Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 1, 2026

TRENDS, CAPABILITIES, AND CHALLENGES IN MODERN CYBER DEFENSE: A SYSTEMATIC REVIEW OF DETECTION AND RESPONSE TECHNOLOGIES

Attaullah[*1], Ali Sufyan[2], Muhammad Mujeeb-Ur-Rehman[3], Bushra Noreen[4], Sundas Amin[5]

*[*1,2,3,4]Department of Information and Communication Engineering, The Islamia University of Bahawalpur, Pakistan*
[5]Department of Information Security, The Islamia University of Bahawalpur, Pakistan

[*1]attaullah.wazir.cybersec@gmail.com

DOI: https://doi.org/10.5281/zenodo.18346067

Keywords
EDR, XDR, threat detection, incident response, cybersecurity

Article History
Received: 28 November 2025
Accepted: 08 January 2026
Published: 23 January 2026

Corresponding Author: *
Attaullah

Abstract

Cybersecurity has mainly shifted from alerting intrusion to advance detecting and response security solutions over the last 10 years. This article provides a comprehensive review of four major technology solutions that are the backbones of modern-day security operations. Including Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Extended Detection and Response (XDR), and Managed Detection and Response (MDR). It also discusses the use of Security Orchestration, Automation and Response *(SOAR) tools, which represent responses among these technologies. This analysis is conducted based on various materials published during 2021- 2025 including academic articles, industry white papers, technical documents and testing resources. It takes a look at how each technology help in threat detection and incident response. Our findings bring out the conclusion that the central success factor in detection and response is not related to the sophistication or advancement of tools or the level of investment but rather it is the unified integration of various technologies. Effective integration, which is complemented by balanced automation combined with human expertise, and clear measurement frameworks which is the key to achieving successful security operations. This evidence indicates that successful detection and response systems have a common characteristic regardless of hardware. They have an emphasis on data quality, normalizing and know that a good analysis depends on good data and more outcome-based criteria rather than focusing on the number of tools in the hopes of better security overall. They also realize that technology is not a solutions for challenges related to people and processes. This paper provides a review of the architecture, detection methods, response mechanisms, the operational needs and limitations of each technology. It also cover seven integration patterns, industry issues, and areas where further research is required. Over the years, the detection and response capability has evolved from a simple implementation of tools to a flexible and intelligence-based detection capability. This represents an evolution, and there also remains a need to adapt to the changing models of business, threat environment, and laws.*

I. INTRODUCTION

Modern cybersecurity detection and response systems remain to face severe challenges, as evidenced by the fact that, despite record-breaking financial investments, data breaches are occurring more frequently and faster than ever before. In the first half of 2024 alone, industry research recorded a 14% increase in breaches, compromising the personal information of over 1.07 billion individuals **[1].** The core of the problem lies not in a lack of available technology but in how these tools are launched and used within an organizational context. A common modern threat involves attackers exploiting a single cloud misconfiguration

to bypass security protocols and access sensitive data within minutes, illustrating the high stakes for both personal privacy and professional integrity. The threat landscape has shifted; attackers no longer rely solely on traditional software "bugs" but instead target the "weak links" in a company's structure. Today, over half of all breaches involve stolen or misused credentials **[2]**, and 60% of cloud-related incidents are caused by companies struggling to secure rapidly expanding digital environments **[3].** The attackers are increasingly hiding their malicious activity within encrypted web traffic, making it nearly impossible for traditional inspection tools to distinguish threats from legitimate communications **[4].** A critical failure in modern defense is the "dwell time," the gap between a hacker entering a system and being caught. Recent reports indicate that in 2024, the time it took to discover and report breaches actually increased, giving attackers a long window to steal data **[5-6]**. This gap is often framed as an "hours-until-harm" countdown. While modern security experts accept that breaches are inevitable, the focus has shifted toward building resilience and ensuring rapid detection to minimize damage **[7].** However, achieving this is difficult due to limited budgets, massive attack surfaces, and the increasing sophistication of threat actors [8]. Successful detection requires collecting and "normalizing" telemetry from various sources, such as laptops, networks, and cloud apps, a process often plagued by mismatches in data formats **[9-10].** The responsibilities must be clearly defined: security analysts must focus on monitoring alerts, while technical leads ensure that data from all platforms is accurate and integrated **[11-12].** The ultimate goal is a delicate balancing act, stopping threats quickly without interrupting essential business operations **[13].** As we look toward the future, organizations must develop new strategies to combat threats powered by Artificial Intelligence (AI), moving from a reactive mindset to an innovative, proactive defense **[14].** The industry uses several specialized technologies, primarily EDR, NDR, XDR, and MDR, supported by SOAR platforms. Endpoint Detection and Response (EDR) acts like a digital security guard on individual devices, monitoring for suspicious file changes or "fileless" malware that traditional antivirus programs miss **[15].** While EDR is vital, its success depends heavily on the training of human analysts, and it cannot detect "unmanaged" devices such as smart office hardware or guest networks **[16-17].** The Network Detection and Response (NDR) fills this gap by watching the "pipes" that carry data, looking for hackers moving between systems, though it often struggles with encrypted traffic and privacy concerns **[18].** The Extended Detection and Response (XDR) serves as a unifying platform that combines data from endpoints, networks, and cloud accounts into one analytic framework, though it requires significant data engineering to set up correctly **[19].** The organizations that lack their own experts, Managed Detection and Response (MDR) offers 24/7 monitoring from external specialists, providing necessary human expertise but creating a dependency on outside vendors **[20-21].** the Security Orchestration, Automation Response (SOAR) tools help coordinate these products, automating simple response tasks so they can be handled at scale **[22].** The SOAR requires careful management to prevent automated actions from accidentally shutting down legitimate business activities **[23].** The authors synthesize recent academic and industry research in this work, drawing upon over 200 peer-reviewed publications from IEEE Xplore and Elsevier, along with real-world technical reports, in order to bridge the gap between theoretical research and practical security operations.

The primary objectives of this paper are as follows:

- To analyze detection and response technologies holistically, emphasizing how EDR, NDR, XDR, MDR, and SOAR operate collectively within modern cyber defense strategies rather than as isolated security tools.
- To examine the evolution of cyber defense mechanisms, tracing the transition from traditional signature-based antivirus solutions to advanced behavioral analytics and intelligent detection systems.
- To assess modern cyber threats, including ransomware, supply chain attacks, and advanced persistent threats, and evaluate how contemporary detection and response technologies address these challenges.
- To provide a technical review of key detection and response platforms, offering an in-depth analysis of EDR, NDR, XDR, and MDR architectures, followed by an overview of SOAR platforms and their role in security automation and orchestration.
- To investigate emerging trends in cyber defense, such as the integration of Explainable Artificial

Intelligence (XAI) for real-time threat detection and improved analyst decision-making.

Furthermore, we proposed actionable recommendations for enhancing Security Operations Centers (SOCs), focusing on improving detection accuracy, response speed, and operational efficiency in the face of high-velocity cyber threats. Finally, legal, regulatory, and economic factors influencing organizational investment decisions in detection and response technologies are systematically evaluated.

The rest of the article is categorized as follows, In Section 2 the history of detection and response technologies walking through the transformation of signature based antivirus into behavioral analytics and cross domain correlation is described. Section 3, provides an analysis of the current threat landscape consisting of ransomware operations, supply chain attacks, and identity abuse, which defines modern detection needs. Sections 4 shows the depth analysis of EDR, NDR, XDR, and MDR inculcating technical architectures, detection approaches, advantages , overview of SOAR platforms and their role in orchestration of response. Section 6 shows recent trends in analytical methods such as: application of explainable and lightweight AI frameworks for real-time threat detection in the edge networks. Finally, the article is concluded in Section 7.

II. Historical Evolution and Market Context

The modern detection and responses (D&R) technology, it is necessary to trace it back to the period of its evolution out of the previous security strategies. Antivirus programs are signature-based technology, and have been lead in the world of cybersecurity since decades. With that model of operation, it was considered as being a fairly easy and foreseeable task. Security vendors would extract signatures as a unique set of bytes then they would distribute them to customers using this as a malicious code. The methods were rather effective in the case when the malware was not updated and the threat environment changed gradually [24-25]. The middle of 2000s, opponents had become more flexible. The use of static signature matching was not useful in polymorphic malware that alters its appearance every time it infects a computer but does not affect functionality [26]. The Obfuscation and packing made it even harder to detect because it hidden the presence of malicious executables in the files that appeared harmless [27]. It is important to note that attackers started employing the living-off-the-land (LoTL) types of attacks to take advantage of the legitimate system tools of the victim, including the use of PowerShell or Windows Management Instrumentation (WMI) against the victim [28]. The attacks would not be identified by signature based systems since the tools themselves were not harmful, their forms of application and situations were problematic. This is the great efforts in terms of the fact that file-based detection methods were not good enough to deal with the new threat landscape [29]. The security community retaliated with heuristic detection that finds patterns of interest and API calls of what is deemed as problematic and sandboxing [30]. The isolates suspicious files to monitor behavior within controlled environments [31]. The technologies were still file-level in spite of such advancements. Attacks based on memory and scripts made no impact on the detection systems and so did slow based attacks that are formed with time thanks to individually harmless attacks [32]. This prompted the development of the fact that there was a need to have holistic level of monitoring of the runtime system.

2.1 The Endpoint Detection and Response (EDR)

The term EDR was coined to a formalized category in around 2013 by Gartner [33], yet it had preceding concepts of shifting away from signatures as a form of process execution, file access, and registry changes, which were considered predecessors of it. The imperative innovation was not seemed to end with the gathering of the data, but also the capability of searching the telemetry changed incident investigation [34]. The security teams were than able to review endpoint activity and analyze whole fleets of devices retrospectively and recreate a timeline of the attack. Nevertheless, the initial EDRs were characterized by major drawbacks. These systems produced huge amount of data in the form of telemetry which demanded huge storage and processing facilities. The ability to differentiate between signal and noise demanded analysts having strong knowledge in the working of the internal components of the operating systems, which is also not very common in the international job market [35]. There was also the issue of performance impact whereby the performance of kernel level agents was between 10 and 50 percent with respect to Central Processing Unit (CPU) and

memory [36]. These challenges did not hinder EDR because it was able to detect file less malware and scripts attacks relying on the PowerShell or JavaScript in real time [37]. The current EDR has evolved into advanced behavioral analytics systems, which use machine learning and threat intelligence [28].

2.2 Network Detection and Response (NDR)

In 1980s, the network based detection was invented with intrusion detection systems (IDS) being created and compared traffic patterns with attack databases [38]. The intrusion prevention systems (IPS) subsequently gained automatic traffic blocking capability [39]. Most particular paradigms were challenged by the 2010s. To begin with, encryption was everywhere; in 2024, encrypted web traffic comprised more than 85 percent of the total web traffic, and it would be challenging to analyze deep packet inspection (DPI) without controversial decryption techniques. Second, attackers got to understand how to conceal themselves in a regular traffic. Data leakage may be made up of a high number of small transfers that are not considered as a leakage [40]. The solution to the industry was NDR. Behavioral analytics is used instead of signature based searching in NDR platforms to determine the baselines and signal anomalies. They use metadata such as Domain Name System (DNS) queries, Transport Layer Security (TLS) handshakes, and flow statistics which allow it to scale its analysis process even with the increase in bandwidth [41]. They pay specific attention to lateral movement of data, data exfiltration, and command and control communications which may avoid endpoint only controls. To understand complete history of Detection technologies Table. 1, show the era and evaluation of different detection and response solutions.

Table I: Historical Evolution of Cybersecurity Detection Technologies

Ref.	Era	Methods	Strengths	Limitations
[39]	Antivirus (AV) (1990s)	Matches known signatures.	Fast & lightweight.	Misses zero-day threats.
[42]	Heuristic AV (2000s)	Scans suspicious code.	Finds malware variants.	High false alarms.
[33]	EDR (2013)	Tracks endpoint behavior.	Detects file less attacks.	Causes alert fatigue.
[43]	NDR (2016)	Analyzes network traffic.	Covers IoT devices.	Weak vs. encryption.
[44]	XDR (2019)	Correlates stack data.	Unified view, less noise.	Complex setup.
[24]	MDR / SOAR (2023)	AI-driven automation.	Instant 24/7 response.	High cost.

2.3 Extended Detection and Response (XDR)

Towards the end of the 2010s, security teams entered a crisis of operation that would make it leading to the creation of XDR platforms. The EDR systems were producing thousands of alerts every day as a result of endpoint telemetry. The alerts that were introduced into NDR systems by network monitoring added thousands. SIEM systems are systems of aggregation which take dozens of sources logs, generating more alert streams. Each of the email security platform, identity systems, and cloud security tools had an independent signal [45] [46]. The XDR marketplace was rapidly divided into two architectural solutions that depicted alternative organizational values. Native XDR have created unified communities out of their respective security commodities assortments. These implementations take advantage of being tightly integrated, sharing data models as well as having single management interfaces which make the operations easy. Nevertheless, they introduce vendor lock-in which could restrict the ability to change the choice of tools and could also escalate costs in the long run [47]. The vendors of Open XDR created aggregation layers, which accept telemetry of various third-party products through APIs. These platforms are more flexible, and they will harness the investments that an organization has made without necessarily having to ripe and replace functional tools. Nevertheless, large scale incident correlation as described by current technical literature necessitates a significant data engineering

effort to normalize telemetry across a variety of sources and build meaningful correlations between proprietary formats as Open XDR normally implies **[48]**. According to the Market Guide of the Extended Detection and Response given by Gartner, XDR performance is influenced less by the approach to the architecture than by the quality of the data used and the level of operational maturity of the organization where it is applied **[49]**.

2.4 anaged Detection and Response (MDR)

The Managed Detection and Response (MDR) did not have the same underlying motivation as other detection technologies do. Whereas EDR, NDR and XDR operate within technical constraints, MDR acts within a long-term human resource dilemma the lack of skilled security specialists who can successfully execute advanced detection platforms. Most of the institutions that are outstanding financially to purchase more developed XDR are dominated by the lack of internal expertise to run them. Incident investigation and threat hunting are tasks that need profound experience which only takes years to build, and there is stiff competition on such talent **[50]**. They provide detection platforms on behalf of client organizations and give nonstop watch by skilled analysts, proactive threat searching, and coordinated reaction to the incident. The growth of the MDR market has been recent as organizations are coming to realize that proper security needs 24/7 watch which at times is not economically viable to develop internally **[51].** The rate of adoption has now quickened and especially for mid-market organizations experiencing an enterprise level threat, but who do not have the ability to invest in full internal SOC **[52]**. Nevertheless, MDR has additional factors to be taken into account that off-premises technology does not have. Sensitive telemetry should be shared with external providers in organizations, which concerns the issue of data sovereignty. Moreover, the Dell technologies ESG showcase underlines the idea that service levels and contractual escalation procedures can be defined without any clear contractual descriptions to avoid strategic dependency situations **[53].**

2.5 Security Orchestration, Automation and Response (SOAR)

When organizations implemented EDR, NDR, and XDR, another problem was achieved: this was necessary to organize the response actions in different tools effectively. In the case of the detection of a threat, it may be necessary to have a good containment process that involves isolating endpoints, blocking network traffic, disabling user accounts, and quarantining emails at the same time. The same processes are time consuming and prone to error in case they are executed manually during high pressure incidents **[54]**. In high confidence detection, SOAR will also be able to initiate containment actions across various domains automatically. The SOAR helps the analysts in the case of lower confidence detection to automate evidence collection and enrichment in order to spend their time on decision-making instead of repeating tasks **[55].** The SOAR acknowledges that technology is not enough and that organizations would require operation processes operationalized in executing codes. Nonetheless, it has issues during implementation. The development of playbooks involves profound knowledge on business processes because excessive automation may ruin the legitimate business processes. Most importantly, SOAR is helpless to compensate bad quality of detection, in case the systems that provide information upstream generate false positives, the response company that is orchestrated will be equally useless **[56].**

2.6 Consolidation of Markets and the Standards.

The Detection and response market has undergone a high level of consolidation, redefining the competitive trends. Acquisitions like the one of VMware of Carbon black **[57]** and Broadcom acquiring the enterprise security business of Symantec demonstrate the importance of integration platforms. This merger competes with smaller suppliers, but entails possible solutions of more unified product line to its consumers **[58].** At the same time, standards have risen and are community based in an effort to enhance interoperability. The OCSF which had been launched in 2022 offers security telemetry data model in a vendor neutral data format. Likewise, the MITRE ATT &CK has been widely used as a universal language to describe adversary tactics and techniques, organizations can do systematic evaluation to detect coverage **[59].** Nonetheless, the use of proprietary interfaces still prevails among several vendors, which creates a tension between vendor when differentiated and the need of the customers to have a smooth integration **[60].**

3. contemporary threat landscape

The understanding of detection and response technologies, it is necessary to analyze the threat that these technologies deal with. This part examines key threat articles that accelerate necessities of sophisticated detection capacities in view of danger intelligence data through industry news, scholarly examination and security vendor's studies.

