FORLENS – A LIGHTWEIGHT AI-DRIVEN ENDPOINT SECURITY SOLUTION FOR REAL-TIME THREAT DETECTION IN SMES

25-26J-076

Project Proposal Report

Nusfa M R F – IT22908742

Bsc (Hons) in Information Technology Specializing in Cyber Security

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

September 2025

FORLENS – A LIGHTWEIGHT AI-DRIVEN ENDPOINT SECURITY SOLUTION FOR REAL-TIME THREAT DETECTION IN SMES

25-26J-076

Project Proposal Report

Nusfa M R F – IT22908742

Bsc (Hons) in Information Technology Specializing in Cyber Security

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

September 2025

Declaration of the Candidate & Supervisor

We declare that this is our own work and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Student Name	Student ID	Signature
NUSFA M.R.F	IT22908742	

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the supervisor :  Date : 12/09/2025

Abstract

Small and medium-sized enterprises (SMEs) are becoming more frequently targeted by cybercriminals due to their insufficient financial resources, qualified staff, and sophisticated technological frameworks to implement enterprise-grade protections like Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), or Endpoint Detection and Response (EDR) systems. This circumstance makes them significantly vulnerable to ransomware, insider threats, lateral movement, and privilege escalation attacks. To tackle this issue, this research, as a component of the ForLens project, suggests the creation and advancement of a Lightweight Endpoint Agent integrated with a honeypot module, particularly tailored for SME environments. The agent is crafted to perpetually observe processes, file access behavior, and network transactions while utilizing minimal system resources, guaranteeing effective operation on SME-standard hardware. Stealth-mode capabilities are included, allowing the agent to stay concealed and resilient against tampering or removal efforts by attackers. In addition to monitoring, the honeypot component serves an essential function by emulating a vulnerable service. In this prototype, the honeypot focuses on the Server Message Block (SMB) protocol to lure attackers and log their interaction patterns. For research purposes, the scope is limited to SMB, but in real-world deployments the architecture can be extended to additional services such as SSH or HTTP for broader deception coverage. These deceptive features offer significant insights into intrusion methods while redirecting threats from actual business resources. To uphold dependability, the data collected from both monitoring and honeypot activities is protected with tamper-proof systems, ensuring that forensic evidence stays intact even amid advanced attacks. By combining endpoint monitoring with deception-driven intelligence, the suggested solution enhances SME resilience against progressing cyber threats while ensuring cost-effectiveness, scalability, and ease of implementation. Additionally, the intelligence produced can be effortlessly incorporated into higher-level AI analysis and SOAR-style automation frameworks within the broader ForLens framework, facilitating immediate detection, contextual notifications, and swift incident management. This research ultimately seeks to provide SMEs with an effective and robust endpoint security solution that connects the limitations of resources with the pressing need for strong cyber protection.

Keywords: *Lightweight Endpoint Agent, Integrated Honeypot, SME Cybersecurity, Threat Detection, Deception-Based Defense.*

Table of Content

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Description
SME	Small and Medium-Sized Enterprises
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
EDR	Endpoint Detection and Response
AI	Artificial Intelligence
IDS	Intrusion Detection System
XAI	Explainable Artificial Intelligence
CNN	Convolutional Neural Network
IoT	Internet of Things
IIoT	Industrial Internet of Things
TLS	Transport Layer Security
SSL	Secure Sockets Layer
GDPR	General Data Protection Regulation
PCI-DSS	Payment Card Industry Data Security Standard
IDE	Integrated Development Environment
API	Application Programming Interface
MSP	Managed Service Provider
VM	Virtual Machine (VirtualBox / VMware)
WSL2	Windows Subsystem for Linux 2
CPU	Central Processing Unit
RAM	Random Access Memory

1. INTRODUCTION

Small and medium-sized enterprises (SMEs) are becoming more frequent targets of contemporary cyberattacks, primarily because of their restricted security funding, insufficient skilled staff, and dependence on outdated or general endpoint security measures. In contrast to larger firms that can invest in advanced SIEM, SOAR, and EDR systems, SMEs face limitations related to cost, complexity of implementation, and the technical demands associated with enterprise-level solutions [20]. As a result, they find themselves disproportionately vulnerable to advanced threats like ransomware, lateral movement, insider threats, and privilege escalation.

In reaction, scholars have investigated deception-based protective measures as a viable and cost-effective method to enhance endpoint security. High-interaction honeypots, like HoneyWin [3] and various enterprise-grade frameworks [2] offer profound understanding of attacker actions but demand considerable computational power, rendering them impractical for SMEs. To overcome these challenges, adaptive honeypots and strategies for cyber deception have been suggested [4], [6], [18], illustrating how attackers can be directed towards decoys while defenders acquire useful intelligence. Nevertheless, the majority of these designs are focused on large-scale or IoT contexts, resulting in a lack of lightweight solutions tailored for SMEs.

Simultaneously, intrusion detection systems have progressed from traditional signature-based methods to advanced approaches that apply machine learning and ensemble-driven anomaly detection [15], [16], [17]. While these methods show strong detection potential, they often depend heavily on cloud infrastructures or resource-intensive models, making them impractical for SMEs. Research on explainable AI (XAI) for anomaly detection [14] highlights the importance of producing interpretable outputs that administrators can trust and act upon. However, very little work has been done to combine such interpretable detection with endpoint-level deception. This creates a clear opportunity for the proposed lightweight endpoint agent, which embeds a honeypot and monitoring functions to generate context-rich telemetry. Such telemetry can later complement higher-level

anomaly detection and XAI models in the broader ForLens framework, while still ensuring SMEs benefit from real-time deception-driven visibility directly on the endpoint. Another ongoing issue is the resilience of endpoint security measures. When cybercriminals gain higher-level access, they have the ability to deactivate, remove, or circumvent current endpoint defenses, eliminating forensic insights and extending the duration of the breach [5]. There has been only a small amount of research focused on stealthy, deletion-proof, and user-friendly deployment strategies designed for SMEs, which are crucial for maintaining robustness, facilitating implementation, and ensuring sustained effectiveness [19], [21].

This research aims to tackle these weaknesses by developing a lightweight, deception-driven endpoint agent that merges endpoint monitoring with an embedded low-interaction honeypot component. The agent features stealth/tampering-resistant capabilities, instant event forwarding, and SME-focused plug-and-play installation. In this prototype, the honeypot element will concentrate on one lure (SMB), but in actual implementations, the architecture can be expanded to accommodate various lures like SSH or HTTP for wider deception coverage. By integrating these elements into a cohesive framework, the research aims to offer SMEs access to enterprise-level security functions via a budget-friendly, resource-efficient, and straightforwardly deployable solution.

