Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Mitigating Advanced Persistent Threats in Resource-Constrained Environments: Design and Implementation of a Lightweight Endpoint Detection and Response (EDR) Framework for Small-Scale Enterprises

Author:
Chermaine Grace Balando
Amstrong Luiese Landeza
Kaisen Joy Cupon
Joey T. Rosales

Co-Author:
Ferdinand C. Somido, PhD

Co-Researcher:
Mr. JaimeYatco

1 – University of Perpetual Help System Laguna

Publication Date: July 20, 2026 DOI: **10.5281/zenodo.21450399**

Abstract

Advanced Persistent Threats (APTs) continue to represent one of the most significant cybersecurity challenges because of their ability to maintain persistent, covert access to target systems while evading conventional security mechanisms (Akbar et al., 2023; Hutchins et al., 2011). The prolonged dwell time and sophisticated attack strategies employed by APT actors often result in substantial operational, financial, and reputational damage before compromise is detected. Micro and small enterprises are particularly susceptible to these threats due to constrained cybersecurity budgets, limited security infrastructure, and insufficient personnel dedicated to continuous monitoring and incident response (Blancaflor et al., 2024; Department of Information and Communications Technology [DICT], 2023). Although commercial Endpoint Detection and Response (EDR) solutions provide comprehensive endpoint visibility and automated threat detection, their acquisition, deployment, and maintenance costs frequently exceed the operational capacity of resource-constrained organizations (Blancaflor et al., 2024).

This study designed, developed, and evaluated a lightweight Endpoint Detection and Response framework specifically intended for micro and small enterprise environments. The proposed framework integrates endpoint telemetry collection, behavioral process monitoring, trust-based process assessment, rule-based detection using YARA and Sigma signatures, external cyber threat intelligence enrichment, heuristic-assisted anomaly detection, dynamic risk scoring, centralized event logging, and dashboard-based incident management to facilitate timely threat detection and analysis. The research adopted the Design Science Research Methodology (DSRM) proposed by Peffers et al. (2007), following the iterative phases of problem identification, objective definition, design and development, demonstration, evaluation, and communication.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Functional and usability evaluation was conducted by five purposively selected domain experts, comprising three information technology personnel and two system administrators, using the ISO/IEC 25010 software quality model. Technical validation was performed within a controlled small-enterprise testbed using MITRE ATT&CK-aligned adversary emulation scenarios, safe malware test artifacts, and a labeled dataset consisting of 512 endpoint events, including 68 malicious and 444 benign activities (MITRE ATT&CK, n.d.; Sikorski & Honig, 2012).

The evaluation results demonstrated that the proposed framework achieved" Highly Evident" ratings across all assessed ISO/IEC 25010 quality characteristics, including functional suitability, performance efficiency, compatibility, reliability, security, maintainability, flexibility, and safety. Comparative analysis of the pre-implementation and post-implementation evaluations showed a statistically significant improvement in the overall weighted mean score from 2.41 (Moderately Evident) to 3.55 (Highly Evident) ($p < 0.001$, $n = 5$). Cybersecurity performance evaluation further indicated robust detection capability, correctly identifying 66 true positives and 435 true negatives while producing only 9 false positives and 2 false negatives. These outcomes correspond to a detection accuracy of 97.85%, precision of 88.00%, recall of 97.06%, false positive rate of 2.03%, and false negative rate of 2.94%. Furthermore, the framework maintained an average detection and response time of 1.8 seconds, average CPU utilization of 4.6%, and average memory consumption of 105 MB, indicating that effective endpoint monitoring and APT detection can be achieved with minimal computational overhead.

Overall, the findings demonstrate that the proposed lightweight EDR framework provides an effective and resource-efficient approach for strengthening endpoint security in micro and small enterprises. By combining behavioral monitoring, signature-based detection, threat intelligence integration, and heuristic analysis within a lightweight architecture, the framework enhances endpoint visibility and supports the timely detection of APT-related activities while maintaining low resource consumption. These results suggest that the proposed solution represents a practical alternative to commercially available EDR platforms for organizations operating under resource constraints.

Keywords: *advanced persistent threats, endpoint detection and response, lightweight EDR, small-scale enterprises, MITRE ATT&CK, endpoint telemetry, cybersecurity metrics*

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

I. INTRODUCTION

The increasing adoption of remote work, cloud computing, and digital business services has transformed organizational operations while simultaneously expanding the cyberattack surface. As organizations rely more heavily on interconnected endpoint devices to access corporate resources, these endpoints have become attractive targets for increasingly sophisticated cyber threats (Department of Information and Communications Technology [DICT], 2023). This challenge is particularly pronounced among micro and small enterprises, which often operate with constrained cybersecurity budgets, limited security infrastructure, and minimal personnel responsible for continuous monitoring and incident response. Consequently, endpoint protection in these organizations frequently depends on conventional security controls, such as antivirus software, firewalls, and manual monitoring practices, which provide limited visibility into advanced attack activities (Blancaflor et al., 2024).

Among contemporary cyber threats, Advanced Persistent Threats (APTs) remain one of the most significant security concerns because of their ability to establish long-term, covert access to organizational systems while avoiding detection. Unlike opportunistic attacks that aim to disrupt services immediately, APT campaigns are characterized by carefully orchestrated, multi-stage operations that enable attackers to infiltrate networks, escalate privileges, establish persistence, move laterally across systems, and exfiltrate sensitive information over extended periods (Hutchins et al., 2011). These attack strategies commonly exploit phishing, malware deployment, credential theft, persistence mechanisms, command-and-control communication, and other techniques documented within the MITRE ATT&CK knowledge base (MITRE ATT&CK, n.d.). Their stealth-oriented nature often allows attackers to remain undetected for prolonged periods, increasing the likelihood of operational disruption, financial loss, and data compromise (Akbar et al., 2023).

The evolving tactics employed by APT actors have reduced the effectiveness of traditional signature-based security mechanisms. Attackers increasingly leverage legitimate administrative tools, polymorphic malware, encrypted communications, and living-off-the-land techniques to evade conventional detection methods (Akbar et al., 2023; Hutchins et al., 2011). Consequently, modern endpoint protection requires continuous telemetry collection, behavioral analytics, anomaly detection, and real-time monitoring to identify malicious activities that cannot be detected through static signatures alone (Akbar et al., 2023; National Institute of Standards and Technology [NIST], 2007). Endpoint Detection and Response (EDR) platforms have emerged as an effective approach by providing continuous endpoint visibility, behavioral monitoring, automated threat detection, and incident investigation capabilities through centralized collection and analysis of endpoint telemetry (Microsoft, n.d.; NIST, 2007).

Despite their effectiveness, commercially available EDR platforms often require substantial financial investment, cloud-based infrastructure, recurring subscription costs, and dedicated cybersecurity expertise for deployment and maintenance. These technical and operational requirements present significant barriers for micro and small enterprises, limiting their ability to adopt enterprise-grade endpoint protection solutions (Blancaflor et al., 2024). As a

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

result, many resource-constrained organizations continue to experience inadequate endpoint visibility, delayed threat detection, and fragmented incident response capabilities, thereby increasing their exposure to sophisticated cyberattacks.

To address these challenges, this study designed, developed, and evaluated a lightweight Endpoint Detection and Response framework tailored for resource-constrained enterprise environments. The proposed framework integrates endpoint telemetry collection, behavioral monitoring, process trust assessment, rule-based detection using YARA and Sigma signatures, threat intelligence enrichment, heuristic-assisted anomaly detection, dynamic risk scoring, centralized event logging, and dashboard-based incident management to support timely detection and analysis of APT-related activities. The framework was evaluated using the ISO/IEC 25010 software quality model, comparative before-and-after statistical analysis, MITRE ATT&CK-aligned adversary emulation, and cybersecurity performance metrics, including detection accuracy, precision, recall, false positive rate, false negative rate, response time, CPU utilization, and memory consumption. The findings provide empirical evidence regarding the feasibility of delivering effective endpoint protection while maintaining low computational overhead, thereby offering a practical cybersecurity solution for micro and small enterprises.

II. LITERATURE REVIEW

Advanced Persistent Threats and Endpoint-Based Detection

Contemporary research indicates that Advanced Persistent Threat (APT) actors increasingly employ legitimate administrative tools, persistence mechanisms, credential abuse, and stealth techniques to evade traditional security controls (Akbar et al., 2023; Hutchins et al., 2011). Consequently, effective detection must extend beyond static signature matching and instead analyze behavioral patterns derived from endpoint telemetry, including process creation, file modifications, authentication events, network connections, system configuration changes, and persistence-related activities (Akbar et al., 2023). Endpoint-centric detection is particularly important because many stages of an APT lifecycle become observable on workstations and servers before corresponding indicators appear in perimeter-based monitoring systems (National Institute of Standards and Technology [NIST], 2007).

Recent systematic reviews further reinforce the growing emphasis on behavior-based endpoint detection. Salim et al. (2023) synthesized findings from 75 studies published between 2012 and 2022 across six scientific databases and reported that contemporary APT detection research increasingly relies on machine learning and behavioral analysis rather than conventional signature-based techniques. Building on these findings, the authors proposed a cyber situational awareness model to improve the detection and prediction of APT activities in mobile environments. Similarly, Al-Kadhimi et al. (2023) reviewed 1,351 publications spanning 2012 to 2023 and introduced a complementary framework that integrates game theory with artificial

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

intelligence to model the tactics, techniques, and procedures of both attackers and legitimate users for enhanced detection of APT activities on smartphones.

Collectively, these studies demonstrate a clear shift from signature-dependent detection toward context-aware, behavior-driven monitoring across diverse computing environments. Although the reviewed frameworks primarily target mobile platforms and incorporate advanced artificial intelligence techniques, they consistently identify continuous endpoint visibility and behavioral analysis as fundamental requirements for detecting sophisticated, multi-stage attacks. These findings provide a strong theoretical foundation for the present study, which adopts the same endpoint-centric principles while emphasizing a lightweight, resource-efficient Endpoint Detection and Response framework tailored to the operational constraints of micro and small enterprises.

Endpoint Detection and Response Systems

Endpoint Detection and Response (EDR) solutions provide continuous endpoint visibility by collecting telemetry, analyzing system activities, and generating alerts that support threat investigation and incident response (Microsoft, n.d.; National Institute of Standards and Technology [NIST], 2007). Endpoint telemetry is typically derived from multiple data sources, including operating system event logs, process monitoring utilities, packet capture mechanisms, and system-level application programming interfaces (APIs), enabling the observation of both system behavior and security-relevant events. Among these sources, Microsoft Sysmon is widely used to record detailed endpoint activities such as process creation, network connections, file creation time modifications, and other events that facilitate threat detection and forensic analysis (Microsoft, n.d.).

Nevertheless, telemetry collection alone is insufficient to provide comprehensive endpoint protection. An effective EDR capability requires the integration of telemetry with complementary components, including detection and correlation engines, centralized data storage, visualization dashboards, and incident response workflows. Together, these components enable the correlation of endpoint events, identification of malicious behavioral patterns, prioritization of security alerts, and timely response to potential threats, thereby transforming raw endpoint data into actionable security intelligence (NIST, 2007).

