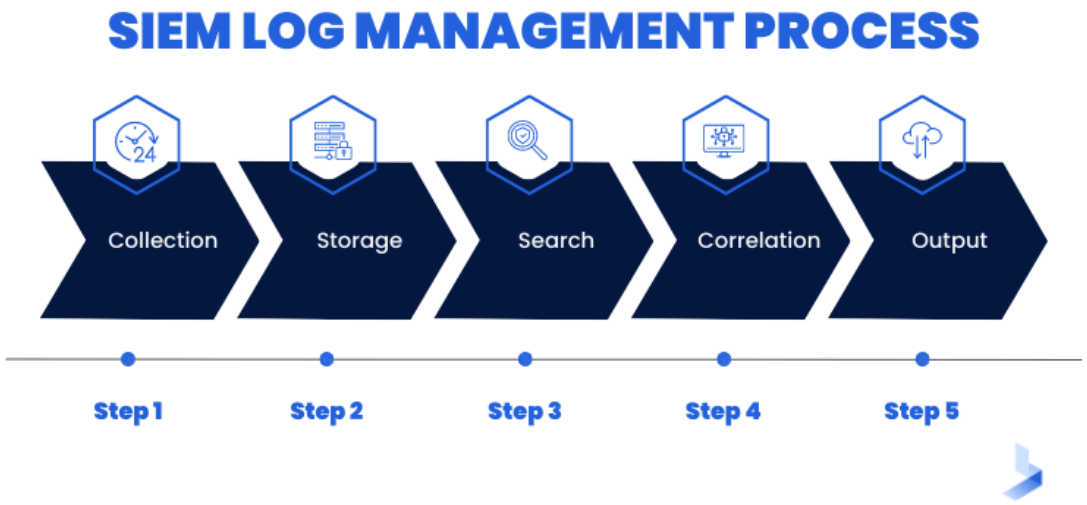


Figure 6. Advanced Log Management

Continuous endpoint monitoring and data collection

A lightweight software agent is deployed on every endpoint—including laptops, desktops, and servers. This agent continuously collects and streams a wide range of telemetry data back to a central cloud or on-premises platform:

a. Process and activity data: Records process creation and termination events, including parent-child relationships and command-line arguments.
b. File and registry data: Monitors file modifications, registry changes, and access timestamps.
c. Network data: Tracks network connections, including DNS requests, connections, and open ports.
d. User data: Logs user authentication events and privilege escalation activities.

Response: Endpoint Detection and Response provides a sophisticated response to threats by round the clock analysing risk patterns, and enabling both automated and manual intervention. This goes far beyond traditional antivirus software (Table 1), which relies on signature-based [34] detection and cannot protect against unknown or "zero-day" exploits.

Table 1. Anti-Viruses Versus EDR. Comparative Service of EDR analysis is different from traditional Antivirus.

Aspect	Traditional Antivirus (AV)	EDR Analysis
Detection Method	Relies primarily on signature-based detection and known malware databases.	Uses behavioural analysis, machine learning, and threat intelligence to detect unknown (zero-day) and fileless threats.
Focus	Prevention of infection.	Assumes a breach is possible and focuses on detection, investigation, and response.
Visibility	Limited to scanning and identifying malicious files on endpoints.	Provides deep, continuous, and real-time visibility into all endpoint activity.
Response	Automatic quarantine or deletion of known malicious files.	Automates containment (e.g., endpoint isolation) and enables manual, precise remediation actions.
Context	Very little context beyond identifying a known malicious file.	Provides rich context, including the full attack timeline, root cause, and attacker TTPs.

2. Background

To understand the integration of EDR-SIEM (Table 2), it helps to first explore their individual backgrounds. The roots of SIEM can be traced back to the early 2000s, emerging from the combination of two separate technologies [35]. Security Information Management (SIM): Focused on the long-term storage, analysis, and reporting of log data. Security Event Management (SEM): Addressed the real-time monitoring, correlation, and alerting of events from various devices and applications. Endpoint Detection and Response (EDR) is a category of security tools designed to provide continuous monitoring and automated response for endpoints (EPP devices). As of 2025, it has evolved into a critical defensive layer against sophisticated attacks that bypass traditional signature-based antivirus [36].

Table 2. EDR Versus SIEM

	EDR	**SIEM**
Area of Focus	The endpoint (e.g., laptops, servers, mobile devices).	The entire IT environment, including networks, cloud services, and applications.
Scope	Provides a deep, granular view of specific endpoint activity.	Offers a broad, aggregated view across the entire infrastructure.
Primary Function	Detects and responds to threats in real-time at the device level, focusing on behaviours.	Aggregates and correlates logs from multiple sources to provide a holistic view of security events.
Key Capability	Incident response and automated containment on the endpoint.	Event correlation across the network for broad threat detection and compliance reporting.

In 2024, **introductory motivation** is understood across different fields as the initial spark or preliminary strategy used to initiate action, engagement, or interest. Whether in a personal, professional, or cybersecurity context, it serves as the "hook" that moves a system or individual from a state of rest to a state of directed activity [37].

In the context of modern security, the introductory motivation for integrating Endpoint Detection and Response with Security Information and Event Management (SIEM) is to eliminate siloed visibility.

- ✓ **The Problem:** EDR provides deep visibility into individual devices but lacks the "macro" network context. SIEM offers broad network-wide visibility but lacks "micro" endpoint-level detail.
- ✓ **The Motivation:** By 2026, organizations are motivated to combine these to achieve **comprehensive cyber resilience**. This integration allows them to link isolated network anomalies (from SIEM) to specific endpoint behaviours (from EDR), drastically reducing the mean time to detect and respond to threats like ransomware.

In 2025, the **technical background** of Endpoint Detection and Response and Security Information and Event Management (SIEM) integration centers on creating a unified, data-rich defense ecosystem that transitions from passive logging to active, automated protection [38].

2.1 Data Telemetry and Normalization

The mechanism begins with data ingestion.

1) **EDR Telemetry:** Lightweight agents installed on endpoints (workstations, servers, mobile) capture deep, real-time activity such as process executions, registry changes, file modifications, and local network connections.
2) **SIEM Log Aggregation:** The SIEM acts as a central repository, ingesting logs from EDR along with data from firewalls, identity providers (IAM), and cloud workloads [39].
3) **Normalization:** To make this diverse data useful, the SIEM normalizes different log formats (e.g., Syslog, JSON, CEF) into a structured format for standardized analysis.

2.2 Multi-Layered Analysis Mechanism

Once the data is centralized, the integrated system applies sophisticated analytics.

a) **Behavioral Baselines:** Modern platforms use AI and machine learning to establish a "normal" baseline for user and system behavior (UEBA). This allows the system to detect "living-off-the-land" attacks that use legitimate tools for malicious purposes [40].
b) **Cross-Domain Correlation:** The SIEM's correlation engine links isolated events from EDR and other sources. For instance, it can correlate a suspicious PowerShell script detected by EDR with a simultaneous unusual cloud login [41] detected by an identity provider, identifying a multi-stage attack.

2.3 Technical Evolution: From Integration to XDR

The 2026 technical landscape is shifting from manual integration to **Extended Detection and Response (XDR)**.

a. **Native Interconnectivity:** While SIEM-EDR integration traditionally required manual "gluing", XDR provides a more "out-of-the-box" experience with deeper, native integration across endpoint, network, and cloud layers.
b. **Reduced Dwell Time:** This technical synergy can reduce attacker dwell time—historically over 200 days—down to hours or minutes through real-time autonomous detection and immediate isolation.

2.4 In a common aspect: Core Technical Components`

Modern EDR solutions typically follow a distributed architecture consisting of three primary layers:

a) Data Collection (Agents): Lightweight software installed on endpoints to log telemetry, including process creation, file modification, registry changes, and network connections.
b) Centralized Data Lake: Telemetry is streamed to a cloud-based or on-premises repository for aggregation and long-term forensic storage.
c) Analytics Engine: Uses AI, machine learning, and behavioural models to correlate millions of events in real time to identify anomalies [42].

2.5 Operational Modes and Privileges

The efficacy of an EDR depends on its interaction with the host operating system:

✓ Kernel Mode (Ring 0): High-privilege access allows the EDR to monitor core system activities like driver loading and direct memory access. While more powerful, errors here can crash the entire system.
✓ User Mode (Ring 3): Standard privilege level where typical applications run. EDR agents often use a hybrid approach, using kernel hooks for visibility and user-mode processes for analytics and UI.

2.6 Detection and Analysis Techniques

a. Behavioral Analytics: Profiles "normal" user and system habits to detect deviations, such as a user suddenly downloading gigabytes of data or a known application [43] executing suspicious code.
b. Indicators of Attack (IOA) vs. Compromise (IOC): Unlike IOCs (which focus on known "bad" files or IPs), IOAs identify the *tactics* of an active attack, such as lateral movement or privilege escalation.
c. Threat Intelligence Integration: Continuously cross-references local telemetry with global databases of known adversary TTPs (Tactics, Techniques, and Procedures).

2.7 Technical Response Capabilities

When a threat is detected, it can be execute several technical remediation actions:

a. Network Containment: Isolating the infected endpoint from the rest of the network while maintaining its connection to the security console for further investigation [44].
b. Process Termination: Instantly "killing" malicious processes or threads identified by the analytics engine.
c. Rollback: Some advanced EDRs (E.g. SentinelOne, Sophos) can automatically restore files encrypted by ransomware to their original state using cached snapshots [45].
d. Forensic Investigation: Providing visual "Storylines" or process trees that show exactly how an attack originated and spread.

Today, SIEM serves as the central command console for a security operations center (SOC), providing a comprehensive, top-down view of an organization's entire IT environment.

EDR technology was developed to address the limitations of traditional, signature-based antivirus software [9]. Traditional antivirus software was effective against known malware but was powerless against new, unknown, or "fileless" attacks that operate in a computer's memory [46].

I.Early 2010s: Attackers began using more advanced methods to bypass perimeter defences, such as

exploiting system protocols or launching fileless attacks. This created a critical security gap, as compromised endpoints could go undetected for months.

II. 2013: Gartner analyst Anton Chuvakin coined the term "Endpoint Threat Detection and Response" to describe emerging tools that provided deeper visibility into endpoint activity. This was shortened to EDR.

III. Key features from inception: EDR was founded on the principles of continuous monitoring, behavioural analysis, and automated response at the endpoint level. This was a shift from a "prevention-first" to a "detection and response" approach [47].

As EDR matured, it began incorporating artificial intelligence and machine learning to improve its ability to identify suspicious behaviours and automate incident response actions like quarantining a compromised device. While both are fundamental to a modern security strategy, they operate at different levels.

3. Literature Survey

A literature survey of Endpoint Detection and Response (EDR) in 2025 reveals a field rapidly transitioning from reactive monitoring to proactive, AI-driven [48] autonomous defense. Recent academic and industry studies focus on three primary themes: the integration of advanced machine learning, the architectural shift toward Extended Detection and Response (XDR), and the operational challenges of managing massive telemetry data. Below are the historical development timelines for both.

3.1 Endpoint Detection and Response

The evolution of EDR marked a shift from reactive, signature-based antivirus to proactive, behavioral monitoring of network "endpoints" (like laptops and servers).

1) Pre-2010 (Precursors): Traditional antivirus (AV) [49] dominated, relying on signatures to identify known threats. As malware became more polymorphic, technologies like Host-based Intrusion Detection Systems (HIDS) and basic behavioral analysis began to emerge.
2) 2011–2012 (Early Innovations): Startups like CrowdStrike launched signatureless, cloud-based modules that focused on "Indicators of Attack" (IoA) rather than just known file hashes.
3) 2013 (Coining the Term): Gartner analyst Anton Chuvakin officially coined the term "Endpoint Threat Detection and Response" to describe tools focused on detecting and investigating suspicious host activities.
4) 2016–2018 (Mainstream Adoption): High-profile ransomware attacks like WannaCry and NotPetya (2017) drove organizations to adopt EDR for real-time monitoring and lateral movement detection.
5) 2019–2022 (Evolution to XDR): EDR expanded into XDR (Extended Detection and Response), integrating data from networks, cloud, and email to provide a more holistic view.
6) 2024–2025 (Modern Era): EDR solutions now heavily utilize AI and Machine Learning to predict attacks. However, "EDR Killers" (malware designed specifically to blind these agents) have also surfaced, leading to a new arms race in kernel-level protection.

3.2. Other EDR Timelines

- ✓ Automotive: Event Data Recorders (vehicle "black boxes") have been regulated since 2004–2006 in the USA. In 2024, they became mandatory for all new cars and vans sold in the EU.
- ✓ Environmental: EDR (Environmental Data Resources), now part of LightBox, has been providing historical aerial photography and due diligence data dating back to the 1930s for property assessments.

XDR (Extended Detection and Response) (Table 3) was developed as a holistic evolution of EDR, moving beyond individual device monitoring to correlate data across networks, cloud, and email [50].