1.1 Background & Literature Survey

Small and medium-sized enterprises (SMEs) are crucial to both national and global economies, yet they encounter significantly higher cybersecurity threats in comparison to larger firms. The main factor contributing to this issue is their limited financial resources, lack of qualified cybersecurity staff, and reliance on outdated antivirus solutions or static rule-based endpoint protections [20]. Larger corporations often manage these risks through sophisticated Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and Endpoint Detection and Response (EDR) systems. Nonetheless, the steep costs, intricate deployment processes, and technical demands of these enterprise-level solutions make them unattainable for SMEs.

Consequently, SMEs are extremely susceptible to ransomware attacks, insider threats, privilege escalation, and advanced hacking strategies that take advantage of unmonitored activities and fragile defenses. Tackling these issues necessitates a solution that integrates a streamlined design, cost-effectiveness, and robust threat intelligence generation while reducing operational complexity.

One of the most extensively researched methods for producing attacker intelligence is the implementation of honeypots. Conventional high-interaction honeypots, like HoneyWin [3], have been utilized in corporate networks to record intricate adversarial actions, encompassing malware infection trends and post-exploitation strategies. Likewise, localized honeypot frameworks have granted researchers crucial understanding of regional botnet behaviors and changing threat dynamics [2]. These systems illustrate the effectiveness of deceit as a defensive approach: by enticing attackers into managed traps, defenders obtain insights into adversary strategies while redirecting threats away from operational assets. Nevertheless, these high-interaction systems necessitate considerable memory, processing, and surveillance resources, rendering them impractical for SME endpoints.

In order to tackle these resource issues, scientists have developed adaptive and low-interaction honeypots that are meant to function with reduced system requirements. Adaptive honeypots [6] modify their decoys and services in real-time to keep attackers interested, which enhances both realism and detection precision. Recent studies, including those incorporating AI-enhanced honeypot frameworks, utilize data integration and anomaly identification to adapt automatically to tactics employed by attackers and improve resource utilization [18], [1]. Research on deception methods verifies that incorporating intelligence and automation into honeypots greatly boosts their effectiveness and detection capabilities [4], [19]. Nevertheless, many of these developments primarily target enterprise or IoT settings, with scant attention given to creating lightweight, endpoint-level honeypots that small and medium-sized enterprises can implement without substantial infrastructure or specialized knowledge.

In conjunction with research on deception, intrusion detection has evolved from static, signature-dependent methods to anomaly-based systems that utilize machine learning. Lightweight supervised intrusion detection systems [15] and ensemble feature selection methods [16] have shown the practicality of identifying complex threats in environments with limited resources. Likewise, lightweight IDS employing convolutional neural networks (CNN) [17] and deep learning techniques have reached impressive detection accuracies, even under fluctuating traffic situations. Although these studies highlight the potential of machine learning in intrusion detection, their significant dependence on cloud infrastructures or resource-intensive models renders them impractical for small and medium enterprises that seek cost-effective, on-device solutions.

A developing trend in anomaly detection research is the application of Explainable AI (XAI) to enhance the clarity of detection results. Conventional black-box models frequently generate alerts that system administrators find difficult to comprehend or verify, resulting in lost response time or overlooked incidents. Research, including Safarov et al. [14], suggests efficient, explainable detection models that offer transparent reasoning behind alerts, thus fostering trust and enhancing usability. While XAI has demonstrated potential in detecting IoT attacks, its incorporation with endpoint deception strategies has been somewhat restricted. In this research, the endpoint agent does not directly implement explainable detection but focuses on generating deception-driven, context-rich data. This data can later feed into explainable detection models within the wider ForLens system, while still ensuring SMEs gain immediate visibility directly at the endpoint

A continual challenge within endpoint security is the ability to withstand tampering. Studies show that when attackers gain elevated privileges, they often turn off, remove, or circumvent endpoint defenses, which effectively eliminates forensic evidence and extends the period of compromise [5]. Although the concepts of stealth-mode honeypots and tamper-evident endpoint designs have been explored [19], [21], there is a lack of research focused on making such resilience lightweight and feasible for SME devices. Incorporating stealth and self-defense capabilities into endpoint agents is essential for

ensuring that security measures remain intact and cannot be easily disabled or deleted, thus maintaining visibility during ongoing attacks.

Aside from resilience, recent studies have underscored the significance of real-time alerting and correlation systems. For instance, Wang et al. [22] show that linking honeypot actions with current endpoint telemetry enhances the precision of detection and minimizes false positive. Correlation engines give defenders more useful intelligence by linking attacker actions to actual process execution and network behavior. However, few of these solutions are specifically designed for SMEs and many of them assume centralized systems. Instead of directly implementing a correlation engine in this component, the endpoint agent forwards honeypots and continuously monitors events. SME visibility can be increased without the need for enterprise-scale back-end systems by correlating these events with other data in the larger ForLens architecture.

Ultimately, the viability of deployment is a significant hurdle for SMEs. Although several enterprise frameworks offer strong detection features, they generally require proficient setup, ongoing upkeep, and compatibility with current infrastructure. Research highlights that for SMEs to effectively adopt these solutions, there is a need for plug-and-play deployment models that involve minimal technical demands [23]. Such configurations enable endpoint agents to be installed and utilized without the need for specialized knowledge, thus lowering the entry barriers for smaller businesses. Concurrently, customizing detection frameworks to address the specific attack surfaces of SMEs such as employee endpoints, small office networks, and restricted cloud workloads ensures that the protective measures are pertinent and efficient for their distinct environments.

The research collectively highlights notable progress in deception-focused honeypots, methods for anomaly detection, explainable artificial intelligence, resilient endpoint architectures, real-time correlation, and adaptable deployment strategies. However, these advancements remain fragmented, with individual studies focusing on different aspects of the problem. A cohesive solution that integrates these elements into a unified, efficient endpoint agent designed for SMEs has not been realized. The proposed research seeks to

tackle this gap by developing a single lightweight endpoint agent that combines monitoring and a built-in low-interaction honeypot module that includes stealth/tamper-proof features, instantaneous event forwarding, and easy deployment. For this prototype, the honeypot component will focus on an SMB lure, while prospective additions may introduce further services like SSH or HTTP to enhance deceptive reach. By integrating deception at the endpoint level and relaying telemetry for advanced AI/ML assessment and SOAR-type automation, the solution provides SMEs with enterprise-level protective capabilities that are affordable, efficient, and straightforward to deploy.