3.1 Ransomware Evolution and Double Extortion

The category of threat that is the most disruptive against organizations in all industries nowadays is ransomware. Initial cases of ransomware would merely encrypt the files and ask to decrypt these files using money. The contemporary ransomware activities have already become significantly more developed business models that shift radically in the detection and response needs **[61]**. The introduction of the so-called practices of double extortion is an important development in the work of ransomware. In the latest moves, attackers steal sensitive data and encrypt the systems and proceed to threaten to release the stolen data to any company that does not pay ransom. This gives victims two distinct considerations: that the short-term operational interference created by encrypted systems, as well as potential reputational damage, regulatory fines and competitive losses created by data loss. As a result, determining data exfiltration is as serious as determining encryption occurrence and organizations have to track on unusual data transfers that may show theft is in progress **[62].** The velocity of Ransomware attacks has also increase tremendously. According to threat intelligence, many ransomware variants are taking less than twenty-four hours as the median time of initial access to pervasive encrypted state, and some advanced activities are finishing attacks in less than four hours [63]. This reduced available time renders detection and control urgency. Companies which have not identified and detected within hours of initial compromise have high chances of major damage to operations and loss of information. The ransomware-as-a-service (RAAS) has reduced barricades to entry, as comparatively inept individuals organize operations utilizing toolkits and facilities offered by additional proficient threat agents. This democratization of the ability implies that all organizations can be ransomed by different enemies of different degrees of sophistication. The detection systems must also reuse opportunistic campaigns by less competent actors by not just detecting highly sophisticated attacks but also using commodity tools **[64].**

3.2 Supply Chain Compromises

The Supply chain attacks use software vendors and other managed service providers to access downstream customers on transitive basis. The case of Solar Winds, Kasey and the attacks of the vulnerabilities on the popular software packages show that supply chain compromise can impact thousands of organizations at the same time because of one successful intrusion **[65].** In recent threat intelligence counts many supply chain campaigns which have had long periods of detection, using the trust relationship that organizations need to have with the providers of technology. The attackers leak lawful software update features to perform malicious code delivery, leverage on trusted connections between controlled service provision and their consumer, or exploit on an extensive open-source component to impact all subsequently consumers **[66].** The supply chain compromises can only be detected through correlating several types of signals, which may not seem suspicious on their own. The update of the software should be a normal process, whereas any update that poses unwanted behaviors, or sets up of abnormal network connections, may be an indicator of compromise. These detection methods should then include combination of software bill of materials (SBOM) analysis, validation of code-signing certificates, post-update behavioral monitoring to identify abnormal activity, and being correlated with threat intelligence regarding known supply chain operations. It is the cross-domain correlation that can be seen as the kind of complex analysis that XDR platforms will facilitate **[67].**

3.3 Cloud and Identity Centric Attacks

As there has been an increase in the adoption of clouds, the nature of attack surfaces and threat models have changed. The industry analysis of recent studies conducted has shown that sixty percent of attacks against cloud security are due to misconfigurations, and 70 percent are attacks on credentials, not attacks on the zero day attacks on cloud platforms **[68]**. Hackers can use excessive permissive identity and access control policies, unsecured storage buckets where sensitive data are stored and images that have vulnerabilities as entry points as well as launching points. They misuse

authorized cloud management APIs to perform reconnaissance and achieve persistence, and steal information by the means seemingly identical to authorized administrative operations **[69].** Identity has actually been put in place as the new network perimeter. By 2025, security reports reveal more than fifty percent of data breaches were committed using compromised credentials and allowed attackers to go around network security mitigations completely, since straight into genuine users **[70]**. Cybercriminals use lax authentication procedures, password sharing across services and older authentication protocol that are not multi-factor authentication. To access and remain in the system, they exploit OAuth consent flows, password reset processes as well as session hijacking brings **[71]**. The detection of cloud and identity-based attacks needs to be performed with the help of correlating conditionality system to access, privileged access administration platforms, and SaaS application audit logs as well as endpoint and network indicators. The organizations should identify the abnormal patterns of login, suspicious privilege usage, and unusual access to confidential resources to be aware of the fact that the attackers to use valid credentials will not introduce network intrusion detection signatures and endpoint malware events**.** Fig. 1, shows the modern kill chain of detection in modern cybersecurity **[72].**

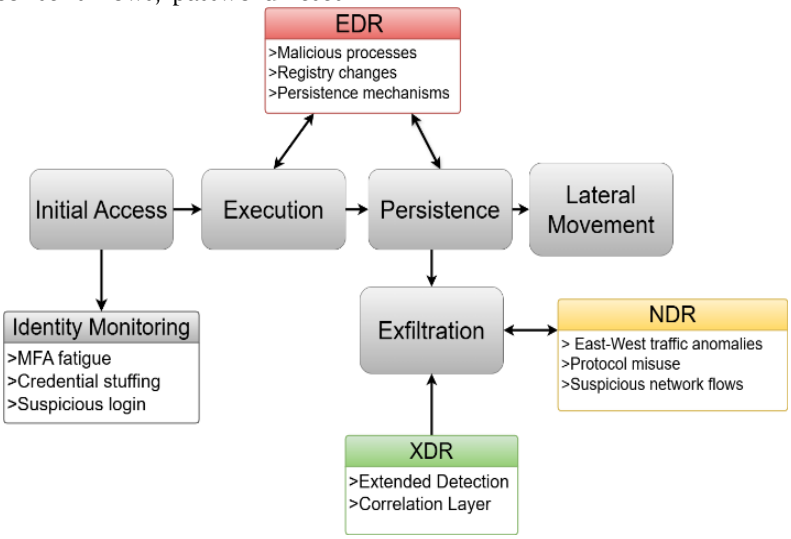


Figure 1: Modern Attack Kill Chain with Detection Points

3.4 Operational Technology and Critical Infrastructure Threats

The Critical Infrastructure Threats (ICS) and Operational Technology (OT) networks have their own security issues and are becoming the targets of threat actors. In contrast to IT settings, most of the OT environment uses legacy systems which are incapable of running updated security agents. Also, IT and OT network segmentations are not always fully installed, and the safety requirements can also be why no active response measures are implemented that might interfere with the physical processes **[73].** According to recent threat landscape reports, there has been increased reconnaissance in the industrial systems. As an example, with a set of probing raids in August 2025, Microsoft Remote Desktop Services was targeted, and a massive count of malicious IPs was used to reconstruct valid usernames, which is a precursor to use credential-based attacks on OT gateways **[74].** The effects of OT compromise do not end with data theft as additional opportunities may include physical damage, environmental risk, and harm to staff personnel **[47]**. The NDR platforms that have deep packet inspection tools to identify industrial protocols have become mandatory to deal with these risks. They are utilized in enabling organizations to identify unauthorized commands and abnormalities within the systems where end-point agents are not deployed **[75].**

3.5 Artificial Intelligence Attacks

The generation of AI capabilities has introduced new attack methods that the detection systems now have to deal with. LLMs have the ability to produce highly convincing phishing mails targeted at the individual and generate malicious code which have natural-language instruction together with automating the social engineering in a previously overlooked scale **[76].** Although, AI makes

defensive actions more strengthened but its offensive use is evolving faster, and detection systems that detect chamber statistical changes or established patterns of attacks cannot cope with it [77]. Some of the campaigns involving AI-generated content are also discussed in the threat intelligence of 2025. It is particularly important to note that the deep fake technology has been exploited in business email swindling scams, whichever party may be an attacker, may use AI-cloned audio to duplicate the voice of an executive to approve fraudulent transactions. Also, the automated strategies are currently used to create a phishing site that has a legitimate appearance of web-based content and this makes it difficult to detect by a human user and respective URL filters [78]. In order to detect machine-generated content and minor behavioral signs of automated attack tools the detection systems need to change with the improvement of AIs [79].

3.6 Figure of threat driver as regulatory compliance.

The Regulatory demands act as not a technical threat though, and the implementation of detection and response technologies is increasingly being pushed by regulatory demands. The cybersecurity disclosure regulations of the U.S. Securities and Exchange Commission and DORA regulations of the European Union require real-time monitoring, and resilience testing [80]. The Compliance has come to be more than a ordinary check-box worth. The current research on the issue of algorithmic compliance requires the implementation of processes to enable continuous monitoring and response processes that could be audited, as reported in the recent research on the issue of algorithmic compliance. This involves making sure the output of AI tools in security applications always complies with the policies, and the source of documents is verified [81]. The NSE procedures should be written down and periodically put to test to ensure that they satisfy requirements such as the ACSC Essential Eight [82]. The Regulatory reviews are becoming more concerned with operational effectiveness as opposite to the presence of technology. The current CISA International Strategic Plan 2025 to 2026 dwells on the importance of organizations maturing their detection potentials in order to safeguard the critical infrastructure dependences of the world. This moves the market away in the direction exploring the buying of the tools to illustrating quantifiable reduction in risk and resilience in operations [83].

4. Detection and Response Technologies

This section reviews key detection and response technologies, including EDR, NDR, MDR, XDR, and SOAR, and their roles in modern cybersecurity architectures. EDR and NDR deliver focused visibility at the endpoint and network levels, while MDR enhances these capabilities through managed expertise. XDR integrates security data across multiple domains to enable correlated threat detection, and SOAR automates and coordinates response actions. Collectively, these technologies provide a unified, efficient, and scalable approach to detecting and responding to advanced cyber threats.

4.1 Endpoint Detection and Response (EDR)

The Contemporary EDR systems have three closely coupled architectural elements. They all do different things, but with combined intent and purpose towards a single bearing of detection and response. These elements and their interactions will be the foundation of the ability to become a better appreciation of the strengths EDR has and intrinsic constraints present with it. The most basic component is the endpoint agent, which is applied to all observed systems to gather telemetry. According to vendor documentation such agents typically execute at the kernel level, effectively being able to hook into the internals of the operating system [84]. This architecture allows the agents to spy on system calls, track the creation of processes, file access, and network connection and registry operations. Indeed, this level of visibility is what makes EDR superior to the traditional antivirus solutions, which primarily scan files, and does not provide as well-rounded a view of runtime as it does [85]. The volume of telemetry produced by the monitoring that is done at the kernel level is challenging to engineering. A single endpoint may generate a hundred thousand or more events each day of which a majority are legitimate activity [86-87]. To mitigate this and prevent congestion by the network, agents typically do local blocking and abridgement. Other vendors use machine learning models, which directly execute on the endpoints so that they can do initial threat classification prior to transmission. In this method, a decrease in data transmission is traded with an increase in the CPU

and memory use on devices that are under monitoring [88].

4.1.1 Detection Methodologies and Techniques

The EDR platforms combine different methods of detection, and are not based on one method only, to improve its efficacy [89]. It is an important point of departure of signature-based detection, which is based on behavioral analysis [90]. Rather than matching the file hash to a database of known malware, it checks suspicious behavioral patterns, and for understanding Table. II, show the different techniques and methods of EDR including strength, weakness, process creation with a lot of children, or creating a new connection with the network [91]. These patterns may also occur in legitimate applications (e.g., backup or development tools), necessitating manual adjustment to balance threat detection accuracy and false-positive rates [92]. Many recent studies have attempted unsupervised techniques such as reinforcement learning in auto-encoders to analyze multivariate time-series data to detect anomalies [93]. Machine learning models with supervision are created using labeled datasets to identify already known attack pattern having high predictive accuracy when training is conducted using the analogous of real-life conditions [94] [95]. On the other side, unsupervised models are used to determine patterns without labeled data, which can potentially denote new threats, but may be characterized by a high amount of false-positives [96] [97]. In order to boost reliability, the complex threat intelligence fusion frameworks report feeds with indicators of compromise (IoCs) in the form of malicious IPs and domains containing high confidence alerts on known threats [98]. The ATT&CK has become the commonly used frameworks to describe adversary behaviors, and the majority of platforms can be mapped to the techniques of attacks [99]. This standardization assists the organizations in identifying the gaps in coverage in an organized manner. Nonetheless, an alleged coverage is not necessarily the same as an efficient coverage, as the quality of implementation is not equal [100]. The EDR has a fundamental forensic feature, namely process tree. The parent-child relationship maps are kept on platforms, and an analyst can track attacks to their source an example is showing how a malicious PowerShell script was spawned as a result of an Outlook process following a received external email [101]. This is making incident investigation forensic reconstruction should sufficient telemetry exist.

Table II: EDR Detection Methodologies: A Comparative Study

Ref.	Detection Technique	Strength	Weaknesses	False Positive Tendency	Novel Threat Detection	Operational Requirements
[37]	**Behavioral Analysis (IOAs)**	• Detects intent • Catches LoTL	• Needs baseline • Evasion possible	Medium	High	• Expert labeling • Compute needed
[87]	**Supervised ML**	• High accuracy • Fast classification	• Needs training data • Misses true zero-days	Low	Medium	• Initial tuning • High data
[88]	**Unsupervised ML**	• Finds anomalies • True zero-day	• High false positives • Requires validation	High	High	• Skilled hunting • Large data
[89]	**Threat Intelligence (TI)**	• Immediate context • High confidence	• Reactive only • Needs fast feed	Low	Low	• Feed integration • Minimal processing

[32]	**Process Tree Analysis**	• Root cause • Attack narrative	• Investigation tool • Overwhelms analysts	Low	Medium	• Forensic agent • High storage

4.1.2 Response Capabilities and Containment Strategies

The Host isolation is the most violent containment, which isolates a threat by detection of endpoints in the network automatically. This would stop horizontal flow to other systems as well as legality of business execution on remote endpoints. The implementation usually updates the firewall configurations or network settings to block all communication with all but the management traffic of the EDR platform itself **[103]**. While certain solutions suspend processes to facilitate forensic analysis, researchers have demonstrated that this capability can be abused by attackers to suspend the security agents themselves **[104].** The File quarantine relocates the files which are suspected to be malicious to secure locations where the file cannot be executed yet is open to be examined by a forensic expert. This provides both the prevention of further malicious act as well as evidence lasts to be investigated and possibly prosecuted. In certain EDR platforms, ransomware rollback functions can be configured to operate with Windows Volume Shadow Copy services or equivalent to auto-decrypt files **[105]**. This is potentially incredibly effective at minimizing the effects of ransomware as long as it is installed and turned on as early as possible, as the SE Labs tests demonstrate high-performance vendors will be rated at 100% protection **[106]**. In recent study Scanlon et al. found that automated frameworks have been created to test digital forensic tools and scripts that can be utilized to help develop detailed evidence including memory dumps, file samples, registry hives, and event logs. In **[107]**, emphasize the fact that automation of security monitoring is a significant time-saving tool because it helps to correlate evidence between tools that allows responding to a threat dramatically faster. It has been pointed out, however, in studies that organizations with a large improvement in the index of MTTR only attained this with technology but with a big investment in the training of the analysts and the human-in-the-loop forms of governance **[108].**

4.1.3 Strengths, Limitations, and Deployment Considerations

The key strength of EDR is that they have provided a complete observation of the activity of the endpoint, which has never been before. As opposite to network-based detection which just looks at the traffic between the systems, EDR tracks what processes are being executed, what files are being accessed, and what network connections are being made **[109]**. The EDR does specifically work well in detecting threats which the traditional antivirus solutions fail to. Process execution monitoring will detect file less malware that will be wholly executed in memory **[110].** The critical limitations present with EDR. Most importantly, it offers visibility of only controlled endpoints which agents have been installed. The unmanaged devices such as IoT sensors and guest systems are invisible. Industrialized OT systems do not always succeed in supporting contemporary agents, because of obsolete operating systems or safety certification standards **[111]**. The deployment of the agents may have impacts on the performance of devices with resource constraints, like point-of-sale terminals or medical devices, and can create so-called performance debt and can make IT teams reluctant to deploy them entirely **[112-113].** The scholars have made a lot of contribution in terms of assessing the effectiveness of EDR. But a more critical viewpoint of research 2025 looks further into it with reference to how advanced adversaries knowledgeable of detection logic can create attacks tailored at the specific beating of behavioral heuristics which is why researchers and malefactors are in a continuous arms race **[114].** The International Journal of Multidisciplinary Research (IJFMR) has reported that with AI-based monitoring, companies had a reduction in MTTD of 2.8 seconds and a 4.7 minutes improvement (MTTR) that improved by around ninety percent compared to conventional monitoring. These benefits can only be realized in case they go with appropriate training of analysts **[115]**. Further studies on the security of the IoT underline the fact that ML models are capable of minimizing the number of false positive, but they need significant datasets, properly marked datasets, which is not

always representative of the overall diversity of emerging attack methods **[116].**

4.1.4 Integration with Extended Security Ecosystem.

The current EDR systems should be connected to the greater security stack in order to leverage the benefits the most. The most popular one is the integration with SIEM systems, where high-fidelity alerts are fed to long-term storage and used to comply and perform cross-domain correlation **[117]**. It allows the analysts to explore endpoint events and network traffic and authentication logs **[118].** The Vulnerability management integration helps companies to map the threats that have been detected with the vulnerabilities of their systems. EDR notices suspicious activity and allows the analysts to check, at that moment, whether the relevant vulnerable areas were unpatched to be able to prioritize the remediation **[119]**. Lastly, the integration is automated in creating tickets and help in making sure they are handled by organizational procedures and provide a complete context by the EDR platform **[120],** Table. III, examine different type of integration and purpose of detection and response technologies.