Table 3. Summary Comparison

Feature	EDR (Endpoint Focus)	XDR (Environment Focus)
Data Scope	Endpoint-specific telemetry	Network, Cloud, Email, Identity
Correlation	Single endpoint	Cross-layer/multi-vector
Main Benefit	Device visibility & low cost	Contextual insights & automation
Typical User	SMBs with simpler networks	Enterprises with hybrid IT

3.3. XDR Historical Development Timeline

a) 2018 (The Origin): The term "XDR" was officially coined by Nir Zuk, CTO and co-founder of Palo Alto Networks. It was introduced as a strategy to break down security silos by integrating telemetry from any source (the "X").
b) 2019 (Market Recognition): The concept gained momentum as organizations realized EDR was blind to threats like lateral movement in the network or credential theft in the cloud.
c) 2020 (The Pandemic Surge): The shift to remote work during COVID-19 accelerated adoption. Distributed work environments created visibility gaps that only cross-domain monitoring could fill.
d) 2021 (Validation): Major industry analysts, including Gartner and Forrester, published their first market guides and evaluations specifically for XDR, legitimizing it as a distinct security category.
e) 2022–2023 (Divergence of Approaches): The market split into two distinct paths:
    1) Native XDR: Tightly integrated tools from a single vendor's portfolio (e.g., Palo Alto Cortex, Microsoft Defender) [51].
    2) Open (Hybrid) XDR: Platforms designed to integrate with diverse third-party security tools regardless of the vendor.
f) 2024 (Shift to Automation): XDR began incorporating Generative AI and advanced orchestration to automate "root cause analysis", reducing the investigation time by up to 88% in some environments.
g) 2025 (The Era of AI-Driven Defense): Modern XDR focuses on real-time, autonomous response. Solutions now prioritize "proactive threat hunting" and use AI [52] models to automatically revert ransomware damages or quarantine compromised identities without manual intervention.

4. Research Motivation

The research motivation behind Endpoint Detection and Response (EDR) stems from the failure of traditional cybersecurity to cope with the escalating complexity, evasiveness, and scale of modern [53] cyber threats. Research has sought to move beyond reactive, signature-based defences to develop proactive, behavioral approaches that give security professionals the visibility and tools to detect and respond to threats that have bypassed perimeter defenses.

Advanced research into EDR is driven by the need to stay ahead of increasingly sophisticated cyber threats. The focus is shifting beyond foundational EDR capabilities toward highly predictive, automated, and context-aware security platforms. The primary advanced research motivations include evolving machine learning, moving beyond simple telemetry correlation, combating advanced persistent threats (APTs), and developing comprehensive security orchestration [54].

Traditional EDR uses machine learning for behavioral analysis, but advanced research is focused on pushing these capabilities to new frontiers.

a) **Predictive analytics:** Research explores using machine learning to not only detect current threats but to predict and anticipate potential attack vectors based on historical data and threat actor patterns. This proactive stance aims to address vulnerabilities before they can be exploited.
b) **Reduced false positives:** A persistent challenge in EDR is alert fatigue caused by a high volume of false positives. Research is motivated by creating more accurate and contextual AI models that can better distinguish between benign anomalies and true threats, allowing security teams to focus on critical incidents.

c) **Automated threat hunting:** By leveraging AI, researchers are developing autonomous systems that can proactively search for hidden threats, indicators of compromise (IOCs), and indicators of attack (IOAs) across an environment. These AI-driven tools can analyse vast datasets at a speed and scale beyond human capability [55].

While Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) are highly complementary and essential tools, using one over the other or failing to integrate them properly can present significant problems. The "problematic" of EDR versus SIEM is not a competitive one, but rather a matter of scope, limitations, and resource management [56].

5. Research Gap

Key research gaps in the integration and operation of EDR and SIEM solutions revolve around the lack of standardization, effective automation to counter alert fatigue, and empirical [57] studies on true operational effectiveness.

A key research gap exists in bridging the functional and data silos between Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) systems [58]. While these tools are designed to be complementary, effectively combining their strengths is an ongoing challenge for security teams [59]. Research efforts are needed to address issues related to data correlation, threat context, alert fatigue, and overall interoperability.

Limitation: EDR platforms generate highly detailed telemetry about endpoint activity (file changes, processes, network connections) but lack the broader context of network-wide events. Conversely, a SIEM has network and identity logs but lacks the endpoint-level detail.

Research gap: Developing and refining methods for the real-time, bidirectional exchange of contextual information between EDR and SIEM systems. Research is needed to explore how SIEM's network traffic analysis and identity logs can be used to enrich EDR alerts, and how EDR's granular endpoint data can add forensic detail to SIEM correlation rules [60].

Advanced AI/ML for correlated threat detection: Current limitation: Both EDR and SIEM use AI/ML, but these models operate within their own data silos. SIEM models analyze network logs for anomalies, while EDR models analyze endpoint behavior [61]. This fragmented approach can miss sophisticated, multi-stage attacks that transition across the network and endpoint layers. **Research gap:** Creating unified machine learning models that can simultaneously ingest and correlate data from both EDR and SIEM sources. This would enable the detection of advanced persistent threats (APTs) and other attacks by identifying subtle patterns across both the network and endpoints.

Intelligent Alert Prioritization and Noise Reduction: Despite the use of AI and machine learning, a significant problem remains the high rate of false positives and alert fatigue. There is a gap in research and development of highly effective, adaptive algorithms that can accurately distinguish critical threats from benign anomalies in the massive, combined data streams of EDR and SIEM [62].

Summary of Key Research Gap: (**Future Direction of Research):** Based on current industry trends, future research in Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) is moving toward tighter integration, enhanced automation with artificial intelligence (AI) [63], and broader, more contextual visibility through Extended Detection and Response (XDR). As cyber threats become more sophisticated, the siloed approach of traditional security tools is proving less effective. In the future, EDR solutions will leverage AI and machine learning (ML) not only to detect threats after they occur but also to analyses historical data and behavioral patterns to predict and prevent attacks before they happen [64]. This represents a shift from reactive detection to proactive defense.

a. **Enhanced visualization and storytelling**: Researchers are exploring new ways to visualize security data to help analysts make sense of complex attack narratives. Future interfaces will be more intuitive, providing a visual summary of user activities and threat provenance to assist with faster decision-making.
b. **Advanced data handling and storage**: Research is essential to enhance the cost-effectiveness and security of storing and analysing the large volumes of data processed by Security Information and Event Management (SIEM) systems. This research should explore innovative storage architectures and data privacy controls. Additionally, this falls within the scope of log management, data retention, and analysis. (Ref. to Results Section) [65].

Future of data analytics: Data analytics is the core function of Endpoint Detection and Response (EDR) solutions, driving their ability to detect, investigate, and respond to advanced cyber threats. EDR tools continuously collect vast amounts of telemetry data from endpoints and apply sophisticated analytics [66] to identify suspicious activity that traditional, signature-based antivirus software would

miss. As the threat landscape evolves, so too will the data analytics capabilities of EDR solutions.

i). **Future EDRs** will increasingly use AI for predictive threat mitigation, analysing historical patterns to forecast and prevent attacks before they happen.
ii). **Holistic (XDR) analytics:** Extended Detection and Response (XDR) represents the evolution of EDR analytics. It expands data collection beyond endpoints to include networks, cloud workloads, and identity tools. This provides a more holistic view and better context for identifying complex, multi-vector attacks.
iii). **Improved operational efficiency:** Analytics will be used to reduce "alert fatigue" by minimizing false positives and automatically triaging low-priority incidents. This will allow security analysts to focus their expertise on the most critical threats.

6. Problem Analysis:

EDR and SIEM solve different problems and have distinct limitations. EDR provides deep, real-time visibility and automated response at the individual device level, while SIEM offers a broad, centralized view of security events across the entire IT infrastructure for correlation and compliance. EDR solutions are designed to address the problem of advanced threats that bypass traditional, signature-based antivirus software, such as fileless malware, zero-day exploits [67], and advanced persistent threats (APTs).

6.1 Problems in EDR:

a. Detection of sophisticated endpoint threats: EDR uses behavioral analytics and machine learning to identify suspicious activities and deviations from normal patterns on endpoints, even for previously unknown threats.
b. Rapid incident response at the source: It provides automated and manual response capabilities directly on the endpoint, such as isolating a compromised device, terminating malicious processes, or rolling back unauthorized changes, which significantly reduces the attacker's "dwell time".
c. In-depth forensic investigation: EDR continuously records endpoint activities, creating a detailed historical timeline of events (a "security DVR" for the endpoint) that enables security teams to trace the full attack chain and perform root cause analysis [68].
d. Proactive threat hunting: It empowers security analysts to proactively search for hidden threats that may have evaded initial detection, using collected endpoint telemetry data.

6.2 Limitations of EDR:

a) Limited scope: EDR's visibility is restricted to the endpoints where agents are deployed. It lacks insight into network activity, cloud workloads, application logs, and identity management systems.
b) Potential for alert fatigue: If not properly tuned, EDR can generate a high volume of alerts, overwhelming analysts.
c) Requires expertise: Effective management and analysis of EDR data often require specialized security skills, which can be expensive and scarce.

SIEM (Security Information and Event Management) solutions address the challenge of managing and making sense of the massive volume of log [69] data generated by diverse systems across an entire enterprise IT environment.

6.3 Problems in SIEM:

✓ Network-wide threat correlation: It uses correlation rules and analytics to link seemingly unrelated events across different systems, helping to identify broader attack patterns and multi-stage campaigns that single-system monitoring would miss.
✓ Detection of insider threats and policy violations: By monitoring user activity and access attempts across the network, SIEM can help spot unusual behavior indicative of insider threats or policy non-compliance.

7. Suggestion for Improvement:

This paper aims to evaluate the serviceability, integration, interoperability, and challenges of the EDR system within the SIEM framework (Mechanism), highlighted in the Method Section. This improvement

was not reflected in the Background and Literature survey of this paper. The integration and interoperability of Endpoint Detection and Response (EDR) are critical for creating a cohesive and effective cybersecurity strategy. By connecting with other security tools, EDR moves beyond a standalone function and becomes a core component of a broader security ecosystem, enabling faster detection, richer context, and more automated responses [70].

a) Implementation: Open-source EDR and SIEM tools can be integrated to build a comprehensive, cost-effective security ecosystem, often forming the core of an open-source XDR (Extended Detection and Response) platform. This is achieved by combining the granular, endpoint-specific data from EDR tools with the broad, log-aggregating capabilities of SIEM platforms.
b) Wazuh: A unified, all-in-one open-source platform that provides both EDR and SIEM capabilities, including log analysis, file integrity monitoring, vulnerability assessment, and automated response. Its agent-based architecture can send data to the Elastic Stack for visualization.
c) Osquery: A powerful endpoint data collection framework that exposes an operating system as a relational database, allowing security teams to write SQL [71] queries to monitor low-level system activities (processes, network connections, file hashes). Its output is typically fed into a SIEM for analysis and alerting.
d) Data Analysis: EDR-to-SIEM: Data Ingestion, log normalization, and Correlation (Ref Result Analysis and Conclusion Section)

8. Research Methodology (Mechanism): Integration of EDR-to-SIEM framework

In 2024–2025, the new approach to integrating Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) has shifted from manual data piping to AI-driven, autonomous ecosystems. This evolution centers on moving away from siloed "point solutions" toward unified platforms that proactively manage threats across all digital layers as follows. This new concept was derived from a background and literature survey and presented in this section as follows [72].

8.1. System Design (Framework)

System design for Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) serves different but complementary security goals. EDR provides deep, real-time protection at the device level, while SIEM offers a broad, centralized view across the entire IT infrastructure [73].

EDR System Design (Deep & Reactive)

EDR architecture is designed for granular visibility and immediate response on individual endpoints like laptops, servers, and mobile devices.

a) Endpoint Agents: Lightweight software installed on each device. These agents monitor activities in both user and kernel space, including file changes, process execution, and network connections.
b) Data Processing Server: A central hub (cloud or on-premises) that receives and analyzes massive telemetry streams from agents using machine learning and behavioral algorithms.
c) Detection Engine: Uses Indicators of Attack (IoA) and Indicators of Compromise (IoC) to identify threats that bypass traditional antivirus, such as fileless malware or lateral movement.
d) Automated Response Module: Triggers immediate actions like isolating a host from the network, killing malicious processes, or rolling back unauthorized system changes.

SIEM System Design (Broad & Strategic)

SIEM architecture is a multi-layered framework designed to aggregate, correlate, and store data from a wide variety of sources for long-term visibility and compliance.

e) Ingestion Layer: Collects logs and events from disparate sources, including firewalls, network devices, cloud APIs, and EDR agents (Ref to API Integration).
f) Parsing & Normalization: Converts "messy" raw logs into a standardized, searchable format for consistent analysis.

g) Correlation Engine: The "brain" of the system. It applies complex rules and AI to link isolated events (e.g., a suspicious login + a firewall block) into a single high-context security incident.

The integration and coordination of EDR-SIEM is considered foundational for modern cybersecurity resilience. This synergy bridges the gap between deep endpoint telemetry and broad, network-wide visibility (Figure 7). This integration creates a layered defense that combines deep device-level visibility with broad, network-wide context [74].