1.2 Research Gap

Despite notable progress in deception technologies and intrusion detection systems, their adoption within small and medium-sized enterprises (SMEs) remains severely limited. High-interaction honeypots such as HoneyWin and localized trap-based systems have shown considerable effectiveness in capturing attacker behaviors and producing forensic insights. Nonetheless, these methods are resource-intensive, demanding substantial computational power and memory, as well as requiring specialized infrastructure, which renders them impractical for immediate implementation on SME endpoints [2], [3]. Although adaptive honeypots and AI-enhanced deception tactics have been proposed in the literature [4], [6], [18], they are primarily tailored for enterprise-level or IoT frameworks, neglecting the cost-effectiveness, ease of implementation, and lightweight design requirements that SMEs urgently need. This underscores an urgent necessity for deception-driven endpoint security frameworks that are not only efficient against advanced threats but also feasible in resource-limited operational environments.

Intrusion detection techniques have also evolved, shifting from classic signature-based systems to models driven by machine learning and ensembles. While some lightweight intrusion detection frameworks have started to surface [15], [16] most still heavily depend on cloud infrastructures, introduce significant computational demands, or lack clarity when implemented directly at the endpoint level. Furthermore, although anomaly detection methods have progressed, current studies infrequently integrate them with

deception technologies to generate context-rich telemetry that can later feed into real-time alerts and forensic visibility within larger frameworks, tailored for SME administrators.

Another significant shortcoming exists in the robustness and durability of endpoint protection itself. After attackers elevate their privileges, they often disable, uninstall, or circumvent defensive measures, wiping out forensic evidence and extending the duration of the breach [5]. While stealth-mode and tamper-proof solutions are available in specific scenarios, only a handful have been designed considering lightweight endpoints. Adding to this problem is the deficiency in focus on plug-and-play deployment models and SME-specific attack surface tailoring, both of which are essential for real-world implementation. In the absence of these features, numerous suggested remedies stay as theoretical models instead of being actionable security structures for SMEs.

Therefore, the central research deficiency resides in the absence of a unified, lightweight endpoint agent that integrates deception-oriented honeypots, stealth/tamper-resistant methods, real-time event forwarding, and SME-customizable plug-and-play implementation into one single cohesive framework.Existing literature discusses these components separately but does not provide a comprehensive, resource-efficient solution that closes the security gap encountered by SMEs. The suggested research specifically focuses on this gap by developing such an endpoint agent, providing a scalable, cost-effective and robust defense framework that provides enterprise-level security without the exorbitant expenses, infrastructure, and intricacies associated with traditional systems.

Features/Contributions	Research [3]	Research [2],[6]	Research [15],[16]	Research [5]	Research [4],[13]	Proposed System
Low-interaction honeypot integrated into endpoint agent	✗	✗	✗	✗	✗	✓

Lightweight deception-based honeypot	✗	✓	✗	✗	✓	✓
Generates context-rich telemetry for integration with anomaly detection	✗	✗	✓	✗	✓	✓
Stealth mode / tamper-resistant operation	✗	✗	✗	✓	✗	✓
Real-time event forwarding	✗	✗	✗	✗	✗	✓
Supports correlation by forwarding honeypot + endpoint telemetry	✗	✗	✗	✗	✗	✓
Plug-and-play deployment (low technical effort)	✗	✗	✗	✗	✗	✓
Tailored for SME-specific attack surfaces	✗	✗	✗	✗	✗	✓
Cost-effective, easy-to-deploy solution for SMEs	✗	✗	✗	✗	✗	✓

Table 1 : Comparison of Previous Research and the proposed Lightweight Endpoint Agent

1.3 Research Problem

Small and medium-sized enterprises (SMEs) are encountering an increasing surge of cybersecurity dangers, comprising ransomware, lateral movement, insider threats, and privilege escalation. In spite of this mounting threat, they still do not have access to enterprise-level defenses like SIEM, EDR, and SOAR systems, mainly because of prohibitive costs, limited resources, and technical difficulties. Consequently, SMEs must depend on obsolete, signature-based solutions or cloud-dominant services, neither of which adequately provide real-time, robust endpoint security.

Current defenses focused on deception, like high-interaction honeypots, offer important perspectives on attacker actions yet are excessively demanding on resources and unsuitable for SME endpoints. Emerging lightweight intrusion detection systems are starting to surface, but they often fall short in terms of covert operation, resilience against tampering, and the ability to integrate with deception-based approaches. Furthermore, most existing solutions fail to provide immediate event forwarding that can later be correlated with endpoint actions in higher-level frameworks.

Another major drawback is the feasibility of deployment. Numerous current endpoint security solutions demand intricate setups and specialized knowledge, rendering them impractical for SMEs. There is minimal focus on plug-and-play deployment models that reduce technical labor, or on affordable structures specifically designed for SME attack surfaces. As a result, SMEs continue to be significantly exposed: when intruders obtain heightened permissions, they are able to deactivate endpoint protections, eliminate forensic evidence, and extend system infiltration without detection.

Therefore, the central research problem lies in the absence of a cohesive, lightweight, and tamper-resistant endpoint agent that unifies low-interaction honeypot deception, stealth/tamper-resistant monitoring, real-time event forwarding to support correlation at higher levels, covert operation, and easy installation in a structure specifically designed for SMEs. In the absence of this type of solution, SMEs remain unduly vulnerable to

sophisticated cyber threats while lacking the cost-effectiveness and ease of use required for implementation.

2. OBJECTIVES

Cybersecurity for small and medium-sized enterprises (SMEs) necessitates solutions that are effective, cost-efficient, and simple to execute, yet still able to counter advanced and changing cyber threats. This research emphasizes the development and execution of a Lightweight Endpoint Agent combined with a low-interaction honeypot component, specifically designed for SME settings. The suggested agent will provide ongoing behavioral surveillance, deception-oriented attacker interaction, immediate event forwarding, stealthy and tamper-resistant functionality, and smooth linkage between honeypot activations and endpoint actions. Its lightweight and easy-to-integrate structure guarantees practicality for SMEs with constrained technical resources while upholding robust defensive features.