Anomaly Detection and Behavioral Analysis

Behavior-based anomaly detection has become a fundamental component of modern endpoint security because it identifies malicious activities that deviate from established patterns of normal system behavior. Unlike signature-based approaches, which depend on previously identified attack patterns, anomaly detection examines behavioral indicators such as abnormal process execution, repeated authentication failures, unusual outbound network communication, unauthorized directory access, persistence-related modifications, and anomalous DNS activity to

detect previously unseen or evolving threats (Akbar et al., 2023; MITRE ATT&CK, n.d.). This capability is particularly valuable for detecting Advanced Persistent Threats (APTs), whose stealth-oriented techniques are specifically designed to evade conventional signature-based defenses.

For micro and small enterprises, behavior-based detection offers a practical alternative to computationally intensive artificial intelligence and machine learning models. Lightweight mechanisms, including rule-based detection, process trust assessment, heuristic analysis, and event correlation, can provide effective threat detection while maintaining low computational overhead, thereby making continuous endpoint monitoring feasible in resource-constrained environments (Akbar et al., 2023). These approaches demonstrate that effective endpoint protection does not necessarily require complex analytical models, provided that meaningful behavioral indicators are continuously collected and correlated.

MITRE ATT&CK as a Validation Framework

The MITRE ATT&CK framework provides a standardized knowledge base of adversary tactics, techniques, and procedures (TTPs) derived from observations of real-world cyber operations (MITRE ATT&CK, n.d.). Because of its comprehensive representation of attacker behavior, the framework has become a widely adopted reference for designing, validating, and benchmarking endpoint security solutions. Mapping detection capabilities to ATT&CK techniques enables researchers to evaluate whether security systems can identify representative attack behaviors across multiple phases of the intrusion lifecycle, including execution, persistence, privilege escalation, credential access, lateral movement, and command-and-control communication (MITRE ATT&CK, n.d.).

The practical value of ATT&CK-based validation is further demonstrated by independent evaluations such as the MITRE Engenuity ATT&CK Evaluations and the AV-Comparatives Endpoint Prevention and Response Test, both of which assess commercial EDR and Extended Detection and Response (XDR) platforms under realistic adversary emulation scenarios (MITRE Engenuity, 2024; AV-Comparatives, 2024). These evaluation methodologies have established ATT&CK-aligned testing as a recognized benchmark for measuring the effectiveness of endpoint security technologies against sophisticated, multi-stage attacks. Accordingly, the present study adopts the same validation framework to ensure that the proposed lightweight EDR solution is assessed using representative adversarial behaviors rather than isolated attack signatures.

Cybersecurity Challenges of Micro and Small Enterprises

Despite increasing exposure to sophisticated cyber threats, micro and small enterprises continue to face significant challenges in implementing comprehensive endpoint security. Limited financial resources, inadequate cybersecurity infrastructure, and a shortage of skilled personnel frequently result in dependence on conventional security controls, including antivirus software, firewalls, and manually administered security procedures (Blancaflor et al., 2024;

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Department of Information and Communications Technology [DICT], 2023). While these controls provide baseline protection, they generally lack the continuous endpoint visibility and behavioral analysis necessary to detect modern APT campaigns.

Although commercial Endpoint Detection and Response platforms provide comprehensive monitoring, behavioral analytics, threat intelligence integration, and automated incident response, their licensing costs, infrastructure requirements, and operational complexity often exceed the capabilities of resource-constrained organizations (Blancaflor et al., 2024). Consequently, there remains a need for lightweight and modular endpoint security solutions that can deliver effective detection capabilities while minimizing deployment costs and computational resource requirements.

Synthesis of Literature and Research Gap

The reviewed literature consistently demonstrates that contemporary endpoint protection is shifting from signature-based detection toward continuous behavioral monitoring supported by endpoint telemetry, threat intelligence, and adversary-informed validation frameworks. Existing studies also establish the effectiveness of behavior-based detection for identifying sophisticated attacks while highlighting the value of standardized evaluation methodologies, particularly those based on the MITRE ATT&CK framework. However, several research gaps remain.

First, existing cybersecurity frameworks primarily provide strategic or conceptual guidance and offer limited implementation-oriented approaches for developing lightweight Endpoint Detection and Response systems specifically designed for the operational constraints of micro and small enterprises (Blancaflor et al., 2024). Second, although previous studies frequently report cybersecurity performance metrics, relatively few integrate objective technical measures—such as detection accuracy, precision, recall, false positive rate, false negative rate, response time, and computational resource utilization—with internationally recognized software quality evaluation frameworks, including ISO/IEC 25010, within a single system development study (Akbar et al., 2023). Third, current commercial EDR platforms provide comprehensive protection but remain financially and technically inaccessible to many resource-constrained organizations because of their licensing models, infrastructure requirements, and maintenance complexity (Blancaflor et al., 2024).

To address these gaps, the present study designed, developed, and evaluated a lightweight Endpoint Detection and Response framework tailored to the operational requirements of micro and small enterprises. The proposed framework integrates endpoint telemetry collection, behavioral rule-based detection, process trust assessment, heuristic-assisted anomaly detection, adaptive risk scoring, centralized monitoring, and dashboard-based incident management within a modular architecture optimized for low computational overhead. The framework was evaluated using the ISO/IEC 25010 software quality model, MITRE ATT&CK-aligned adversary emulation scenarios, and objective cybersecurity performance metrics, including detection accuracy, precision, recall, false positive and false negative rates, response time, CPU utilization, and memory consumption. By integrating software quality assessment with comprehensive

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

cybersecurity performance evaluation, this study contributes a practical, deployable, and resource-efficient endpoint security framework that addresses the operational needs of micro and small enterprises while extending the current body of knowledge on lightweight EDR system development.

III. METHODOLOGY

3.1 Research Design

This study adopted a design and development research approach to design, implement, and evaluate a lightweight Endpoint Detection and Response (EDR) framework. Unlike descriptive research, which focuses on examining existing conditions, design and development research emphasizes the creation and systematic evaluation of artifacts that address identified practical problems. The development process followed the Design Science Research Methodology (DSRM) proposed by Peffers et al. (2007), incorporating iterative cycles of requirements analysis, system design, prototype implementation, demonstration, evaluation, and refinement. An Agile development process complemented the DSRM by enabling continuous improvement of system requirements, detection rules, user interface components, and functional capabilities based on iterative testing and evaluation outcomes.

Table 1. Research Design Phases

Phase	Activities	Output
Requirements Analysis	Identified SME cybersecurity limitations, endpoint monitoring needs, user roles, and APT-related detection requirements.	System requirements and detection scope
System Design	Prepared system architecture, data flow, module descriptions, database structure, and interface design.	EDR architecture and design specifications
Development	Built the endpoint agent, telemetry collector, detection engine,	Working lightweight EDR

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Phase	Activities	Output
	dashboard, incident module, and reporting module.	prototype
Testing	Conducted functional testing, resource monitoring, safe malware-test validation, and MITRE ATT&CK-aligned adversarial emulation.	Technical test results and defect logs
Evaluation	Administered the ISO/IEC 25010 questionnaire and compared pre-implementation and post-implementation assessment results.	Acceptability results and statistical analysis
Refinement	Improved detection rules, interface labels, reports, performance settings, and documentation based on results.	Improved EDR framework

3.2 Respondents and Sampling Technique

Purposive sampling was used to identify five domain experts consisting of three information technology (IT) personnel and two system administrators from a small-scale enterprise. The participants were selected based on their direct involvement in system administration, endpoint management, technical support, and security monitoring, enabling them to provide informed evaluations of the proposed Endpoint Detection and Response (EDR) framework. Their professional experience ensured that the assessment reflected the practical requirements and operational realities of deploying endpoint security solutions in resource-constrained organizational environments.

Participant selection was based on predefined inclusion criteria to ensure the technical expertise necessary for software quality evaluation. Eligible respondents were required to: (1) perform hands-on responsibilities related to IT support, system administration, or endpoint management; (2) possess working knowledge of endpoint security, security monitoring, or security incident management; and (3) voluntarily participate in the demonstration and

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

evaluation of the developed framework. Following the system demonstration and technical validation, the respondents assessed the framework using the ISO/IEC 25010 software quality model. The evaluation covered functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, flexibility, and the framework's overall applicability to resource-constrained enterprise environments.

Table 2. Respondent Profile

Respondent Group	Number	Role in Evaluation
Information Technology Personnel	3	Assessed functionality, performance efficiency, compatibility, maintainability, and technical usability.
System Administrators	2	Assessed security, reliability, incident review, alert interpretation, and operational practicality.
Total	5	Completed ISO/IEC 25010-based evaluation and provided user feedback.

3.3 Research Environment and Deployment Setup

The proposed framework was evaluated within a controlled small-scale enterprise testbed designed to emulate the operational characteristics of a resource-constrained organizational environment. The test environment consisted of standard workstation hardware connected through a conventional local area network (LAN) and intentionally excluded specialized enterprise-grade security infrastructure beyond baseline endpoint protection. This configuration was selected to reflect the typical computing environment of micro and small enterprises while providing a realistic setting for technical evaluation.

The experimental evaluation aimed to determine whether the proposed lightweight Endpoint Detection and Response (EDR) framework could provide continuous endpoint telemetry collection, behavioral monitoring, and timely alert generation while maintaining low computational overhead. System performance was therefore assessed not only in terms of threat detection capability but also with respect to operational efficiency, including CPU utilization, memory consumption, and response time, to verify its suitability for deployment in resource-constrained environments.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Table 3. Deployment Environment and Implementation Specifications

Component	Implementation Specification
Endpoint Agent	Python 3.x lightweight service using operating-system APIs and resource-monitoring utilities for process, connection, and system telemetry.
Packet and Network Inspection	Scapy-based packet inspection for selected TCP, UDP, DNS, and outbound connection events.
Central Server / Log Receiver	Flask-based REST API service receiving telemetry through encrypted HTTP requests in JSON format.
Database	SQLite for prototype storage of endpoint inventory, telemetry logs, alerts, incident records, and configuration settings. MySQL may be used for multi-endpoint production deployment.
Dashboard	Web-based dashboard using HTML, CSS, JavaScript, and Bootstrap responsive components.
Security Controls	User authentication, role-based access, log retention, alert severity tagging, and incident status tracking.
Deployment Model	On-premise workstation/server deployment suitable for SMEs; optional cloud hosting may be considered for future versions.

3.4 Functional and Non-Functional Requirements

The functional requirements of the proposed lightweight Endpoint Detection and Response (EDR) framework were derived from the operational requirements of endpoint security in resource-constrained enterprise environments. The framework was designed to support continuous endpoint telemetry collection, real-time behavioral monitoring, anomaly detection, security alert generation, incident investigation, centralized log management, malicious activity reporting, file integrity verification, and basic response capabilities, including process review and administrator-assisted handling of flagged events. Collectively, these functions were intended to improve endpoint visibility and facilitate timely identification and analysis of suspicious activities.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The non-functional requirements focused on ensuring that the framework remained practical for deployment within micro and small enterprises. Accordingly, the system was designed to maintain low CPU and memory utilization while providing reliable operation, usability, maintainability, compatibility with existing security tools, scalability to support additional endpoints, and operational safety that minimizes disruption to legitimate user activities. These requirements served as the basis for evaluating both the technical performance and software quality of the developed framework.