Figure 7. EDR & SIEM Correlation

How They Work Together: In a 2025 security environment, the integration follows a continuous cycle of data sharing and automated action:

1. **Telemetry Feeding:** EDR agents on workstations and servers collect granular data—such as process executions and registry changes—and forward this telemetry to the SIEM.
2. **Cross-Layer Correlation:** The SIEM ingests the EDR data alongside logs (Table 4) from firewalls, cloud services, and identity providers. It uses advanced correlation rules to link seemingly isolated events (e.g., a suspicious login in the cloud followed by a new process on a laptop).
3. **Unified Alerting:** Instead of analysts checking separate consoles, the integrated system surfaces a single "incident story".
4. **Coordinated Response:** If the SIEM identifies a multi-stage attack, it can trigger the EDR to take direct action, such as isolating the affected endpoint, while simultaneously updating firewall rules or revoking user access.

Table 4. Key Strengths of Each Component

Feature	EDR (The Micro" View)	SIEM (The "Macro
Focus	Individual devices (laptops, servers, Mobile).	Entire infrastructure
Data Type	Real-time behavior, process trees, and file changes.	Log data, event timestamps
Detection	Behavioral analysis, AI-driven anomaly detection.	Rule-based correlation
Response	Immediate: killing processes, isolating hosts, rolling back files.	Strategic: alerting, compliance reporting, and orchestration.

8.1.1 Implementation Best Practices

a. Prioritize Open APIs: Select solutions with robust API support to ensure seamless data exchange and command execution.
b. Map to Frameworks: Use the MITRE ATT&CK Framework to standardize data mapping and identify defensive gaps across both platforms. The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework serves as the "common language" that binds EDR and SIEM together into a cohesive defense strategy. The primary role of MITRE ATT&CK is to provide a structured matrix of Tactic**s** (the attacker's goals, like "Privilege Escalation") and Techniques (the methods used, like "Process Injection") [75].

c. Phase Deployment: Start by integrating critical systems (e.g., domain controllers) before expanding across the enterprise to manage data volume.
d. Adopt Cloud-Native Architectures: Cloud-native SIEM and EDR platforms offer better scalability for hybrid work environments and lower maintenance costs compared to traditional on-premises setups.
e. Data Tiering & Storage: Employs a multi-tiered approach—Hot Storage for real-time monitoring and Cold Storage for long-term compliance retention (often required for 1–7 years).
f. Visualization Console: Provides dashboards and reporting tools for SOC analysts to investigate historical trends and meet regulatory audit requirements.

Integrated Architecture: The SOC Unified View: In a modern Security Operations Center (SOC), EDR and SIEM work as a "feedback loop".

- Data Flow: EDR feeds granular endpoint telemetry into the SIEM, enriching network-wide correlation (Ref to Mechanism Page No. 5).
- Coordinated Response: A SIEM alert (e.g., suspicious cloud activity) can trigger an automated EDR action (e.g., quarantining the associated user's laptop) through an integrated SOAR platform.
- Threat Hunting: Analysts use SIEM for broad pattern searches and then "pivot" into EDR for deep-dive forensic investigations on specific machines.

8.1.2 API Integration

API Integration: In 2025, API integration is the standard [76] method for connecting EDR platforms to SIEM systems. This allows for real-time telemetry streaming, automated alert synchronization, and bidirectional response actions. In this integration of **Push** and **Pull** API architectures, primarily used to build highly responsive, hybrid systems that balance real-time responsiveness with controlled data retrieval (Figure 4).

Core Architecture

- ✓ Pull API (Request-Driven): The client initiates the request to fetch data from the server. This is ideal for scenarios where data updates are infrequent or where the client needs granular control over when to retrieve information. Pull Model (On-Demand):[66] The SIEM periodically "polls" the EDR's API endpoints (e.g., RESTful APIs) to fetch new logs or detailed metadata. This model is commonly used for batch processing or retrieving historical forensic data [77].
- ✓ Push API (Event-Driven): The server proactively sends data to the client as soon as it becomes available, often using protocols like WebSockets, Server-Sent Events (SSE), or Webhooks. This is essential for time-sensitive, real-time data, such as live scores, financial trading, or instant notifications. Push Model (Real-Time): The EDR acts as a producer, immediately pushing alerts or telemetry to the SIEM as events occur. This is often achieved using Webhooks or Event Streams, ensuring the SIEM receives critical threat data within seconds.
- ✓ The Bi-Directional Workflow: API-based integrations enable data to flow in both directions: EDR to SIEM (Telemetry & Alerts): The EDR sends granular device-level data—such as process trees, registry changes, and local risk scores—to the SIEM for broad correlation. SIEM to EDR (Orchestrated Action): When the SIEM identifies a multi-stage threat (e.g., a "high-risk" device attempting unauthorized database access), it uses the EDR's Response APIs to trigger immediate actions. Automated Commands: Examples include isolating a host from the network, terminating a malicious process, or initiating a remote malware scan [78].

Modern integrations utilize two primary models to ensure data remains fresh and actionable:

a. **Real-Time Data Pushing:** The EDR acts as an active producer, using **Webhooks** or event streams to instantly push alerts or telemetry to the SIEM [79] as they occur (Table 5).
b. **On-Demand Data Pulling:** The SIEM utilizes **RESTful APIs** (Figure 5) to query the EDR for specific forensic metadata, such as process trees or file hashes, to enrich its correlation logic during an investigation

8.1.3 Integration Tools and Functionalities

Table 5. API Integration & Tools

EDR Provider	Primary Integration API / Method	Data Format
SentinelOne	Management API (for alerts/activities) & Cloud Funnel (streaming raw logs via AWS S3).	JSON / OCSF
CrowdS	Falcon Data Replicator (FDR) (streams to AWS S3/SQS) and Alerts API (replacing the deprecated Detects API as of Sept 2025).	JSON
Microsoft Defender1	Streaming API for raw event data; integrates natively with Microsoft Sentinel via the Microsoft Graph Security API.	JSON / CEF

A. Key Technical Components

a. Authentication: Modern integrations almost exclusively use OAuth 2.0 or API Tokens generated within the EDR management console [80,81].
b. Data Normalization (OCSF): In 2025, many providers have adopted the Open Cybersecurity Schema Framework (OCSF). This standardizes endpoint and network data into a common format, reducing the need for custom parsers in the SIEM [82–84].
c. Rate Limiting: EDR APIs often enforce limits (e.g., 25 requests per second) to prevent overloading the management console. High-volume telemetry should always use streaming APIs rather than standard REST polling.

B. Bidirectional Workflow (Response APIs)

Beyond log ingestion, API integration enables the SIEM [85] or a connected SOAR platform to send commands back to the EDR (Table 6):

- ✓ Host Isolation: Automatically disconnect a compromised machine via API in the discussion Section.
- ✓ Process Termination: Remotely kill a malicious process detected by the SIEM's correlation rules.
- ✓ Alert Updates: Sync incident status (e.g., "Closed") between the SIEM and EDR dashboards.

Integrating EDR-SIEM provides a unified defense by combining granular endpoint telemetry with broad network-wide log correlation [86].

Table 6. EDR vs. SIEM Integration Summary

Feature	Endpoint Detection & Response (EDR)	Security Information & Event Management (SIEM)	Integration Value (Unified Visibility)
Primary Focus	Deep visibility into specific host/endpoint activity (laptops, servers).	Aggregate and correlate logs from the entire network (firewalls, cloud, identity).	Correlates endpoint process execution with suspicious firewall traffic or logins.
Data Types	Process logs, registry changes, file modifications, local network connections.	Syslog, SNMP, Netflow, API logs, and specialized security events.	Normalizes disparate EDR telemetry into a standardized format for long-term storage.
Detection Speed	Real-time or near real-time detection of local malicious behavior.	Historical analysis and correlation of patterns across multiple systems.	Reduces "Mean Time to Detect" (MTTD) by surfacing complex multi-stage attack chains.
Response	Automated containment (isolating a host, killing a process).	Alerting and ticket creation; often requires SOAR integration for automated action.	Automated SOAR workflows triggered by SIEM can instruct EDR to isolate compromised hosts.
Use Case	Preventing ransomware and local malware execution.	Compliance reporting, forensic investigation, and cross-platform auditing.	Provides "forensic context" by proving how a file arrived via email (SIEM) and then executed (EDR).

CASE-1

SentinelOne Integration

In 2025, SentinelOne will provide a unified ecosystem where EDR and SIEM are no longer separate silos but are integrated into the Singularity Platform. This integration is achieved through a cloud-native architecture that combines endpoint telemetry with a high-speed data lake [87].

Integration Architecture: SentinelOne's approach focuses on a unified agent and a centralized backend:

a) Singularity Data Lake: Acting as the foundation, this index-free, columnar data lake ingests and stores massive volumes of data (at exabyte scale) from both SentinelOne agents and third-party sources.
b) Unified Agent: The same agent used for EDR functions also performs log collection, capturing OS event logs and application data without requiring separate log forwarders.
c) AI SIEM Integration: SentinelOne's Singularity AI SIEM natively integrates with EDR data, allowing for sub-second query speeds across "always-hot" data for up to seven years [88].

Key Integration Features

a. Purple AI: A generative AI analyst that allows security teams to use natural language queries to search across integrated EDR and SIEM data, accelerating investigation times [89].
b. Singularity Hype automation: A no-code workflow engine that can trigger responses based on correlated alerts. For example, a SIEM alert can automatically prompt the EDR agent to isolate a compromised host [90].
c. Open Integration (OCSF Support): The platform uses the Open Cybersecurity Schema Framework (OCSF) to normalize data from diverse sources—including competitor EDRs and cloud logs—into a common format for easier correlation in the SIEM [91].
d. Storyline Technology: Links related events together automatically, reducing manual investigation by providing a clear chronological account of an attack across endpoints and the broader network.

Common Deployment Methods: Organizations can integrate SentinelOne with SIEM capabilities in three primary ways:

1. Native AI SIEM: Using SentinelOne's own built-in SIEM platform for a fully unified "single pane of glass" experience.
2. External SIEM Connector: For organizations keeping a legacy SIEM (like Splunk or Microsoft Sentinel), SentinelOne provides API-based connectors and syslog support to stream EDR logs directly into those external platforms [92].
3. Marketplace Integrations: The Singularity Marketplace offers one-click integrations with third-party security tools, including NDR, IAM, and cloud platforms, to enrich SIEM data.

CASE-2

CrowdStrike Integration: In 2025, CrowdStrike integrates EDR and SIEM through its Falcon Next-Gen SIEM, which is built on the Falcon LogScale data architecture (Figure 5). This integration unifies native endpoint telemetry with third-party log data into a single, high-speed, AI-native platform [93].

Architecture and Core Integration: Unified Data Foundation: The integration uses an index-free architecture that allows for sub-second, petabyte-scale searches, reportedly performing up to 150x faster than legacy SIEMs [94].

a. Native Telemetry Ingestion: CrowdStrike EDR (Falcon Insight) automatically streams over 600 types of endpoint telemetry directly into the SIEM, including process executions, network connections, and identity logons.
b. Falcon Onum: A key 2025 component that provides real-time telemetry pipelines to filter and enrich data before ingestion. This reduces data storage costs by up to 50% and speeds up incident response by 70%.
c. CrowdStream: Acts as an observability pipeline to connect and route third-party data sources into the platform, ensuring all security signals are normalized and correlated alongside EDR data.

AI and Automation Capabilities (2025)

a) Charlotte AI & Agentic SOC: CrowdStrike uses Agentic AI to automate complex SOC tasks. AI agents can autonomously perform data transformation, generate correlation rules, and conduct search analysis using natural language [95].
b) Falcon Fusion SOAR: This no-code orchestration layer is natively integrated, allowing an EDR detection to automatically trigger SIEM-level response playbooks, such as isolating a host or updating firewall rules across the enterprise.
c) Proactive Threat Hunting: Analysts use a unified query language to hunt for threats across both endpoint and third-party data, enriched by real-time Adversary Intelligence.

Third-Party SIEM Integration

For organizations not using Falcon Next-Gen SIEM as their primary platform, CrowdStrike maintains robust support for external integrations:

- ✓ Falcon Data Replicator (FDR): Continues to be the primary method for streaming high-volume raw EDR data to external SIEMs like Splunk, Microsoft Sentinel, or Elastic Security [96].
- ✓ SIEM Connectors: Turnkey APIs and connectors allow for the seamless export of refined alerts and event streams to third-party security platforms for further correlation.