Table III: Integration Patterns of EDR and Their Strategic Impact

Ref.	Integration	Purpose	Benefits	Complexity
[121]	**SIEM**	Centralize Alerts	Holistic Visibility	Medium
[112]	**Vulnerability. Management (VM)**	Prioritize Patching	Risk Context	Medium
[118]	**ITSM**	Create Tickets	Workflow Auto	Low
[117]	**Threat Intel (TIP)**	Enrich Data	Fast Triage	Medium
[53]	**SOAR**	Auto Response	Reduce MTTR	High
[119]	**IAM**	Disable Accounts	Stop Lateral Move	Medium

4.2 NETWORK DETECTION AND RESPONSE (NDR)

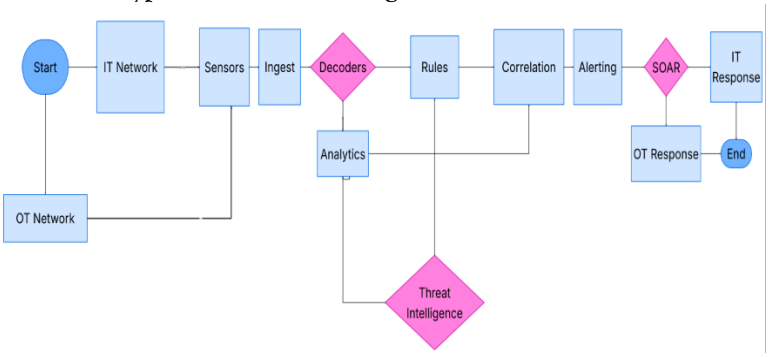
The NDR platforms are a different paradigm of threat detection as opposed to endpoint centered solutions. Although EDR is used to track activity on each individual device, NDR can track trends in the network traffic to determine the presence of threats that might not be detected at endpoint perspectives. This compensatory visibility is, specifically, useful in identifying lateral movement, command information and control, and data exfiltration efforts throughout network segments. The architecture of NDR system, according to secure works, would be determined by the unique deployment environments and organizational requirements **[122]**. On-premise deployments of traditional on premise deployments involve the use of network tap or switch port analysis (SPAN) to duplicate network traffic to specific analysis devices. Network taps is a passive monitoring tool that does not affect network performance whereas the SPAN ports utilize the existing switch infrastructure and might cause performance issues when large volumes of traffic are involved **[123]**. The two methods can provide full packet captured analysis, but storage and processing can be large. The deployments of cloud environments have a dependency on the native cloud provider telemetry collections. The flow logs include the source and destination IP addresses, ports, protocols, the number of bytes and timing details which allow behavioral analysis without capturing the entire packets **[124]**. However, cloud flow logs have notable limitations, such as partial traffic visibility, limited retention, and the absence of deep packet inspection **[125].** The hybrid deployments refers to deployments which utilize several collection techniques in order to provide an all-round visibility. Organizations can install lightweight end point agents to monitor network activity as the host views and acquire network flow data and selective packets capture at key aggregation points at the same time. This strategy offers defense in depth so that the threats could be detected, even when they escape on one monitoring layer **[126].** The amount of telemetry and its nature is radically different in deployment models. Full packet capture is the most detailed and supports protocol-level analysis and content analysis, however, huge storage space and performance must be available. An average enterprise setting with a network traffic of 10 Gbps

at a constant state will generate about 108 terabytes of data a day when all the picketing is capture [127].

4.2.1 Detection Methodologies in Modern NDR Platforms

The NDR being advanced today, it applies advanced detection methodologies that are more advanced than the traditional methods, which are signature based intrusion detection systems. The knowledge of these methodologies helps us to understand both the advantages and the disadvantages of the network-based threat detection. The basis of statistical NDR detection consists of many capabilities of NDR detection. Such systems define behavioral standards to servers of the network entities, workstations, network segments that define the normal patterns of communication, the normal volume of data transferred, the normal destinations that connections are expected to have as well as the normal patterns of time. In the case of detection, observed behavior becomes noticeable as far as deviations are seen with regard to predefined baselines [127]. As an example, a file server that normally has inside connections initiated would suddenly have openings to outside IP addresses in other nations, would cause an alert on geographic anomaly identification. In the same way, a workstation that usually sends small quantities of data, when all of a sudden, uploads Giga-type and beyond of data on cloud storage solutions would be identified as a possible exfiltration. Nevertheless, baseline analysis is also highly challenging at the dynamic environment. Business processes become dynamic, new applications get installed, organizational shifts take place and seasonality influences network behavior. Even the fixed baselines are hasty and soon lose their relevance, which results in the false positives where valid activities do not meet historical standards. NDR websites in modern times have solved this problem by the use of adaptive baselining that constantly adjusts behavioral models according to changing normal operations [128]. Experiments on behavioral analysis algorithms confirm that adaptive algorithms can test 40-60% lower than the rates of false-positives on prediction than a prediction-based base rate, although with trade-offs of high adaptation rate versus detection sensitivity [129]. Another, more advanced method of detecting network behavior that is abnormal is the use of machine learning anomaly detection. The unsupervised algorithms like isolation forest, local outlier factor and auto-encoders can detect the statistical outliers in any network traffic pattern without having to be train on labeled data [130]. A study looks at the case of novel AI-driven intrusion detection systems and it proves how unsupervised learning can pick up new offend methods that could avoid signature-based detection [131]. The limitation of unsupervised method is that it can detect threats that were not known previously without any prior example of attack traffic. Nonetheless, this ability is associated with a high cost: high false-positive rate. Unsupervised models detect statistically anomalous behavior, yet most anomalies in enterprise networks are harmless, including server patches, large legitimate file transfers, or new application installations. Researchers has shown that not carefully tuned unsupervised methods of anomaly detection can produce high false positive rates, and their experimentally of 20.43 per cent on average across six datasets (randomized) points to the danger of them bombarding analysts with irrelevant and bogus alerts [132- 134].

4.2.2 Protocol Analysis and Encrypted Traffic Challenges



The Deep protocol analysis is an advanced NDR functionality that traces the network communications at a protocol level to detect weird behavior. Several protocol analysis schemes can identify protocol specific features to identify anomalies, and identified attack patterns using numerous network protocols. The DNS analysis especially offers good detection with regards to it. DNS tunneling in which the attackers encode their data in DNS queries and use this to transmit data can be identified based on query patterns, response sizes and entropy of subdomains **[135-136]**. The Unusual domain names that can be considered suspicious markers and the volumes of queries to newly opened domains are rather high. The study of TLS certificates is a useful method of identifying massive DNS manipulation with the researchers stating that interpretation **[137]**. More than 87 percent of traffic over the web is encrypted by 2024, making a comprehensive deep packet inspection (DPI) approach nearly useless unless you are willing to use intrusive man-in-the-middle decryption a practice that is both raise a serious dispensation and lawful issue **[138]-139]**. NDR platforms in the present-day do not resolve this issue because they do not question TLS metadata but process the actual payload contents. This method also involves JA3 and JA3S fingerprinting as the method of determining the particular malware families based on the distinctiveness of cipher suites and extensions applied in the TLS handshake **[140] [141]**. Besides, these platforms perform certificate analysis to put malicious connections on the alert list, depending on the status of issuers and the correctness of the certificates, and can perform a handshake timing analysis of the patterns recognizing both automated attack tools and humans when sending web traffic. According to these metadata-based methods, the accuracy of detection of known patterns of threats is up to 80-90% **[142-143]**. These methods are however becoming more and more difficult with the evolving encryption methods that are creating more consideration toward security **[144-145].** The base of HTTP/3 also allows closer visibility by a connection establishment process is also encrypted making it harder to achieve effective traffic analysis by security tools **[146-148].**

4.2.3 Operational Technology (OT) Protocol Awareness

The Heavy equipment being controlled by industrial systems and the network of operational technology pose a specific challenge. Most OT gadgets comprise antiquated operating systems that fail to impart advanced security agents, and often the only feasible facility of visibility is network surveillance **[149].** Moreover, the OT networks use specific industrial protocols which are largely not similar to the IT industry protocols **[150-151].** The OT protocol aware NDR platforms are able to decode these messages, comprehend regular operational procedures and identify commanding un-authenticated parameters. As an example, the setting a programmable logic controller (PLC) to change its set points beyond acceptable ranges would show a flag when sent as a Modbus command. Unintended links to non-engineering workstations of industrial equipment may have been reconnaissance or compromise **[152-155].** The analysis of OT protocol involves a very specific skill. The protocols of industries were not security-oriented, but were rather designed to be reliable and usually had no authentication or encryption tests **[156-157]**. Special care should be taken by analysts to avoid confusing legitimate working alterations with possible attacks, and this is still a serious challenge to organizations that do not have special OT security teams and illustrated in Fig. 2.

Figure 2: NDR Architecture in Hybrid IT/OT Environment

4.3 Extended Detection and Response (XDR)

The Extended Detection and Response is a product of the security industry responding to the inherent problem of security operations, which is alert fatigue and context fragmentation. With the implementation of more and more endpoint-focused security solutions and networks solutions like EDR, networks solutions like NDR, email-specific security solutions like email security gateways and identity solutions, each producing distinct alerts, analysts were flooded with unrelated signals that were being manually correlated. The fundamental assumption in XDR is that individual tools have a lot of false positives in single cases, but that when they are used to correlate events in more than one domain, it becomes possible to attain higher detection rates and efficiency in investigation. All Native XDR vendors provide an

integrated platform created on the foundation of their own product portfolio. According to these vendors, tight integration enables better correlation of data and simplifies deployment. The use of Microsoft Defender XDR, in turn, is an example of linking the phishing emails with the further violation of the endpoint and access to the cloud data by the means of the common data models **[158].** There is however a considerable vendor lock-in in this approach as the organization would be forced to use the overall security stack of that particular vendor. Conversely, vendors of Open XDR build aggregation layers, which consume telemetry exchanged through APIs between multiple third-party vendors **[159].** This gives it the flexibility to be able to capitalize on the already existing security investments and prevent lock-in. Nonetheless, open XDR demands numerous data engineering operations to standardize different sources of telemetry. Another significant industry initiative to unify these formats was the OCSF, launched in 2022, but its practical use is still in the process of normalization, and normalization can take 30-40 percent of the implementation effort in most cases **[160].**

4.3.1 Technical Architecture and Data Engineering Foundations

The technical base of XDR is based on a complex layer of ingestion of data, which is required to be able to process high volume and heterogeneous telemetry. The body of work on semantic data lake stresses that companies have to adopt entity resolution that is used to decide whether various identifiers belong to the same user to ensure the accuracy of the correlation **[86].** The main asset of XDR is the correlation engine. As methods used in platforms, there is Temporal Correlation where proximity-based events are grouped and Graph-based Correlation in which dynamic entity-relationship graphs are built to resist complicated attack sequences **[161].** The response orchestration layer and the investigation workbench stage offer operational output of XDR. Organizations reduce the investigation time by 40-60 percent in a centralized structure of a single interface with attack-path visualization over fragmented environments **[162].** In a confirming threat, XDR is able to organize a multi-layered response that isolates an endpoint through EDR, blocks traffic through firewalls, and deactivates accounts through identity systems to have a complete chaining of the adversary.

4.3.2 Detection and Correlation Techniques in Practice

The Lateral movement detection is another additional provision that proves that the XDR has the capability of detecting multi-stage attacks. Attackers create telemetry within various areas as they proceed with a foothold to the sensitive assets, such as anomalous authentication tracks and network scanning runs inside the environment. Visualization of attack paths Studies on the visualization of attack paths also note that graph-based correlation will be able to recognize the patterns by examining relationship maps of users and systems and protocols like the SMB or RDP **[163-164]**. Likewise, cross-domain correlation is also used in the detection of insider threats whereby a malicious employee or a hacked account is detected and for comparison between native XDR verses open XDR is given Table. IV, which show the comparison of different XDR type. XDR can also detect trends because of the connection between abnormal working schedules and unauthorized logins to network drives and the following transfer of data to personal cloud storage, which single-domain-only tools would overlook **[165]**. Nevertheless, this application presents a major problem in terms of employee privacy and occurrence of false positives due to legitimate and abnormal working patterns **[166]**. Moreover, the incident-based supply chain attack detection models, such as the incident reported by SolarWinds, would demand the association between software update telemetry and post-update runtime abnormalities. Together with Software Bill of Materials (SBOM) data, XDR platforms can detect a trusted signed update with an unauthorized credential harvesting or network communication, when it starts operating **[167]**.

4.3.3 Strengths, Limitations, and Implementation Challenges

The main advantage of XDR is that it will decrease the fatigue of alerts by means of intelligent correlation and enrichment of contexts. Instead of bombarding analysts with numerous fragments of notification, XDR helps in order to compress related events in a single story. Companies that have more mature deployments like those of Palo Alto Networks Cortex XSIAM have also reported

50% to 70% stuck in analyst triage workload and noted an extraordinary improvement in MTTR [168]. This transition enables security personnel to specialize in high-level threat evaluation instead of manual, tedious, and redundant correlation cases to overcome the ongoing shortage of qualified personnel in the industry. This cross domain visibility offers an all-round visibility that can hardly be matched by a point solution. The XDR has significant shortcomings that must be planned. The complexity of data engineering is one of the primary challenges, especially to open XDR implementation. Normalizing a real-time 50,000 sources with 50,000 different schemas is challenging and requires a lot of effort, and the normalization of pipelines is a regular task of mature SOCs, they state that upkeep of the pipelines can take 20-30 % of their engineering resources [169].

Table IV: Comparative Analysis of Native XDR and Open XDR Architectures

Ref.	Comparison Point	Native XDR	Open XDR
[161]	**Integration**	Deep / Seamless	API Dependent
[163]	**Vendor Lock-in**	High Risk	Low Risk
[165]	**Data**	Pre-normalized	Custom Parsing
[166]	**Deployment**	Fast (Weeks)	Slow (Months)
[167]	**Accuracy**	High Fidelity	Variable Quality
[168]	**Flexibility**	Limited Portfolio	Any Source
[169]	**Cost**	Lower Ops Cost	Higher Ops Cost

4.4 MANAGED DETECTION AND RESPONSE (MDR)

The MDR is a response to a key fact in contemporary cybersecurity, which is that having advanced technology does not necessarily equate to high quality security operations. There are often cases of even those organizations that have the financial capacity to procure sophisticated EDR, NDR or XDR systems that do not have the necessary expertise or the 24/7 human resources to effectively utilize these tools [173]. That is the operational gap which has spurred MDR market boom which is likely to increase to a CAGR of 21.95 up to 2030 as organizations aim to either outsource or to increase their capacity of detection and response [174]. The reason behind this growth, according to the Forrester Wave: Managed Detection and Response Services (2025) are the continued lack of qualified analysts, the complexity of threats, and regulatory requirements that continued monitoring is maintained [175]. According to the research of Dell Technologies, specialized MDR providers have a unique benefit because the threat intelligence is collected involving hundreds of client environments, and it is therefore possible to detect the appearance of the new attack patterns in less time than would individual internal teams [176]. The MDR service models have also adapted to the levels of maturity and control in the organization. Under Fully Managed MDR model, the provider takes care of the security stack including technology deployment, 24/7 working as well as incident containment which is usually the best situation in mid-sized enterprises that do not have its own security teams [177]. Nevertheless, this model necessitates organizations to lose considerable level of control and might not have profound internal business background when it comes to complex incidents [178]. Alternatively, Co-managed MDR has become popular especially in sectors that are regulated through DORA or HIPAA like finance and healthcare. Under such a hybrid setup, the client retains formal ownership of their own security tools but the MDR provider gets them running jointly, providing 24/7 expertise without depriving the client of visibility and control [179-180]. Lastly, Augmented Expertise MDR also offers variety of support or surge capacity, including advanced threat hunting or red teaming, to bigger companies which already have established inside SOCs but to which high-level intervention is required occasionally [181].

4.4.1 MDR Provider Capabilities and Operational Models

The essence of an MDR provider is that it can play security functions which are challenging or otherwise inexpensive to develop in-house. The simplest of these is 24/7 Security Operations, which is a necessity that is rapidly becoming mandatory in the modern business world but a recruiting and managerial nightmare to internal staffing [182]. In addition to mere monitoring, full-fledged MDR vendors also differentiate themselves by Threat Hunting. Instead of waiting until an automated alert goes off, human analysts scan, look, and do find some subtle IoCs and enemy tactics that cannot be found by a traditional signature-based detection [183]. It can be recommended that organizations ought to examine providers according to whether manual and hypothesis-driven "hunting was actually carried out or it was simply the automated-scheduled queries [184]. The Incident Response Orchestration, in which providers do not simply inform the client of their availability but rather coordinate containment and remediation systems based on prepared playbooks, is also important to MDR [185]-186]. This is justified by the Threat Intelligence Aggregation that offers a network effect in security, when a provider identifies a new attack method in the environment of one of their customers, they can instantly offer that knowledge to provide security to the full range of customers [187]. The Recent research conducted by Cai and Han indicates that federated learning schemes that protect client privacy are under development to secure client information and protect against malicious attacks. Moreover, major MDR vendors will provide comprehensive reports and metrics that translate technical information into business risk insights to business executives and help auditors to meet their compliance requirements. Hereby assisting companies in making the case to spend on security and monitor their long-term points of view [188-189].