2.1 Main Objective

The main objective of this research is to create and build a lightweight, tamper-proof endpoint security agent for small and medium-sized businesses. The approach combines ongoing endpoint monitoring with an incorporated low-interaction honeypot to entice and capture attacker interactions, forwarding context-rich events for forensic analysis, and function in stealth mode to avoid detection or elimination by attackers. By closing the divide between basic antivirus options and resource-intensive enterprise deception systems, the suggested framework aims to deliver SMEs an cost-effective, implementable, and efficient security approach that enhances the ability to withstand contemporary cyber dangers.

2.2 Specific Objectives

This initiative seeks to accomplish the subsequent distinct goals:

- Lightweight Endpoint Monitoring - To create an endpoint agent that can oversee essential system operations (e.g., process initiation, file changes, and network links) in real time, while utilizing minimal computing resources to maintain practicality in small and medium-sized enterprise environments.

- Integrated Honeypot Module - To integrate a low-interaction honeypot that mimics susceptible assets and services, attracts attackers, and records their actions without jeopardizing operational systems.
- Stealth and Tamper-Resilience – To establish stealth-mode functionality and deletion-resistant mechanisms that stop intruders from readily identifying, deactivating, or eliminating the agent and its telemetry.
- Real-Time Event Forwarding – To forward honeypot interaction events and endpoint telemetry in real time, enabling richer, context-aware detection when analyzed in higher-level frameworks such as ForLens.
- Intelligence Support for Higher-Level Detection– To organize endpoint and honeypot information in a way that allows smooth incorporation with upper-tier analytics engines or automated response systems, even if those elements are beyond the purview of this module.
- Plug-and-Play Deployment – To ensure the agent can be easily deployed and configured in SME environments with minimal technical effort, supporting usability and scalability.
- Validation in SME Context– To assess the suggested agent in relation to SME-concerning threat situations (e.g., ransomware, botnet infections, privilege escalation, and insider abuse), gauging its efficacy based on detection precision, performance impact, stealth level, and robustness.

3. METHODOLOGY

The design, development, and assessment of a lightweight endpoint agent integrated with a low-interaction honeypot module that is especially tailored for SME environments are guided by an organized methodology in this study. By emphasizing real-time telemetry transmission, deception-based intelligence collection, lightweight endpoint monitoring, and stealth/tamper-resilient operation, the methodology guarantees that the solution directly satisfies the fundamental needs of SME security. To guarantee that the suggested approach stays resource-efficient, hidden from attackers, and feasible for implementation in actual SME settings, every stage of the methodology—from system design and agent development to telemetry transmission and evaluation—has been meticulously planned.

3.1 System Architecture

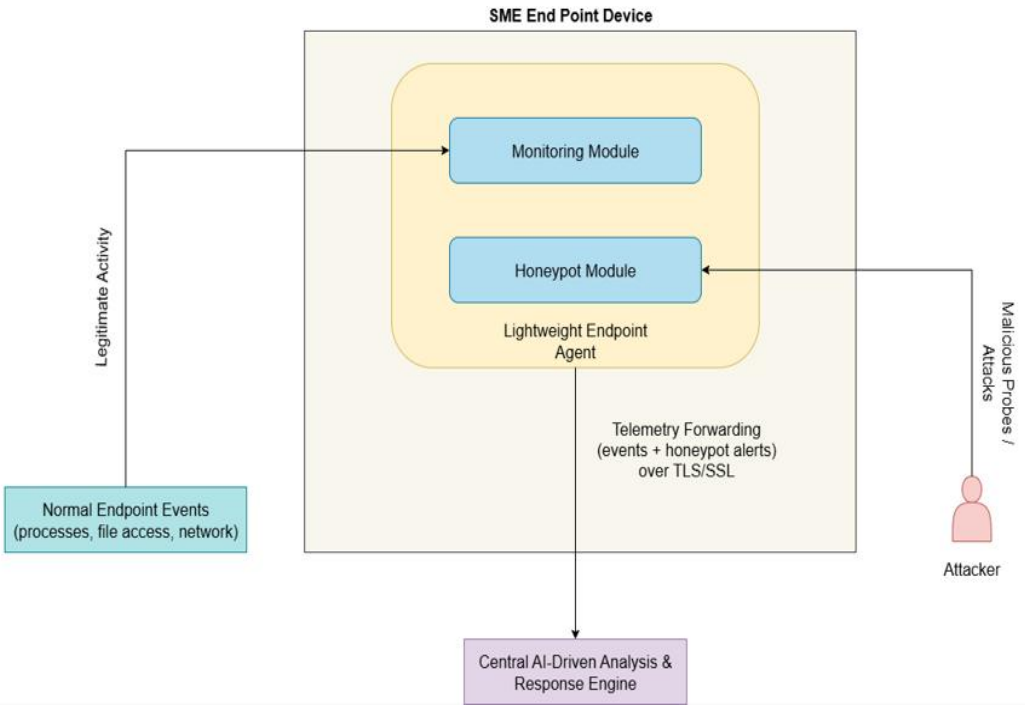

Figure 1: System Architecture Diagram

The design of the suggested solution focuses on a Lightweight Endpoint Agent installed on SME endpoints. The agent consists of two main components:

- Monitoring Module, which consistently monitors essential endpoint actions like process startup, file retrieval, and network interactions with minimal strain to accommodate SME hardware.
- Honeypot Module, which replicates at-risk services/assets to draw in adversaries and log their interaction behaviors without affecting genuine operational systems.

Both components collaborate to offer deception-driven, context-rich telemetry. When questionable behavior is detected, the agent creates real-time telemetry that merges endpoint occurrences with honeypot notifications. This data is sent securely through TLS/SSL to a Central AI-Powered Analysis & Response Mechanism (Higher level system), that enhances the information, connects occurrences, and facilitates advanced automated reactions.

By consolidating observation, misdirection, and safe telemetry transmission into a streamlined and tamper-resistant structure, the system guarantees that SMEs receive enterprise-grade detection and response capability in an economical and simple-to-implement solution.

3.2 Implementation Strategy

The study will be carried out in four primary stages:

Phase 1: Design

- Specify functional and non-functional needs for efficient deployment.
- Identify attack surfaces relevant to SMEs, such as vulnerable SMB shares and frequently exposed ports.

Phase 2: Endpoint Agent & Honeypot Creation

- Develop components for monitoring processes, files, and networks.
- reate the embedded honeypot focusing on SMB (for prototype) as a low-interaction bait, with the design extensible to other services in real-world use.
- Integrate stealth-mode and deletion-resistant mechanisms to prevent detection and removal by attackers.