Comparison: In 2026, the integration comparison between CrowdStrike Falcon and SentinelOne Singularity highlights two distinct philosophies: CrowdStrike's ecosystem-led, modular platform and SentinelOne's **autonomous**, unified agentic model (Table 7)

Table 7. Comparison CrowdStrike vs. SentinelOne

Feature	CrowdStrike Falcon Platform	SentinelOne Singularity Platform
Integration Philosophy	Intelligence-Led: Deeply integrated with its own "Threat Graph" for global context.	Autonomous/API-First: Built for automated workflows and "Singularity Marketplace" extensibility.
Architecture	Cloud-native; requires a connection for full intelligence capabilities.	Hybrid-ready; AI agent can function autonomously offline.
Data Retention	Standard 7-15 days; extended retention available via extra modules.	Higher default retention (up to 30 days) via unified Data Lake.
Third-Party Ecosystem	Extensive integrations via APIs (Microsoft, AWS, ServiceNow).	Direct marketplace apps for SIEM, Firewall, and Identity platforms.
Recovery/Rollback	Manual remediation tools and expert-led response.	One-click rollback to a clean state via VSS (Volume Shadow Copy).
Pricing Model	Modular; pay-per-feature (can become costly as modules stack).	Tiered bundles typically include more features in base packages.

8.1.4. Integration Architecture

- ✓ **CrowdStrike Falcon:** Utilises a cloud-native, API-forward architecture. It acts as a central control plane for highly standardized environments, offering deep, native integrations with the **Microsoft stack** (Azure, Intune, Defender) and AWS. It is optimized for "one control plane" management through its extensive marketplace [97].
- ✓ **SentinelOne Singularity:** Focuses on a "bring your data" posture via its **Singularity Data Lake**. It integrates well with hybrid and multi-cloud environments, emphasizing endpoint autonomy so that integration with the cloud is not required for real-time response.

Automation & AI Integration

a. **CrowdStrike (Charlotte AI):** AI is integrated to accelerate triage and human-led investigation. It proposes actions that are then routed through policy-trusted workflows, making it ideal for mature SOC teams seeking granular control.
b. **SentinelOne (Purple AI):** Emphasizes "hyper automation" and agentic autonomy. The AI can hunt, write timelines, and "pull the trigger" on containment automatically, designed to provide immediate relief for lean security teams [98].

Operational Comparison

Their integration capabilities differ primarily in their philosophy: CrowdStrike leverages a massive, cloud-native global intelligence graph, while SentinelOne focuses on autonomous, on-device AI and unified data lake integration.

Key Integration Strengths

- ✓ CrowdStrike is best for enterprises that want a fully managed ecosystem. Its integration with CrowdStrike Falcon OverWatch provides human-led threat hunting that acts as a direct extension of the customer's security team.
- ✓ SentinelOne excels in automated orchestration. Its Singularity Marketplace allows users to trigger actions in third-party tools [99] (like disabling a user in Okta or blocking an IP on a Cisco firewall) automatically when a threat is detected.

Performance Benchmark

A comparative performance study between SentinelOne and CrowdStrike reveals two industry leaders that excel in different architectural and operational categories. While both consistently earn high marks in **Gartner Peer Insights**, their impact on system performance and response speed differs by design. Independent Benchmarks (MITRE ATT&CK) are highlighted below: In recent tests, CrowdStrike has achieved 100% detection coverage in several scenarios [100].

SentinelOne also performs strongly, often achieving 100% detection, though some evaluations noted a higher volume of telemetry alerts or slightly lower surgical detection rates compared to CrowdStrike.

Independent performance benchmarks for SentinelOne and CrowdStrike highlight critical differences in system impact and detection speed.

System Performance Benchmarks:

- ✓ Local Resource Usage: SentinelOne performs most analysis directly on the endpoint via its AI-driven agent. While this can result in higher local processing, it is rated 4.7/5 for EPP performance by users on Gartner Peer Insights.
- ✓ Cloud Dependency: CrowdStrike utilizes a cloud-native model that minimizes local impact by offloading heavy data analysis to its Threat Graph. It is often preferred for maintaining low CPU overhead during standard operations.
- ✓ Network Bandwidth: CrowdStrike [101] typically consumes 5-10 MB of bandwidth per endpoint per day. SentinelOne's bandwidth usage remains similarly low, with traffic spikes limited to initial deployment and periodic updates.

Cost and Licensing

- ➢ **CrowdStrike:** Follows a **modular pricing model**, where costs increase as you stack modules for Identity, Cloud, or Next-Gen SIEM.
- ➢ **SentinelOne:** Uses a **tiered subscription model** that typically includes more features (like EDR and MDR) in lower-tier packages compared to CrowdStrike.

These comparisons outline the modular vs. tiered pricing, Microsoft ecosystem integration, and operational complexity of CrowdStrike Falcon and SentinelOne Singularity [102].

- ✓ Tool bloat: Adding another tool, even a powerful EDR, can increase the complexity of the security stack if not integrated strategically. Disparate, standalone solutions result in fragmented security and visibility gaps.
- ✓ API incompatibility: Ensuring seamless communication and data exchange between the new EDR and existing tools like SIEM or SOAR can be technically challenging due to API compatibility issues[103].

8.1.5 Correlation of EDR and SIEM

In 2025, the correlation of Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) has evolved from basic log matching into a high-speed, AI-driven process that provides a holistic view of the attack surface (Table 8).

1). The Correlation Engine: How It Works

Correlation is the process of linking isolated events from EDR (deep endpoint telemetry) with events from SIEM (broad network, cloud, and identity logs) to identify complex attack patterns.

a. Data Normalization (OCSF): Modern platforms use the Open Cybersecurity Schema Framework (OCSF) to standardize disparate fields (e.g., matching src_ip from a firewall with client_ip from an endpoint) into a common language, allowing correlation rules to work independently of the vendor.
b. Behavioural Baselining (UEBA): AI-powered SIEMs use User and Entity Behaviour Analytics (UEBA) to learn "normal" behaviour for users and devices. Correlation occurs when an EDR flags an endpoint anomaly while the SIEM concurrently detects unusual network traffic or unauthorized cloud access.
c. Risk Scoring: Incidents are correlated and assigned a dynamic risk score. Instead of seeing thousands of separate alerts, analysts see a single "incident" that connects every step of the attack chain.

2). Correlation Details as follows

Table 8. Common Correlation Use Cases

Initial Event (Source)	Correlated Activity (Other Source)	Identified Threat
SIEM: "Impossible travel" login (e.g., NY then London).	EDR: Unknown process execution on the user's primary laptop.	Credential Theft / Account Takeover.
EDR: PowerShell launching an encoded script on a workstation.	SIEM: Unusual RDP connection from that workstation to a critical server.	Lateral Movement / Insider Threat.
SIEM: Massive data transfer to an unknown external IP.	EDR: Recent file modifications in a sensitive directory on the local host.	Data Exfiltration / Ransomware.

3). Strategic Benefits of Unified Correlation

a. Reduced Alert Fatigue: AI correlation can reduce noise by 50–80% by grouping related alerts into a single, high-fidelity incident.
b. Faster Investigation (MTTR): Timeline reconstruction that used to take hours now takes minutes. AI "Analyst" tools automatically map out the attack path from the initial compromise to the current state.
c. Autonomous Response: High-confidence correlations can trigger automated playbooks through SOAR (Security Orchestration, Automation, and Response), such as isolating an endpoint immediately after a confirmed network-level credential abuse.
d. Compliance & Forensics: SIEM provides the long-term historical context (retaining logs for months or years) while EDR provides the "nitty-gritty" process details needed for deep root-cause analysis.

In Brief: EDR-SIEM are complementary technologies. EDR excels at deep, rapid, automated response to threats at the endpoint level, while SIEM provides broad, centralized visibility and correlation across the entire infrastructure for overall security management and compliance. Using both in tandem helps to eliminate security gaps and provides a more comprehensive, layered defense [104].

9. Results Analysis

Endpoint Detection and Response (EDR) results require assessing the output of its advanced detection engines and interpreting the rich telemetry data they provide. Organizations must move beyond a simple pass/fail metric to evaluate the effectiveness of their EDR solution, the performance of their security team, and the maturity of their overall security posture.

Experimental Results from 2025 security performance benchmarks demonstrate that while EDR and SIEM are effective individually, their coordinated use significantly outperforms siloed deployments across key metrics like response time, detection coverage, and cost-efficiency.

9.1 Performance Metrics & Efficiency

Research conducted throughout 2024 and 2025 highlights the quantitative impact of integrating AI-native SIEM with EDR:

1) Response Time (MTTR): Coordinated systems reduced the Mean Time to Respond by up to 90%.
2) Investigation Efficiency: Organizations using AI-driven integration saw a 34% reduction in investigation time and improved overall response times by 75%.
3) Cost Savings: Extensive use of AI and automation in these systems saved organizations an average of $1.88 million per data breach compared to those not using such technologies.
4) Search Speed: AI-native platforms (like SentinelOne) reported search and detection speeds up to 100x faster than traditional, legacy SIEM tools.

9.2 Detection Coverage & Accuracy

Experimental analysis of cross-domain telemetry reveals a marked improvement in identifying complex attacks:

a. **Telemetry Synergy:** EDR provides deep visibility into endpoint behavior (process trees, file

writes), while SIEM correlates this with identity and network flows. This combination is essential for detecting **"low and slow"** attacks and lateral movement that individual tools often miss.

b. **Reduced False Positives:** AI-driven correlation can reduce alert volume by **40–60%** by filtering out noise through contextual risk scoring.

c. **Detection Gaps:** Benchmarks show that 54% of organizations still struggle with tool fragmentation; failing to integrate EDR with SIEM results in "dead zones" where malware can reside undetected on endpoints for days.

9.3 Case Study Insights

- ✓ **Financial Sector:** Integrated platforms have shown a measurable reduction in financial fraud by automating compliance reporting alongside real-time threat detection.
- ✓ **Ransomware Simulation:** In experimental attack scenarios, EDR successfully stops initial execution (e.g., PowerShell scripts), while the coordinated SIEM detects the broader attempt at lateral movement across critical file shares.
- ✓ **Cloud Evolution:** 2025 results indicate that legacy SIEMs monitoring only 5% of sources due to high storage costs are significantly less effective than cloud-native, AI-integrated counterparts that process raw telemetry more efficiently.

9.3.1 Experimental Analysis

Recent experimental analyses and field studies of integrated cybersecurity and API architectures highlight significant performance gains when coordinating multi-layered systems.

a) EDR-SIEM Integration Analysis

Recent 2026 studies on integrated security operations centers (SOCs) demonstrate that moving from siloed to coordinated EDR and SIEM environments directly impacts efficiency[105]:

b) **Alert Volume Reduction:** Field data from SaaS organizations show a 40% drop in alert volume when endpoint priority signals are integrated into a unified console (XDR/SIEM hybrid) [106].

c) Response Efficiency: Coordination between platforms allows for automated playbooks that reduce manual onboarding time by **30%** and accelerate "time-to-value" within the first three months of implementation.

d**) Resource Consumption:** Experimental testing of integrated open-source SIEM/IDS systems (e.g., ELK Stack with Zeek) during DoS attacks reveals that database components (Elasticsearch) consume the most resources, reaching 78% CPU and 2.3GB RAM, while the detection engines remain lightweight at roughly 3.5% CPU [14,15].

e) **Accuracy:** Integrated XDR/EDR platforms achieved 100% detection accuracy in independent 2025 and 2026 laboratory malware tests (AVLabs and SE Labs), compared to lower rates for fragmented, legacy systems.

9.3.2 Push vs. Pull API Integration Analysis (Figure 5)

Empirical performance evaluations in 2025 and 2026 highlight the distinct efficiency profiles of these two communication models (Table 9):

a) **Latency & Speed:** Push-based architectures are significantly faster, eliminating the need for servers to verify and process individual requests before responding. In streaming scenarios, push-based sources are up to 2x more performant than pull-based designs under constrained resources.

b) **Network Efficiency:** 2026 trends indicate that AI and large language models (LLMs) will increase API usage by **30%**. Integrating push mechanisms can manage this load more effectively by reducing the server strain caused by the thousands of "idle" pull requests typical of large-scale systems.

c) **Throughput & Stability:** Experimental results in real-time communication show that push-pull protocols (like REST-API or ZeroMQ) achieve **better latency** than pub-sub protocols by eliminating intermediate broker layers.

d) **Comparison of Rewards:** In goal-oriented communication, unified architectures using adaptive scheduling in push-pull systems consistently achieve higher "rewards" (system fulfilment objectives) as available channels increase.

Table 9. Summary of Performance Metrics

Feature	Pull API (Request-Driven)	Push API (Event-Driven)
Latency	Higher (due to polling delay)	Lower (real-time updates)
Throughput	Limited by request frequency	Higher in real-time streaming
Complexity	Lower; easier to scale statelessly	Higher; requires stateful connection management
Security	Easier to audit; client-controlled	Requires stronger auth for open connections

9.3.3 Practical Scenarios of Open-Source Tools

Several powerful open-source platforms combine Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) capabilities for a unified security monitoring solution. Other open-source tools can be integrated to achieve similar functionality, allowing for deep customization without licensing costs. All-in-one open-source platforms: Wazuh is a free, open-source security platform that unifies XDR [107] (Extended Detection and Response) and SIEM capabilities (Table 10).