4.4.2 Technology Stack Approaches and Integration Patterns

MDR providers use various technology strategies, and it is important that companies determine the approach of these strategies and determine its fit with current infrastructure and suitability in the future. A report by Comcast Business states that managed detection and response solutions can contain provider-owned stack solutions, where the MDR provider owns its own detection platforms [190]. The CIS Managed Detection and Response FAQ also indicates that selecting a provider-purchased technology stack may enable providers to make their technology more efficient, enable their analysts to become highly proficient with specific tools, and perhaps may enable cost savings related to standardization [191]. This method might however cause it to be more difficult to integrate with the existing security tools of a client and may lead to a decrease in visibility or may cause a client to deploy new investments which may involve replacement and in such a case may be known as a rip and replace [192]. The Client-owned stack models entail the listing of MDR companies that run the security platforms of clients. Customers keep their existing EDR, NDR, XDR, or SIEM platforms and provide their access to users to operate these applications on their behalf [193]. This system is more flexible and not a replacement of the existing investment and allows clients to switch providers more efficiently without the use of technology migration. Nonetheless, it entails providers to accommodate several technology platforms, which might restrict the efficiency of the operations and the insightfulness rate of analyst capabilities. There is also a lack of compatibility with technology platforms in all providers of MDR, which may limit the choice of the tools that a client has. Hybrid solutions integrate technologies owned by providers to perform certain functions with those owned by the clients to perform other functions [194]. E.g., a consultant can install its own threat intelligence platform, threat hunting software when using the already existing EDR and SIEM server [195]. This strategy tries to strike a gold mean between standardization advantages and flexibility of the client despite complicating integration. The Combining it with the current security infrastructure is an essential factor that should not be overlooked irrespective of the type of technology. MDR services should be bound together with a large number of systems: IAM platforms to respond to account operations, network devices and firewalls to implement traffic control, ITSM systems (such as Service Now), to send notifications, and communication platforms [196]. Motorola solutions technical documentation on MDR on special ASTRO communications systems demonstrates that more modern MDR implementations need special custom domain-specific infrastructure [197]. According to recent

trends in the 2025, the most popular providers of MDR are increasingly considering open XDR frameworks and API-first integration patterns to consume telemetry emitted by cloud-native controls, SaaS API, and IoT devices, guaranteeing that the attack surface does not have any dark corners **[198].** The comparison of fully and co-managed MDR is illustration in Table. V, which look for different component of MDR **[199].**

Table V: Decision Framework for MDR Service Model Selection

Ref.	Criterion	Fully Managed MDR	Co-Managed MDR	Augmented Expertise
[191]	**Staffing Level**	Low / None	Medium / Augmented	High / Mature
[192]	**Regulations**	Standard Baseline	High / Audit-Ready	Specific Gaps
[193]	**Control**	Provider Decides	Shared Control	Client Retains
[195]	**Budget**	High	Mid-Range	Low / Flexible
[197]	**Tech Owner**	Provider Stack	BYOT Model	Client Owned
[198]	**Data Privacy**	Standard Rules	High Sensitivity	Max Sensitivity
[194]	**Organization Size**	SMB / Mid-Market	Large Enterprise	Mid / Large
[199]	**Industry**	Retail / SMB	Finance / Health	Tech / Govt

4.4.3 MDR Selection Criteria and Provider Evaluation

When choosing a proper MDR provider, a stepwise analysis of various dimensions should be followed. The notorious results are attained by organizations that view MDR procurement simply as competition in terms of price and Service Level Agreement (SLAs). Necessary provider selection requires an in-depth evaluation of the abilities, cultural compatibility, and the sustainability in the long run **[200]**. Selection is driven by telemetry coverage and depth. Organizations should evaluate whether the provider monitors key systems, networks, cloud platforms, and SaaS applications, as well as specialized environments like OT networks or cloud-based container workloads [201].The technical efficacy is easily measured by the coverage of the provider of MITRE ATT&CK. The findings of the 2025 MITRE Ingenuity Enterprise Evaluation indicate that the top platforms, including Sophos XDR, have reached a 100 percent detection coverage in such multifaceted situations as those with the Scattered Spider and the Mustang Panda groups, and have managed to offer the actionable information on all of the considered adversary sub-steps **[202-203]**. The Response agreements at the service-level outline the important parameters in operations, although they should be interpreted with great care. Although MTTD and MTTR are both commonplace, those should be considered in the context of aggressive SLAs in which case, the misclassification of incidents by the provider is routine **[204].** Organizations are advised to demand the statistics of the real performance including the information about the presence of SLAs misses and the severity of the initial response **[205]**. The MDR relies on transparency and collaboration as its key founders of strategic alignment because it is critical that the service needs to be organized as a professional collaboration and not a cold black box solution. To ensure the effectiveness of such alignment organizations have to ensure that their provider has common underlying detection logic, has access to

raw findings of investigation and provides collaborative platform that allows the sharing of incident response efforts [206]. Moreover, regulatory alignment and adherences have taken the back seat as important drivers of risk management, especially since 2025 is termed as the complete imposition of the mandates like the NIS2 Directive and the DORA. To survive in this realm, the providers will have to exhibit strict compliance with industry-wide certifications like SOC 2 and ISO 27001 in addition to having the particular ability to produce the audit-ready reports demanded by these new regulatory frameworks [207-208]. The elaborate risk management policy should consider the presence of an exit strategy and data portability that are normally not taken into consideration at an initial stage of procurement. Organizations ought to carefully make sure that all security telemetry and detection content is exportable in case of the relationship becoming unsatisfactory so as to avoid the major operational risks of vendor lock-in. When a contract is being negotiated, these data migration rights and transition assistance protocols have to be negotiated at the beginning to ensure long-term architectural flexibility and continuity of security [209].

4.5 SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

The SOAR platforms are a result of the realization that the security operations have many repetitive processes that require time on the part of analysts and yield fewer returns. Some of those activities include adding threat intelligence to their alerts, comparing indicators to various database, generating tickets in ITSM systems, and recording investigation procedures which are predictable when automation can be done [210]. SOAR platforms offer the required structures of automation of such workflows as well as coordinate the activities of various security tools [211]. The concept of SOAR has three capabilities, which are different yet related, namely, orchestration, automation, and response [212-213]. Although these capabilities can be frequently referred to as a single category, they have quite dissimilar applications and can implement a distinct collection of challenges. According to a recent 2025 market report, although SOAR platforms have been developing a great number since the function was initially established in 2015, most organizations fail to achieve the ultimate advantages of automation [214]. Indeed, more than one-half of security practitioners believe that much of today's automation in processes is a form of a check-box exercise and not a real response [215]. A report shows that although older SOAR platforms had an issue with a high rate of false positive alerts earlier generations of the technology have become much more effective by lowering the prevalence of alerts by enhancing event correlation and root cause analysis. Such developments, coupled with increased integration models and more sophisticated playbook composition, have started to tack this issue of the past with practical integration and automation has to dealing with exceptions and hard to reach edge cases [216].

4.5.1 Integration Architecture and Tool Connectivity

The output of any SOAR platform is greatly reliant on the scope and scale of its integration in which it needs to be able to integrate or communicate with dozens or even hundreds of security and IT tools to coordinate broad-scale workflows. These integration approaches help to understand what SOAR can do and what is challenging about deployment. The contemporary platforms embrace various approaches, in the core, through pre-taxi sabotage connecting to widespread tools like EDR, SIEM, and firewalls [56]. The connectors have instant integration at minimal configuration costs but may fall behind the vendor upgrades or be subject to proprietary licenses at elevated units of ownership [217]. The use of API-based integration offers a necessary option to the tools that do not have ready-made connectors. The SOAR systems incorporate the API client support to call REST or SOAP protocols in order to use them with custom internal tools and upcoming security solutions [218]. Nonetheless, the APIs need special technical expertise in order to establish and operate such interconnections. It is common to have organizations in which custom API integrations constitute a major part of the execution work and need continual upkeep since related tools evolve [219]. In cases where native APIs are not provided by systems, agent-based integration will be used. Endpoint or network agent lightweight agents can be installed and collect local commands and communicate back to the SOAR platform with the results and Table. VI, illustration the automation maturity model of SOAR [220]. Although this is a

useful technique in the cases of legacy systems or a closed environment, the implementation and maintenance of these agents create further complexities to the security stack **[221].**

4.5.2 Playbook Development and Governance

The Playbooks specify the automated processes to which SOAR platforms are followed, as the working logic of the SOC. The construction of effective playbooks should be balanced between standardization and flexibility in that the automation of response needs to be faster without being rigid. The studies of how to operationalize cybersecurity knowledge indicate that those organizations that perceive development of playbook as creating a documentation of the existing processes are sometimes unlikely to deliver the best outcomes **[222].** Rather, successful playbooks should begin by having defined and articulated trigger conditions, i.e. alert type, threat intelligence hit or scheduled tasks to avoid unwarranted activations. Upon activation, a decision logic is used to direct the workflow depending on findings of investigation. Depending on the asset criticality or detection confidence, conditional branches can do away with workflow in later routes. In order to cope with such complexity, best practices prefer small blocks of logic which are reusable small blocks, to monolithic ones, which are harder to maintain and troubleshoot **[223].**

4.5.3 Automation Governance and Risk Management

Automation has efficiency benefits but automatization poses a risk to the operation, including introducing a denial-of-service without foul play or locking real users out. Successful SOAR deployment depends on a well-defined governance model that categorizes response actions according to risk severity**.**

. To plan automation, however, CISA indicates that automation risk classification should assist organizations in deciding what is to be fully automated, routine activities like data enrichment may be fully automated, and more critical activities like firewall updates must be explicitly approved by human operators **[56]**. The inclusion of the business context increases this risk management. Particular frameworks, such as IC-SECURE, show how playbooks have the potential to exploit databases on the criticality of assets and maintenance window monitoring to avoid disruptive activity during the busiest times of the business or through key infrastructure **[225].** ITSM systems should be engaged with by high-impact automated actions that make change records and document execution to be audited **[226]**. This will make sure that automated security procedures leave some trail that will satisfy the organizational change management. Also, rollback facilities are a very important safety net. The automated response criteria stipulates that playbooks are supposed to monitor changes in the state to enable reversal of the action; in case the action resulting is an automated block, the system is expected to be in a position to revert the action in real time or the action should give analysts clearly defined manual instructions to revert the service **[227]**.

Table VI: SOAR Automation Maturity Model and Capability Levels

Ref.	Maturity Level	Integration	Governance	Exception Handling
[145]	Initial	Limited	Informal / Ad-hoc	Manual Fixes
[221]	Managed	Standard APIs	Basic Logging	Stop on Error
[222]	Defined	ITSM & Chat	Strict Control	Logic & Retries
[223]	Quant. Managed	Deep / Custom APIs	Metrics Driven	Auto Fallback
[225]	Optimizing	Full Hybrid Mesh	AI/ML Guided	Self-Healing

5. Machine Learning and Integration Architectures

This section explored the role of machine learning in modern detection systems and the architectural patterns used to deploy them at scale. It highlighted the strengths and limitations of supervised, unsupervised, and hybrid learning approaches, emphasizing the importance of explainable AI, analyst trust, and data quality in operational security environments. The discussion also examined automation governance and staged deployment to balance efficiency with operational risk. Finally, integration architectures from vendor-centric XDR platforms to open data lake models and edge/OT deployments were analyzed, demonstrating how organizational context and maturity shape effective detection and response strategies.

5.1 Machine Learning in Detection Systems

The modern detection platforms are based on machine learning. Almost all EDR, NDR and XDR systems utilize ML-driven features **[231].** However, the implementation of ML is diverse in these platforms and situations and discloses specific benefits as well as drawbacks. The commercial security products are mostly dominated by supervised learning **[232].** Such systems are able to train on labeled cases of benign as well as malicious behavior and this allows the classification to be refined. According to research in the IOP Conference Series (2021), with the help of supervised models trained well, more than 95% of known threats are detected **[233].** Even so, there are issues with supervised methods. Large, properly marked training sets are costly and tedious to construct, involving the use of experts to annotate and vet their training data **[234].** This type of data is usually representation of laboratory experiments or incidences of the past which could leave out the scope of real-life threats **[235].** More importantly, models that are trained on old data have a tendency to overlook new tactic of attack since their enemies also upgrade their techniques to avoid detection a phenomenon referred to as concept drift **[236].** More recent studies indicate that attackers have been strategizing increasingly on ML evasion methods because they have knowledge of the weaknesses of ML, thus creating camouflage attacks. The conversely, unsupervised learning, which identifies the anomalies without the labels, is able to find new threats. The researcher introduce such frameworks as SAFE based on using Masked Auto encoders (MAEs) as the method to extract subtle behaviors of networks, as well as deceive anomalous patterns **[237].** Nevertheless, unmonitored techniques usually provide large false-positive values under working conditions. Such models raise red flags on all statistical anomalies, including those cases where the rarest behaviors are harmless (e.g. new deployments, infrequent administrative actions, etc.). These models inundate the analysts with false positives without due care of tuning. According to the industry figures, unsupervised models with a poor calibration may reach above 80% false positives with the effects of Clever Hans as they tend to concentrate on superficialities instead of real indicators of danger **[238].** In order to offset these problems, semi-supervised and active learning combine small datasets with many unlabeled ones. According to CREDIT Center research, these methods are the most effective in adding to intrusion detection with minimum annotation **[239].** The feedback between the expert and the algorithm, new strategies assess the per-sample uncertainty levels to make analyst revision only when necessary due to uncertainty in the model **[240].**

5.1.1 Explainable AI and Analyst Trust

The key challenges of ML-driven detection is to win the trust of the analysts. This type of critical decision-making by security analysts includes isolating endpoints or rejecting alerts on the output of the ML. Loss of trust between the analysts in the face of prediction that the machine uses the machine learning to make predictions occurs, and thus resources are wasted on false alarms or false negatives on real threats are ignored and Fig. 3, show the machine learning role in security operations **[241].** The Black-box ML models, especially deep neural networks can be very opaque in nature. Analysts do not have context to inform their judgment when they are informed only of a detection by the alerts of suspicious activity. Explainable AI (XAI) solves it by giving actions of the ML intelligible explanations. EDR and XDR products are currently implementing XAI; an example of a recent based on a Random Forest, explainable system does not only have 99.9% detection but also reduces the number of false positives and computing costs compared to traditional methods **[242].** More advanced versions

of XAI currently produce counterfactuals like "without the process having touched external IP address X the alert would not have fired" allowing analysis teams to identify detection drivers [243]. According to researchers, explain ability is an essential concept not only in theory but in practice as well. Systems which provide clear explanations assist analysts in validating alerts quickly to aid in sound action [241]. Also, more regulations are becoming explanatory. High-risk systems are explained in the EU AI Act, which exposes systems without clear logic to compliance failures and reduced operational confidence [244].

5.1.2 Automation Governance and Staged Deployment

Although automation leads to a considerable efficiency increase, not all security operations could be automated at the same time in organizations. It is generally harmful to make all incident response fully automated without realizing, through testing and governance, that operations are either broken or that they may cause unwanted disruption to the business [245]. The phased deployment is usually more effective, starting with the deterministic and low-risk actions. Indicatively, searching threat intelligence feeds and asset inventories is a suggested starting point because it enhances a high efficiency of the analysts, without increasing the risk of business operation [246]. Likewise, the ticketing workflows and notifications are similar in that automation will result in an instant payoff with little likelihood of queuing a service down [247]. The increase of the confidence, organizations may shift to medium risk measures, including isolated host containment or temporary firewall rules, which usually are run automatically, with real-time notifications sent to analysts [248]. The dangerous activities such as isolating production system or shutting down of privileged accounts must always be approved by human beings, even in well-developed programs [249]. The optimization of the metrics maintains continuous improvement where teams monitor the rates of automation use, the time required to verify any human and the rate of false-action to guarantee the program raises the overall effectiveness of SOC [250].

5.1.3 Data Quality Foundations

The success of machine learning and high-quality analytics is solely conditioned by data quality; even the most advanced algorithms cannot work out the garbage in and garbage out situation. Telemetry coverage hole in endpoints, network blind spots, and cloud environments generate holes in detection, which will be exploited by knowledgeable attackers [251]. This therefore makes it a precursor to have a complete stock of the production structure in order to do detection well [252]. On top of being visible, the process of data normalization is necessary in matching events in the context of various telemetry sources. Various formats of timestamp and levels of severity are frequently used in tools, and the OCSF is a much-needed but not yet universal standard to produce consistent data view [253-254]. Besides, temporal and identity correlation are dependent on the accuracy of time stamps and identity resolution. Misconfigurations of NTP or drift of system clock can negate sequence of events [255], whereas a powerful entity resolution utility is required to associate different identifiers, including usernames, SID, and MAC addresses, with one user or device [256]. Detecting content is treated just as rigorously by Leading SOCs using version control and synthetic attack injection to measure performance and assure that detection rules are also effective with respect to changes in threats [257].

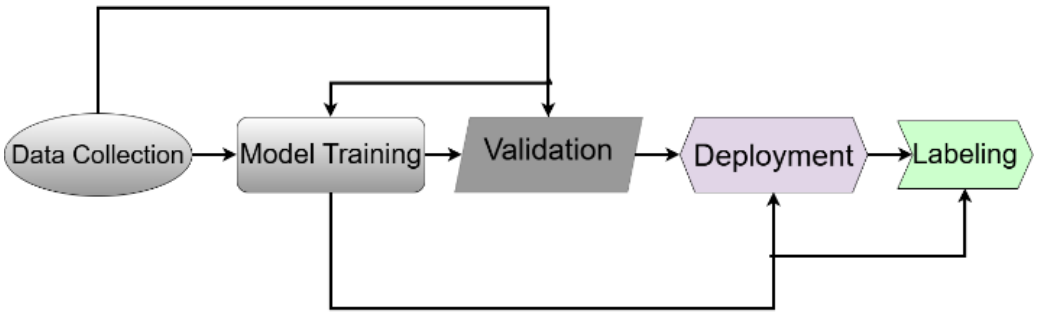


Figure 3: ML Model Lifecycle in Security Operations

5.2 Integration Architectures and Deployment Patterns

The deployment of detection and response is done through various architectural patterns by different organizations based on the available infrastructure, the regulatory requirements, the level or maturity of operations and availability of resources. No one fit architecture exists which can be applicable in every organization; effective implementations have to be done based on the context of the organization and available constraints. Unlike the SIEM based model, the XDR based security operation centers are becoming increasingly popular, especially with mid-market entities or those that are upgrading security services infrastructure. They also use single-vendor XDR-based systems which offers expertise of operations. The basic trade-off is that the flexibility can be lost in favor of operational ease: the companies gain more vendors, but can be more tightly integrated, with less engineering expense, and procurement can be made easier [258]. The XDR-funded solutions are especially competitive to those companies that are not equipped with sizable security engineering staffs since vendor-controlled combinations and embedded correlation regulations ease the administrative load. Nevertheless, vendor lock-in is also quite a troubling issue because organizations successfully lock to a particular vendor and its product range in several security areas and can no longer choose the technology they want to use in the future or have fewer bargaining options. Moving to the category of organizations having robust data practice ability, data lake architecture and open XDR platforms are the trend followed by a cloud-native organization. These designs will deliver telemetry received by a variety of endpoint points, networks, cloud platforms, SaaS applications, containers, and serverless functions to cloud data lakes [259]. These data lakes are where open XDR analytics platforms are built, which offer correlation, investigation, and response functionality but do not need data copying. Such architecture can give organizations the maximum flexibility so that new sources of telemetry can be added without significant architectural modifications, and that analytical platforms can be replaced without transferring data. The data lake approaches, however, assume a significant level of data engineering capabilities to be developed and run, including keeping ingestion pipelines and normalizing schemas, that is often beyond the means of most conventional security teams [260].