3.5 System Architecture

The proposed lightweight EDR framework adopted a modular client–server architecture to separate endpoint data acquisition from centralized analysis and management. Each protected endpoint executed a lightweight agent responsible for continuously collecting telemetry related to process execution, file system activities, authentication events, network connections, DNS queries, and other security-relevant system events. The collected telemetry was securely transmitted to a centralized server, where a data ingestion pipeline normalized, filtered, and stored the events within a centralized repository for subsequent analysis.

The analytical component integrated multiple detection mechanisms to identify potentially malicious activities. A behavioral analysis module examined endpoint events for anomalous patterns, while a process trust evaluation module assessed process legitimacy using attributes such as executable name, file path, digital publisher, execution behavior, and installation location. These indicators were combined through a dynamic risk-scoring engine that classified observed activities into predefined risk categories (e.g., safe, suspicious, or dangerous) to support threat prioritization and investigation.

A web-based administrative dashboard provided centralized visibility into endpoint security status by presenting real-time alerts, incident records, telemetry summaries, security reports, and system resource utilization metrics. This modular architecture enables efficient telemetry collection, scalable event processing, and timely incident monitoring while maintaining low computational overhead, thereby supporting the operational requirements of resource-constrained enterprise environments.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Figure 1. Proposed Lightweight EDR Framework Architecture

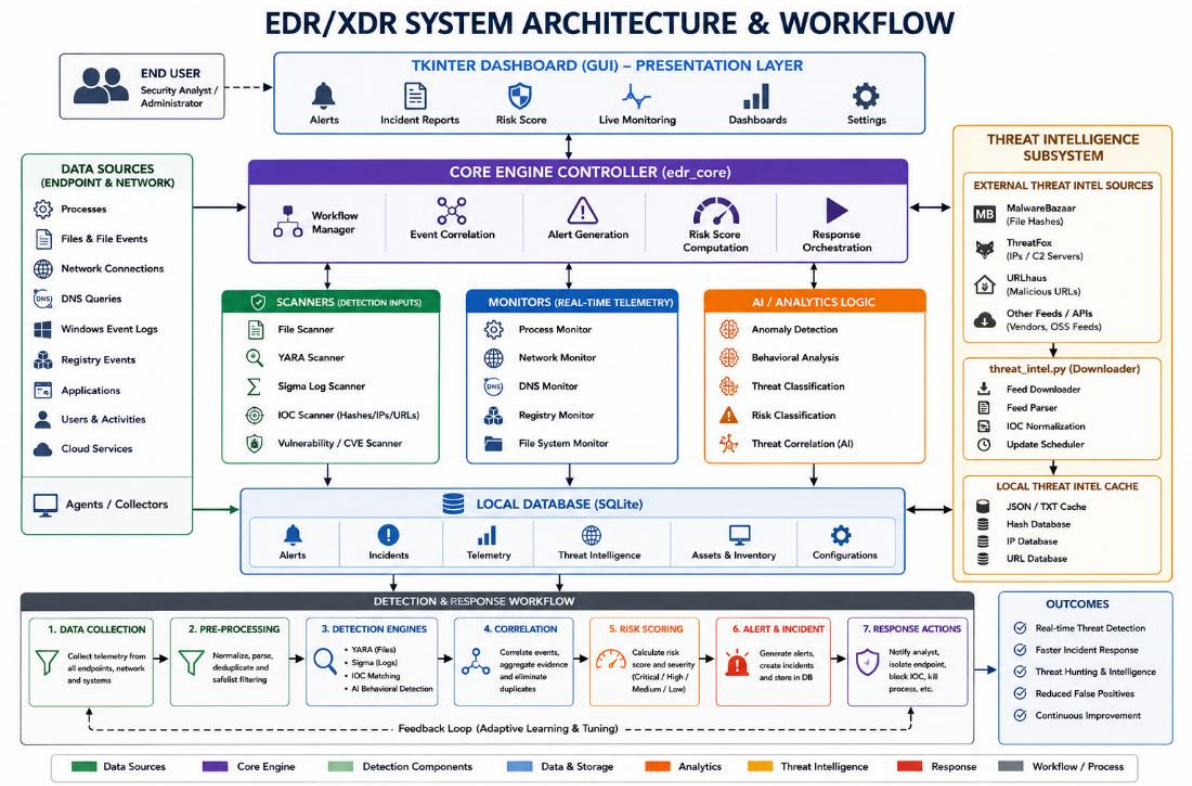


Table 4. EDR Framework Modules

Module	Description
End User (Security Analyst / Administrator)	Interacts with the EDR/XDR framework to monitor endpoint security, investigate incidents, configure detection policies, and review alerts, risk scores, and reports.
Tkinter Dashboard (Presentation Layer)	Provides a graphical user interface that displays real-time alerts, incident reports, risk scores, endpoint status, system logs, dashboards, and configuration settings for centralized security monitoring.
Core Engine Controller (edr_core)	Serves as the central orchestration component responsible for coordinating telemetry collection, detection workflows, event correlation, alert generation, response execution, and

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Module	Description
	communication among all framework modules.
Workflow Manager	Controls the execution sequence of monitoring, detection, analysis, correlation, and response tasks to ensure efficient processing of endpoint telemetry.
Event Correlation Engine	Aggregates and correlates related security events collected from multiple detection engines and telemetry sources to identify attack patterns and reduce duplicate alerts.
Alert Generation Module	Generates security alerts based on detection results, assigns severity levels, and records incidents in the local database for further investigation.
Risk Scoring Engine	Calculates dynamic risk scores using behavioral indicators, threat intelligence matches, detection confidence, and event severity to prioritize security incidents.
Response Orchestration Module	Coordinates automated or analyst-assisted response actions such as process termination, IOC blocking, endpoint isolation, and alert notification.
Data Collection Module	Collects endpoint telemetry from processes, files, network connections, DNS queries, registry activities, Windows event logs, and user activities for security analysis.
Process Monitor	Continuously monitors running processes, process creation events, parent-child relationships, and abnormal process behavior to detect suspicious activities.
Network Monitor	Captures active network connections, IP addresses, ports, protocols, and communication patterns to identify suspicious network behavior and command-and-control communications.
DNS Monitor	Monitors DNS queries and responses to detect communications with malicious domains, phishing sites, and known command-

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Module	Description
	and-control infrastructure.
Registry Monitor	Tracks modifications to Windows Registry keys and startup locations that may indicate persistence mechanisms or malicious system configuration changes.
File System Monitor	Observes file creation, deletion, modification, and execution events to identify malicious file activity and unauthorized changes within the endpoint.
File Scanner	Performs static inspection of files and executables prior to or during execution to detect malicious content using signature-based and heuristic techniques.
YARA Detection Engine	Applies YARA rules to identify known malware families and malicious file characteristics through signature-based pattern matching.
Sigma Detection Engine	Evaluates Windows event logs against Sigma detection rules to identify suspicious system activities and known attack techniques.
IOC Scanner	Compares file hashes, IP addresses, domains, URLs, and other Indicators of Compromise (IOCs) against locally cached threat intelligence feeds to detect known threats.
Vulnerability/CVE Scanner	Identifies vulnerable software components and maps detected weaknesses to Common Vulnerabilities and Exposures (CVE) records for risk assessment.
Behavioral Analysis Engine	Analyzes endpoint behaviors and sequences of events to identify suspicious activities that may not match predefined signatures, enabling detection of previously unknown threats.
Anomaly Detection Engine	Detects deviations from normal endpoint behavior using behavioral baselines and heuristic analysis to identify potential

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Module	Description
	Advanced Persistent Threat (APT) activities.
Threat Classification Module	Classifies detected events according to severity, attack type, confidence level, and potential impact to assist analysts in incident prioritization.
AI Risk Classification Module	Utilizes artificial intelligence techniques to estimate threat severity based on behavioral indicators, detection evidence, and contextual information.
AI Threat Correlation Module	Uses AI-assisted analysis to correlate multiple low-level security events into meaningful attack chains representing complex or multi-stage intrusions.
Threat Intelligence Downloader (threat_intel.py)	Automatically retrieves and updates threat intelligence feeds from external sources, parses downloaded data, normalizes IOC formats, and stores them in the local threat intelligence repository.
Threat Intelligence Repository	Maintains locally cached threat intelligence data, including malicious file hashes, IP addresses, domains, URLs, and reputation information used during IOC matching.
MalwareBazaar Integration	Retrieves malicious file hashes and malware metadata to improve file-based threat detection capabilities.
ThreatFox Integration	Provides continuously updated threat intelligence on malicious IP addresses, command-and-control servers, and network-based Indicators of Compromise.
URLhaus Integration	Supplies malicious URLs and phishing domain intelligence used for detecting web-based threats and suspicious outbound communications.
SQLite Database	Stores endpoint telemetry, security alerts, correlated incidents, threat intelligence records, risk scores, asset information, and

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Module	Description
	system configurations for analysis and reporting.
Telemetry Repository	Maintains collected endpoint telemetry to support historical analysis, threat hunting, forensic investigations, and model improvement.
Alert Repository	Stores generated security alerts, associated metadata, timestamps, and severity levels for investigation and auditing purposes.
Incident Repository	Maintains correlated security incidents and investigation records to support incident response and post-event analysis.
Configuration Manager	Stores system settings, detection rules, scan schedules, and operational parameters that control framework behavior.
Reporting Module	Generates security reports, detection summaries, incident statistics, and performance metrics for analysts, administrators, and management.
Adaptive Learning and Feedback Module	Utilizes analyst feedback and historical detection outcomes to refine behavioral baselines, optimize detection rules, and improve future detection accuracy.

3.6 Threat Intelligence Integration

The proposed Endpoint Detection and Response (EDR) framework incorporates external cyber threat intelligence to enhance its rule-based and behavior-based detection capabilities. Threat intelligence feeds obtained from MalwareBazaar, ThreatFox, and URLhaus provide continuously updated Indicators of Compromise (IOCs), including malicious file hashes, IP addresses, command-and-control (C2) infrastructure, and malicious domains. These intelligence feeds are periodically retrieved, parsed, normalized, and stored within a local threat intelligence repository, enabling efficient offline IOC matching during endpoint monitoring while minimizing dependence on continuous Internet connectivity.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

During operation, security-relevant endpoint artifacts—including file hashes, network connections, and domain requests—are automatically compared against the locally maintained IOC repository. Matches contribute additional evidence to the framework's risk assessment process by increasing the confidence associated with suspicious events and supporting alert generation, incident correlation, and threat prioritization. Consequently, the threat intelligence module complements behavioral monitoring by enabling the identification of previously known malicious artifacts that may not exhibit sufficiently distinctive behavioral characteristics during initial execution.

Maintaining a synchronized local repository also improves operational resilience by reducing repeated queries to external intelligence services and allowing IOC-based detection to continue during temporary network interruptions or service unavailability. Nevertheless, the effectiveness of this capability depends on the timeliness, completeness, and reliability of the underlying threat intelligence feeds. Accordingly, periodic synchronization with trusted intelligence providers is required to maintain detection effectiveness against newly emerging threats.

The threat intelligence component operates in conjunction with YARA rule matching, Sigma-based log analysis, process trust assessment, and heuristic-assisted behavioral anomaly detection to provide a layered detection strategy. By combining internal endpoint telemetry with externally curated threat intelligence, the framework improves detection confidence, enhances contextual understanding of security events, and strengthens its ability to identify Advanced Persistent Threat (APT)-related activities while maintaining low computational overhead suitable for resource-constrained enterprise environments.