- Enable real-time event forwarding from honeypot interactions and endpoint telemetry, allowing correlation in higher-level frameworks (e.g., ForLens)

Phase 3: Telemetry Forwarding & Secure Transmission

- Forward endpoint monitoring data and honeypot alerts through secure channels (TLS/SSL)
- Ensure confidentiality and integrity of telemetry during transmission to the central AI-driven response engine.

Phase 4: Testing & Evaluation

- Implement the solution in a test environment resembling that of an SME.
- Emulate authentic threat situations (e.g., ransomware deployment, port probing, lateral mobility).
- Assess resource overhead, stealthiness, tamper resistance, event forwarding reliability, and response time.
- The evaluation will emphasize the prototype's ability to generate and forward deception-driven telemetry, leaving advanced AI/ML-based correlation to the broader ForLens framework

3.3 Tools and Materials

- Programming: C/C++ (agent), Python (scripting and analysis for honeypots).
- Honeypot Frameworks: Adapted low-interaction honeypot frameworks such as Cowrie or Dionaea, configured specifically for SMB services in the prototype.
- Test Environment: VirtualBox / VMware to simulate SME environment.
- Datasets: No external datasets will be used. Evaluation will rely on telemetry generated directly from honeypot engagements and simulated attack scenarios within the test environment.

3.4 Data Gathering & Assessment Strategy

Information will be gathered in two primary categories:

- Endpoint activity records (process runs, file modifications, network activities).

- Honeypot interaction records (attacker commands, exploit attempts, and unauthorized access via the SMB lure).

Evaluation metrics include:

- Resource overhead (CPU, memory usage).
- Stealthiness (capacity to stay unnoticed by attackers).
- Tamper resistance (whether it survives deletion attempts).
- Event forwarding reliability (does it always forward telemetry without loss?).
- Response time (velocity of identification and documentation).

This self-assessment strategy guarantees that the solution is verified against both technical and operational goals pertinent to SMEs.

3.5 Task Scheduling

- Months1–2: Requirement Analysis and architectural Design - Articulate functional and non-functional requirements, pinpoint SME attack vectors, and create the overarching system architecture design.
- Months3–4: Development of Endpoint Agent & Honeypot Module - Establish monitoring for processes/files/networks, create honeypot decoys, and incorporate stealth/self-defense functionalities.
- Month 5: Telemetry Forwarding & Real-Time Events - enable real-time forwarding of honeypot and endpoint events for later correlation in higher-level frameworks (e.g., ForLens)
- Month 6: Controlled Testing - Implement in an SME-style setting, replicate attacks (ransomware, port scanning, lateral movement), and assess resource overhead, stealthiness, tamper resistance, event forwarding reliability, and response time.
- Months 7–8: Evaluation & Refinement - Examine performance indicators (overhead, stealthiness, tamper resistance, event forwarding reliability, response time), improve the system, and create documentation.

A Gantt chart (Figure 6) and the Work Breakdown Structure (Figure 5) offer a comprehensive visual depiction of activities, schedules, and key milestones.

3.6 Anticipated Outcome

The ultimate resolution is anticipated to:

- Deliver efficient, real-time tracking of endpoint actions with low resource consumption.
- Collect adversarial insights by utilizing the integrated honeypot component.
- Provide real-time event forwarding of honeypot and endpoint activity, enabling correlation and detection at higher-level frameworks (e.g., ForLens)
- Operate stealthily to avoid detection and disablement by attackers.
- Offer SMEs a cost-effective, lightweight, and easily deployable endpoint security solution that can forward telemetry for higher-level analysis or AI-driven frameworks.

4.REQUIREMENTS

4.1 Functional Requirements

These specify what the system is required to accomplish:

1. The Lightweight Endpoint Agent will consistently observe process executions, file accessibility, and network actions on SME endpoints.
2. The Honeypot Module is designed to mimic insecure services, files, or ports to attract attackers and document their actions.
3. The system will safely gather telemetry (authorized actions + harmful interactions) and send it for evaluation.
4. The system will include stealth and tamper-resilient mechanisms to prevent attackers from easily detecting or disabling it.
5. The system will forward honeypot interactions and endpoint telemetry in real time for later correlation and alerting in higher-level frameworks (e.g., ForLens).
6. The system shall support plug-and-play deployment for easy installation in SME environments with minimal technical expertise.
7. The system shall ensure reliable, real-time forwarding of telemetry whenever questionable or harmful actions are detected at the honeypot or monitoring module.

4.2 Non-Functional Requirements

These guarantee excellence, effectiveness, and dependability:

1. Performance: The agent must use low CPU (<10%) and memory (<100 MB) to guarantee a lightweight installation on SME endpoints.
2. Scalability: The solution must facilitate deployment across various SME endpoints without the need for advanced infrastructure.
3. Security: Telemetry forwarding (endpoint events + honeypot alerts) must be securely transmitted (e.g., TLS/SSL) to prevent interception or tampering during transfer.
4. Stealth: The agent will function in a covert manner to evade detection and elimination by adversaries.

5. Resilience: The system must incorporate anti-tampering and self-protection measures to prevent attackers from disabling or uninstalling the agent.
6. Usability: Installation needs to be straightforward (plug-and-play approach) needing little technical knowledge from SMEs.

4.3 User Requirements

These outline what users (SMEs / administrators) anticipate:

1. SME administrators should be capable of installing the agent effortlessly on endpoint devices without requiring extensive technical expertise.
2. "Users should be assured that all telemetry related to harmful activities and endpoint state is reliably forwarded for higher-level analysis and alerting
3. The system should not disrupt standard business functions (minimal overhead, fluid performance).
4. Users should be confident that the agent cannot be disabled or bypassed by attackers (tamper-resilience and stealth mode).
5. Users ought to have the capability to combine the solution with current SME security instruments (when relevant).

4.4 System Requirements

These define hardware, software, and environment needs:

Hardware:

- SME endpoints: At least a Dual-core CPU, 2 GB of RAM, 100 MB of available storage.
- Central server (for AI-driven analysis/response engine): Quad-core CPU, 8 GB RAM, 50–100 GB storage (for telemetry processing).

Software:

- Endpoint agent: Operates on Windows/Linux SME endpoints.
- Honeypot module: Modified low-interaction version of Cowrie/Dionaea tailored for SME endpoints.