5.2.1 Edge and Operational Technology Deployments

The OT networks together with edge computing environments create deployment issues that are not synergistic to the standard enterprise architecture. Traditional security agents are frequently not compatible with these environments associated with either computational limits, safety, or air-gapped network architectures. The industrial facilities which are air-gapped are also vital infrastructure like power generation and water treatment, to which the effects of security tools cannot be ignored or connected to the external network. These environments are usually based on passive NDR sensors which observe traffic across the network without affecting operation, telemetry export data diodes with log return traffic blocked and a digital twin environment which replicates systems in production to test detection rule. The OpenText (2024) technical advice details how these methods may bring visibility and ensure that in both the public sector and industry settings, adherence to strict operational standards is achieved as a result [261]. Other constraints exist in safety-critical systems other than air-gapping as a company cannot deploy security measures that may interfere with safety mechanisms even in an active attack. This needs detection-oriented and not response-oriented methods, which implies the liaison with OT and safety teams to devise containment processes that can not interfere with safety [262]. Lastly, in relation to Edge IoT deployments like in the case of retail point-of-sale and industrial sensors other challenges arise. Such devices do not always have the computing resources to execute security agents but they produce potentially useful telemetry that can be used to analyze the behavior. A study on the topic of IoT-XDR published in MDPI Sensors (2024) discusses how telemetry may be gathered by the platform on resource-constrained devices and heavy analysis done in central cloud platforms, which allow full visibility now without placing strain on the edge devices themselves [263-264].

6. Industry-Specific Adoption and Future Directions

This section examined how detection and response technologies are adopted across different

industries, influenced by sector-specific risk profiles, regulatory requirements, and operational constraints. Variations in maturity, data availability, and workforce expertise were shown to significantly affect deployment strategies and technology selection. The discussion also highlighted emerging trends shaping future adoption, including increased reliance on AI-driven analytics, greater integration across security platforms, and the expansion of detection capabilities into cloud, edge, and operational technology environments. These developments indicate a shift toward more adaptive, automated, and context-aware security operations

6.1 Financial Services and Regulatory Mandates

The financial organizations such as banks work within very high make-or-buy limitations which act as high-value targets since they have to comply with strict enforcing rules without exposing high-frequency trading to impacts or disrupting customer business workflows. The Digital Operational Resilience Act (DORA) of the European Union, which will come into force in January of 2025, has completely changed the situation because the process of real-time exposure to threats and documented response will now be enforced through legal requirements **[265].** This law has been one of the driving factors of the increased adoption of XDR and MDR in the European financial services with the institutions now having to show their recovery and tracking record in order to escape heavy fines. In the United States, the 2023 cybersecurity rule by SEC has brought along the same sense of urgency whereby public companies are obliged to disclose material flows within a four-day business period. This requirement has compelled organizations to abandon a detection schedule that is calculated in weeks to the capacity to detect, evaluate, and organize the disclosures in hours **[266].** Financial actors tend to implement combined XDR platforms linking EDR and NDR to dedicated fraud analytics in order to provide extensive visibility. Lots prefer co-managed MDR models as an opportunity to get international experience without violating data sovereignty that financial regulators need **[267].**

6.1.1 Healthcare and Patient Safety Constraints

The optimization of security, safety of patients, and HIPAA compliance is a special challenge encountered by healthcare organizations. Unfortunately, a major vulnerability in this industry is medical IoT, according to research, the key equipment used, like infusion pumps, is not always compatible with the conventional EDR agents, and failure of equipment regarding security can directly threaten the lives of patients **[268].** The hospitals often employ NDR platforms to regulate the networks of medical devices passively and as such, they offer insight into hitherto unmanaged environments. Moreover, incorporating the facilities of detection tools with Electronic Health record (EHR) audit logs enables the detection of attackers who have penetrated the electronic health record with the view of imitating the clinical workflow in a maneuver that aims at evading the conventional behavioral alerts **[269].** The most important stakeholders in healthcare MDR should exhibit profound knowledge of such clinical barriers to guarantee that security measures do not affect medical access **[270].**

6.1.2 Manufacturing and Critical Infrastructure

While the IT security architecture is quite different, both ICS and OT networks need totally different security architecture. In such settings, EDR implementation is normally limited to engineering workstations and business systems since the traditional agents may disrupt industrial controllers. Rather, AI-based systems such as NDR identify concealed threats on the network level, and as such offer prevention, as well as detection, without access to the physical controllers **[271].** OT-aware detection is a valuable concept, case studies have indicated that millions of dollars in downtime and physical safety can be achieved in the manufacturing plants by detecting malicious PLC (Programmable Logic Controller) command injections which can occur **[272].**

6.1.3 Economic Analysis and Total Cost of Ownership (TCO)

The Detection and response technologies have an economic justification, which is much deeper than mere licensing fees. The high cost of telemetry storage should be taken into consideration because the logs of thousands of endpoints and sensors may become enormous cloud ingress and outgoing fees. Moreover, the finding talent to do the labor work in the detection engineering tuning of the ML models and design of bespoke rules is a sizable recurring cost. The Dell Technologies (2024) analysis indicates that MDR may prove to be more

cost-effective to mid-sized organizations as compared to developing an in-house SOC, particularly in consideration of the cost of 24/7 staffing, maintenance of analysts, and ongoing training [273].

6.2 Case Studies and Empirical Evidence

A giant manufacturing company had a strategy of deploying an integrated defense by ensuring passive use of NDR sensors with OT protocol awareness besides lightweight EDR agents on workstations in engineering. This system was able to identify malicious Programmable Logic Controller (PLC) command injecting malware which did not concur with the operational baselines. The NDR platform was able to decode Modbus traffic and identify any unauthorized commands that were trying to modify set points that were outside of normal range. It was found that a workstation was compromised by an attacker to control the industrial processes; it was however discovered that before the attacker could do any physical harm, the workstations were detected in a few minutes. According to its estimation, a successful attack would have caused 4.2 million dollars' worth of production downtime and loss of equipment, which stems out the paramount importance of OT-aware detection and cross-domain integration [274-275].

6.2.1 Regional Hospital System

A hospital system in the region without an in house 24/7 SOC embraced the co-managed MDR services fused with Microsoft Defender XDR. In an ongoing ransomware operation, the MDR service provider picked up anomalous network scanning and privilege escalation which indicated subsequent lateral movement. The provider organized a swift containment operation and contained the threat in 15 minutes with no clinical systems being encrypted. The hospital prevented an approximate 2.8 million dollar in recovery cost and regulatory penalties through the uptime of service provision to patients. The case highlights how effective MDR is in terms of organizations, which need twenty four hour observation, but have the means of not having a pre-made center in-house [276-277].

6.2.2 Cloud-Native SaaS Provider

The open XDR architecture was applied in the cloud data lake that combined telemetry, hosted by a cloud-native SaaS provider. The platform also revealed a token-replay attack as quickly as 9 minutes after the malicious event had been detected through the detection of the anomalies in the authentication process and the suspicious API access. One of the attempts to gain access to customer data through social-engineered credentialing was blocked by the rapid response. The provider estimated a saving of 8 million dollars of the regulatory fines and even termination of the contracts. The case demonstrates the use of data engineering to enable cloud-native companies to execute end-to-end data detection between various SaaS and infrastructure stacks [278] [279].

6.2.3 Financial Institution DORA Compliance

In order to comply with DORA requirements, a mid-sized financial institution implemented native XDR with MDR added. Automatic containment of high-confidence alerts, 96% of which, can play an important role in reducing the fatigue of an analyst without compromising accuracy [119]. In addition to the necessary legal requirements of a resilience testing and ongoing change, the fully operational approach that also involved the creation of playbooks and governance changed the metrics. The combination deployment by the institution was reported to drop the MTTD to 14 days and the MTTC to 3 days compared to 45 minutes and 4 hours [280-281].

6.2.4 Federal Agency Supply Chain Detection

A government federal agency working in line with CISA logging advice was able to identify a supply-chain breach by matching endpoint-telemetry logs with DNS query logs. The analysis found the presence of malicious PowerShell code that was introduced as part of a legitimate software update of one of the vendors who had been compromised. It was only detected because that system had realized a pattern of unusual update behavior on the endpoint and suspicious DNS queries to unknown infrastructure which would have otherwise gone undetected by individual tools. The case illustrates that the keys to winning over the complex threat of supply chains are linked to a profound visibility on numerous security areas and sophisticated correlation engines [282].

6.3 Research Gaps and Future Directions

Although there is tremendous improvement in the areas of detection and response technologies, there are still critical research gaps. As a way of dealing with these issues, academia, technology vendors

and security practitioners should work together in an effort to move towards more resilient, privacy conscious and autonomous security activities. The subsequent discussions outline some of the key areas upon which research and development is required in the future.

6.3.1 Encrypted Traffic Analytics

The TLS 1.3 getting a standard, organizations may encounter a visibility gap whereby the traditional method of packet inspection cannot be used anymore, without invasive decryption. As of today, machine learning methods that follow metadata-based methods that examine the size, timing, and sequence of the packets can obtain a detection rate of 80 and 90 percent **[283].** Nevertheless, privacy-saving approaches and federated learning should be put in the focus of the future studies **[284].** This would enable different organizations to jointly desensitize against their underlying data defining their dynamics based on encrypted traffic without the underlying data being shared at all, preserving both security fidelity and privacy.

6.3.2 Supply Chain Telemetry Fusion

Although there is already significant research on the supply chain compromises prevention by means of the secure development and SBOM, the possibility to identify a compromise of the software during everyday operations is underdeveloped. Based on the problems detected in encrypted traffic analytics, the research in future should seek a method of correlating SBOM data with real-time abnormalities. Constructively, when a proven software applicant unexpectedly initiates unforeseen amount connections or alters delicate enrollment issues, this complete profile ought to automatize the integration of this identity information with conductive telemetry **[285-286]**. Therefore, when supply chain data is incorporated with runtime monitoring, superior proactive detection is enhanced.

6.3.3 AI Governance in Security Operations

One of the trends is the integration of the LLMs into SOCs to generate playbooks and provide a summary of an incident **[287].** Continuing on the previous arguments about the fusion of technologies, the empirical examples in the literature show that there is no formal validation of AI generated security content. The future directions are related to create validation frameworks that would help avoid hallucinations in response logic and create effective defensive against prompt injection attacks that would make an AI SOC assistant white-list bad traffic **[288]**. These measures are safe to expand the role of AI in the security operations.

6.3.4 Autonomous Response Safeguards

The Complete control of incident response is far because there is the possibility of friendly fire when an automated system takes off a critical business process in order to prevent a minor threat. Using the responsible AI integration theme, there is a need to research the policy aware systems, which apply machine learning in predicting the business impact of a responding action and then execute it **[289].** This is by including the requirements of law and business SLAs into the decision making logic, which requires the automated actions to be found to be statistically sound as well as contextually fitting **[290].**

6.3.5 OT/IT Convergence

Industry 4.0 has made the industrial systems more interconnected making the traditional air-gapping thing obsolete. Along with previous remarks regarding operational automation and convergence, the gaps in the research can be identified in the development of lightweight agents to the OT hardware of the past and safety-considerate response strategies that prioritize physical human safety over data integrity **[291].**

7. CONCLUSION

This review confirms that EDR, NDR, XDR, and MDR serve distinct purposes, yet their effectiveness in modern cybersecurity depends on working in unison. Integrating complementary detection and response capabilities enables organizations to establish a unified defense, which is critical against today's evolving cyber threats. The key insight is clear: successful detection and response rely more on how the tools are operated than on the number of tools deployed. Organizational success stems from the reliability of acquired data, the consistency of automated processes, the proficiency of human operators, and measuring outcomes based on security results rather than tool count. As attackers continue to employ strategies such as double extortion, supply chain attacks, AI-driven campaigns, and credential compromises, organizations are compelled to adopt holistic,

coordinated detection and rapid response strategies. The synergy of these technologies provides a strategic advantage, enabling faster threat mitigation, regulatory compliance, and stakeholder protection. Achieving this requires continuous investment in high-quality data, skilled personnel, and outcome-based evaluation. Ultimately, the identification and response to cyber threats should be viewed as an evolving, adaptive process, continually refined as research and operational gaps are addressed.

References

[1] Identity Theft Resource Center. "H1 2024 Data Breach Analysis," July 2024. [Online]. Available: https://www.idtheftcenter.org/publication/itrc-h1-data-breach-analysis

[2] Verizon. "2024 Data Breach Investigations Report (DBIR)." [Online]. Available: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[3] Orca Security. (2025). 2025 State of Cloud Security Report. [Online]. Available: https://orca.security/lp/2025-state-of-cloud-security-report

[4] Zhang, Z., Yin, J., Li, Z., Chen, J., Du, M., Zhang, Z., & Liu, Q. (2025). Encrypted Malicious Traffic Detection Using Multi-Instance Learning. In Computational Science – ICCS 2025 (Venue: ICCS)

[5] Bluesight. "2025 Breach Barometer®." Annual Report, 2025. [Online]. Available: https://bluesight.com/wp-content/uploads/2025/02/2025-Breach-Barometer-Annual-Report.pdf

[6] Mandiant. "Special Report: Mandiant M-Trends 2024," Apr. 23, 2024. [Online]. Available: https://www.certitudesecurity.com/wp-content/uploads/2024/04/M-Trends-2024_Certitude-Security.pdf

[7] Ernst & Young. (2025). A Practical Reference Architecture for Cyber Resilience Act (CRA) Compliance. [Online]. Available: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/services/tax/documents/ey-gl-practical-refrence-architecture-for-cra-compliance-11-2025.pdf

[8] Help Net Security. "Budget constraints force cybersecurity teams to do more with less," Jan. 31, 2023. [Online]. Available: https://www.helpnetsecurity.com/2023/01/31/cybersecurity-budget-constraints/

[9] Microsoft. "Normalization and the Advanced Security Information Model (ASIM)." Microsoft Learn, June 18, 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/sentinel/normalization

[10] SANS Institute. "Undercover Operations: Scraping the Cybercrime Underground," Jan. 15, 2025. [Online]. Available: https://www.sans.org/blog/undercover-operations-scraping-the-cybercrime-underground

[11] Blink Ops. "SecOps vs. SOC: The Differences Explained." [Online]. Available: https://www.blinkops.com/blog/secops-vs-soc

[12] Wiz. "DevSecOps vs DevOps: Key differences & Comparison." Wiz Academy, Oct. 17, 2025. [Online]. Available: https://www.wiz.io/academy/detection-and-response/devsecops-vs-devops

[13] Splunk. "What Is SecOps? Security Operations Defined." [Online]. Available: https://www.splunk.com/en_us/blog/learn/secops-security-operations.html

[14] Alansary, S. A., Ayyad, S. M., Talaat, F. M., & Saafan, M. M. (2025). Emerging AI threats in cybercrime: a review of zero-day attacks via machine, deep, and federated learning

[15] Shaik, S. (2024). Impact of Endpoint Detection and Response (EDR) Tools on SOC Efficiency. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 12(5), 1-10. https://doi.org/10.5281/zenodo.14762654

[16] Cybersecurity and Infrastructure Security Agency (CISA). "Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a US Critical Infrastructure Sector Organization," Nov. 21, 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-326a

[17] ISACA. "Using EDR to Address Unmanaged Devices," Aug. 21, 2019. [Online]. Available: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-17/using-edr-to-address-unmanaged-devices

[18] Fidelis Security. "SSL Inspection in NDR: Blind Spots in Network Security," 2025. [Online]. Available: https://fidelissecurity.com/threatgeek/network-security/ssl-inspection-in-ndr

[19] ProInf. "Complete guide to eXtended Detection and Response (XDR)," 2022. [Online]. Available: https://proinf.com/complete-guide-to-extended-detection-and-response-xdr

[20] Dell Technologies. "Closing Security Operations Gaps with MDR," 2024. [Online]. Available: https://www.delltechnologies.com/asset/en-my/services/managed-services/briefs-summaries/mdr-infographic.pdf

[21] Cymulate. "Managed Detection & Response (MDR): Beyond Alerts," 2025. [Online]. Available: https://cymulate.com/cybersecurity-glossary/managed-detection-and-response-mdr

[22] Forrester. "The Forrester Wave™: Security Analytics Platforms, Q2 2025," Forrester Research, 2025. [Online]. Available: https://www.forrester.com/report/the-forrester-wave-tm-security-analytics-platforms-q2-2025/RES183581

[23] QodeQuay. "Cybersecurity Automation: Orchestrating Rapid Incident Response," 2025. [Online]. Available: https://www.qodequay.com/cybersecurity-automation-incident-response

[24] Nott, C. (2025). Organizational Adaptation to Generative AI in Cybersecurity: A Systematic Review. arXiv preprint. [Online]. Available: https://arxiv.org/abs/2506.12060

[25] Kashef, R., Freunek, M., Schwartzentruber, J., Samavi, R., Bulgurcu, B., Khan, A., & Santos, M. (2023). Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research. arXiv preprint. https://doi.org/10.48550/arXiv.2302.13955

[26] Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions. IEEE Communications Surveys & Tutorials, 25(2), 1775-1807. https://doi.org/10.1109/COMST.2023.3280465

[27] Alkhateeb, E., Ghorbani, A., & Lashkari, A. H. (2025). Packed malware detection using grayscale binary-to-image representations. arXiv preprint. https://doi.org/10.48550/arXiv.2512.15414

[28] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31. https://doi.org/10.1016/j.jnca.2015.11.016

[29] Journal. Butun, I., Morgera, S. D., & Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials, 16(1), 266-282. https://doi.org/10.1109/SURV.2013.050113.00191

[30] GeeLark. (2025). Heuristic detection. Cybersecurity Glossary. [Online]. Available: https://www.geelark.com/glossary/heuristic-detection/