3.7 Evaluation Procedure

The evaluation of the proposed lightweight Endpoint Detection and Response (EDR) framework comprised four complementary stages designed to assess its functional correctness, operational performance, software quality, and cybersecurity effectiveness. First, functional testing verified that each system component operated according to its intended design, including endpoint telemetry collection, centralized log management, behavioral anomaly detection, real-time alert generation, incident investigation, and security report generation. Second, performance testing measured the framework's computational overhead by monitoring CPU utilization, memory consumption, and response time during continuous endpoint monitoring and alert processing. Third, software quality evaluation was conducted through expert assessment using the ISO/IEC 25010 software quality model, providing measures of functional suitability, performance efficiency, compatibility, reliability, security, maintainability, flexibility, and safety.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Finally, cybersecurity validation was performed using MITRE ATT&CK-aligned adversary emulation scenarios and safe malware test artifacts to evaluate the framework's capability to detect representative Advanced Persistent Threat (APT) behaviors without exposing the experimental environment to uncontrolled malicious software (MITRE ATT&CK, n.d.; Sikorski & Honig, 2012).

Experimental Environment

The proposed lightweight EDR framework was implemented using Python 3.12 as the primary development language. The graphical user interface was developed using the Tkinter library, while endpoint telemetry collection and system monitoring were implemented using the **psutil**, **watchdog**, and **pywin32** libraries. Detection capabilities combined YARA-based malware signature matching with Sigma rule analysis through the pySigma library to identify suspicious endpoint activities. External cyber threat intelligence was integrated from MalwareBazaar, ThreatFox, and URLhaus, with downloaded Indicators of Compromise (IOCs) periodically synchronized and maintained within a local repository in JSON and text formats. Endpoint telemetry, security alerts, incident records, and threat intelligence data were managed using an embedded SQLite database.

Experimental evaluation was conducted on a Windows-based workstation representative of the computing environment typically found in micro and small enterprises. The test platform was intentionally configured using commodity hardware and standard operating system components without specialized enterprise-grade security infrastructure to reflect realistic deployment conditions for resource-constrained organizations. The hardware and software specifications of the experimental platform are summarized in Table 5**.**

Table 5. Experimental Environment

Component	**Specification**
Operating System	Windows 11 Pro (64-bit)
Processor	Intel Core i5 (or equivalent)
Memory	8 GB RAM
Storage	SSD
Programming Language	Python 3.12

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Component	Specification
Database	SQLite
GUI Framework	Tkinter
Detection Engines	YARA, pySigma
Threat Intelligence Sources	MalwareBazaar, ThreatFox, URLhaus
Risk Scoring	Custom heuristic-based engine

3.8 Cybersecurity Validation Metrics

The cybersecurity performance of the proposed framework was evaluated using established quantitative metrics that measure both detection effectiveness and operational efficiency. Detection accuracy was calculated as the proportion of correctly classified endpoint events relative to the total number of evaluated events. The false positive rate (FPR) quantified the proportion of benign events incorrectly classified as malicious, whereas the false negative rate (FNR) measured the proportion of malicious events that were not detected by the framework. Precision was used to assess the reliability of generated alerts by measuring the proportion of detected events that were true positives, while recall evaluated the framework's detection capability by measuring the proportion of actual malicious events correctly identified.

Operational efficiency was assessed using performance metrics that reflect the framework's suitability for resource-constrained environments. Response time was defined as the elapsed interval between the occurrence or detection of a security-relevant event and the generation of the corresponding alert. Computational overhead was evaluated by measuring average CPU utilization and memory consumption of the endpoint agent during continuous monitoring. Collectively, these metrics provide a comprehensive assessment of the framework's ability to achieve accurate threat detection while maintaining low resource utilization, thereby supporting its intended deployment in micro and small enterprise environments.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Table 6. Cybersecurity Validation Metrics

Metric	Formula / Basis	Purpose
Detection Accuracy	(TP + TN) / (TP + TN + FP + FN) x 100	Measures overall correctness of classification.
False Positive Rate	FP / (FP + TN) x 100	Measures the rate of legitimate activities incorrectly flagged.
False Negative Rate	FN / (FN + TP) x 100	Measures the rate of malicious activities missed by the system.
Precision	TP / (TP + FP) x 100	Measures alert quality and correctness.
Recall / Detection Rate	TP / (TP + FN) x 100	Measures the ability to detect actual malicious events.
Average Response Time	Mean elapsed time from event occurrence to alert generation	Measures alert speed.
CPU and Memory Usage	Average endpoint resource consumption during monitoring	Measures lightweight performance.

Cybersecurity Validation Procedure

Cybersecurity validation was conducted in a controlled laboratory environment to evaluate the detection effectiveness and operational efficiency of the proposed lightweight Endpoint Detection and Response (EDR) framework under representative endpoint attack scenarios. During the evaluation, the endpoint agent continuously collected telemetry from multiple data sources, including file system activities, process execution, Windows event logs, DNS queries, registry modifications, and network connections. Prior to analysis, the collected telemetry underwent preprocessing through a safelist filtering mechanism that excluded trusted operating system processes and verified benign activities, thereby reducing unnecessary analysis and minimizing false alerts.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The detection pipeline combined multiple complementary detection mechanisms to improve overall detection capability. YARA rules were applied to identify known malicious files through signature matching, Sigma rules analyzed Windows event logs for suspicious system activities, and locally maintained threat intelligence feeds were used to match Indicators of Compromise (IOCs), including malicious file hashes, IP addresses, and domains. In parallel, a heuristic-assisted behavioral analysis module evaluated endpoint activities for anomalous patterns indicative of Advanced Persistent Threat (APT) behavior. Detection outputs from these components were subsequently correlated by the event correlation engine, which computed a dynamic risk score for each security event before generating alerts and recording incidents within the SQLite database.

Technical validation was performed using a labeled dataset consisting of 512 endpoint events, comprising 68 malicious and 444 benign activities. Malicious scenarios included MITRE ATT&CK-aligned adversary emulation techniques, unauthorized script execution, suspicious process behavior, malicious file execution, and network communications associated with known Indicators of Compromise. Benign events represented routine endpoint activities, including legitimate application execution, normal file operations, web browsing, and standard operating system processes. This combination of malicious and benign scenarios enabled evaluation of the framework under conditions representative of typical enterprise endpoint operations.

Detection performance was assessed using a confusion matrix consisting of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). These values were used to calculate detection accuracy, precision, recall, specificity, false positive rate, false negative rate, and F1-score, providing a comprehensive assessment of the framework's classification performance. Operational efficiency was evaluated by measuring average CPU utilization, memory consumption, and response time during continuous monitoring. The resulting performance metrics were subsequently compared with predefined acceptance criteria and published benchmark ranges for lightweight and commercial Endpoint Detection and Response solutions to determine the technical effectiveness and practical suitability of the proposed framework for deployment in resource-constrained enterprise environments.

3.9 Threat Scenario Design and Safe Adversarial Testing Procedure

To ensure ethical, safe, and reproducible experimentation, cybersecurity validation was conducted without executing uncontrolled live malware or exposing production systems to malicious code. Instead, the evaluation employed controlled adversarial emulation scenarios and non-destructive malware test artifacts designed to reproduce representative Advanced Persistent Threat (APT) behaviors under laboratory conditions (Sikorski & Honig, 2012). This approach enabled systematic assessment of the proposed Endpoint Detection and Response (EDR) framework while eliminating the operational and legal risks associated with live malware execution.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The experimental scenarios were derived from the MITRE ATT&CK knowledge base to ensure that the evaluation reflected adversary behaviors commonly observed in real-world intrusion campaigns (MITRE ATT&CK, n.d.). The test cases included safe antivirus test files (e.g., EICAR), benign scripts that simulated suspicious command execution, repeated authentication failures, indicators of privilege escalation attempts, startup persistence modifications, unauthorized file system changes, and anomalous outbound network communications. Each scenario was designed to emulate one or more ATT&CK tactics or techniques while avoiding destructive system modifications or unauthorized access.

All scenarios were executed individually within a controlled laboratory environment to ensure repeatability and to isolate their effects on the monitored endpoint. During execution, the framework continuously collected endpoint telemetry, applied YARA rule matching, Sigma-based log analysis, threat intelligence correlation, and heuristic-assisted behavioral analysis, and generated corresponding risk scores and security alerts. Detection performance was subsequently verified by comparing the generated alerts with the expected outcomes for each scenario, thereby determining whether the framework accurately identified the simulated malicious activities while avoiding unnecessary alerts for legitimate system behavior.

Table 7. Adversarial Testing Scenarios

Scenario	MITRE ATT&CK Mapping	Validation Method	Expected Detection
Unauthorized script or process execution	T1059 - Command and Scripting Interpreter	Benign script executed from an unusual directory.	Alert for suspicious process execution.
Brute-force authentication attempts	T1110 - Brute Force	Repeated failed login attempts were generated in a controlled account.	Alert for credential access anomaly.
Privilege escalation indicator	T1068 - Exploitation for Privilege Escalation	A safe test routine simulated an elevation attempt.	Alert for privilege escalation behavior.
Startup persistence modification	T1547 - Boot or Logon Autostart Execution	Test entry was added to and removed from an	Alert for persistence behavior.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Scenario	MITRE ATT&CK Mapping	Validation Method	Expected Detection
		autostart location.	
Abnormal outbound connection	T1071 - Application Layer Protocol	Repeated outbound requests to a non-standard endpoint were generated.	Alert for suspicious external communication.
Unauthorized file modification	T1565 - Data Manipulation	A test file was repeatedly modified in a monitored folder.	Alert for abnormal file activity.

3.10 Statistical Treatment of Data

Descriptive and inferential statistical techniques were employed to analyze the evaluation results. Descriptive statistics, specifically the weighted mean, were used to summarize the respondents' assessments of the proposed Endpoint Detection and Response (EDR) framework based on the ISO/IEC 25010 software quality characteristics. The weighted mean provided an overall measure of respondent agreement regarding the framework's functional suitability, performance efficiency, compatibility, reliability, security, maintainability, flexibility, and safety.

To determine whether the implementation of the proposed framework resulted in a statistically significant improvement in software quality, pre-implementation and post-implementation evaluation scores were compared using a paired-sample *t*-test. This test was selected because the same group of respondents evaluated the framework before and after implementation, resulting in paired observations. Statistical significance was evaluated at an alpha level of 0.05, with $p < 0.05$ indicating a statistically significant difference between the two assessment periods.

The framework's cybersecurity performance was evaluated independently using objective quantitative metrics derived from the confusion matrix and system performance logs collected during controlled laboratory testing. Detection effectiveness was assessed using detection accuracy, precision, recall, specificity, false positive rate, false negative rate, and F1-score, while operational efficiency was measured through average CPU utilization, memory consumption, and response time. These metrics provided a comprehensive assessment of both the technical effectiveness and computational efficiency of the proposed framework.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

IV. RESULTS AND DISCUSSION

4.1 System Acceptability Results

The respondent-based evaluation indicated that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved high levels of acceptability across the assessed ISO/IEC 25010 software quality characteristics. These findings suggest that the framework was perceived by domain experts as functionally appropriate and operationally suitable for deployment within resource-constrained enterprise environments. However, because user evaluations are inherently subjective, the acceptability results were interpreted in conjunction with objective cybersecurity performance measures, including detection effectiveness and operational efficiency. This complementary evaluation approach provided a more comprehensive assessment of the framework by integrating expert judgment with empirical evidence derived from controlled technical validation.