Table 10. Comparison of Open Source EDR and SIEM Tools

Tool Type	Primary Tools	Key Security Features	Best For	2025 Status
EDR (Endpoint Focus)	Wazuh Agent, OSSEC	Real-time monitoring, File Integrity Monitoring (FIM), vulnerability detection, and autonomous response (killing processes, isolating hosts).	Protecting individual workstations, servers, and cloud workloads.	Wazuh is a leading choice for unified EDR/XDR in 2026.
SIEM (Log & Analytics Focus)	ELK Stack (Elasticsearch, Logstash, Kibana), OpenSearch	Massive log ingestion, deep indexing, complex event correlation across multiple sources (network, identity, cloud), and advanced data visualization.	Broad network-wide visibility, long-term data retention for forensics, and compliance auditing.	ELK/Elastic remains a top-tier open-source SIEM for highly technical teams.
Incident Response (Management Focus)	The Hive, Cortex	Case management, automated alert enrichment, and coordination of analyst workflows during a breach.	Managing the "after-alert" lifecycle: investigation, evidence collection, and ticketing.	TheHive Project is the standard for open-source case management.

Wazuh uses an agent-based approach to collect security data from endpoints (servers, workstations, cloud workloads, containers) and sends it to the central Wazuh server for analysis. Its integration capabilities are primarily achieved through log analysis.

Log Data Analysis: Wazuh collects and analyzes logs from various sources, including third-party EDR solutions, to identify threats and anomalies.

Osquery transforms an operating system (Windows, macOS, Linux) into a relational database, allowing security teams to query system data using SQL. This capability is invaluable for EDR as it provides real-time and historical insight into endpoint activities.

- Real-time Visibility: Security teams can run live, ad-hoc queries during an incident investigation to quickly assess the scope and severity of a potential threat.
- Threat Hunting: It allows proactive threat hunting by querying for specific indicators of compromise (IOCs), such as unauthorized processes, suspicious network connections, or file changes.

Integrating open-source EDR and SIEM solutions poses unique serviceability challenges, mainly due to the absence of dedicated vendor support, the requirement for extensive technical expertise, and the difficulties associated with maintaining and scaling custom integrations[108].

In 2025, the landscape of open-source security tools has matured, with several platforms offering robust EDR and SIEM capabilities. Many organizations combine these tools to create a unified **SOC (Security Operations Center)** stack.

How Open Source Integrates: Most open-source deployments follow a standard three-tier architecture:

1. Collection: Wazuh agents installed on endpoints collect local telemetry and forward it to a central manager.

2. Analysis & Storage: The Wazuh Manager processes these logs and feeds them into the Elasticsearch/OpenSearch engine via Filebeat for powerful indexing and cross-platform correlation.
3. Visualization & Response: Analysts use Kibana or OpenSearch Dashboards for real-time monitoring. Critical alerts can be automatically pushed to TheHive via APIs to trigger a formal investigation.

9.3.4 Integration:

Connecting with EDR and SIEM: Integration involves configuring EDR and SIEM platforms to communicate seamlessly, typically by forwarding EDR telemetry and alerts to the SIEM.

a. Data forwarding: EDR agents continuously collect granular endpoint telemetry, including process execution, file modifications, network connections, and user activity. This data is forwarded to the SIEM for centralized collection and storage.
b. API connectivity: Many vendors offer native, out-of-the-box integrations through application programming interfaces (APIs), Figures 3 and 5 ensuring consistent data transfer between the two platforms [67].
c. Connector configuration: For vendors without native integration, connectors or agents are configured to format and send EDR data to the SIEM using standard formats like Syslog or CEF (Common Event Format).

9.3.5 Interoperability

Interoperability ensures that the integrated EDR and SIEM systems work together effectively, with each platform leveraging the other's capabilities to enhance overall security.

Core aspects of interoperability:

I. Context enrichment: A SIEM can enrich raw EDR alerts with broader context. For example, a suspicious EDR alert on an endpoint can be cross-referenced with SIEM data regarding network traffic, user identity, and threat intelligence to determine if the activity is part of a larger attack.
II. Response orchestration: The integration can initiate automated response actions. For instance, a high-severity alert correlated in the SIEM could trigger a SOAR (Security Orchestration, Automation, and Response) playbook to instruct the EDR agent to isolate the compromised endpoint.
III. User and Entity Behavior Analytics (UEBA): Advanced SIEMs with UEBA capabilities can use endpoint data from EDR to establish behavioral baselines for users and devices. This allows the SIEM to detect and alert on subtle, anomalous behavior that might indicate an insider threat or compromised account [15].

9.3.6 Correlation

Correlation is the process of linking together seemingly disparate events from both EDR and SIEM data to identify patterns indicative of a multi-stage attack. It transforms noise into actionable security intelligence

Key Correlation use cases: Lateral movement detection:

a. EDR signal: An EDR agent detects an unusual process spawning on an endpoint.
b. SIEM signal: The SIEM receives logs showing a failed login attempt from that same endpoint against a different server.
c. Correlation: The SIEM correlates these events to identify a lateral movement attempt across the network, even if no single event appeared malicious on its own.

Benefits of EDR and SIEM Correlation

✓ Comprehensive visibility: Provides a holistic view that covers both endpoint-specific and network-wide security events.
✓ Enhanced threat detection: The ability to correlate events across layers allows for the detection of sophisticated, multi-stage threats that operate "below the radar" of a single tool.
✓ Faster, coordinated response: Automated orchestration based on correlated alerts reduces

response time and minimizes damage by enabling rapid containment across the entire attack surface.

✓ Improved threat hunting: The combined data gives security analysts a richer dataset for proactive threat hunting, allowing them to search for hidden threats that may have evaded initial detection.

Recommendation: Strategies for Large Volumes of Logs

Managing the massive data volumes requires specific strategies:

a. Log Filtering and Prioritization: Not all logs are equally important. Implement dynamic filtering rules to reduce noise and prioritize high-value logs (e.g., privileged access logs, firewall denies) for immediate analysis in hot tiers.
b. Data Normalization and Enrichment: SIEM systems normalize logs into a standardized format for easier analysis across heterogeneous sources. Enriching raw logs with metadata (e.g., geolocation, asset criticality) allows for faster and more informed threat analysis.
c. Tiered Storage and Retention Policies (Compliance): Define data retention policies based on compliance requirements (e.g., PCI DSS, HIPAA [11] often require 1–7 years of retention) and operational needs. Use cost-effective storage solutions like cloud-based data lakes for long-term "cold" data storage.
d. Advanced Analytics and Machine Learning: Next-generation SIEMs leverage User and Entity Behavioural Analytics (UEBA) and machine learning to automatically establish behavioural baselines and identify anomalies that might be missed by simple correlation rules, reducing false positives.
e. Scalable Architecture: Employ cloud-native or hybrid SIEM solutions that can scale efficiently to handle petabyte-scale data ingestion without performance bottlenecks.
f. Automation and SOAR/SIEM Integration: Use Security Orchestration, Automation, and Response (SOAR) tools to automate responses to common alerts, reducing the manual workload on security teams and ensuring faster remediation.

9.3.7 Log Management:

Large volume log management for Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) is a critical challenge due to the immense volume of data generated by modern IT environments. By implementing these strategies, organizations can effectively manage the immense volume of EDR and SIEM logs (Figure 6), transforming raw data into actionable intelligence for a robust security posture. Log management for EDR and SIEM solutions provides a wide array of statistics essential for monitoring security posture, system health, and compliance. These metrics help security teams prioritize threats, optimize performance, and ensure efficient resource allocation.

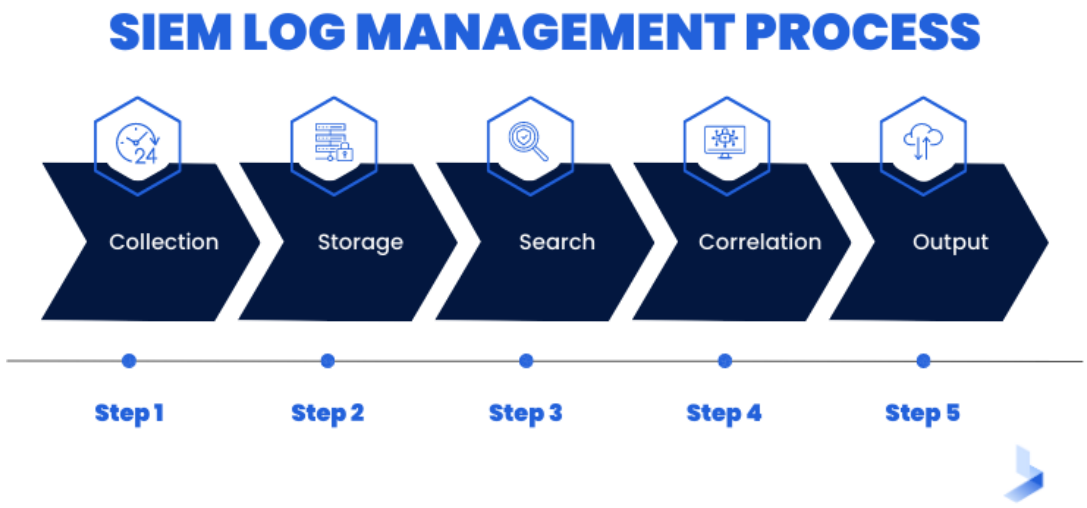


Figure 6. Advanced Log Management

Key Log Statistics (Risk Assessment)

Security and Threat-Related Statistics

a. Alert and Incident Volume: The total number of alerts generated, broken down by severity (critical, high, medium, low) and type (e.g., malware detection, unauthorized access attempt, policy violation).
b. Threat Detections (by Type): Statistics on specific threats identified, such as ransomware instances, zero-day exploits, suspicious process activities, or successful firewall denies.
c. Suspicious User Activity: Metrics on unusual behaviour detected by User and Entity Behaviour Analytics (UEBA), such as access attempts from unknown IPs, changes in user privileges, or access to critical systems outside of normal hours.
d. Failed vs. Successful Logins: Statistics on authentication logs, which are crucial for detecting brute-force attempts and compromised credentials.
e. Attack Patterns and Trends: Identification of recurring attack sources, methods, or targeted assets, enabling proactive defense adjustments.

Operational and Performance Statistics

a) Log Ingestion Rate: The volume of raw log data (Table 11) being processed per second/minute/hour, often measured in Events Per Second (EPS) or data volume (GB/TB per day) (Figure 7).
b) Data Volume by Source Type: A breakdown of how much data is coming from different sources (e.g., endpoints, firewalls, cloud services), helping identify data bottlenecks or storage needs.
c) Data Storage and Retention Metrics: Statistics on current storage consumption, estimated time until storage capacity is reached, and adherence to defined data retention policies.
d) System Health and Latency: Performance metrics of the EDR/SIEM platform itself, including indexing speed, search query response times, and processing latency (the delay between a log being generated and it appearing in the system for analysis).
e) Endpoint Coverage (EDR specific): The number and percentage of active endpoints being monitored, highlighting any gaps in coverage where agents are offline or inactive.

Compliance and Reporting Statistics (Major Achievements)

1) Audit Trail Completeness: Metrics ensuring all necessary logs for compliance frameworks (like PCI DSS, HIPAA) are being collected and stored correctly.
2) Report Generation Frequency and Status: Statistics on the frequency and success rate of scheduled compliance reports.

These statistics provide the empirical data necessary to demonstrate a strong security posture to auditors and management, and to improve the efficiency of security operations continuously. The integration of EDR and SIEM involves a structured process that centralizes endpoint data for comprehensive analysis across the entire network infrastructure.

Table 11. EDR-to-SIEM Log Management Data Flow

Step	EDR Function	Log Management (Data Flow)	SIEM Function
1.Data Collection	EDR agents collect high-resolution, granular data directly from endpoints (laptops, servers, etc.), including process execution, file changes, and network connections.	EDR transmits specific, security-relevant logs and events to the SIEM via a secure channel (like Syslog or API).	SIEM receives event data from various sources, including EDR, firewalls, network devices, and cloud services.
2. Normalization & Parsing	EDR data is often pre-processed at the endpoint level before transmission.	The SIEM platform normalizes and parses the collected data into a uniform format for standardized analysis.	Data from EDR and other sources are formatted consistently, making correlation across disparate logs possible.
3. Aggregation & Storage	The EDR platform maintains its own database for in-depth endpoint-specific forensics.	Logs are aggregated in a central repository, often with a data lake architecture, for long-term storage and forensic analysis.	The SIEM stores the massive volume of log data to establish baselines and enable historical investigations.

4. Analysis & Correlation	EDR focuses on behavioral analysis and threat hunting, specifically on the host device.	The key value-add: SIEM correlates EDR endpoint data with network, identity, and cloud logs to detect multi-stage attacks.	The SIEM correlation engine identifies patterns, anomalies, and potential incidents by analyzing data across all sources.
5. Alerting & Response	EDR can initiate automated, immediate actions on the endpoint (e.g., isolating a device) upon detection of a threat.	When a correlated event exceeds a security threshold, an alert is generated and sent to the Security Operations Center (SOC) team.	SOC analysts use the holistic view from the SIEM to investigate the complete context of an alert and orchestrate a broader incident response.