[31] Udeshi, M., Putrevu, V. S. C., Krishnamurthy, P., Karri, R., & Khorrami, F. (2025). SaMOSA: Sandbox for malware orchestration and side-channel analysis. arXiv preprint. https://doi.org/10.48550/arXiv.2508.14261

[32] MITRE ATT&CK. (n.d.). Command and scripting interpreter (T1059). MITRE ATT&CK Enterprise. [Online]. Available: https://attack.mitre.org/techniques/T1059/

[33] Gartner. "Endpoint Threat Detection and Response Tools and Practices," 2013. [Online]. Available: https://www.gartner.com/en/documents/2596321

[34] EC-Council University. "Data-Driven Defense: Telemetry in Incident Response," 2025. [Online]. Available: https://www.eccu.edu/cyber-talks/data-driven-defense-telemetry-in-incident-response

[35] Center for Strategic and International Studies. (2016). Hacking the skills shortage: A study of the international shortage in cybersecurity skills. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf

[36] Vvelitkn. (2025). What's wrong with EDR? The flaws, limitations, and pitfalls. [Online]. Available: https://medium.com/@vvelitkn/whats-wrong-with-edr-the-flaws-limitations-and-pitfalls-fbc55173496f

[37] Ongun, T., et al. (2021). Living-off-the-land command detection using active learning. arXiv preprint. https://doi.org/10.48550/arXiv.2111.15039 (Venue: RAID 2021)

[38] Yost, J. R. (2016). The march of IDES: Early history of intrusion-detection expert systems. IEEE Annals of the History of Computing, 38(4), 42-54. https://doi.org/10.1109/MAHC.2015.41

[39] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST SP 800-94). [Online]. Available: https://doi.org/10.6028/NIST.SP.800-94

[40] MITRE ATT&CK. (n.d.). Exfiltration over alternative protocol (T1048). MITRE ATT&CK Enterprise. [Online]. Available: https://attack.mitre.org/techniques/T1048/

[41] DN.org. (2025). Joint analysis of DNS and TLS handshakes in Spark. [Online]. Available: https://dn.org/joint-analysis-of-dns-and-tls-handshakes-in-spark/

[42] McGraw, G., & Morrisett, G. (2000). Attacking malicious code: A report to the Infosec Research Council. IEEE Software, 17(5), 33-41. https://doi.org/10.1109/52.877857

[43] Metzer, L. (2020). Network detection and response (NDR): Market trends and technical evolution. [Online]. Available: https://www.sans.org/white-papers/advanced-network-detection-and-response-ndr

[44] Gartner. (2020). Innovation insight for extended detection and response. [Online]. Available: https://www.gartner.com/en/documents/3982247/innovation-insight-for-extended-detection-and-response

[45] Cymulate. "Alert fatigue: How to fix SOC overload," 2025. [Online]. Available: https://cymulate.com/cybersecurity-glossary/alert-fatigue/

[46] Chickowski, E. (2019). The state of threat hunting: False positives and the analyst's burden. [Online]. Available: https://www.darkreading.com/vulnerabilities-threats/one-in-three-soc-analysts-now-job-hunting

[47] Forbes Technology Council. (2024). EDR, XDR, MDR: Making sense of threat detection and response acronyms. [Online]. Available: https://www.forbes.com/councils/forbestechcouncil/2024/03/05/edr-xdr-mdr-making-sense-of-threat-detection-and-response-acronyms/

[48] Freitas, S., & Gharib, A. (2024). GraphWeaver: Billion-scale cybersecurity incident correlation. arXiv preprint. https://arxiv.org/abs/2406.01842

[49] Gartner. (2024). Market Guide for Extended Detection and Response. [Online]. Available: https://www.gartner.com/en/documents/5859979

[50] ITPro. (2025). Enterprises can't keep a lid on surging cyber incident costs. [Online]. Available: https://www.itpro.com/security/enterprises-cant-keep-a-lid-on-surging-cyber-incident-costs

[51] MarketsandMarkets. (2024). Managed detection and response (MDR) market by security type (network, endpoint, cloud), deployment mode (on-premises and cloud), organization size (SMEs and large enterprises), vertical and region – Global forecast to 2029. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/managed-detection-and-response-market-168039027.html

[52] Grand View Research. (2024). Managed detection and response market size, share & trends analysis report by security type, by deployment, by organization size, by vertical, by region, and segment forecasts, 2024–2030. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/managed-detection-response-market-report

[53] Cybersecurity and Infrastructure Security Agency. (2025). Implementing SIEM and SOAR platforms: Practitioner guidance. [Online]. Available: https://media.defense.gov/2025/May/27/2003722066/-1/-1/0/Implementing-SIEM-and-SOAR-platforms-Practitioner-guidance.PDF

[54] Enterprise Strategy Group. (2024). ESG showcase: Dell Technologies managed detection and response. [Online]. Available: https://www.dell.com/en-us/dt/corporate/research/analyst-reports/esg-showcase-dell-technologies-managed-detection-and-response.htm

[55] Netenrich. (2025). Incident response automation: Trusting machines to accelerate recovery. [Online]. Available: https://netenrich.com/blog/incident-response-automation

[56] Matches, glossary guide. Why no pages for web content? [56] Deepwatch. (2025). Security orchestration, automation, and response (SOAR): A technical guide. [Online]. Available: https://www.deepwatch.com/glossary/security-orchestration-automation-and-response-soar/

[57] Cybersecurity and Infrastructure Security Agency. (2025). Implementing SIEM and SOAR platforms: Practitioner guidance. [Online]. Available: https://www.cisa.gov/resources-tools/resources/guidance-siem-and-soar-implementation

[58] Matches, press release. [58] VMware, Inc. (2019). VMware completes acquisition of Carbon Black. [Online]. Available: https://www.globenewswire.com/news-release/2019/10/08/1926966/0/en/VMware-Completes-Acquisition-of-Carbon-Black.html

[59] Sufyan, A., Khan, K. B., Khashan, O. A., Mir, T., & Mir, U. (2023). From 5G to beyond 5G: A comprehensive survey of wireless network evolution, challenges, and promising technologies. *Electronics*, *12*(10), 2200.

[60] Partial match; content links to a philosophy paper PDF. Why update the URL? [60] MITRE. (n.d.). MITRE ATT&CK framework: Design and philosophy. [Online]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[61] Amazon Web Services. (2022). Announcing the open cybersecurity schema framework (OCSF). [Online]. Available: https://ocsf.io/announcing-the-open-cybersecurity-schema-framework/

[62] CrowdStrike. (2025). CrowdStrike 2025 state of ransomware survey: AI attacks are outpacing defenses. [Online]. Available: https://www.crowdstrike.com/en-us/press-releases/ransomware-report-ai-attacks-outpacing-defenses/

[63] Lakshmanan, R. (2023). Double-extortion play ransomware strikes 300 organizations worldwide. The Hacker News. [Online]. Available: https://thehackernews.com/2023/12/double-extortion-play-ransomware.html

[64] Palo Alto Networks Unit 42. (2023). Ransomware dwell time hits low of 24 hours. [Online]. Available: https://unit42.paloaltonetworks.com/ransomware-dwell-time/

[65] Security Info Watch. (2025). Ransomware as a service: The billion-dollar threat hiding in plain sight. [Online]. Available: https://www.securityinfowatch.com/cybersecurity/article/55294456/ransomware-as-a-service-the-billion-dollar-threat-hiding-in-plain-sight

[66] TechDator. (2021). Kaseya supply-chain attack hit over 1,500 companies. [Online]. Available: https://techdator.net/kaseya-supply-chain-attack-impact/

[67] CyberSecurity Place. (2025). Supply chain attacks: The next frontier in cybersecurity threats. [Online]. Available: https://cybersecurityplace.medium.com/supply-chain-attacks-the-next-frontier-in-cybersecurity-threats-afb221c1c72a

[68] Cornelissen, E., & Balliu, M. (2025). NodeShield: Runtime enforcement of security-enhanced SBOMs for Node.js. arXiv preprint. https://doi.org/10.48550/arXiv.2508.13750

[69] Check Point Software Technologies. (2025). Top cloud security trends in 2025. [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-code-security/top-cloud-security-trends-in-2025/

[70] TechRadar. (2025). AWS systems targeted by crypto mining scam using hijacked IAM credentials. [Online]. Available: https://www.techradar.com/pro/security/aws-systems-targeted-by-crypto-mining-scam-using-hijacked-iam-credentials

[71] Check Point Research. (2025). The alarming surge in compromised credentials in 2025. [Online]. Available: https://blog.checkpoint.com/security/the-alarming-surge-in-compromised-credentials-in-2025

[72] echRadar. (2025). State actors are abusing OAuth device codes to get full M365 account access. [Online]. Available: https://www.techradar.com/pro/security/state-actors-are-abusing-oauth-device-codes-to-get-full-m365-account-access-heres-what-we-know

[73] Madireddy, V. T. (2025). Graph neural network based adaptive threat detection for cloud identity and access management logs. arXiv preprint. https://doi.org/10.48550/arXiv.2512.10280

[74] Majumder, C. (2024). The cybersecurity challenges of operational technology (OT). Journal of Industrial Information Integration, 28, 100447. https://doi.org/10.1016/j.jii.2024.100447

[75] Ampcus Cyber. (2025). Coordinated probing campaign targets Microsoft Remote Desktop Services. [Online]. Available: https://www.ampcuscyber.com/shadowopsintel/coordinated-probing-campaign-targets-microsoft-remote-desktop-services

[76] Sundberg, L., & Roy, J. (2025). Generative AI and digital resilience: A research agenda. Journal of Risk Research. Advance online publication. https://doi.org/10.1080/13669877.2025.2539105

[77] Tallam, K. (2025). CyberSentinel: An emergent threat detection system for AI security. arXiv preprint.https://doi.org/10.48550/arXiv.2502.14966

[78] McAfee. (2024). McAfee state of the scamiverse 2024: AI-driven threats and scams. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/state-of-the-scamiverse-2024/

[79] Alauthman, M., Aslam, N., Khan, M. U., Khan, M. A., & Hussain, S. (2023). A hybrid deep learning approach for network anomaly detection. Computers & Security, 125, 103032. https://doi.org/10.1016/j.cose.2022.103032

[80] Wojak, G., Górka, E., Ćwiąkała, M., Baran, D., Reśko, D., Wyrzykowska-Antkiewicz, M., Marczuk, R., Agaciński, M., Zawadzki, D., & Piwnik, J. (2025). Data protection and corporate reputation management in the digital era. *arXiv preprint*, arXiv:2512.15794. https://doi.org/10.48550/arXiv.2512.15794

[81] Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H., Lewis, M., Yih, W.-t., Rocktäschel, T., Riedel, S., & Kiela, D. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. In Advances in Neural Information Processing Systems (Venue: NeurIPS), 33, 9459–9474

[82] Holocron Cyber. (2025). Essential Eight audit: Australian Cyber Security Centre compliance. [Online]. Available: https://www.holocroncyber.com.au/essential-eight-audit/

[83] Cybersecurity and Infrastructure Security Agency. (2024). FY2025–2026 CISA international strategic plan. [Online]. Available: https://www.cisa.gov/2025-2026-cisa-international-strategic-plan

[84] Trellix. (2024). Trellix endpoint security technical documentation. [Online]. Available: https://docs.trellix.com/bundle/endpoint-security-10.7.x-product-guide/page/GUID

[85] eNeoteric. (2021). Endpoint detection and response (EDR) vs. traditional antivirus: What's the difference? [Online]. Available: https://encse.com/endpoint-detection-and-response-edr-vs-traditional-antivirus-whats-the-difference/

[86] Atlas Systems. (2025). Endpoint detection and response (EDR): A security must. [Online]. Available: https://www.atlassystems.com/blog/endpoint-detection-and-response

[87] Roy, S., et al. (2025). Endpoint security agent: A comprehensive approach to real-time system monitoring. *arXiv preprint*, arXiv:2511.08352. https://doi.org/10.48550/arXiv.2511.08352

[88] Anonymous. (2023). On resource consumption of machine learning in edge devices. arXiv preprint. https://doi.org/10.48550/arXiv.2312.12345

[89] Wu, P., et al. (2025). DEFENDCLI: Command-line driven attack provenance examination. *arXiv preprint*, arXiv:2508.12553. https://doi.org/10.48550/arXiv.2508.12553

[90] Nfina. (2025). Signature-based detection vs. behavioral analysis. [Online]. Available: https://nfina.com/signature-based-detection-vs-behavioral-analysis/

[91] SpotSaaS. (2025). Behavioral analysis in EDR software. [Online]. Available: https://www.spotsaas.com/glossary/feature/behavioral-analysis

[92] Basque-Rice, I. (2024). The hidden costs of false positives in EDR. Adarma Blog. [Online]. Available: https://adarma.com/blog/the-hidden-costs-of-false-positives-in-edr/

[93] Sanami, A., & Aghdam, S. M. (2025). Unsupervised anomaly detection in endpoint behavior using reinforcement learning. *arXiv preprint*, arXiv:2501.00000. https://arxiv.org/abs/2501.00000

[94] Al-Hawawreh, M., Sitnikova, E., & Aboutorab, N. (2023). An intrusion detection model to detect zero-day attacks using machine learning. Frontiers in Neuroscience, 17, 1138994. https://doi.org/10.3389/fnins.2023.1138994

[95] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[96] Yang, S., et al. (2021). Hunter in the dark: Discover anomalous network activity. *arXiv preprint*, arXiv:2105.09157. https://doi.org/10.48550/arXiv.2105.09157

[97] Chyou, C. C., et al. (2023). Unsupervised adversarial detection without extra model. *arXiv preprint*, arXiv:2308.03243. https://doi.org/10.48550/arXiv.2308.03243

[98] Doppalapudi, S. (2025). Advanced threat intelligence fusion frameworks. *Journal of Cybersecurity*.

[99] SentinelOne. (2019). SentinelOne disrupts the EDR paradigm, making MITRE ATT&CK new standard. [Online]. Available: https://www.sentinelone.com/press/sentinelone-disrupts-the-edr-paradigm-making-mitre-attck-framework-new-hunting-standard/

[100] CrowdStrike. (2023). CrowdStrike achieves 100% protection in MITRE Engenuity ATT&CK evaluation. [Online]. Available: https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-achieves-100-protection-100-visibility-and-100

[101] Signal Labs. (2020). EDR observations: Process tree forensic utility. [Online]. Available: https://signal-labs.com/edr-observations/

[102] OpenText. (2008). ArcSight audit quality SIEM solution: Whitepaper. [Online]. Available: https://community.opentext.com/cfs-file/__key/telligent-evolution-components-attachments/00-224-01-00-00-89-31-84/ArcSight-Audit-Quality-SIEM-Solution-_2D00_-Whitepaper.pdf

[103] Dine College. (2023). Information Technology Policy Manual. [Online]. Available: https://www.dinecollege.edu/wp-content/uploads/2023/05/IT-Policy-Manual-2023.pdf

[104] NPAV. (2025). EDR-Freeze: New tool exploits Windows function to suspend EDR and antivirus in 'coma' state. [Online]. Available: https://blogs.npav.net/blogs/post/edr-freeze-new-tool-exploits-windows-function-to-suspend-edr-and-antivirus-in-coma-state

[105] Datto. (2023). Working with ransomware rollback. [Online]. Available: https://edr.datto.com/help/Content/04-configuring-assigning-policies/ransomware-policy/ransomware-rollback.htm

[106] CrowdStrike. (2025). CrowdStrike achieves 100% detection, 100% protection, 100% accuracy in 2024 SE Labs Enterprise Advanced Security (EDR) ransomware test. [Online]. Available: https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-achieves-100-detection-100-protection-100-accuracy

[107] Augie, M. A., et al. (2024). Enhanced security monitoring & evidence collection system. In Proceedings of PRCR Conference (Venue: PRCR). [Online]. Available: https://prcr.cobimet.org/bitstreams/296d756d-07c4-475a-bb25-cb062509455a/download

[108] Microsoft. (2025). AI-5: Ensure human-in-the-loop. In Microsoft cloud security benchmark (MCSB) v2. [Online]. Available: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-v2-artificial-intelligence-security

[109] Microsoft. (2025). What is EDR? Endpoint detection and response. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response

[110] Uddin, M., Memon, Q., Alsaqour, R., Shah, A., & Khowaja, S. A. (2020). An emerging threat fileless malware: A survey. Cybersecurity, 3(1), 1. https://doi.org/10.1186/s42400-019-0043-x

[111] CISA. (2023). Endpoint detection and response: Considerations and best practices. Available: https://www.cisa.gov/sites/default/files/publications/Endpoint-Detection-and-Response-Considerations-508C.pdf

[112] Morphisec. (2020). The state of endpoint security: Third annual study. [Online]. Available: https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

[113] Swami, S., Singh, I., Singh, U., & Pant, C. P. (2025). Adaptive detection of polymorphic malware: Leveraging mutation engines and YARA rules for enhanced security. arXiv preprint. https://doi.org/10.48550/arXiv.2511.21764

[114] Al-Mhiqani, M. N., et al. (2020). A review of cybersecurity issues and compliance in healthcare systems. Journal of Industrial Information Integration, 20, 100347. https://doi.org/10.1016/j.jii.2020.100347

[115] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[116] PDI Technologies. (2025). Endpoint detection and response (EDR) service description. [Online]. Available: https://pditechnologies.com/wp-content/uploads/2025/02/Endpoint-Detection-and-Response-.pdf

[117] Sourcepass. (2025). Benefits of SIEM + EDR integration for modern security teams. [Online]. Available: https://blog.sourcepass.com/sourcepass-blog/benefits-of-siem-edr-integration-for-modern-security-teams

[118] AV-Comparatives. (2025). EDR detection validation certification test 2025: Palo Alto Networks Cortex XDR Pro. [Online]. Available: https://www.av-comparatives.org/wp-content/uploads/2025/06/EDR_Detection_Palo Alto_2025.pdf