Table 8. System Acceptability Results

Quality Characteristic	Composite Mean	Interpretation
Functionality	3.60	Highly Evident / Strongly Acceptable
Performance Efficiency	3.60	Highly Evident / Strongly Acceptable
Interaction Capability	3.56	Highly Evident / Strongly Acceptable
Compatibility	3.80	Highly Evident / Strongly Acceptable
Reliability	3.48	Highly Evident / Strongly Acceptable
Security	3.56	Highly Evident / Strongly Acceptable
Maintainability	3.52	Highly Evident / Strongly Acceptable

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Quality Characteristic	Composite Mean	Interpretation
Flexibility	3.56	Highly Evident / Strongly Acceptable
Safety	3.44	Highly Evident / Strongly Acceptable

Among the evaluated ISO/IEC 25010 quality characteristics, compatibility obtained the highest mean score (3.80), indicating that the proposed lightweight Endpoint Detection and Response (EDR) framework integrated effectively with existing endpoint devices, conventional security controls (e.g., antivirus software and firewalls), and commonly used office applications. This finding suggests that the framework can be deployed with minimal disruption to existing enterprise environments. In contrast, safety received the lowest mean score, although it remained within the favorable evaluation range. While the results indicate that the framework operates safely under normal conditions, they also suggest opportunities for further enhancement, particularly in minimizing potential operational disruptions and strengthening safeguards associated with response and remediation actions.

4.2 Test of Significant Difference Before and After System Development

Table 9. Before-and-After Comparison

Variable	Before EDR	After EDR	Mean Difference	t-value	p-value	Decision
Functionality	2.41	3.60	1.19	8.94	0.000	Reject H0
Reliability	2.38	3.48	1.10	8.56	0.000	Reject H0
Usability / Interaction Capability	2.45	3.56	1.11	8.31	0.000	Reject H0

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Variable	Before EDR	After EDR	Mean Difference	t-value	p-value	Decision
Overall	2.41	3.55	1.14	8.60	0.000	Reject H0

The statistical analysis demonstrated a significant improvement in the evaluation scores following the implementation of the proposed lightweight Endpoint Detection and Response (EDR) framework. For all evaluated software quality characteristics, the paired-sample *t*-test yielded *p*-values below the predetermined significance level of 0.05, resulting in the rejection of the null hypothesis. These findings indicate that the post-implementation evaluation scores were significantly higher than the corresponding pre-implementation scores, providing statistical evidence that the developed framework improved the assessed software quality attributes.

4.3 Cybersecurity Metric Results

To further evaluate the technical effectiveness of the proposed lightweight Endpoint Detection and Response (EDR) framework, cybersecurity validation was performed using controlled adversarial emulation and benign activity scenarios. The framework was evaluated against a labeled dataset comprising 512 endpoint events, including 68 malicious and 444 benign activities, to assess its capability to distinguish malicious behaviors from legitimate system operations. The resulting classifications were summarized using a confusion matrix (Table 10), from which standard cybersecurity performance metrics were derived.

Table 10. Confusion Matrix Results

Classification	Count	Description
True Positive (TP)	66	Malicious or suspicious activities correctly detected.
True Negative (TN)	435	Legitimate activities correctly classified as benign.
False Positive (FP)	9	Legitimate activity incorrectly flagged as suspicious.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Classification	Count	Description
False Negative (FN)	2	Malicious activity missed by the framework.

Table 11. Cybersecurity Performance Results

Metric	Result	Reference Benchmark	Interpretation
Detection Accuracy	97.85%	>= 90%	Passed
False Positive Rate	2.03%	<= 5%	Passed
False Negative Rate	2.94%	<= 10%	Passed
Precision	88.00%	>= 75%	Passed
Recall / Detection Rate	97.06%	>= 90%	Passed
F1-score	92.31%	>=90%	Passed
Specificity	97.97%	>=95%	Passed
Average Response Time	1.8 seconds	<= 5 seconds	Passed
Average CPU Utilization	4.6%	<= 10%	Passed
Average Memory Usage	105 MB	<= 300 MB	Passed

As presented in Table 11, the proposed framework achieved a detection accuracy of 97.85%, indicating a high level of overall classification performance across the evaluated endpoint events. The framework correctly identified 66 of the 68 malicious activities while accurately classifying 435 legitimate activities, producing only nine false positives and two false negatives. These results

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

demonstrate that the combined use of behavioral analysis, YARA signature matching, Sigma rule evaluation, threat intelligence correlation, and dynamic risk scoring provided effective discrimination between malicious and benign endpoint behaviors within the controlled evaluation environment.

The framework recorded a false positive rate of 2.03%**,** indicating that legitimate activities were infrequently misclassified as malicious. Maintaining a low false positive rate is particularly important in operational environments because excessive false alerts may contribute to alert fatigue and reduce the effectiveness of incident response. Likewise, the false negative rate of 2.94% suggests that only a small proportion of malicious activities remained undetected, demonstrating a high level of detection coverage while recognizing that no practical detection system can completely eliminate missed detections.

The framework further achieved a precision of 88.00% and **a** recall of 97.06%**.** The high recall indicates that the proposed framework successfully detected the majority of malicious activities included in the evaluation dataset, whereas the slightly lower precision reflects a limited number of false alerts generated during monitoring. This trade-off is generally considered acceptable for endpoint security systems because prioritizing high detection rates helps minimize the likelihood of overlooking genuine threats, particularly those associated with Advanced Persistent Threat (APT) campaigns.

In addition to detection effectiveness, the framework demonstrated strong operational efficiency. The average response time of 1.8 seconds indicates that security events were processed and corresponding alerts generated with minimal latency, supporting near real-time endpoint monitoring. Resource utilization also remained low throughout continuous operation, with an average CPU utilization of 4.6% and average memory consumption of 105 MB. These results indicate that the framework can provide continuous endpoint monitoring without imposing substantial computational overhead, making it suitable for deployment in resource-constrained enterprise environments.

Overall, all evaluated cybersecurity metrics satisfied the predefined acceptance criteria, providing empirical evidence that the proposed lightweight EDR framework effectively balances detection performance and computational efficiency. Although the reported results were obtained from a controlled dataset of 512 endpoint events and should therefore be interpreted as preliminary, they demonstrate the feasibility of delivering effective endpoint protection using a lightweight architecture designed for micro and small enterprises.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

4.4 MITRE ATT&CK Validation Results

Table 12. MITRE ATT&CK Validation Results

Attack Scenario	ATT&CK Technique	Detected	Result
Unauthorized process execution	T1059	Yes	Passed
Brute-force login attempts	T1110	Yes	Passed
Privilege escalation indicator	T1068	Yes	Passed
Abnormal outbound connection	T1071	Yes	Passed
Startup persistence modification	T1547	Yes	Passed
Unauthorized file modification	T1565	Yes	Passed

Table 12 presents the results of the MITRE ATT&CK-aligned adversarial validation. The proposed framework successfully detected all evaluated attack scenarios, including unauthorized process execution (T1059), brute-force authentication attempts (T1110), privilege escalation indicators (T1068), abnormal outbound communications (T1071), startup persistence modifications (T1547), and unauthorized file modifications (T1565). These techniques represent multiple phases of the ATT&CK adversary lifecycle, including execution, credential access, privilege escalation, command and control, persistence, and impact-related activity.

The successful detection of these scenarios demonstrates that the framework was capable of identifying representative APT-related endpoint behaviors within the controlled experimental environment. The results also indicate that the integration of behavioral monitoring, YARA rule

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

matching, Sigma-based log analysis, threat intelligence correlation, and dynamic risk scoring enabled the framework to detect diverse attack patterns across multiple telemetry sources. Nevertheless, some behavioral rules may require additional tuning in operational deployments to minimize false positives associated with legitimate administrative activities, software updates, or authorized maintenance procedures.

4.5 Comparison with Commercial EDR Solutions and Recent Research

To contextualize the performance of the proposed framework, its detection effectiveness and resource utilization were compared with findings reported in recent EDR research and publicly available descriptions of commercial EDR platforms (Table 13). Because the compared systems were evaluated using different datasets, attack scenarios, telemetry sources, and testing methodologies, the comparison is intended for contextual benchmarking rather than direct performance equivalence.

Table 13. Comparison with Commercial EDR Platforms and Recent Research

Feature	**Proposed Lightweight EDR**	**Microsoft Defender for Endpoint**	**CrowdStrike Falcon**	**SentinelOne Singularity**
Framework / Study	Detection Approach	Reported Detection Performance	Resource Consumption	Remarks
Proposed Lightweight EDR Framework	Behavioral monitoring, YARA, Sigma, Threat Intelligence, Risk Scoring	97.85%	4.6% CPU, 105 MB RAM	Lightweight architecture designed for small enterprises
Akbar et al. (2023)	Behavior-based endpoint detection	High detection performance reported	Not reported	Demonstrated effectiveness against APT-related behaviors

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Feature	Proposed Lightweight EDR	Microsoft Defender for Endpoint	CrowdStrike Falcon	SentinelOne Singularity
Blancaflor et al. (2024)	Lightweight EDR Framework	Prototype validation	Low resource utilization	Focused on affordability for SMEs
Microsoft Defender for Endpoint	AI-assisted EDR/XDR	Not directly comparable (vendor-reported performance)	Higher than lightweight solutions	Enterprise-scale cloud-assisted protection
CrowdStrike Falcon	Cloud-native EDR/XDR	Not directly comparable (vendor-reported performance)	Cloud-assisted architecture	Advanced behavioral analytics and threat intelligence
SentinelOne Singularity	Autonomous EDR/XDR	Not directly comparable (vendor-reported performance)	Moderate endpoint overhead	AI-driven autonomous detection and response

The proposed framework achieved a detection accuracy of 97.85%, precision of 88.00%, and recall of 97.06% while maintaining low computational overhead, with average resource consumption of 4.6% CPU utilization and 105 MB memory usage. These results demonstrate that the framework can provide effective endpoint monitoring and threat detection within a lightweight architecture suitable for resource-constrained environments.

Compared with recent academic studies, the proposed framework extends prior lightweight EDR research by integrating endpoint telemetry collection, behavioral monitoring, YARA-based signature detection, Sigma rule analysis, external threat intelligence, heuristic-assisted anomaly detection, dynamic risk scoring, and centralized incident management within a modular client-server architecture. In addition, the evaluation combined objective cybersecurity

performance metrics derived from a confusion matrix with software quality assessment based on the ISO/IEC 25010 model, providing both technical and operational perspectives on framework effectiveness.

Commercial platforms such as Microsoft Defender for Endpoint, CrowdStrike Falcon, and SentinelOne Singularity incorporate large-scale cloud telemetry, proprietary analytics, automated response capabilities, and extensive threat intelligence infrastructures that were beyond the scope of this study. Therefore, the present framework should not be viewed as a replacement for enterprise-grade commercial EDR solutions. Rather, the findings suggest that a modular, resource-efficient architecture can provide meaningful endpoint visibility and detection capability for micro and small enterprise environments where financial, technical, and infrastructure constraints may limit the adoption of full-scale commercial platforms.