Networking:

- Secure TLS/SSL channel for telemetry forwarding (events + honeypot alerts).
- Internet or LAN link between endpoints and central AI engine.

4.5 Use Cases

Use Case 01		
Use Case ID	U001	
Name	Monitor Normal Endpoint Devices	
Description	The Monitoring Module captures and forwards normal endpoint activity (such as process execution, file access, or network connections) to the central analysis engine via secure transmission.	
Application	SME endpoints (PCs, servers) with a lightweight endpoint agent.	
Primary Actor	The SME Endpoint Device	
Pre-condition	Endpoint agent has been installed and is operational.	
Trigger	Process, file, and network operations are started by system boot or user activity.	
Basic Flows	**Steps**	**Actions**
	1	Endpoint agent begins to work when your system boots.
	2	The monitoring module monitor, detect and log process/file/network activities.
	3	Captured telemetry is temporarily buffered by the agent.
	4	Telemetry is securely transmitted (TLS/SSL) to the next layer.
Alternative Flows	**Steps**	**Branching Actions**

	2a	Telemetry is cached locally until the connection is restored if the system is down.
	3a	If local buffer is near capacity, the agent overwrites oldest entries and notifies the admin.
	4a	If the transmission is unsuccessful, try again using a new authentication token.
Post-condition	Normal endpoint activity securely captured and forwarded, ready for use by higher-level frameworks	

Table 2: Use Case 01

Use Case 02		
Use Case ID	U002	
Name	Capture Malicious Activity	
Description	While staying separate from actual assets, the Honeypot Module records attacker interactions, exposes simulated susceptible assets and services (e.g., an SMB lure in the prototype), and forwards telemetry for higher-level analysis	
Application	On SME endpoints, a lightweight endpoint agent with an integrated low-interaction honeypot	
Primary Actor	Attacker (internal or external)	
Pre-condition	The deployed honeypot module is operating in stealth mode and is separated from production files and services.	
Trigger	A honeypot service (a false SMB share) is scanned, probed, or interacted with by an attacker.	
Basic Flows	**Steps**	**Actions**

	1	Inbound connections and probes are received locally by the honeypot service on the endpoint agent
	2	The interaction is fingerprinted by the module (source IP/host, tool patterns, and command sequences).
	3	Requests, payloads, file operations, and commands are all captured.
	4	The event is forwarded as telemetry to higher-level frameworks (e.g., ForLens) for analysis
Alternative Flows	**Steps**	**Branching Actions**
	2a	Honeypot continues capturing and forwarding all scanner traffic without affecting the endpoint.
	3a	All suspicious or unusual interaction is forwarded unchanged to higher-level frameworks for interpretation
	4a	If the local buffer is full, older entries are replaced while new telemetry is forwarded.
Post-condition	Attacker behavior is captured by the honeypot and forwarded as telemetry to higher-level frameworks (e.g., ForLens) for analysis.	

Table 3:Use Case 02

Use Case 03	
Use Case ID	U003
Name	Stealth and Tamper-Resilience

Description	The endpoint agent has tamper-resilient capabilities to guard against deactivation, deletion, or alteration, and it runs in stealth mode to evade discovery by attackers	
Application	On SME devices, a lightweight endpoint agent is installed.	
Primary Actor	Attacker (trying to disable or go around the agent).	
Pre-condition	The agent has self-defense turned on and is operating in stealth mode.	
Trigger	An attacker attempts to find, stop, remove, or change the agent's files, services, or processes.	
Basic Flows	**Steps**	**Actions**
	1	To find the agent, the attacker looks through service lists, registry entries, and active processes.
	2	By employing stealth tactics, such as veiled service names and camouflaged processes, the agent stays hidden.
	3	The tamper-resilient module prevents any attempts to kill or remove the agent.
	4	The attempt is forwarded as telemetry to higher-level frameworks (e.g., ForLens) for analysis
Alternative Flows	**Steps**	**Branching Actions**
	2a	Tamper attempt is captured and forwarded before disable is successful
	3a	If tampering escalates, the agent attempts to continue until terminated.

	4a	Tamper-attempt records are cached locally and sent after the network connection is restored if it is not accessible.
Post-condition	Tampering attempts are blocked or mitigated, stealth is maintained, and all events are securely forwarded for analysis without exposing the agent's presence to attackers	

Table 4: Use Case 03

4.7 Test Cases

The following test cases (Functional – F, Security – S, Performance – P, Resilience – R, Usability – U, Validation – V) are designed to systematically evaluate the proposed Lightweight Endpoint Agent with Honeypot. Each test case includes objective, preconditions, steps, expected results, and pass criteria

Test Case ID	**Objective**	**Pre-conditions**	**Steps**	**Expected Result**	**Pass Criteria**
TC-F01	Verify endpoint activity monitoring	Agent installed and running	1. Start a process 2. Open a file 3. Connect to a network resource	Events captured by monitoring module and sent to higher level	≥95% of activities captured and forwarded telemetry successfully received by higher-level system
TC-F02	Validate honeypot deception trigger	Honeypot module active in stealth mode	1. Attacker scans decoy port 2. Attacker attempts to	Honeypot captures interaction and forwards it as honeypot	Telemetry successfully received by higher-level system

			access trap SMB share	telemetry to higher-level frameworks for analysis.	within 5 seconds.
TC-F03	Dashboard shows linked alert with both honeypot + endpoint context	Both monitoring & honeypot modules active	1. Attacker interacts with honeypot 2. Attacker runs process on endpoint	Agent forwards honeypot + endpoint telemetry in real time for correlation in higher-level frameworks.	Both honeypot + endpoint telemetry are visible in higher-level system log
TC-S01	Make sure the system is tamper-resistant and stealth	Self-defense is enabled and the agent is active.	1. The attacker attempts to halt the agent's service or process 2. Try to remove the agent files.	Tamper attempt is detected by the agent's self-defense module; the agent resists termination or auto-recovers, and the tamper event is forwarded as telemetry to higher-level frameworks	The agent keeps running and forwards the tamper event to higher level
TC-P01	Calculate the resource overhead.	SME endpoint with the agent installed	1. Execute standard tasks (Word, Excel, and browser) 2. Track CPU and memory utilization	Resource usage: ≤150 MB RAM and ≤10% CPU	Under typical load, thresholds are not exceeded.