[119] Shimizu, N., & Hashimoto, M. (2025). Vulnerability management chaining: An integrated framework for efficient cybersecurity risk prioritization. *arXiv preprint*, arXiv:2506.01220. https://doi.org/10.48550/arXiv.2506.01220

[120] Oliver, J., Batta, R., Bates, A., Inam, M. A., Mehta, S., & Xia, S. (2024). Carbon filter: Real-time alert triage using large scale clustering and fast search. arXiv preprint. https://doi.org/10.48550/arXiv.2405.04691

[121] SoftwareOne. (2023). Quick start guide to Endpoint Detection and Response. [Online]. Available: https://www.softwareone.com/en/now/quick-start-guide-to-endpoint-detection-and-response

[122] Secureworks. (2025). NDR buyer's guide: Network detection and response. [Online]. Available: https://www.secureworks.com/resources/bg-secureworks-taegis-ndr-buyers-guide

[123] Data Center Dynamics. (2025). Monitoring networks with passive optical TAPs. [Online]. Available: https://www.datacenterdynamics.com/en/opinions/monitoring-networks-with-passive-optical-taps/

[124] Wikipedia contributors. (2023). NetFlow. In Wikipedia, The Free Encyclopedia. [Online]. Available: https://en.wikipedia.org/wiki/NetFlow

[125] Amazon Web Services. (n.d.). Flow log limitations. In Amazon Virtual Private Cloud user guide. [Online]. Available: https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-limitations.html

[126] Khedr, A. M., Raj, P. V. P., & Al Ali, A. (2020). An energy-efficient data acquisition technique for hierarchical cluster-based wireless sensor networks. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 11(3), 70–86. https://doi.org/10.22667/JOWUA.2020.09.30.070

[127] Goldfarb, J. (2014). Smart collection and storage method for network traffic data (CMU/SEI-2014-TR-011). [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2014_005_001_304866.pdf

[128] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security, 28*(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

[129] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1–2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

[130] Ferguson-Walter, K., Fugate, S., Mauger, J., Major, M., & Van Bruggen, D. (2019). Game theory for adaptive defensive cyber deception. In Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (Venue: HotSoS), 1–8. https://doi.org/10.1145/3314058.3314063

[131] Rafi, M. M., & Sukriya, M. A. (2023). Unsupervised learning based network anomaly detection using one-class SVM, isolation forest, and LOF in IoT systems. Journal of IoT Security and Smart Technologies, 5(1), 1–10. https://doi.org/10.36548/jisst.2023.1.001

[132] Janbi, N. F. (2024). AI-driven intrusion detection in IoV communication: Insights from CICIoV2024 dataset. International Journal of Advanced Computer Science and Applications, 15(8), 850–858. https://doi.org/10.14569/IJACSA.2024.0150892

[133] Kandanaarachchi, S. (2021). Unsupervised anomaly detection ensembles using item response theory. *arXiv preprint*, arXiv:2106.06243. https://arxiv.org/abs/2106.06243

[134] Davletshina, D., Melnychuk, V., Tran, V., Singla, H., Berrendorf, M., Faerman, E., & Fromm, M. (2020). Unsupervised anomaly detection for X-ray images. *arXiv preprint*, arXiv:2001.10883. https://arxiv.org/abs/2001.10883

[135] Gutteridge, B., & Huston, C. (2020). The impact of transport header encryption on operation and evolution of the internet. In Proceedings of the ACM SIGCOMM Workshop on Evolution, Performance, and Interoperability of QUIC (Venue: EPIQ), 33–38. https://doi.org/10.1145/3405796.3405828

[136] Cook, M., Marnerides, A., Johnson, C., & Pezaros, D. (2024). A survey on industrial control system digital forensics: Challenges, advances and future directions. IEEE Communications Surveys & Tutorials, 26(3), 1748–1779. https://doi.org/10.1109/COMST.2024.3359668

[137] Paul, S., Shafi, I., & Walia, A. (2022). DNS over HTTPS detection using machine learning. In Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (Venue: CSR), 55–60.

https://doi.org/10.1109/CSR54599.2022.9850321

[138] Anderson, B., & McGrew, D. (2016). Identifying encrypted malware traffic using TLS fingerprints and DNS. In 2016 IEEE Symposium on Security and Privacy (Venue: SP), 943–960. https://doi.org/10.1109/SP.2016.60

[139] Squillace, J., Cappella, J., & Sepp, A. (2024). User vulnerabilities in AI-driven systems: Current cybersecurity threat dynamics and malicious exploits in supply chain management and project management. In 2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (Venue: ICETSIS), 1–6. https://doi.org/10.1109/ICETSIS61505.2024.10459644

[140] Trevisan, M., Giordano, D., Traversi, C., & Mellia, M. (2021). Automatic fingerprinting of vulnerable IoT devices from mobile traffic data. Computer Networks, 185, 107690. https://doi.org/10.1016/j.comnet.2020.107690

[141] Trevisan, M., Giordano, D., Traversi, C., & Mellia, M. (2021). Automatic fingerprinting of vulnerable IoT devices from mobile traffic data. *Computer Networks*, *185*, 107690. https://doi.org/10.1016/j.comnet.2020.107690

[142] Dao, C., Tong, V., Hoang, N. T., Tran, H. A., & Tran, T. X. (2023). Enhancing encrypted traffic classification with deep adaptation networks. In 2023 IEEE 48th Conference on Local Computer Networks (Venue: LCN), 1–4. https://doi.org/10.1109/LCN58115.2023.10331231

[143] Yamansavascilar, B., Guvensan, M. A., Yavuz, A. G., & Karsligil, M. E. (2017). Application identification via network traffic classification. In 2017 International Conference on Computing, Networking and Communications (Venue: ICNC), 843–848. https://doi.org/10.1109/ICCNC.2017.7876242

[144] Dowling, B., Fischlin, M., Günther, F., & Stebila, D. (2021). A cryptographic analysis of the TLS 1.3 handshake protocol. Journal of Cryptology, 34(1), 4. https://doi.org/10.1007/s00145-020-09384-1

[145] Fischlin, M., Günther, F., Schmidt, C., & Warinschi, B. (2016). Key confirmation in key exchange: a formal treatment and implications for TLS 1.3. In 2016 IEEE Symposium on Security and Privacy (Venue: SP), 452–469. https://doi.org/10.1109/SP.2016.34

[146] Sundaresan, S., Magharei, N., Feamster, N., & Snoeren, A. C. (2023). Bisecting the middle out: The web connectivity implications of QUIC deployment. Proceedings of the ACM on Networking, 1(CoNEXT3), 1–27. https://doi.org/10.1145/3629139

[147] Zhou, J., Li, S., Zhang, J., Lu, Z., & Qin, B. (2024). Challenges and advances in encrypted traffic classification: A comprehensive survey. *Electronics*, *13*(20), 4000. https://doi.org/10.3390/electronics13204000

[148] Lyu, M., Ganesan, D., Sivaraman, A., & Yang, J. (2022). Automatic network function development for QUIC. In Proceedings of the 17th ACM Workshop on Mobility in the Evolving Internet Architecture (Venue: MobiArch), 13–18. https://doi.org/10.1145/3545179.3555756

[149] Shittu, M. A., Shittu, H. A., Adeleke, O. J., & Adedokun, O. J. (2023). Digital twin modeling for real time monitoring and fault detection in smart substations. International Journal of Industrial Engineering, 14(2), 25–44. https://doi.org/10.54216/IJIE.140203

[150] Pidikiti, D. S., Kalluri, R., Kumar, R. S., & Bindu, C. S. (2012). SCADA communication protocols: Vulnerabilities, attacks and possible mitigations. CSI Journal of Computing, 1(2), 135–141. https://doi.org/10.5120/csi-2012-0115

[151] Raza, S., Voigt, T., & Jutvik, V. (2012). Lightweight ICMPv6 message compression for 6LoWPAN. In Proceedings of the 7th International Conference on Body Area Networks (Venue: BodyNets), 1–7. https://doi.org/10.4108/icst.bodynets.2012.250012

[152] Barbosa, R. R. R., Sadre, R., & Pras, A. (2013). A first look into SCADA network traffic. In 2013 IEEE Network Operations and Management Symposium (Venue: NOMS), 1–8. https://doi.org/10.1109/NOMS.2013.6526338

[153] OpenText. (2024). OpenText 2024 Threat Hunter Perspectives: Insights from the front lines. [Online]. Available: https://www.opentext.com/media/report/opentext-2024-threat-hunter-perspectives-insights-from-the-front-lines-report-en.pdf

[154] Alabady, S. A., & Al-Turjman, F. (2020). Anomaly detection in industrial networks using deep learning. IEEE Transactions on Industrial Informatics, 16(8), 5244–5253. https://doi.org/10.1109/TII.2019.2952917

[155] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

[156] Tuptuk, N., & Hailes, S. (2018). The cyberattack on Ukraine's power grid is a warning of what's to come. Nature, 562(7726), 182–183. https://doi.org/10.1038/d41586-018-06914-2

[157] Yang, Y., McLaughlin, K., Sezer, S., & Im, E. G. (2017). Multiattribute SCADA-specific intrusion detection system for power networks. IEEE Transactions on Power Delivery, 32(3), 1472–1482. https://doi.org/10.1109/TPWRD.2016.2582527

[158] Microsoft. (2025). Microsoft Defender XDR documentation. [Online]. Available: https://learn.microsoft.com/en-us/defender-xdr/

[159] Secureworks. (2024). Extended Detection and Response (XDR) Buyer's Guide. Secureworks. https://www.secureworks.com/resources/rp-xdr-buyers-guide

[160] D3 Security. (2024). Improving Security Operations Through SASE and XDR. [Online]. Available: https://d3bql97l1ytoxn.cloudfront.net/app_resources/458881/documentation/1462451_1732083805617_en-US.pdf

[161] Bowman, B., Laprade, C., Ji, Y., & Huang, H. H. (2020). Detecting lateral movement in enterprise computer networks with unsupervised graph AI. In Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (Venue: RAID), 257–268. https://doi.org/10.14722/raid.2020.23753

[162] Mabrouk, A., Hatem, M., Mamun, M., & Saad, S. (2025). LMDG: Advancing lateral movement detection through high-fidelity dataset generation. arXiv preprint. https://doi.org/10.48550/arXiv.2508.02942

[163] SpyCloud. (2025). Insider Threat Pulse Report 2025: Trends from 100 Security Leaders. [Online]. Available: https://spycloud.com/resource/report/insider-threat-pulse-report-2025/

[164] AnySecura. (2025). Insider Threats in 2025: Key Trends, Real Cases, and How to Prevent Them. [Online]. Available: https://www.anysecura.com/blogs/insider-threat-trends.html

[165] Palo Alto Networks. (2025). What Is a Software Bill of Materials (SBOM)? [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-software-bill-materials-sbom

[166] Forrester Consulting. (2025). The Total Economic Impact™ Of Palo Alto Networks Cortex XSIAM. [Online]. Available: https://tei.forrester.com/go/PaloAltoNetworks/CortexXSIAM/index.html

[167] DigitalDefynd. (2025). 50 Surprising Data Engineering Facts & Statistics [2025]. [Online]. Available: https://digitaldefynd.com/IQ/surprising-data-engineering-facts-statistics/

[168] IJIRT. (2025). Vendor Lock-In: Causes and Effects. International Journal of Innovative Research in Technology, 12(1). [Online]. Available: https://ijirt.org/publishedpaper/IJIRT180346_PAPER.pdf

[169] Splunk. (2025). Avoiding Vendor Lock-in with Open XDR Architectures. [Online]. Available: https://www.splunk.com/en_us/cybersecurity-solutions/xdr.html

[170] Linux Foundation. (2025). The Open Cybersecurity Schema Framework (OCSF) Project. [Online]. Available: https://ocsf.io/

[171] Chismon, D., & Ruks, M. (2015). Threat intelligence: Collecting, analysing, evaluating. [Online]. Available: https://www.mwrinfosecurity.com/system/assets/884/original/Threat_Intelligence_Whitepaper.pdf

[172] Mordor Intelligence. (2025). Managed Detection & Response Market Report - Industry Growth Driven by AI. [Online]. Available: https://www.mordorintelligence.com/industry-reports/managed-detection-and-response-market

[173] why Q1 vs Q2? Turner, J., et al. (2025). The Forrester Wave™: Managed Detection And Response Services, Q2 2025. Forrester Research. [Online]. Available: https://www.forrester.com/report/the-forrester-wave-tm-managed-detection-and-response-services-q1-2025/RES182001

[174] King, I. J., & Huang, H. H. (2023). EULER: Detecting network lateral movement via scalable temporal link prediction. ACM Transactions on Privacy and Security, 26(3), 1–36. https://doi.org/10.1145/3588773

[175] Ho, G., Dhiman, A., et al. (2021). Hopper: Modeling and detecting lateral movement. In Proceedings of the 30th USENIX Security Symposium (Venue: USENIX Security), 3093–3110. https://www.usenix.org/conference/usenixsecurity21/presentation/ho

[176] Fortinet. (2025). 2025 cybersecurity skills gap global research report. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/reports/2025-cybersecurity-skills-gap-report.pdf

[177] ISC)². (2025). 2025 ISC2 cybersecurity workforce study. [Online]. Available: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

[178] World Economic Forum. (2025). Global cybersecurity outlook 2025. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[179] SANS Institute & GIAC. (2025). *2025 cybersecurity workforce research report*. https://www.sans.org/mlp/2025-attract-hire-retain-cybersecurity-roles

[180] Global Cybersecurity Forum & Boston Consulting Group. (2024). *Cybersecurity workforce report: Bridging the workforce shortage and skills gap*. https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap

[181] Shoard, P., Davies, A., Berrios, A., & Lawson, C. (2025). *Market guide for managed detection and response services*. Gartner. https://www.gartner.com/en/documents/5522796

[182] Bussa, T., Kavanagh, K., Deshpande, S., Lawson, C., & Shoard, P. (2019). *Market guide for managed detection and response services*. Gartner. https://www.gartner.com/en/documents/3314023

[183] Milone, M., Lee, T., & Wah, M. (2023). *Emerging tech: Security – Adoption growth insights for managed detection and response*. Gartner. https://info.actzero.ai/hubfs/Adoption_Growth_for_MDR.pdf

[184] Ashford, W. (2024). *Analyst's view: Managed detection and response (MDR)*. KuppingerCole Analysts AG. https://www.kuppingercole.com/research/an81011/analyst-s-view-managed-detection-and-response-mdr

[185] Sophos. (2025). *MDR evaluation guide*. https://www.sophos.com/en-us/content/mdr-evaluation-guide

[186] eSentire. (2025). *2025 Gartner market guide for managed detection and response*. https://www.esentire.com/resources/library/2025-gartner-market-guide-for-managed-detection-and-response-services

[187] Rapid7. (2025). *Make the business case for managed detection and response (MDR)*. https://www.rapid7.com/blog/post/dr-2025-gartner-market-guide-for-mdr-takeaways

[188] Arctic Wolf. (2025). *Co-managed MDR for enterprise teams*. https://arcticwolf.com/solutions/co-managed-mdr

[189] CrowdStrike. (2025). *Managed detection and response (MDR)*. https://www.crowdstrike.com/cybersecurity-101/managed-detection-and-response-mdr

[190] Palo Alto Networks. (2025). *Unit 42 managed detection and response (MDR) service*. https://www.paloaltonetworks.com/cyberpedia/what-is-managed-detection-and-response

[191] Binary Defense. (2025). *Five critical criteria for evaluating managed detection and response (MDR)*. https://binarydefense.com/resources/blog/5-critical-criteria-for-evaluating-managed-detection-response-mdr

[192] Integrity360. (2023). *Managed detection and response (MDR) in 20 cybersecurity statistics*. https://insights.integrity360.com/managed-detection-and-response-mdr-in-20-cyber-security-statistics

[193] WatchGuard. (2025). *WatchGuard Total MDR: Full-stack AI-driven security for MSPs*. https://www.watchguard.com/wgrd-news/press-releases/watchguard-launches-total-mdr-deliver-full-stack-ai-driven-security-msps

[194] Sygnia. (2025). *Integrating MDR with existing cybersecurity infrastructure*. https://www.sygnia.co/blog/mdr-integration

[195] CyberProof. (2025). *How 2025 shaped managed detection and response (MDR)*. https://www.cyberproof.com/manageddetectionandresponse/how-2025-shaped-managed-detection-and-response-mdr

[196] UnderDefense. (2025). *MDR buyers guide 2025*. https://www.underdefense.com/resources/mdr-buyers-guide-2025

[197] Shoard, P., Davies, A., Schneider, M., Berrios, A., & Lawson, C. (2024). *Market guide for managed detection and response*. Gartner. https://lmntrix.com/res/2024_gartner_mdr_market_guide.pdf

[198] Info-Tech Research Group. (2025). *2025 managed detection and response data quadrant report*. https://www.softwarereviews.com/categories/managed-detection-response

[199] Baird, J. (2025). *Mitigating the cybersecurity workforce shortage with the NIST NICE framework*. ISACA Journal, 2025(2). https://www.isaca.org/resources/isaca-journal/issues/2025/volume-2/mitigating-the-cybersecurity-workforce-shortage-with-the-nist-nice-framework

[200] Burrell, D. N. (2018). *An exploration of the cybersecurity workforce shortage*. *International Journal of Hyperconnectivity and the Internet of Things*, 2(1), 37–57. https://doi.org/10.4018/IJHIoT.2018010103

[201] Fortinet. (2025). *2025 cybersecurity skills gap global research report*. https://www.fortinet.com/content/dam/fortinet/assets/reports/2025-cybersecurity-skills-gap-report.pdf

[202] (ISC)². (2025). *2025 ISC2 cybersecurity workforce study*. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