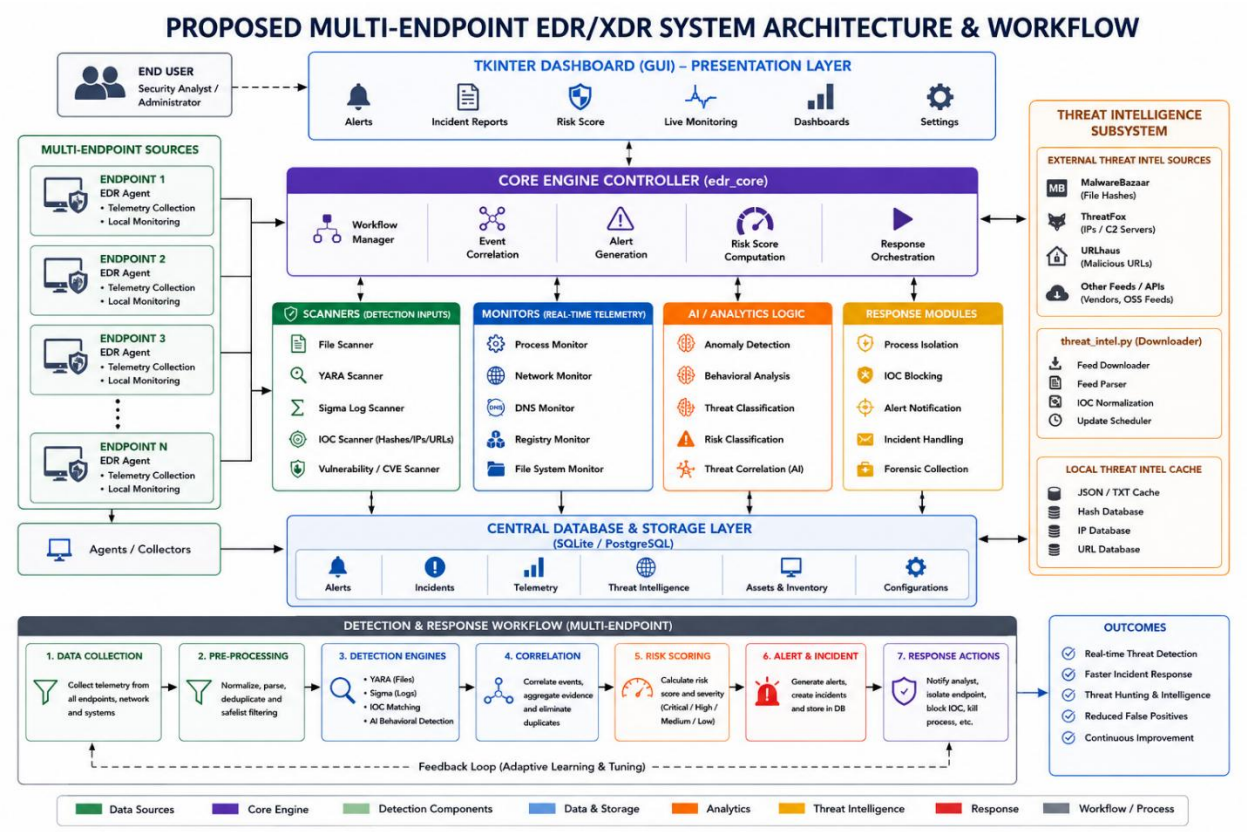
4.6 Scalability Analysis

Although the experimental evaluation was conducted using a single endpoint, the proposed Endpoint Detection and Response (EDR) framework was designed using a modular client–server architecture that supports future deployment across multiple endpoints. As illustrated in Figure 2, lightweight endpoint agents can be deployed on multiple devices to collect endpoint telemetry and securely transmit security events to a centralized EDR server. The centralized server is responsible for telemetry aggregation, event correlation, threat intelligence matching, dynamic risk scoring, alert generation, and incident management, thereby providing unified visibility across distributed endpoints while maintaining minimal computational overhead at the endpoint level.

It should be noted, however, that multi-endpoint deployment and large-scale performance were beyond the scope of the present study and were not experimentally evaluated. Consequently, the proposed architecture demonstrates scalability by design rather than empirically validated scalability. Future research should investigate the framework's performance under multi-endpoint deployments to evaluate its scalability, communication overhead, event processing throughput, and resource utilization in larger enterprise environments.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Figure 2. Proposed Multi-Endpoint Architecture



4.7 Detailed Quality Characteristic Results

Tables 13 through 22 present the item-level evaluation results for each ISO/IEC 25010 software quality characteristic that underlie the composite scores summarized in Table 7. These detailed results provide greater transparency by showing the respondents' assessments for individual evaluation criteria, thereby complementing the aggregated weighted mean scores. Examining the item-level ratings also enables identification of specific strengths and areas for potential improvement within each quality characteristic, supporting a more comprehensive interpretation of the framework's software quality evaluation.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Table 14. Functional Suitability

Indicator	Mean	Interpretation	Rank
The system provides complete functions needed for endpoint monitoring and threat detection.	3.40	Highly Evident	4.5
The system performs its intended functions correctly based on the needs of a small-scale enterprise.	3.40	Highly Evident	4.5
The system detects suspicious endpoint activities such as unusual process execution, file modification, and abnormal network activity.	3.80	Highly Evident	1.5
The system generates accurate and timely alerts when possible threats are detected.	3.80	Highly Evident	1.5
The system records endpoint activities and security events properly for monitoring and review.	3.60	Highly Evident	3
Overall Mean	3.60	Highly Evident	

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of functional suitability, with an overall weighted mean of 3.60, corresponding to the Highly Evident interpretation. This finding suggests that the framework effectively supports its intended functions, including endpoint telemetry collection, behavioral monitoring, threat detection, alert generation, and security event logging, within the operational context of resource-constrained enterprise environments.

Among the evaluated indicators, the highest ratings were assigned to the framework's capability to detect suspicious endpoint activities and to generate timely security alerts. These results indicate that the core detection mechanisms—including behavioral monitoring, YARA rule matching, Sigma-based log analysis, threat intelligence correlation, and dynamic risk scoring—were perceived as effectively supporting the timely identification of potentially malicious activities. Because early detection and prompt alert generation are fundamental objectives of Endpoint Detection and Response systems, these findings provide evidence that the framework successfully fulfills its primary operational purpose.

Although the indicators related to the completeness of system functions and alignment with small-enterprise operational requirements received comparatively lower ratings, they remained within the Highly Evident category. Rather than indicating functional deficiencies, these results suggest opportunities for further enhancement, such as expanding supported detection capabilities, refining administrative features, or incorporating additional incident response functions to address a broader range of operational requirements.

Overall, the findings demonstrate that the proposed framework provides the essential functionality expected of a lightweight Endpoint Detection and Response solution while maintaining a design appropriate for deployment in micro and small enterprise environments. These respondent-based assessments are further supported by the objective cybersecurity performance results presented in the subsequent sections, indicating consistency between expert evaluation and technical validation.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Table 15. Performance Efficiency

Indicator	Mean	Interpretation	Rank
The system processes endpoint activities, logs, and security alerts within an acceptable time.	3.40	Highly Evident	4.5
The system runs in the background without causing noticeable slowdown on endpoint devices.	3.40	Highly Evident	4.5
The system uses minimal CPU, memory, and storage resources while performing endpoint monitoring.	3.60	Highly Evident	3
The system maintains stable performance while monitoring multiple endpoint activities.	3.80	Highly Evident	1.5
The system loads dashboards, logs, and reports within a reasonable response time.	3.80	Highly Evident	1.5
Overall Mean	3.60	Highly Evident	

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of performance efficiency, with an overall weighted mean of 3.60**,** corresponding to the Highly Evident interpretation. This finding suggests that the framework performs its endpoint monitoring and threat detection functions efficiently while maintaining acceptable responsiveness and resource utilization within resource-constrained enterprise environments.

The highest-rated indicators were associated with system stability during continuous endpoint monitoring and the responsiveness of dashboards, logs, and reporting functions. These results indicate that the framework provides a consistent user experience while supporting timely access to security information, both of which are essential for effective endpoint monitoring and incident investigation. The positive evaluation of these operational characteristics suggests that the modular architecture and lightweight design successfully balance monitoring capability with system responsiveness.

Although the indicators related to background execution and processing efficiency received comparatively lower ratings, they remained within the Highly Evident category, indicating that respondents did not perceive these aspects as significant operational limitations. Instead, these findings suggest opportunities for further optimization of event processing and resource management, particularly as the framework evolves to support larger deployment environments and increased monitoring workloads.

The respondent-based assessment is further supported by the objective cybersecurity performance evaluation, which demonstrated an average response time of 1.8 seconds**,** 4.6% CPU utilization**,** and 105 MB average memory consumption during continuous monitoring. Together, these subjective and objective results indicate that the proposed framework achieves effective endpoint monitoring while maintaining the low computational overhead required for deployment in micro and small enterprise environments.

Table 16. Interaction Capability

Indicator	Mean	Interpretation	Rank
The system dashboard is easy to access and navigate.	3.60	Highly Evident	2.5
The system provides clear menus, labels, and buttons.	3.60	Highly Evident	2.5

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Indicator	Mean	Interpretation	Rank
The system presents endpoint status, alerts, logs, and reports in an understandable format.	4.00	Highly Evident	1
The alert messages are easy to interpret and useful for decision-making.	3.40	Highly Evident	4
The system can be used with minimal training by authorized users.	3.20	Highly Evident	5
Overall Mean	3.56	Highly Evident	

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of interaction capability and usability, with an overall weighted mean of 3.56, corresponding to the Highly Evident interpretation. This finding suggests that the framework provides an intuitive user interface that enables administrators to perform endpoint monitoring and security management tasks effectively within resource-constrained organizational environments.

The highest-rated indicator was associated with the presentation of endpoint status, security alerts, logs, and reports in a clear and understandable format. This result highlights the importance of effective information visualization in endpoint security, as timely interpretation of security events supports more efficient incident investigation and decision-making. Similarly, the favorable ratings for dashboard accessibility and interface navigation indicate that the framework's administrative interface facilitates routine monitoring and operational management without imposing unnecessary complexity on users.

Although the indicator related to minimal training received the lowest mean score, it remained within the Highly Evident category, suggesting that respondents generally considered the framework usable while recognizing opportunities to further improve user onboarding and operational guidance. Enhancements such as integrated help features, contextual documentation, interactive tutorials, or administrator training materials may further reduce the learning curve, particularly for organizations with limited cybersecurity expertise.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Overall, the findings demonstrate that the proposed framework successfully balances technical functionality with usability, an important consideration for micro and small enterprises where endpoint security solutions must be both effective and straightforward to operate. By presenting security information in a clear and accessible manner, the framework supports timely situational awareness and facilitates informed security decision-making during endpoint monitoring and incident response.