TC-R01	Verify resilience in the event of a network outage.	Network unavailable; agent active	1. Disconnect the network. 2. Create activity on the endpoint and honeypot.	Agent temporarily caches telemetry locally until connection is restored	After the connection is restored, cached telemetry is successfully sent to higher-level systems without causing any data loss.
TC-U01	Test the implementation of plug-and-play	New SME endpoint without any previous configuration	1. Launch the installer 2. Auto-starting agents	Agent deployment doesn't require complicated setup.	It takes about five minutes to install and doesn't require any setup.
TC-V01	Honeypot module active in stealth mode	The test environment is ready.	1. Simulate attacker probing SMB port 2. Attempt unauthorized file access via SMB trap share	Honeypot captures the interaction and forwards telemetry	Telemetry successfully received by higher-level system within 5 seconds; SME attack attempt detected without disrupting normal operations

Table 5: Test Cases

4.8 Wireframes

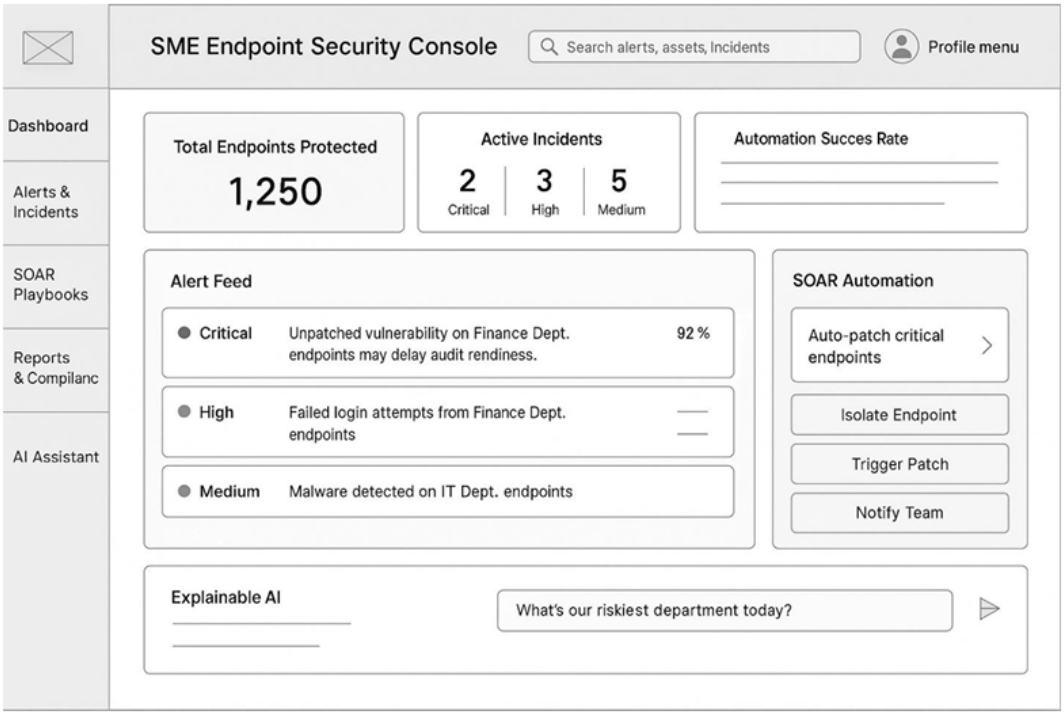

Figure 2: Wireframe 01

A direct dashboard interface is not offered by the Endpoint Agent with embedded honeypot. Rather, the higher-level module receives all of the telemetry that has been recorded, including endpoint activities, honeypot interactions, and tamper events. The dashboard wireframe, which displays data from several sources, including the suggested agent, is shown in Figure 2. Through this integration, centralized analysis, automated reaction, and decision-making are supported by ensuring that agent-generated alerts (such as SMB trap interactions or anomalies in endpoint activity) are exposed alongside other issues.

5.WORK BREAKDOWN STRUCTURE (WBS)

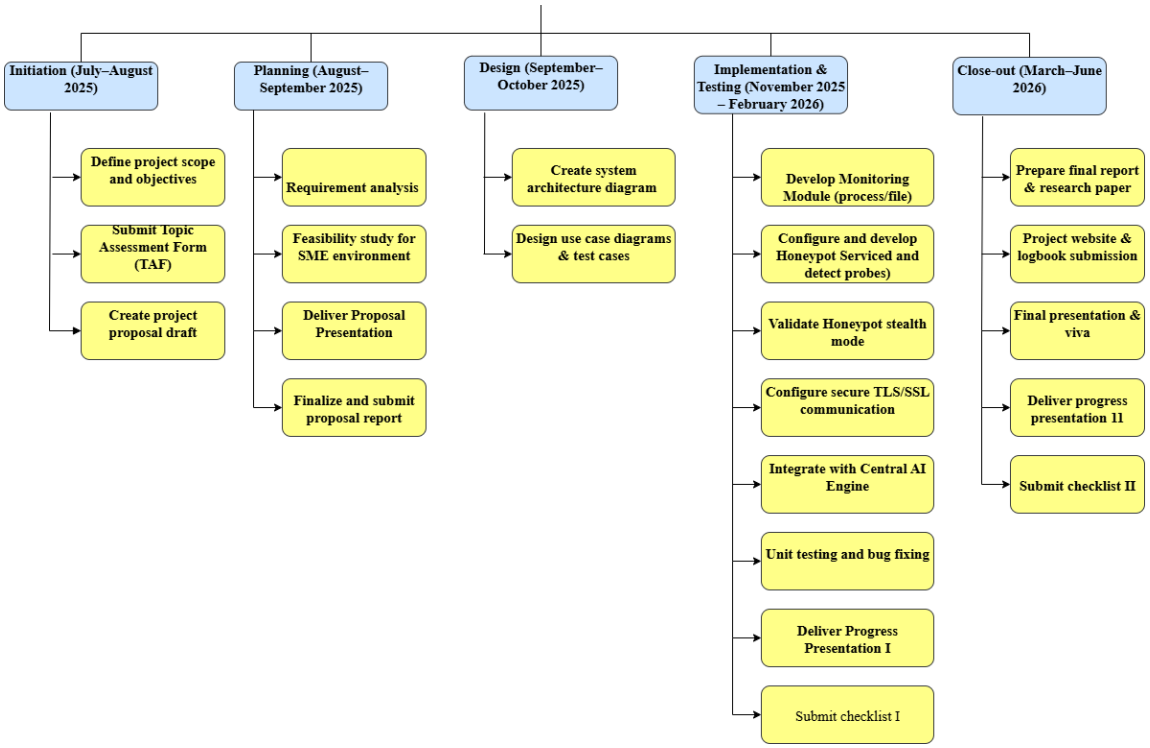

Figure 3: Work Breakdown Structure

The Work Breakdown Structure for this project divides the research process into five key stages: Initiation, Planning, Design, Implementation and Testing, and Close-out. Each phase encompasses duties, outputs, and achievable schedules that correspond with the official project evaluation timeline.