10. Discussion

An EDR tool is a crucial security solution for protecting endpoints by continuously monitoring, detecting, and responding to cyber threats that evade traditional defenses. A discussion of EDR tools highlights their core functions, benefits, limitations, and how they fit into the broader security landscape.

a) AI and Machine Learning: The future of EDR and XDR is being shaped by advancements in AI and ML. These technologies enable more accurate and predictive threat detection, automate complex investigations, and reduce the burden of alert triage on security analysts.
b) Best practices for implementation: To maximize the value of an EDR tool, organizations should define clear security objectives, deploy in a phased approach, integrate with existing security infrastructure (like SIEM and SOAR), and continuously fine-tune policies to reduce false positives [97].

Specific Improvement as follows:

These valuable approaches are not included in the Background and Literature sections of this paper. The author emphasizes new concepts for improved technology management to optimize costs and enhance performance efficiently and effectively.

Serviceably: Open-source solutions enhance capabilities by offering transparency, flexibility, and cost-effectiveness, enabling organizations to build highly customized, community-driven security ecosystems that can rival commercial offerings. This modular approach avoids vendor lock-in and fosters rapid innovation through global community contributions.

Scalability and performance: A solution's ability to scale with a growing number of endpoints and a corresponding increase in data volume is crucial for long-term serviceability. The EDR agent on each endpoint should be lightweight, minimizing its impact on system performance.

Cost and performance are two of the most critical factors to consider when choosing an Endpoint Detection and Response (EDR) solution. The total cost of ownership (TCO/ROI) extends far beyond the initial purchase price, and performance is a balance between robust threat detection and minimal impact on system resources.

Zero Trust integration: Zero-Trust integration of EDR and SIEM involves a security approach where no user, device, or network component is implicitly trusted, and every access request is rigorously verified based on all available data. This integration moves beyond traditional perimeter security to enforce granular, identity-driven access controls and enable continuous monitoring and dynamic response to threats across the entire infrastructure.

Within a Zero Trust Architecture (ZTA), Endpoint Detection and Response (EDR) is a foundational and indispensable technology. While ZTA is a strategic framework based on the principle of "never trust, always verify", EDR is the tactical tool that provides the visibility, enforcement, and response capabilities necessary to execute that strategy at the device level. EDR helps enforce the continuous, context-based validation required by a zero-trust model, ensuring that endpoints do not become a weak link in the security chain.

Strengths of EDR

a) Defense against advanced threats: EDR's behavioural and AI-based analysis is effective against sophisticated, evasive threats like zero-day exploits, ransomware, and fileless malware that bypass traditional antivirus software.
b) Improved visibility: EDR provides granular, real-time visibility into what is happening on endpoints, which are often the initial point of compromise.

c) Reduced attacker dwell time: Automation and faster detection capabilities significantly reduce the time an attacker can remain undetected within a network.
d) Enhanced forensics and reporting: The detailed telemetry data collected by EDR is invaluable for post-incident analysis, reconstruction, and compliance reporting.

Continuous Verification and Investigation:

I. Real-time monitoring: EDR continuously monitors endpoint activity, including processes, file changes, and network connections. This provides the critical, up-to-the-minute telemetry that ZTA's policy engine uses to verify the integrity and security posture of a device before granting or maintaining access.
II. Device health checks: ZTA requires continuous validation of device health. EDR contributes by checking for up-to-date operating systems, running security software, and patch levels. If a device becomes non-compliant, EDR detects it and can trigger automatic remediation or access restriction.
III. IoT security: As the number of IoT devices grows, EDR technology will need to extend its visibility and protection to these resource-constrained devices.
IV. Cloud-native EDR: With more workloads moving to the cloud, EDR solutions are becoming cloud-native to protect cloud workloads and overcome the challenges of hybrid environments.

10.1. Unresolved Challenges

In 2024–2025, despite significant advances in autonomous defense, the integration of Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) continues to face several critical unresolved challenges.

10.1.1. Data Management and Scaling Issues

- ✓ **Data Volume Overload:** EDR platforms generate massive amounts of telemetry that can overwhelm SIEM storage and processing capacities. In high-traffic scenarios, this "deluge" leads to performance degradation and delayed real-time analysis.
- ✓ **Log Heterogeneity:** Systems across an enterprise use diverse formats (Syslog, JSON, XML), making the normalization and parsing process essential but technically difficult to maintain.
- ✓ **Hidden Integration Costs:** Beyond initial licensing, organizations often face unpredictable costs related to high-volume data ingestion, long-term forensic storage, and the professional services required for ongoing tuning.

10.1.2. Operational Obstacles

a) **Alert Fatigue:** Even when integrated, the volume of low-fidelity or false-positive alerts remains high. Security teams often become desensitized, leading to genuine, critical threats being missed.
b) **Skill Gaps:** Both EDR and SIEM require specialized knowledge to configure and monitor effectively. Many organizations lack the internal talent to manage these complex systems, necessitating a reliance on Managed Detection and Response (MDR) services.
c) **Continuous Maintenance Burden:** These are not "set it and forget it" tools. Constant updates to correlation rules are required as organizational environments and threat landscapes evolve.

10.1.3. Visibility and Compatibility Gaps

a) **Legacy System Incompatibility:** Older hardware and software often lack standardized APIs or modern logging formats, requiring complex custom connectors that create "blind spots" in security visibility.
b) **Cloud-Native Blind Spots:** Standard EDR-SIEM stacks often struggle to monitor Kubernetes workloads, serverless functions, and cloud API activity effectively.

c) **Vendor Lock-In:** Proprietary log formats from specific vendors often do not communicate well with other platforms, leading to fragmented monitoring where some areas of the business are better protected than others.

10.1.4. Strategic and Regulatory Hurdles

Compliance Complexity: Stricter global regulations (e.g., GDPR, HIPAA) mandate precise log retention and data privacy controls. Misconfigurations in how data is shared between EDR and SIEM can lead to severe regulatory penalties. It is challenging to map integrated data to stringent regulatory requirements, such as GDPR and HIPAA.

Zero Trust Gaps: While integration supports Zero Trust principles, attackers have shifted toward Identity-based compromises (token theft, MFA bypass), which traditional EDR and SIEM tools may miss if they lack dedicated Identity Threat Detection and Response (ITDR) capabilities.

In 2025, the challenge has shifted from "knowing the query language" to "knowing how to talk to the AI".

a. The Problem: Junior analysts often lack the deep forensic knowledge required to ask the right questions of an integrated EDR/SIEM AI assistant (Table 12).

b. Unresolved Aspect: Without senior-level oversight, the AI-integrated SOC becomes a "black box" where incidents are closed based on AI recommendations that the staff does not fully understand.

Table 12. Summary of Key Challenges (2025). API compatibility issues between Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) systems typically arise from data structural differences, vendor-specific limitations, and the lack of standardization in how security signals are exchanged

Challenge	Impact on Security	Root Cause
BYOVD Attacks	Blinds the EDR and SIEM.	Kernel-level vulnerabilities.
Telemetry Bloat	High costs lead to data gaps.	High volume vs. storage budgets.
AI Hallucinations	False sense of security/accuracy.	LLM limitations in security context.
API Friction	Delayed autonomous response.	Lack of universal "Response" APIs.

11. Future Research

Endpoint Detection and Response (EDR) will focus on addressing its inherent limitations, such as endpoint-centric visibility and susceptibility to advanced evasion techniques. This will involve leveraging more advanced AI and machine learning, integrating EDR into holistic security platforms like XDR, extending protection to diverse environments like the cloud and IoT, and developing new defensive and management strategies. Advanced AI and machine learning for proactive and resilient EDR. While current EDR solutions use AI and ML, future research aims to make these models more predictive, context-aware, and resilient against adversarial attacks.

1) Predictive threat detection: Develop predictive models that analyse threat intelligence and behavioural patterns to anticipate likely attack vectors before they occur, shifting EDR from a reactive to a proactive defence posture.

2) Contextual behavioural analytics: Research is needed to develop more sophisticated behavioural analytics that understand attack patterns across entire organizations, not just individual endpoints. This will help in distinguishing between legitimate administrative tasks and malicious "living off the land" (LotL) techniques.

3) Adversarial AI countermeasures: Investigate how attackers manipulate EDR models and develop more robust, self-improving ML systems that are resilient to these evasion tactics.

4) Intelligent alert prioritization: Enhance AI-driven systems to automatically triage, prioritize, and enrich alerts by correlating them with other data sources. This will reduce false positives and combat alert fatigue for security teams.

Securing diverse computing environments: As the IT landscape evolves, EDR research must extend

its focus to new and non-traditional computing environments.

a) Edge and IoT security: Develop lightweight, adaptive EDR agents and protocols that can provide essential security capabilities for resource-constrained Internet of Things (IoT) and edge computing devices without impacting performance.

b) OT security integration: Focus on integrating EDR with Operational Technology (OT) and Industrial Control Systems (ICS) to secure critical infrastructure and protect against threats that could disrupt physical operations.

c) Cloud-native EDR: Research new techniques for providing consistent EDR coverage across hybrid and multi-cloud environments, including containerized and serverless workloads.

Privacy-preserving EDR and quantum security: Future research must also address emerging concerns around data privacy and the threat of quantum computing.

- Privacy-preserving analytics: Explore the use of technologies like differential privacy and homomorphic encryption to analyse EDR data without exposing sensitive user information.
- Quantum-resistant security: Research and implement post-quantum cryptographic methods into EDR communications and data protection to prepare for the advent of quantum computing.

12. Conclusion

Endpoint Detection and Response (EDR) tools have evolved from foundational antivirus software into a necessity for modern cybersecurity, providing a dynamic defence against advanced threats. The conclusion of an EDR tool's role is its strategic importance in securing the expanding attack surface of a distributed workforce and ever-evolving threat landscape. EDR is no longer just a standalone product but a critical, foundational component of an organization's overall security architecture. Endpoint Detection and Response (EDR) is a mature, critical cybersecurity technology that has evolved beyond traditional antivirus to combat advanced, persistent, and evasive threats. The conclusion of EDR is a two-part insight: its undeniable importance as a core component of modern security and its complementary, rather than absolute, role in a comprehensive security strategy.

Serviceability: Requires proactive resource management, such as implementing log filtering and data compression to manage data volumes. Smaller organizations can also use Managed Detection and Response (MDR) services to access expert personnel. Serviceability, enhance testing and refining automated playbooks. Many organizations integrate a Security Orchestration, Automation, and Response (SOAR) platform to effectively manage and automate response workflows. Serviceability is the integrated solution that must provide powerful forensic and search capabilities, enabling analysts to trace events across the network and deep into endpoints. EDR provides the detailed, real-time endpoint data that enhances the broader context of the SIEM, allowing for more accurate correlation and faster, more informed incident response across the entire network.

a) **Enhanced Detection**: EDR data (e.g., a specific file hash or suspicious process) feeds into the SIEM, enabling correlation with network activity or user behavior for a holistic view of an attack.

b) **Streamlined Response**: The combination allows for automated playbooks where a SIEM alert can trigger a specific EDR response action, such as isolating a host, which improves efficiency and reduces manual effort [31].

Enhancement of Open-Source Tools: The value-added open-source tools optimize cost, time, and resources while improving integration, service capabilities, interoperability, Correlation, Scalability, Reliability, and Performance.

Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) offer cost-effective and high-performance platforms that are highly customizable and transparent. These solutions integrate multiple layers of security for comprehensive threat monitoring and response. Open-source tools enhance incident response by providing scalable, reliable, and customizable solutions that increase speed and efficiency throughout every stage of the incident response lifecycle. These tools excel at automating tasks, enabling collaboration, and delivering in-depth forensic insights.

Serviceability: (Transparency and Trust Management): Access to the source code allows independent security audits, ensuring no hidden backdoors and building trust in the tool's integrity. Scalable Log

Management: Platforms like the Elastic Stack and OpenSearch are built to handle massive volumes of data, scaling horizontally to meet the demands of a growing infrastructure without proprietary limitations. Wazuh: A prominent platform that unifies SIEM, EDR, and host-based intrusion detection (HIDS) into a single solution. It offers features like file integrity monitoring (FIM), vulnerability detection, and active response across cloud and on-premise environments.

Security Onion (Log Analysis): This is a free, open-source platform designed for network security monitoring and log management. It integrates tools such as Suricata and Zeek for intrusion detection, along with Elasticsearch for log analysis, making it effective for comprehensive network monitoring and incident response. Elastic Stack (ELK): This is a collection of tools—including Elasticsearch, Logstash, and Kibana—that work together to ingest, store, and visualize log data for security monitoring and analysis.

12.1. Correlation process in practice

Open-source EDR and SIEM stack, the correlation typically follows these steps:

a. Deployment: Install the EDR agents (e.g., osquery or Velociraptor) on the endpoints you need to monitor.

b. Data collection: The EDR agents collect and forward endpoint telemetry data (e.g., process executions, network connections, file access) to a central location.

c. Log aggregation: The data from your EDR agents is sent to your SIEM solution. For many open-source EDRs, this means configuring the agent to send logs to a log shipper like Logstash or Fluentd, which then sends the data to a SIEM platform like the ELK Stack (Elasticsearch, Logstash, Kibana).

d. Correlation and analysis: The SIEM correlates the endpoint telemetry with other security data, such as firewall logs, network traffic data (from tools like Snort or Suricata), and authentication logs. This process identifies potential threats that would be invisible from just a single data source.

e. Visualization and alerting: The SIEM's dashboard (e.g., Kibana for the ELK Stack) is used to visualize the correlated data. Security teams can set up alerts to be notified when specific correlations indicate a potential security incident, enabling a faster response.