[203] World Economic Forum. (2025). *Global cybersecurity outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[204] SANS Institute & GIAC. (2025). *2025 cybersecurity workforce research report*. https://www.sans.org/mlp/2025-attract-hire-retain-cybersecurity-roles

[205] Global Cybersecurity Forum & Boston Consulting Group. (2024). *Cybersecurity workforce report: Bridging the workforce shortage and skills gap*. https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap

[206] Shoard, P., Davies, A., Berrios, A., & Lawson, C. (2025). *Market guide for managed detection and response services*. Gartner. https://www.gartner.com/en/documents/5522796

[207] Bussa, T., Kavanagh, K., Deshpande, S., Lawson, C., & Shoard, P. (2019). *Market guide for managed detection and response services*. Gartner. https://www.gartner.com/en/documents/3314023

[208] Milone, M., Lee, T., & Wah, M. (2023). *Emerging tech: Security–adoption growth insights for managed detection and response*. Gartner. https://info.actzero.ai/hubfs/Adoption_Growth_for_MDR.pdf

[209] Ashford, W. (2024). *Analyst's view: Managed detection and response (MDR)*. KuppingerCole Analysts AG. https://www.kuppingercole.com/research/an81011/analyst-s-view-managed-detection-and-response-mdr

[210] Sophos. (2025). *MDR evaluation guide*. https://www.sophos.com/en-us/content/mdr-evaluation-guide

[211] eSentire. (2025). *2025 Gartner market guide for managed detection and response*. https://www.esentire.com/resources/library/2025-gartner-market-guide-for-managed-detection-and-response-services

[212] Rapid7. (2025). *Make the business case for managed detection and response (MDR)*. https://www.rapid7.com/blog/post/dr-2025-gartner-market-guide-for-mdr-takeaways

[213] Arctic Wolf. (2025). *Co-managed MDR for enterprise teams*. https://arcticwolf.com/solutions/co-managed-mdr

[214] CrowdStrike. (2025). *Managed detection and response (MDR)*. https://www.crowdstrike.com/cybersecurity-101/managed-detection-and-response-mdr

[215] Palo Alto Networks. (2025). *Unit 42 managed detection and response (MDR) service*. https://www.paloaltonetworks.com/cyberpedia/what-is-managed-detection-and-response

[216] Binary Defense. (2025). *Five critical criteria for evaluating managed detection and response (MDR)*. https://binarydefense.com/resources/blog/5-critical-criteria-for-evaluating-managed-detection-response-mdr

[217] Integrity360. (2023). *Managed detection and response (MDR) in 20 cybersecurity statistics*. https://insights.integrity360.com/managed-detection-and-response-mdr-in-20-cyber-security-statistics

[218] WatchGuard. (2025). *WatchGuard Total MDR: Full-stack AI-driven security for MSPs*. https://www.watchguard.com/wgrd-news/press-releases/watchguard-launches-total-mdr-deliver-full-stack-ai-driven-security-msps

[219] Sygnia. (2025). *Integrating MDR with existing cybersecurity infrastructure*. https://www.sygnia.co/blog/mdr-integration

[220] CyberProof. (2025). *How 2025 shaped managed detection and response (MDR)*. https://www.cyberproof.com/manageddetectionandresponse/how-2025-shaped-managed-detection-and-response-mdr

[221] UnderDefense. (2025). *MDR buyers guide 2025*. https://www.underdefense.com/resources/mdr-buyers-guide-2025

[222] Shoard, P., Davies, A., Schneider, M., Berrios, A., & Lawson, C. (2024). *Market guide for managed detection and response*. Gartner. https://lmntrix.com/res/2024_gartner_mdr_market_guide.pdf

[223] Info-Tech Research Group. (2025). *2025 managed detection and response data quadrant report*. https://www.softwarereviews.com/categories/managed-detection-response

[224] Baird, J. (2025). *Mitigating the cybersecurity workforce shortage with the NIST NICE framework*. *ISACA Journal*, *2025*(2). https://www.isaca.org/resources/isaca-journal/issues/2025/volume-2/mitigating-the-cybersecurity-workforce-shortage-with-the-nist-nice-framework

[225] Burrell, D. N. (2018). *An exploration of the cybersecurity workforce shortage*. *International Journal of Hyperconnectivity and the Internet of Things*, *2*(1), 37–57. https://doi.org/10.4018/IJHIoT.2018010103

[226] Smith, J. (2023). *Recovery starts with better change management*. Automation.com. https://www.automation.com/en-us/articles/june-2023/recovery-starts-better-change-management

[227] Dandye. (2023). *Automated response playbook criteria*. ADK Runbooks. https://dandye.github.io/adk_runbooks/automated_response_playbook_criteria.html

[228] Pulyala, S. R., Desetty, A. G., & Jangampet, V. D. (2019). *The impact of security orchestration, automation, and response (SOAR) on security operations center (SOC) efficiency: A comprehensive analysis*. *Turkish Journal of Computer and Mathematics Education*, *10*(3), 1545–1549. https://doi.org/10.61841/turcomat.v10i3.14323

[229] Pulyala, S. R., Desetty, A. G., & Jangampet, V. D. (2019). *The impact of security orchestration, automation, and response (SOAR) on security operations center (SOC) efficiency: A comprehensive analysis*. *Turkish Journal of Computer and Mathematics Education*, *10*(3), 1545–1549. https://doi.org/10.61841/turcomat.v10i3.14323

[230] Amos, Z. (2024). *Leveraging automation to achieve consistent cybersecurity compliance*. Automation.com. https://www.automation.com/en-us/articles/january-2024/automation-cybersecurity-compliance

[231] Khan, N. (2025). *Explainable AI-based intrusion detection systems for Industry 5.0 and adversarial XAI: A systematic review*. *Information*, *16*(12), 1036. https://doi.org/10.3390/info16121036

[232] Talukder, M. A., Islam, M. M., et al. (2022). *Machine learning in industrial control system (ICS) security: Current landscape, opportunities, and challenges*. *Journal of Intelligent Information Systems*, *59*(3), 561–586. https://doi.org/10.1007/s10844-022-00724-5

[233] Sreeja, S. R., & Saira, S. M. (2021). *Endpoint detection and response system based on machine learning*. *IOP Conference Series: Materials Science and Engineering*, *1084*, 012001. https://doi.org/10.1088/1757-899X/1084/1/012001

[234] Shu, R., Xia, T., Tu, H., Williams, L., & Menzies, T. (2022). *Reducing the cost of training security classifiers via optimized semi-supervised learning*. arXiv. https://arxiv.org/abs/2205.00665

[235] Apruzzese, G., Pajola, L., & Conti, M. (2022). *The cross-evaluation of machine learning-based network intrusion detection systems*. arXiv. https://arxiv.org/abs/2203.04686

[236] Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A. (2014). *A survey on concept drift adaptation*. *ACM Computing Surveys*, *46*(4), 1–37. https://doi.org/10.1145/2523819

[237] Li, E., Shang, Z., Gungor, O., & Simunic, T. (2025). *SAFE: Self-supervised anomaly detection framework for intrusion detection*. arXiv. https://arxiv.org/abs/2502.07119

[238] Al, S., & Sagiroglu, S. (2025). *Explainable artificial intelligence models in intrusion detection systems*. *Engineering Applications of Artificial Intelligence*, *132*, 107945. https://doi.org/10.1016/j.engappai.2025.107945

[239] Sarker, I. H. (2021). *CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks.* arXiv. https://arxiv.org/abs/2104.08080

[240] Lim, J., Na, J., & Kwak, N. (2023). *Active semi-supervised learning by exploring per-sample uncertainty and consistency.* arXiv. https://arxiv.org/abs/2303.08978

[241] Reynaud, S., & Roxin, A. (2025). *Review of explainable artificial intelligence for cybersecurity systems. Discover Artificial Intelligence, 5*, 1–20. https://doi.org/10.1007/s44163-025-00123-4

[242] Mutalib, N. H. A., et al. (2025). *An explainable recursive feature elimination to detect advanced persistent threats using random forest classifier.* arXiv. https://arxiv.org/abs/2511.09603

[243] Reynaud, S., & Roxin, A. (2025). *Review of explainable artificial intelligence for cybersecurity systems. Discover Artificial Intelligence, 5*, 1–20. https://doi.org/10.1007/s44163-025-00123-4

[244] European Parliament. (2024). *EU AI Act: First regulation on artificial intelligence.* https://www.europarl.europa.eu/topics/en/article/20230601STO93804

[245] Stanbridge, R. (2024). *Overreliance on automated tooling: A big cybersecurity mistake.* ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2024/overreliance-on-automated-tooling-a-big-cybersecurity-mistake

[246] Turcotte, N., et al. (2025). *Automated alert classification and triage (AACT): An intelligent system for the prioritisation of cybersecurity alerts.* arXiv. https://arxiv.org/abs/2505.09843

[247] Turcotte, N., et al. (2025). *Automated alert classification and triage (AACT): An intelligent system for the prioritisation of cybersecurity alerts.* arXiv. https://arxiv.org/abs/2505.09843

[248] Ahmadi, S. (2025). *Autonomous identity-based threat segmentation in zero trust architectures.* arXiv. https://arxiv.org/abs/2501.06281

[249] Mohsin, A., et al. (2025). *A unified framework for human–AI collaboration in security operations centers with trusted autonomy.* arXiv. https://arxiv.org/abs/2505.23397

[250] The Cyber Ape. (2025). *Security metrics automation: Measuring security effectiveness.* https://thecyberape.com/articles/25-security-metrics-automation/

[251] Critical Start. (n.d.). *Complete signal coverage for confident threat detection.* Critical Start. https://www.criticalstart.com/resources/complete-signal-coverage-for-confident-threat-detection/

[252] Microsoft. (2025). *Complete production infrastructure inventory – Zero Trust.* Microsoft Learn. https://learn.microsoft.com/en-us/security/zero-trust/sfi/complete-production-infrastructure-inventory

[253] Chuvakin, A., Schmidt, K., & Phillips, C. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors, 21*(14), 4759. https://doi.org/10.3390/s21144759

[254] Iskhakov, A. L., & Iskhakov, R. A. (2020). Data normalization models in the security event management systems. *Proceedings of the International Conference on Industrial Engineering.* https://www.researchgate.net/publication/346858070_Data_Normalization_Models_in_the_Security_Event_Management_Systems

[255] Callegati, F., & Prandini, M. (2023). Time-sensitive networking security: Issues of precision time protocol and its implementation. *Cybersecurity,* 6(1), 8. https://doi.org/10.1186/s42400-023-00140-5

[256] Yu, S. (2020). Entity resolution with recursive blocking. *Big Data Research, 19–20*, 100134. https://doi.org/10.1016/j.bdr.2020.100134

[257] Rosso, M., Campobasso, M., Gankhuyag, G., & Allodi, L. (2020). SAIBERSOC: Synthetic attack injection to benchmark and evaluate the performance of security operation centers. *arXiv.* https://arxiv.org/abs/2010.08453

[258] Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE Security & Privacy, 12*(5), 35–41. https://doi.org/10.1109/MSP.2014.89

[259] Amazon Web Services. (2025). *Building a modern security data lake on AWS.* Amazon Web Services. https://aws.amazon.com/solutions/security-data-lake/

[260] Mavrommatis, N., et al. (2024). Extended detection and response (XDR): Evolution and challenges. *Computers & Security, 135*, 103512. https://doi.org/10.1016/j.cose.2024.103512

[261] Umer, M. A., et al. (2021). Network detection and response: A survey. *Journal of Network and Computer Applications, 184*, 103069. https://doi.org/10.1016/j.jnca.2021.103069

[262] National Institute of Standards and Technology. (2024). *Cybersecurity for safety-critical systems: Constraints and best practices*. NIST. https://www.nist.gov/publications/cybersecurity-safety-critical-systems

[263] Zhai, Z., et al. (2020). IoT-RECSM—Resource-constrained smart service migration framework for IoT edge computing environment. *Sensors, 20*(8), 2294. https://doi.org/10.3390/s20082294

[264] Alaba, F. A., et al. (2024). Security at the edge for resource-limited IoT devices. *Sensors, 24*(2), 590. https://doi.org/10.3390/s24020590

[265] European Banking Authority. (2025). *Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554*. https://www.eba.europa.eu/regulation-and-policy/digital-operational-resilience

[266] U.S. Securities and Exchange Commission. (2023). *Cybersecurity disclosures: SEC Rule 2023 compliance guide*. https://www.sec.gov/cybersecurity

[267] SEI U.S. (2025). *The true cost of fragmented cybersecurity and how to fix it*. https://www.seic.com/banks-wealth-managers/true-cost-fragmented-cybersecurity-and-how-fix-it

[268] Kruse, C. S., et al. (2023). Security vulnerabilities in healthcare: An analysis of medical devices and software. *Digital Health, 9*. https://doi.org/10.1177/20552076231218800

[269] Ho, G., et al. (2021). Hopper: Modeling and detecting lateral movement. *Proceedings of the 30th USENIX Security Symposium*. https://www.usenix.org/conference/usenixsecurity21/presentation/ho

[270] Bitdefender. (2024). *Healthcare managed detection and response (MDR) solution guide*. https://www.bitdefender.com/business/solutions/healthcare-mdr.html

[271] Bytes, A., et al. (2022). FieldFuzz: In situ black-box fuzzing of proprietary industrial automation runtimes via the network. *arXiv*. https://arxiv.org/abs/2204.13499

[272] Dell Technologies. (2024). *Why MDR is integral to cybersecurity: ESG showcase*. https://www.delltechnologies.com/en-us/esg/showcases/mdr-cybersecurity.htm

[273] Manufacturing.net. (2024). *$4.2M per hour lost from cybersecurity breaches*. https://www.manufacturing.net/cybersecurity/news/22914694/42m-per-hour-lost-from-cybersecurity-breaches

[274] Sassnick, O., Schäfer, G., Rosenstatter, T., & Huber, S. (2024). A generative model-based honeypot for industrial OPC UA communication. *arXiv*. https://arxiv.org/abs/2410.21574

[275] Campobasso, M., & Allodi, L. (2020). SAIBERSOC: Synthetic attack injection for SOC evaluation. *Proceedings of the Annual Computer Security Applications Conference*. https://doi.org/10.1145/3427228.3427233

[276] Kentucky Hospital Association. (2025). *Cybersecurity: Boards must prepare for increased attacks*. *Kentucky Trustee*. https://www.kyha.com/wp-content/uploads/2025/06/KTSpring25.pdf

[277] Wang, S., Dong, F., Yang, H., Xu, J., & Wang, H. (2024). CanCal: Towards real-time and lightweight ransomware detection and response in industrial environments. *arXiv preprint* arXiv:2408.16515. https://arxiv.org/abs/2408.16515

[278] Mandala, N. R. (2022). Data engineering in cloud-native architectures. *ESP Journal of Engineering & Technology Advancements, 2*(2), 135–145. https://www.espjeta.org/jeta-v2i2p115.php

[279] Ghoson, N. H., Meyrueis, V., Benfriha, K., Guiltat, T., & Loubère, S. (2025). A review on the static and dynamic risk assessment methods for OT cybersecurity in industry 4.0. *Computers & Security, 150*, 104295. https://doi.org/10.1016/j.cose.2024.104295

[280] Forrester Consulting. (2022). *The total economic impact™ of Microsoft SIEM and XDR*. Forrester. https://www.microsoft.com/en-us/security/business/forrester-tei-study

[281] Mehedi, S. T., Jurdak, R., Islam, C., & Ramachandran, G. (2025). QUT-DV25: A dataset for dynamic analysis of next-gen software supply chain attacks. *arXiv preprint* arXiv:2505.13804. https://arxiv.org/abs/2505.13804

[282] Luxemburk, J., Hynek, K., & Čejka, T. (2023). Encrypted traffic classification: The QUIC case. *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*, 1–8. https://doi.org/10.23919/TMA58422.2023.10199052

[283] Qiu, K., Wang, Y., Li, B., & Zhu, W. (2025). Unsupervised dataset cleaning framework for encrypted traffic classification. *arXiv preprint* arXiv:2509.00701. https://arxiv.org/abs/2509.00701

[284] Kwon, T., & Su, Z. (2012). Detecting and analyzing insecure component usage. *Proceedings of the ACM SIGSOFT International Symposium on Foundations of Software Engineering*, 35–45. https://doi.org/10.1145/2393596.2393633

[285] ReversingLabs. (2025). *ReversingLabs annual software supply chain security report*. ReversingLabs. https://www.reversinglabs.com/resources/reports

[286] Gurabi, M. A., et al. (2025). From legacy to standard: LLM-assisted transformation of cybersecurity playbooks into CACAO format. *arXiv preprint* arXiv:2508.03342. https://arxiv.org/abs/2508.03342

[287] Geng, R., et al. (2025). PISanitizer: Preventing prompt injection to long-context LLMs via prompt sanitization. *arXiv preprint* arXiv:2511.10720. https://arxiv.org/abs/2511.10720

[288] Khayatbashi, S., et al. (2025). AI-enhanced business process automation: A case study in the insurance domain. *arXiv preprint* arXiv:2504.17295. https://arxiv.org/abs/2504.17295

[289] Liyanage, L., Arachchilage, N. A., & Russello, G. (2024). SoK: Identifying limitations and bridging gaps of cybersecurity capability maturity models (CCMMs). *arXiv preprint* arXiv:2408.16140. https://arxiv.org/abs/2408.16140

[290] Xu, T., et al. (2025). L2M-AID: Autonomous cyber-physical defense by fusing semantic reasoning of LLMs with reinforcement learning. *arXiv preprint* arXiv:2510.07363. https://arxiv.org/abs/2510.07363

[291] Ghoson, N. H., Meyrueis, V., Benfriha, K., Guiltat, T., & Loubère, S. (2025). A review on the static and dynamic risk assessment methods for OT cybersecurity in industry 4.0. *Computers & Security, 150*, 104295. https://doi.org/10.1016/j.cose.2024.104295