Table 17. Compatibility

Indicator	Mean	Interpretation	Rank
The system works properly with existing endpoint devices used in the organization.	3.80	Highly Evident	2.5
The system can operate alongside existing antivirus, firewall, and security tools without conflict.	3.80	Highly Evident	2.5
The system does not interfere with common office applications.	3.80	Highly Evident	2.5
The system can be installed without requiring major changes to the current IT infrastructure.	3.80	Highly Evident	2.5
Overall Mean	3.80	Highly Evident	

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved the highest rating among the assessed ISO/IEC 25010 quality characteristics, with an overall weighted mean of 3.80, corresponding to the Highly Evident interpretation. This finding suggests that the framework is highly compatible with the

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

existing technological environment of resource-constrained organizations and can be integrated into current endpoint infrastructures with minimal operational disruption.

The consistently high ratings across all compatibility indicators demonstrate that the framework was perceived to operate effectively alongside commonly deployed endpoint devices, conventional security controls, and standard office applications without adversely affecting their normal operation. The uniformity of these evaluations indicates broad respondent agreement that the framework can coexist with existing hardware and software environments while requiring only minimal changes to the organization's information technology infrastructure.

This characteristic is particularly important for micro and small enterprises, where financial and technical constraints often limit the feasibility of extensive infrastructure upgrades or the replacement of existing security solutions. A framework that integrates seamlessly with current systems reduces deployment complexity, facilitates adoption, and minimizes implementation costs and operational downtime.

Overall, the findings demonstrate that compatibility is a key strength of the proposed framework, supporting its intended role as a practical endpoint security solution for organizations seeking to enhance cybersecurity without introducing substantial infrastructure or operational burdens.

Table 18. Reliability

Indicator	Mean	Interpretation	Rank
The system performs consistently during endpoint monitoring activities.	3.20	Highly Evident	5
The system remains available and operational during regular security monitoring.	3.40	Highly Evident	3.5
The system continues to record endpoint activities and security events without interruption.	3.60	Highly Evident	2

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Indicator	Mean	Interpretation	Rank
The system generates alerts reliably when suspicious activities are detected.	3.80	Highly Evident	1
The system can recover or resume monitoring after endpoint restart or temporary interruption.	3.40	Highly Evident	3.5
Overall Mean	3.48	Highly Evident	

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of reliability, with an overall weighted mean of 3.48**,** corresponding to the Highly Evident interpretation. This finding suggests that the framework consistently performs its core monitoring and security functions, supporting continuous endpoint visibility and timely detection of suspicious activities during routine operation.

Among the evaluated indicators, the framework received the highest rating for its ability to generate reliable alerts when suspicious activities were detected. This result underscores the importance of dependable alert generation in endpoint security, as timely and accurate notifications enable administrators to respond promptly to potential security incidents. Similarly, the favorable assessment of uninterrupted endpoint telemetry collection indicates that the framework can maintain continuous monitoring, which is essential for identifying attack behaviors that develop over extended periods, such as those associated with Advanced Persistent Threats (APTs).

Although the indicators related to operational consistency and recovery after temporary interruptions received comparatively lower ratings, they remained within the Highly Evident category. These results do not indicate deficiencies in system reliability but rather identify opportunities for further enhancement. Future improvements may focus on strengthening fault tolerance, optimizing service recovery mechanisms, and improving monitoring continuity following endpoint restarts or temporary service interruptions, particularly in larger deployment environments.

Overall, the findings demonstrate that the proposed framework provides reliable endpoint monitoring and alert generation while maintaining continuous collection of security events.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Together with the objective technical evaluation presented in the cybersecurity performance analysis, these results support the framework's suitability for sustained endpoint monitoring in resource-constrained enterprise environments.

Table 19. Security

Indicator	Mean	Interpretation	Rank
The system protects user access through secure login authentication.	3.60	Highly Evident	2.5
The system prevents unauthorized users from accessing the EDR dashboard, logs, and security records.	3.40	Highly Evident	4.5
The system detects suspicious endpoint activities such as unauthorized process execution and abnormal network behavior.	3.40	Highly Evident	4.5
The system generates security alerts when possible threats are detected.	3.80	Highly Evident	1
The system maintains security logs that support accountability and incident investigation.	3.60	Highly Evident	2.5
Overall Mean	3.56	Highly Evident	

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of security, with an overall weighted mean of **3.56**, corresponding to the **Highly Evident** interpretation. This finding suggests that the framework provides appropriate security mechanisms for protecting endpoint environments while supporting continuous monitoring, threat detection, and incident investigation.

The highest-rated indicator was associated with the framework's ability to generate security alerts when suspicious activities were detected, highlighting the importance of timely notification in facilitating rapid incident response. Favorable ratings for secure user authentication and the maintenance of security logs further indicate that respondents perceived the framework as supporting fundamental security requirements, including controlled administrative access, accountability, and forensic analysis. Together, these capabilities contribute to strengthening endpoint visibility and improving administrators' ability to investigate and respond to potential security incidents.

Although the indicators related to preventing unauthorized access to the EDR platform and detecting suspicious endpoint activities received comparatively lower ratings, they remained within the **Highly Evident** category. These findings suggest opportunities for further enhancement, such as implementing more granular access-control mechanisms, strengthening authentication procedures, and continuously refining detection rules to improve resilience against evolving attack techniques while minimizing false alerts.

Overall, the respondent-based evaluation demonstrates that the proposed framework provides an effective security foundation for endpoint monitoring and protection. These perceptions are further supported by the objective cybersecurity validation, which demonstrated high detection accuracy, a low false positive rate, and efficient resource utilization, indicating consistency between expert assessment and empirical technical performance.

Table 20. Maintainability

Indicator	Mean	Interpretation	Rank
The system can be checked, updated, and maintained by authorized personnel.	3.60	Highly Evident	2
The system allows administrators to modify	3.60	Highly Evident	2

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Indicator	Mean	Interpretation	Rank
detection rules, alert settings, and security configurations.			
The system has organized modules that make errors easier to identify and correct.	3.60	Highly Evident	2
The system provides logs and records that help in diagnosing problems.	3.40	Highly Evident	4.5
The system documentation and configuration settings support easier maintenance and troubleshooting.	3.40	Highly Evident	4.5
Overall Mean	3.52	Highly Evident	

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of maintainability, with an overall weighted mean of 3.52**,** corresponding to the Highly Evident interpretation. This finding suggests that the framework is designed to support efficient system administration, enabling authorized personnel to update, configure, and maintain its security functions without excessive operational complexity.

The highest-rated indicators were associated with the framework's support for system updates, modification of detection rules and security configurations, and the modular organization of its components. These results indicate that respondents perceived the framework as sufficiently flexible to accommodate routine maintenance activities while facilitating the identification and correction of operational issues. The modular architecture also supports future enhancement by allowing individual components to be updated or refined without requiring substantial modifications to the overall system.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Although the indicators related to diagnostic support and system documentation received comparatively lower ratings, they remained within the Highly Evident category. These findings suggest opportunities for further improvement, particularly through the development of more comprehensive technical documentation, enhanced diagnostic capabilities, and additional troubleshooting resources to simplify system maintenance and administrator support.

Overall, the findings demonstrate that maintainability is a notable strength of the proposed framework. This characteristic is especially important for micro and small enterprises, where limited technical personnel often require security solutions that can be efficiently maintained, configured, and updated with minimal administrative effort while remaining adaptable to evolving cybersecurity requirements.

Table 21. Flexibility

Indicator	Mean	Interpretation	Rank
The system can be adapted to the endpoint security needs of different small-scale enterprises.	3.60	Highly Evident	2.5
The system can be configured based on the number of endpoint devices being monitored.	3.40	Highly Evident	4.5
The system can support changes in monitoring rules, alert settings, and security policies.	3.40	Highly Evident	4.5
The system can gradually scale as the organization adds more endpoint devices.	3.60	Highly Evident	2.5
The system allows future integration with other	3.80	Highly Evident	1

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Indicator	Mean	Interpretation	Rank
cybersecurity tools or reporting platforms.			
Overall Mean	3.56	Highly Evident	

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of flexibility, with an overall weighted mean of 3.56, corresponding to the Highly Evident interpretation. This finding suggests that the framework's modular design was perceived as capable of accommodating evolving organizational requirements, configuration changes, and future system enhancements within resource-constrained enterprise environments.

The highest-rated indicator was associated with the framework's potential for future integration with other cybersecurity tools and reporting platforms. This result reflects the respondents' confidence that the modular architecture can facilitate interoperability with complementary security technologies, thereby supporting the gradual expansion of endpoint security capabilities as organizational requirements evolve. Similarly, the favorable ratings for adaptation to different enterprise environments and the ability to support additional endpoint devices indicate positive perceptions regarding the framework's architectural extensibility.

Although the indicators related to configuration flexibility and support for changing monitoring rules and security policies received comparatively lower ratings, they remained within the Highly Evident category. These findings suggest opportunities to further enhance administrative customization by expanding configuration options, improving policy management, and simplifying the modification of detection rules to accommodate diverse operational requirements.

It should be noted, however, that the perceived scalability and integration capabilities reflected in this evaluation are based on the framework's architectural design rather than empirical validation through multi-endpoint deployment. As discussed in the system architecture, the experimental evaluation was limited to a controlled single-endpoint environment. Future research should therefore validate the framework under larger-scale deployments to assess its scalability, interoperability, and performance across distributed enterprise environments.

Overall, the findings indicate that the proposed framework provides a flexible architectural foundation capable of supporting future enhancement and deployment scenarios while remaining aligned with the operational needs of micro and small enterprises.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Table 22. Safety

Indicator	Mean	Interpretation	Rank
The system performs endpoint monitoring without causing harmful interruption to normal operations.	3.20	Highly Evident	5
The system provides warning alerts before users take critical security actions.	3.40	Highly Evident	3
The system allows administrators to review detected threats before applying response actions.	3.40	Highly Evident	3
The system supports safe handling of security incidents without exposing sensitive endpoint information.	3.80	Highly Evident	1
The system supports business continuity by detecting threats while allowing legitimate work activities to continue.	3.40	Highly Evident	3
Overall Mean	3.44	Highly Evident	

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The respondents' evaluation indicates that the proposed lightweight Endpoint Detection and Response (EDR) framework achieved a high level of flexibility, with an overall weighted mean of 3.56**,** corresponding to the Highly Evident interpretation. This finding suggests that the framework's modular architecture was perceived as capable of accommodating evolving organizational requirements, configurable security policies, and future system enhancements within resource-constrained enterprise environments.

The highest-rated indicator was associated with the framework's potential for future integration with other cybersecurity tools and reporting platforms. This result reflects respondents' confidence in the framework's extensible design, which supports interoperability with complementary security technologies and facilitates incremental enhancement as organizational security requirements evolve. Likewise, the favorable ratings for adaptability to different small-enterprise environments indicate that the framework can be configured to support varying operational needs while maintaining its lightweight design.

Although the indicators related to configuration flexibility, policy customization, and support for additional endpoint devices received comparatively lower ratings, they remained within the Highly Evident category. These findings suggest opportunities to further enhance administrative configuration options, simplify policy management, and improve support for diverse deployment scenarios.

It should be noted, however, that the perceived scalability and integration capabilities reflected in this evaluation are based on the framework's architectural design rather than empirical validation. The experimental evaluation was conducted in a controlled single-endpoint environment; therefore, the framework demonstrates **scalability by design** rather than experimentally verified scalability. Future studies should evaluate multi-endpoint deployments to assess communication overhead, event throughput, resource utilization, and overall system performance in larger organizational environments.