12.2. EDR-to-SIEM data ingestion: Key Serviceability Benefits

a. Cost-Effective Implementation: The primary benefit is the elimination of expensive vendor licensing fees. This allows organizations with limited budgets to deploy enterprise-grade security monitoring tools (like Wazuh, the Elastic Stack, or Security Onion) and allocate resources to skilled personnel or hardware instead.

b. Transparency and Control: Access to the source code allows internal teams to audit the tools for security flaws, understand exactly how data is handled and analyzed, and maintain complete control over the infrastructure, avoiding vendor lock-in.

c. Flexibility and Customization: Organizations can tailor the tools precisely to their environment and specific security policies. Security teams can build custom parsers for unique log formats, write specific detection rules (e.g., in Osquery), and integrate specialized local tools using open APIs.

d. Active Community Support: Vibrant open-source communities often provide rapid bug fixes, share configuration insights, and develop new features faster than some commercial vendors. Community forums and public repositories (like GitHub) serve as extensive knowledge bases for troubleshooting.

In summary, EDR offers deep, immediate, and automated protection at the device level, while SIEM provides broad, centralized visibility and analysis for compliance and overall security management. Both require specific operational expertise and tuning for optimal performance. In brief, EDR concludes that it is a powerful and indispensable technology, but its ultimate value is realized not in isolation, but as a core pillar of a broader, multi-layered security strategy that adapts to an ever-evolving threat landscape.

Funding
No Funding available

Conflict of Interest Statement
No Conflict of Interest

Data Availability Statement
Data Availability based on Request

References

1. 2022 Cyber Attacks Trends: Mid-Year Report. Available at: https://research.checkpoint.com/2022/check-points-2022-mid-year-cyber-attack-trends-report/ (Accessed 28 Nov 2023).
2. Katie Bykowski, Automated Incident Response: Respond to Every Alert, Available at: https://swimlane.com/blog/automated-incident-response-respondevery-alert/ (Accessed on date: 17 Sep 2017)
3. Alanazi, A. T., & Alanazi, A. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. Cureus, 15(10), 2023. DOI: 10.7759/cureus.47026.
4. Ajinkya, "Endpoint Detection and Response Market Expected to Witness an Imperishable Growth over 2029, Market Plan, 2019, Available at: https://themarketplan.com/endpoint-detection-and-response-marketexpected-to-witness-an-imperishable-growth-over-2029/26078/(Accessed on 19 Dec 2025).
5. Anton Chuvakin, "Our 'Understanding Insider Threats' Paper Publishes", Gartner Inc., 2016. Available at: http://blogs.gartner.com/anton-chuvakin/2016/05/09/ourunderstanding-insider-threats-paper-publishes (Accessed on date: 29 Oct 2025).
6. A. Chuvakin, "The Complete Guide to Log and Event Management", Available at: https://www.novell.com/docrep/documents/9x1wixnqhd/Log_Event_Mgmt_WP_DrAnton Chuvakin_March2010_Single_en.pdf. (Accessed on date: 17 Sep 2017)
7. A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint Detection & Response: A Malware Identification Solution*", 2021 International Conference on Cyber Warfare and Security (ICCWS)*, *IEEE,* pp. 1–8, 2021, doi: 10.1109/ICCWS53234.2021.9703010.
8. A. Zibak, C. Sauerwein, and A. Simpson, "A success model for cyber threat intelligence management platforms", *Computers & Security*, 111,102466, 2021
9. A. Johnson and R. J. Haddad, "Evading Signature-Based Antivirus Software Using Custom Reverse Shell Exploit", In *Southeast Con 2021* (pp. 1-6). IEEE, doi: 10.1109/SoutheastCon45413.2021.9401881.
10. A. Sridharan and V. Kanchana, "SIEM integration with SOAR", in *Proc. Int. Conf. Futuristic Technol. (INCOFT),* pp. 1–6, 2022.
11. A. Chuvakin, "SIEM: Moving Beyond Compliance", Available at:http://www.securitywarriorconsulting.com /pdfs/chuvakin_RSA_2010_SEIMBC_WP_0810.pdf (Accessed on date: 04 Feb 2018)
12. A. Chuvakin, "Anton Chuvakin Homepage", Available at: http://www.chuvakin.org/. (Accessed on date: 13 Jan 2018)
13. A. Chuvakin, "Why No Open Source SIEM, EVER?", Available at: http://chuvakin.blogspot.co.at/2009/06/why-no-open-sourcesiem-ever.html. (Accessed on date: 13 Jan 2018)
14. Anton Chuvakin, "UEBA Shines Where SIEM Whines?" Available at: https://blogs.gartner.com/anton-chuvakin/2016/11/14/ueba-shines-where-siemwhines/. (Accessed on date: 11 Feb 2018).
15. A. Srivastava, "Mitre Attack Dataset for Knowledge Graph-Enhanced RAG Cyber Threat Intelligence", *IEEE Dataport*, July 13, 2025. doi: 10.21227/9559-9p78.
16. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B, "MITRE ATT&CK: Design and philosophy", Available at: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf (Accessed on date: 2 Jan 2024).

17. Crowd Strike. (2018 a). CrowdStrike Falcon endpoint detection and response (EDR): Streaming the threat detection and response lifecycle with speed, automation and unrivaled visibility. Available at: https://www.crowdstrike.com/wp-content/brochures/Falcon-Insight-DS-PW-edits.pdf (Accessed on date: 2 Feb 2024).
18. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2)*. Available at: https://csrc.nist.gov/pubs/sp/800/61/r2/final (Accessed on date: 3 April 2025).
19. Clarke, M., & Martin, K. Managing cybersecurity risk in healthcare settings. In *Healthcare Management Forum*, pp. 17-20, 2024.
20. The MITRE Corporation, "CAPEC - Common Attack Pattern Enumeration and Classification," *MITRE*, n.d. Available at: https://capec.mitre.org. (Accessed on date: 28-Aug-2025).
21. C. H. Chi, S. Y. Ooi, E. H. Binti, Y. H. Pang, M. K. B. A. Yan, and K. I. B. Sidin, "Intelligent-based SIEM security email alert", in *2023 11th International Conference on Information and Communication Technology (ICoICT),* pp. 481-486, 2023
22. David Brumley, Newso James, Dawn Song, Hao Wang, and Somesh Jha. Towards automatic generation of vulnerability-based signatures. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pp 2–16, 2006.
23. Dong, S., Su, H., Hou, R., & Shankar, A. "Improved PBFT Consensus Mechanism Based on Voting Sort Clustering Partition With Group Signature for IoT." *IEEE Transactions on Intelligent Transportation Systems* (2024).
24. Cynet, "EDR security and protection for the enterprise," *Cynet*, 2019. Available at: https://www.cynet.com/platform/threat-protection/edr-endpoint. (Accessed on date: 29 Sep 2019).
25. Ziften Technologies, "Endpoint security in today's threat environment," *Ziften Technologies*, White Paper, 2019. Available at: ziften.com. [Accessed on date: 4 Jun 2026).
26. Ewoh, P., & Vartiainen, T. "Vulnerability to cyberattacks and sociotechnical solutions for healthcare systems: systematic review". *Journal of medical Internet research*, 26, e46904, 2024.
27. Forum, W.E. "Wild Wide Web Consequences of Digital Fragmentation", Available at: https://reports.weforum.org/globalrisks-report-2020/wild-wide-web/(Accessed on date: 8 July 2021).
28. Gartner Peer Insights, "Endpoint detection and response solutions market," *Gartner*, 2019. Available at: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions. (Accessed on date: 04-Jun-2026).
29. GEORGE, D. A. S., George, A. H., Baskar, T., & Pandey, D, "XDR: The Evolution of Endpoint Security Solutions-Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future." *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* 8.(1): 493–501, 2021.
30. George, A. Shaji, et al. "Extending detection and response: how MXDR evolves cybersecurity." *Partners Universal International Innovation Journal*, 1(4): 268–285, 2023.
31. G. González-Granadillo, M. Faiella, I. Medeiros, R. Azevedo, and S. González-Zarzosa, "ETIP: An enriched threat intelligence platform for improving OSINT correlation, analysis, visualization and sharing capabilities", *Journal of Information Security and Applications*, *58*, 102715, 2021.
32. George, A. S., Sagayarajan, S., Baskar, T., & George, A. H. "Extending detection and response: how MXDR evolves cybersecurity." *Partners Universal International Innovation Journal*, 1.(4): 268–285, 2023.
33. H. Gonaygunta, G. S. Nadella, P. P. Pawar, and D. Kumar, "Study on Empowering Cyber Security by Using Adaptive Machine Learning Methods", in *2024 Systems and Information Engineering Design Symposium (SIEDS)*, 166-171, 2024. DOI: 10.1109/sieds61124.2024.10534694.

34. H. J. Ofte and S. Katsikas, “Understanding situation awareness in SOCs, a systematic literature review”, *Computers & Security,* 126, 103069, 2023.
35. Jing LI, Xutao LU, Feng LIU, Xiangquan HUANG, He LIN, and Yifeng REN. “Research on power internet of things model and resource allocation based on edge computing”. In: *U.P.B. Sci. Bull*. Series C, 85 (1), pp. 105–116, 2023.
36. J. C. Haass, “Cyber threat intelligence and machine learning”, *IEEE Xplore*, vol. 2, no. 1, pp. 156–159, 2022.
37. J. Kinyua and L. Awuah, “AI/ML in security orchestration, automation and response: Future research directions”, *Intell. Autom. Soft Comput*., vol. 28, no. 2, pp. 527–545, 2021.
38. K. Prabu and P. Sudhakar, “An automated intrusion detection and prevention model for enhanced network security and threat assessment”, *Int. J. Comput. Netw. Appl.*, vol. 10, no. 4, p. 621,. 2023.
39. Lima, Sidney ML, et al “Next generation antivirus endowed with bitwise morphological extreme learning machines.” *Microprocessors and Microsystems*, 81 103724, 2021.
40. L. Gudala, M. Shaik, and S. Venkataramanan, “Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An exploration of real-time anomaly identification and adaptive mitigation strategies”, *J. Artif. Intell. Res.*, vol. 1, no. 2, pp. 19–45, 2021.
41. McShane, I., Firstbrook, P., & Ouellet, E. (2017).”*Redefining endpoint protection for 2017 and 2018 (ID G00337106)”*. Available at: https://www.gartner.com/doc/reprints?id=1-4MO1GFS&ct=171221&st=sb.(Accessed on date:26 May 2026)
42. Mario Aragones Lozano, Israel Pérez Llopis, Alfonso Climente Alarcón, and Manuel Esteve Domingo. “A Machine Learning-Driven Threat Hunting Architecture for Protecting Critical Infrastructures”. In: *2023 19th International Conference on the Design of Reliable Communication Networks (DRCN)*, pp. 1–5, 2023.
43. Wurzenberger, M., Höld, G., Landauer, M., & Skopik, F. Analysis of statistical properties of variables in log data for advanced anomaly detection in cyber security: Computers *& Security*, *137*, 103631, 2023.
44. M. N. Hossain, S. M. Milajerdi, J. Wang, B. Eshete, R. Gjomemo, R. Sekar, S. D. Stoller, and V. Venkatakrishnan, “SLEUTH: Real-time attack scenario reconstruction from COTS audit data”, in *26th USENIX Security Symposium (USENIX Security 17),* 487–504, 2017.
45. Murali, Ritwik, and C. Shunmuga Velayutham. “Adapting novelty towards generating antigens for antivirus systems.” In *Proceedings of the Genetic and Evolutionary Computation Conference*. pp. 1254–1262, 2022.
46. “New Research from Advanced Threat Analytics Finds MSSP Incident Responders Overwhelmed by False-Positive Security Alerts”, Available at: https://prn.to/2uTiaK6, 2019. (Accessed on date: 12 Feb 2028)
47. N. Afzaliseresht, Y. Miao, S. Michalska, Q. Liu, and H. Wang, “From logs to stories: human-centred data mining for cyber threat intelligence”, *IEEE Access*, 8, 19089–19099, 2020.
48. J. Oltsik, “Security operations challenges, priorities, and strategies,” ESG, Research Report, 2017. Available at: siemplify.co. (Accessed date: 8 July 2021).
49. Ö. Sen, D. van der Velde, K. A. Wehrmeister, I. Hacker, M. Henze, and M. Andres, “On using contextual correlation to detect multi-stage cyber-attacks in smart grids”, *Sustainable Energy, Grids and Networks*, 32, 100821, 2022.
50. Puspita Dash, Balaji S, Ragul S, Sriram S, 2024. AI Enhanced Anomaly Detection of System logs in Cyber Security, In *2024 International Conference on System, Computation, Automation and Networking (ICSCAN)* , pp. 1-6, 2024.
51. P. Alaeifar, S. Pal, Z. Jadidi, M. Hussain, and E. Foo, “Current approaches and future directions for cyber threat intelligence sharing: A survey”, *Journal of Information Security and Applications*, 83, 103786*,* 2024,
52. Q. Wang, W. U. Hassan, D. Li, K. Jee, X. Yu, K. Zou, J. Rhee, Z. Chen, W. Cheng, C. Gunter, and H. Chen, “You are what you do: Hunting stealthy malware via data provenance analysis”, In *NDSS*, 2020.

53. Razvan Stoleriu, Catalin Negru, Bogdan-Costel Mo-canu, and Florin Pop. “Malicious Short URLs Detection Technique”. In: *2023 22nd RoEduNet Conference: Networking in Education and Research*, pp. 1–6, 2023.
54. Razvan Stoleriu, Catalin Negru, and Dragos Radulescu, “Modern Cyber Security Attacks, Detection Strategies, and Countermeasures Procedures ”. In: *2023 24th International Conference on Control Systems and Computer Science (CSCS)*. 198–205, 2023.
55. R. Kwon, T. Ashley, J. Castleberry, P. McKenzie, and S. N. G. Gourisetti, “Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping”, in *2020 Resilience Week (RWS),* 106–112, 2020.
56. R. Patel, K. Müller, G. Kvirkvelia, J. Smith, and E. Wilson, “Zero trust security architecture raises the future paradigm in information systems”, *Informatica Digit. Insight J.*, 1(1), 24–34, 2024
57. Somil Tyagi, Dr. Rajesh Kumar Tyagi, Dr. Pushan Kumar Dutta, and Dr. Priyanka Dubey. “Next Generation Phishing Detection and Prevention System using Machine Learning ”. In: *2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)*. 1–6, 2023.
58. S. Sharifi, “A Novel Approach to the Behavioural Aspects of Cybersecurity”, *arXiv preprint arXiv:2303.13621*, 2023. doi: 10.13140/RG.2.2.11304.85761
59. S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, “Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities”, *IEEE Access*, 10, pp. 112392–112415, 2022.
60. Soleman, D. and Soewito, B. Information Security System Design Using XDR And EDR. *Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi*, 9 (1), pp. 51–57, 2024.
61. S. Karagiannis, A. Tokatlis, S. Pelekis, M. Kontoulis, G. Doukas, C. Ntanos, and E. Magkos, “A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations: Deploying and Documenting Realistic Cyberattack Scenarios-A Rootkit Case Study”, in *Proceedings of the 25th Pan-Hellenic Conference on Informatics*, 328–333, 2021.
62. S. Caimi, “MITRE ATT&CK: The Magic of Mitigations”, Available at: https://cscoblogs-prod-17bj.appspot.com/security/mitre-attck-the-magic-of-mitigations (Accessed on date: 11 November 2022).
63. Riley, M., Elgin, B., Lawrence, D., & Matlack, C. (2014, March 17). *Missed alarms and 40 million stolen credit card numbers: How Target blew it*. Bloomberg. https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data(Accessed on date: 17 Mar 2014).
64. Osterman Research. (2019, April). *The critical role of endpoint detection and response* (White Paper). SonicWall. https://bit.ly/39NrNwo (Accessed on date: 29 Apr 2019)
65. T.Simonite, “The Antivirus Era Is Over”, Available at: http://www.technologyreview.com/news/428166/the-antivirus-era-is-over, (Accessed on date: 11 Jun 2012)
66. Ben Canner, “5 Critical Use Cases for EDR (Endpoint Detection and Response)”, Available at: https://solutionsreview.com/endpoint-security/5-critical-use-cases-for-edr-endpoint-detection-and-response/ (Accessed on date: 26 May 2021).
67. J.-M. Roberts, “VirusShare,” *VirusShare Malware Repository*, n.d. Available at: https://virusshare.com/. (Accessed on date: 10 Aug 2020)
68. Techopedia, “What is Endpoint Detection and Response (EDR)? - Definition from Techopedia,” *Techopedia*, May 15, 2025. Available at: techopedia.com. (Accessed on date: 15-May-2025).
69. W. U. Hassan, M. A. Noureddine, P. Datta, and A. Bates, “OmegaLog: High-fidelity attack investigation via transparent multi-layer log analysis”, in *NDSS*, 2020.
70. X. Han, T. Pasquier, A. Bates, J. Mickens, and M. Seltzer, “UNICORN: Runtime provenance-based detector for advanced persistent threats”, in *NDSS*, 2020.

71. Y. Shevchenko, “EPP plus EDR: The future of endpoint cybersecurity,” *Kaspersky*, Jun. 30, 2020. Available at: https://www.kaspersky.com/blog/epp-edr-importance/22366/. (Accessed on date: 30-Jun-2020)..
72. Y. Kwon, F. Wang, W. Wang, K. H. Lee, W.-C. Lee, S. Ma, X. Zhang, D. Xu, S. Jha, G. Ciocarlie et al., “MCI: Modelling-based causality inference in audit logging for attack investigation”, In *Network and Distributed Systems Security (NDSS) Symposium*, 2018.
73. Duna, Y. T., Ab Razaka, M. F., Zolkiplib, M. F., Beea, T. F., & Firdausa, A. “Grasp on next-generation security operation center (NGSOC): Comparative study”, *Int. J. Nonlinear Anal. Appl*., 12(2), 867–896, 2021.
74. Z. T. Sworna, C. Islam, and M. A. Babar, “APIRO: A framework for automated security tools API recommendation”, *ACM Trans. Softw. Eng. Methodol*., vol. 32, no. 1, pp. 1–42, 2023.
75. Hassan, A., Rauf, A., Shafqat, N., Latif, R., & Khan, H. “ZenGuard a machine learning-based zero trust framework for context-aware threat mitigation using SIEM, SOAR, and UEBA”. *Scientific Reports*, 15(1), 35871, 2025.
76. J. Doe, "EDR-SIEM Integration”, *IEEE Trans.*, vol. 1, no. 2, pp. 10–20, 2024.
77. Khowaja, S. A., & Patel, M. B. Performance evaluation of open-source endpoint detection and response (EDR) solutions. *IEEE Access*, *10*, 97161-97175, 2022.
78. MITRE Corporation, “MITRE ATT&CK®”, Available at: https://attack.mitre.org/ (Accessed on date: 7 Jan 2026).
79. Check Point Software Technologies – EDR vs SIEM, Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/edr-vs-siem/? , (Accessed on date: 8 Nov 2022).
80. Kasey Cross, SIEM vs EDR. Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/siem-vs-edr/? (Accessed on date: 18 Feb 2026).
81. SentinelOne, Understanding the Difference Between EDR, SIEM, SOAR, and XDR. Available at: https://www.sentinelone.com/cybersecurity-101/xdr/understanding-the-difference-between-edr-siem-soar-and-xdr/? (Accessed on date: 13 Aug 2025).
82. Exabeam, SIEM vs EDR: Key Features, Differences, and How to Choose. Available at: https://www.exabeam.com/explainers/siem/siem-vs-edr-key-features-differences-and-how-to-choose/? (Accessed on date: 24 Oct 2025).
83. ConnectWise, EDR vs SIEM: What’s the Difference and Why Do You Need Both? Available at: https://www.connectwise.com/blog/edr-vs-siem-whats-the-difference-and-why-do-you-need-both (Accessed on date: Mar. 7, 2025).
84. Logpoint, The Difference Between SIEM and EDR (SIEM vs EDR). Available at: https://guardsix.com/blog/the-difference-between-siem-and-edr (Accessed on date: 30 Nov 2022).
85. TechTarget, EDR vs. SIEM: Key differences, benefits and use cases. Available at: https://www.techtarget.com/searchsecurity/tip/EDR-vs-SIEM-Whats-the-difference (Accessed on date: 24 Oct 2024).
86. SentinelOne, “Endpoint protection,” *SentinelOne*, n.d. Available at: https://www.sentinelone.com/lp/endpointprotection/. (Accessed on date: 4 Jun 2026).
87. Huntress, SIEM vs. EDR vs. MDR: What's the Difference? Available at: https://www.huntress.com/cybersecurity-education/siem-vs-edr-vs-mdr(Accessed on date: 16 Apr 2024).
88. Exabeam, Five Key Ways to Navigate XDR, EDR, NDR, and SIEM for Effective Cybersecurity. Available at: https://www.exabeam.com/resources/guides/five-key-ways-to-navigate-xdr-edr-ndr-and-siem-for-effective-cybersecurity/ (Accessed on date: 1 Nov 2024).

89. T. H. Hai, V. Van Thieu, T. T. Duong, H. H. Nguyen and E. -N. Huh, "A Proposed New Endpoint Detection and Response With Image-Based Malware Detection System," *IEEE Access*, vol. 11, pp. 122859-122875, 2023, doi: 10.1109/ACCESS.2023.3329112.

90. ManageEngine, "Endpoint Security," Available at: https://www.manageengine.com/products/desktop-central/endpoint-central-endpoint-security.html?network=g&device=c&keyword=edr&campaignid=8901901565 (accessed on date: 30 Oct 2025).

91. Kaur, H., Sanjaiy SL, D., Paul, T., Kumar Thakur, R., Kumar Reddy, K. V., Mahato, J., & Naveen, K. "Evolution of endpoint detection and response (EDR) in cyber security: A comprehensive review." *E3S Web of Conferences*. Vol. 556. 01006, 2024. DOI: https://doi.org/10.1051/e3sconf/202455601006

92. Kamruzzaman, A., Ismat, S., Brickley, J. CEDR., Liu, A., & Thakur, K., "A comprehensive review of endpoint security: Threats and defenses." In *2022 International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1–7, 2022.

93. Universitas Dr. Soetomo Surabaya, Inform: Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi, Available at: https://garuda.kemdiktisaintek.go.id/journal/view/10419?issue=Vol.%2010%20No.%201%20(2025) (Accessed on date: 30 Oct 2025).

94. Park, S. H., Yun, S. W., Jeon, S. E., Park, N. E., Shim, H. Y., Lee, Y. R., ... & Lee, I. G. "Performance evaluation of open-source endpoint detection and response combining Google Rapid Response and osquery for threat detection." *IEEE Access* 10, 20259-20269, 2022.

95. SentinelOne, "EDR vs. NDR vs. XDR: How to Pick a Detection Response Solution",. https://www.sentinelone.com/cybersecurity-101/endpoint-security/edr-vs-ndr-vs-xdr/ (Accessed on date: 5 Jun 2026).

96. Palo Alto Networks, "What Is the Difference Between EDR vs SIEM?" Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-edr-vs-siem (Accessed on date: 7 Mar 2025).

97. A. Chuvakin, "Anton Chuvakin Homepage," *chuvakin.org*. https://www.chuvakin.org/ (accessed Aug. 29, 2024).

98. ManageEngine, "Endpoint Security," *ManageEngine Endpoint Central*. Available at: https://www.manageengine.com/products/desktop-central/endpoint-security/ (Accessed on date: 17 Mar 2026).

99. Microsoft, "Phase 2 NGAV Integration Guide", Available at: https://www.microsoft.com/ (Accessed on date: 9 Jan 2024).

100. A. Chuvakin and G. Peterson, "Logging in the Age of Web Services", *IEEE Security & Privacy*, vol. 7, no. 3, pp. 82–85, 2009.

101. C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to Cyber Threat Information Sharing", Available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf. (Accessed on date: 9 Jan 2024).

102. S. M. Lima, D. M. Souza, R. P. Pinheiro, S. H. Silva, P. G. Lopes, R. D. de Lima, and W. P. dos Santos, "Next-generation antivirus endowed with bitwise morphological extreme learning machines," *Microprocessors and Microsystems*, vol. 81, p. 103724, 2021, doi: 10.1016/j.micpro.2020.103724.

103. Nanang, H., Hayadi, B. H., Sukmana, H. T., Durahman, Y., Arifin, V., & Azhari, M. "The importance of Security Risk and Protection in Education Systems: A study of the Extended Detection and Response (XDR)

Method in Data Security". In *2024 Ninth International Conference on Informatics and Computing (ICIC)*, pp. 1–4. 2024.

104. Gilad David Maayan, "Machine Learning and Artificial Intelligence (AI/ML): The Secret Sauce Behind XDR", Available at: https://www.computer.org/publications/tech-news/trends/the-secret-sauce-behind-xdr (Accessed on date: 12 Apr 2023).
105. Vijay Kanade, "What Is Extended Detection and Response (XDR)? Definition, Components, Advantages, and Best Practices", Available at: https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-xdr (Accessed on date: 18 Jan 2024).
106. Gilad David Maayan, "Machine Learning and Artificial Intelligence (AI/ML): The Secret Sauce Behind XDR", Available at: https://www.computer.org/publications/tech-news/trends/the-secret-sauce-behind-xdr (Accessed on date: 12 Apr 2023).
107. Vijay Kanade, "What Is Extended Detection and Response (XDR)? Definition, Components, Advantages, and Best Practices", Available at: https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-xdr (Accessed on date: 18 Jan 2024).