Overall, the findings indicate that the proposed framework provides a flexible architectural foundation that can support future enhancement and broader deployment while remaining aligned with the operational requirements of micro and small enterprises.

4.8 Comparison with Existing Studies

Table 23 provides a contextual comparison between the proposed lightweight Endpoint Detection and Response (EDR) framework and selected recent studies related to endpoint threat detection and behavioral monitoring. Because the compared studies differ in research objectives, datasets, evaluation methodologies, and reported performance measures, the comparison is intended to provide contextual benchmarking rather than establish direct quantitative equivalence.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Table 23. Contextual Comparison of the Proposed Framework with Selected Endpoint Detection Studies

Study	Detection Accuracy	CPU Usage	Memory
Proposed Framework	97.85%	4.6%	105 MB
Akbar et al. (2023)	High (Behavior-based)	Not Reported	Not Reported
Salim et al. (2023)	Conceptual Framework	N/A	N/A
Commercial EDR	95–99%	Higher	Higher

As shown in Table 23, the proposed framework achieved a detection accuracy of 97.85% while maintaining low computational overhead, with average resource utilization of 4.6% CPU and 105 MB of memory during continuous monitoring. In contrast, recent academic studies have primarily emphasized the effectiveness of behavior-based detection techniques or proposed conceptual detection frameworks without reporting comparable implementation-level resource consumption metrics. Similarly, commercial Endpoint Detection and Response platforms generally report high detection performance but rely on cloud-scale analytics, proprietary detection technologies, and enterprise infrastructures that differ substantially from the lightweight architecture evaluated in this study.

These findings suggest that the primary contribution of the proposed framework lies not in replacing enterprise-grade commercial EDR solutions but in demonstrating that effective endpoint monitoring and threat detection can be achieved using a modular and resource-efficient architecture suitable for micro and small enterprises. The combination of behavioral monitoring, YARA rule matching, Sigma-based log analysis, threat intelligence integration, and dynamic risk scoring enabled the framework to achieve high detection effectiveness while maintaining the low computational overhead required for deployment in resource-constrained environments.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

4.9 Limitations of the Study

Several limitations should be considered when interpreting the findings of this study.

First, the respondent-based evaluation involved only five participants. Although the paired-sample *t*-test indicated consistent improvements in the post-implementation evaluation scores, the limited sample size restricts statistical power and the extent to which the findings can be generalized. Consequently, the statistical results should be interpreted as preliminary evidence of improvement rather than definitive inferential conclusions. Future studies should recruit a larger and more diverse group of evaluators or employ non-parametric methods, such as the Wilcoxon signed-rank test, when sample sizes are limited.

Second, the cybersecurity performance evaluation was conducted using a controlled dataset comprising 512 labeled endpoint events. While the framework demonstrated high detection accuracy, precision, and recall under these experimental conditions, the dataset does not fully capture the diversity of user behavior, endpoint configurations, network environments, and attack techniques encountered in operational enterprise settings. Accordingly, the reported performance metrics should be interpreted as evidence of effectiveness within a controlled laboratory environment rather than as estimates of performance under all real-world deployment conditions.

Third, the framework was evaluated in a short-term simulated enterprise environment rather than through long-term production deployment. Consequently, the study did not assess operational stability, detection consistency, or maintenance requirements over extended periods of continuous use.

Fourth, adversarial validation employed controlled attack emulation and safe malware-test artifacts instead of uncontrolled live malware. This approach was adopted to ensure ethical, legal, and operational safety while enabling reproducible experimentation (Sikorski & Honig, 2012). However, it may not fully reflect the complexity and adaptive behavior exhibited by contemporary Advanced Persistent Threat (APT) campaigns.

Fifth, the validation scenarios represented only a subset of the techniques described in the MITRE ATT&CK knowledge base and therefore do not encompass the full spectrum of adversary tactics, techniques, and procedures observed in real-world cyber operations (MITRE ATT&CK, n.d.). Expanding the range of evaluated techniques would provide a more comprehensive assessment of detection coverage.

Sixth, the proposed framework emphasizes a lightweight architecture based on rule-based detection, behavioral monitoring, threat intelligence correlation, and heuristic analysis. It does not incorporate advanced machine learning models, large-scale cloud telemetry, or automated response capabilities commonly available in enterprise-grade commercial EDR platforms. As a result, the framework should be viewed as a practical solution for resource-constrained environments rather than a replacement for comprehensive commercial security platforms.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

Finally, although the framework was designed using a modular client–server architecture that supports future multi-endpoint deployment, scalability was not empirically validated. The experimental evaluation was limited to a single endpoint, and therefore the framework demonstrates scalability by design rather than experimentally verified scalability. Future research should evaluate large-scale deployments to examine communication overhead, event throughput, centralized processing performance, and resource utilization across distributed enterprise environments.

Taken together, these limitations indicate that the reported software quality assessments and cybersecurity performance metrics represent an initial proof of feasibility obtained under controlled experimental conditions. Future studies involving larger-scale deployments, broader adversarial scenarios, extended operational periods, and more diverse evaluation datasets will further strengthen the empirical evidence supporting the framework's effectiveness and applicability.

V. CONCLUSION AND RECOMMENDATIONS

This study designed, implemented, and evaluated a lightweight Endpoint Detection and Response (EDR) framework intended for resource-constrained enterprise environments. The proposed framework integrates endpoint telemetry collection, behavioral monitoring, process trust evaluation, YARA and Sigma rule-based detection, threat intelligence correlation, heuristic-assisted anomaly detection, dynamic risk scoring, centralized logging, and dashboard-based incident management within a modular client–server architecture. The framework was developed to improve endpoint visibility and support timely detection of Advanced Persistent Threat (APT)-related activities while maintaining low computational overhead.

The evaluation demonstrated that the proposed framework achieved favorable software quality ratings across the assessed ISO/IEC 25010 characteristics and exhibited statistically higher post-implementation evaluation scores than the corresponding pre-implementation assessments. Technical validation further demonstrated high detection effectiveness, achieving 97.85% detection accuracy**,** 88.00% precision**,** and 97.06% recall, while maintaining low resource consumption, with an average response time of 1.8 seconds**,** 4.6% CPU utilization, and 105 MB of memory usage. Collectively, these findings indicate that the framework can effectively balance detection capability and operational efficiency within the controlled experimental environment considered in this study.

The principal contribution of this research lies in demonstrating the feasibility of implementing a lightweight, modular EDR framework that combines behavioral monitoring, rule-based detection, threat intelligence integration, and objective performance evaluation within a single architecture tailored to the operational constraints of micro and small enterprises. Although the framework is not intended to replace enterprise-grade commercial EDR platforms, the results suggest that it provides a practical approach for improving endpoint monitoring and threat detection where financial, computational, or infrastructure resources are limited.

Online ISSN: 3082-5121
Aloysian Interdisciplinary Journal of Social Sciences, Education, and Allied Fields
https://journals.aloysianpublications.com
Volume 2 Issue 7 (2026)

The findings should be interpreted within the scope of the study's limitations, including the controlled laboratory evaluation, limited respondent sample, single-endpoint deployment, and restricted set of adversarial scenarios. Consequently, the reported results provide evidence of feasibility rather than definitive estimates of operational performance across diverse production environments.

Future research should evaluate the framework under multi-endpoint enterprise deployments to investigate scalability, communication overhead, event processing throughput, and long-term operational performance. Additional enhancements may include the integration of distributed database technologies, asynchronous messaging architectures, Security Information and Event Management (SIEM) platforms, automated response orchestration, expanded threat intelligence synchronization, and adaptive machine learning techniques to further improve detection capability, scalability, and operational resilience.

REFERENCES

Akbar, K. A., Wang, Y., Ayoade, G., Gao, Y., Singhal, A., Khan, L., Thuraisingham, B., & Jee, K. (2023). Advanced persistent threat detection using data provenance and metric learning. *IEEE Transactions on Dependable and Secure Computing, 20*(5), 3957–3969. https://doi.org/10.1109/TDSC.2022.3221789

Al-Kadhimi, A. A., Singh, M. M., & Khalid, M. N. A. (2023). A systematic literature review and a conceptual framework proposition for advanced persistent threats (APT) detection for mobile devices using artificial intelligence techniques. *Applied Sciences, 13*(14), Article 8056. https://doi.org/10.3390/app13148056

AV-Comparatives. (2024). *Advanced threat protection test 2024 – Enterprise*. https://www.av-comparatives.org/tests/advanced-threat-protection-test-2024-enterprise/

AV-Comparatives. (2024). *Endpoint prevention & response (EPR) test 2024*. https://www.av-comparatives.org/tests/endpoint-prevention-response-epr-test-2024/

Blancaflor, E., Pasco, J. A., Tamargo, J., Jonson, J. A., & Doydoy, J. D. (2024). Comparative analysis and application of cybersecurity framework to Philippine small and medium enterprises (SMEs). In *Proceedings of the 2024 9th International Conference on Intelligent Information Technology* (pp. 109–113). Association for Computing Machinery. https://doi.org/10.1145/3654522.3654565

CrowdStrike. (2024). *CrowdStrike Falcon platform*. https://www.crowdstrike.com/platform/

Cybersecurity and Infrastructure Security Agency. (2024). *Known exploited vulnerabilities catalog*. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Department of Information and Communications Technology. (2023). *National cybersecurity plan 2023–2028*. Government of the Philippines.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In *Proceedings of the 6th International Conference on Information Warfare and Security* (pp. 113–125).

IBM. (2024). *X-Force threat intelligence index 2024*. https://www.ibm.com/reports/threat-intelligence

Microsoft. (n.d.). *Sysmon*. Microsoft Learn. https://learn.microsoft.com/sysinternals/downloads/sysmon

Microsoft. (2024). *Microsoft Defender for Endpoint documentation*. https://learn.microsoft.com/microsoft-365/security/defender-endpoint/

MITRE ATT&CK. (n.d.). *MITRE ATT&CK framework*. MITRE. https://attack.mitre.org/

National Institute of Standards and Technology. (2007). *Guide to intrusion detection and prevention systems (IDPS) (Special Publication 800-94)*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-94/final

National Institute of Standards and Technology. (2025). *Computer security incident handling guide (Special Publication 800-61 Revision 3)*. https://csrc.nist.gov/publications

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Rahman, M. R., Basak, S. K., Hezaveh, R. M., & Williams, L. (2024). *Attackers reveal their arsenal: An investigation of adversarial techniques in cyber threat intelligence reports*. *arXiv*. https://arxiv.org/abs/2401.01865

Salim, A., Buniyamin, N., Shukur, Z., & Idris, M. Y. I. (2023). A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model. *Heliyon, 9*(7), Article e17156. https://doi.org/10.1016/j.heliyon.2023.e17156

SentinelOne. (2024). *Singularity platform*. https://www.sentinelone.com/platform/

Shen, X., Li, Z., Burleigh, G., Wang, L., & Chen, Y. (2024). *Decoding the MITRE Engenuity ATT&CK Enterprise Evaluation: An analysis of EDR performance in real-world environments*. *arXiv*. https://arxiv.org/abs/2401.15878

Sikorski, M., & Honig, A. (2012). *Practical malware analysis: The hands-on guide to dissecting malicious software*. No Starch Press.

Verizon. (2024). *2024 data breach investigations report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/