1. Initiation (July–August 2025):This stage emphasizes outlining the project's scope and goals, completing the Topic Assessment Form (TAF), and drafting the initial proposal. In this phase, the proposal features initial requirements, feasibility assessments, and provisional design concepts to illustrate the project's direction. These elements will be improved in subsequent phases.
2. Planning (August–September 2025):In the planning phase, more extensive tasks are carried out. This encompasses thorough requirement analysis (functional, non-functional, system, and user), feasibility studies customized for SMEs.The

presentation of the proposal is given, and the final proposal document is provided after integrating feedback. The actions taken at this stage enhance and confirm the provisional details previously outlined in the proposal draft.

3. Design (September–October 2025):This phase completes the overarching system architecture, intricate use case diagrams and test cases. Although preliminary designs were included in the proposal report, this stage aims to create finalized, technically robust artifacts that will direct implementation.
4. Implementation & Testing (November 2025–February 2026): This phase represents the core development stage, focusing on the creation and validation of the Monitoring Module and Honeypot Module. The honeypot module involves configuring lightweight services (e.g.SMB) to simulate vulnerable assets, detect probes, and validate stealth capabilities to evade attacker detection. This stage also includes establishing TLS/SSL secure communication, integrating with the central AI engine, and performing unit testing and bug fixing to ensure reliability. Deliverables consist of Progress Presentation I and Checklist I, ensuring consistent monitoring of progress and alignment with project milestones.
5. Close-out (March–June 2026): The concluding phase involves the preparation and submission of the final report and research paper, creating the project website, and turning in the logbook. The project wraps up with Progress Presentation II, Checklist II, along with the final presentation and viva, showcasing both technical results and research contributions.

Task	May	June	July	August	September	October	November	December	January	February	March	April	May	June
Brainstorming session														
Team formation														
Topic Finding														
Initiation														
Define project scope and objectives														
Submit Topic Assessment Form (TAF) and assessment														
Create project proposal draft														
Planning														
Requirement analysis														
Feasibility study for SME environment														
Deliver Proposal Presentation														
Finalize and submit proposal report														
Design														
Create system architecture diagram														
Design use case diagrams & test cases														
Implementation & Testing														
Develop Monitoring Module														
Develop Honeypot Module														
Validate honeypot stealth mode														
Configure secure TLS/SSL communication														
Integrate with Central AI Engine														
Unit testing and bug fixing														
Deliver Progress Presentation I														
Submit checklist I														
Close-out														
Deliver Progress Presentation II														
Prepare final report & research paper														
Final presentation & viva														
Project website & logbook submission														

Figure 4: Gantt Chart

6.DESCRIPTION OF PERSONAL AND FACILITIES

6.1 Personnel

This segment of research is conducted independently by Nusfa (IT22898742) a senior undergraduate student focusing on Cyber Security at SLIIT Under the guidance of the designated academic supervisor. For this section, the emphasis is on the planning and creation of a Lightweight Endpoint Agent featuring a built-in low-interaction honeypot optimized for SME settings. The designated supervisor will offer ongoing support to guarantee suitable alignment with the overall ForLens structure and enable access to technical resources when necessary. The responsibilities include:

- Designing, developing, and validating the endpoint agent" for monitoring processes, files, and networks.
- Incorporating a honeypot component to simulate vulnerable service and capture attacker interactions.
- Implementing stealth-mode functions to evade detection by adversaries.
- Ensuring reliable collection of honeypot and agent telemetry for integration with higher-level AI analysis components.

Supervision and guidance:

The supervisor, Mr. Kanishka Yapa will offer technical guidance on endpoint surveillance, honeypot deception strategies, and secure log integration. Weekly meetings will guarantee that research advancement aligns with goals. The supervisor will also help in enhancing implementation methods and confirming the uniqueness of the solution within SME settings.

6.2 Technical Facilities

Software Resources:

- Development Tools: PyCharm (Python IDE), Visual Studio Code, GitHub for source control.

- Libraries & Frameworks: Python psutil and socket libraries for monitoring endpoint processes and networks, Scapy and associated instruments for traffic interception and honeypot emulation.
- Databases SQLite for minimal telemetry storage on endpoints; PostgreSQL for testing integration in a simulated SME setting.
- Testing Tools: Kali Linux and Metasploitable for simulating assaults; Wireshark for analyzing traffic; Burp Suite for testing harmful requests.

Hardware Resources:

- Primary Development Machine: Personal computer (Intel i5/i7, 16GB RAM, 512GB SSD) operating on Windows 11 with WSL2 for testing based on Linux.
- Testing Lab Access to SLIIT Cybersecurity laboratories for operating virtualized setups (VirtualBox/VMWare Workstation) to implement and assess various endpoint agents in SME-like scenarios.

Library and Research Resources: Access to IEEE Xplore, ACM Digital Library, and SpringerLink via the SLIIT library will aid in the literature review and current trends analysis.

Collaboration Infrastructure: Version control through GitHub repositories will be utilized for managing code and integrating with the wider ForLens framework. Microsoft Teams will serve for weekly discussions and supervisor meetings.

7. COMMERCIALIZATION & BUSINESS POTENTIAL

7.1 Market Opportunity

The envisioned lightweight endpoint agent that incorporates honeypot functionalities tackles a significant deficiency in cybersecurity for small and medium-sized enterprises (SMEs). Worldwide, SMEs represent almost 90% of all businesses and account for more than fifty percent of overall employment, but the majority are still inadequately safeguarded because of the steep expenses associated with enterprise-grade SIEM, SOAR, or EDR solutions. This results in significant vulnerability to dangers like ransomware, internal misuse, and privilege escalation.

Regulatory frameworks such as GDPR, ISO 27001, and PCI-DSS are progressively requiring more robust security measures, compelling SMEs to look for cost-effective but trustworthy options. Based on market research, the SME cybersecurity sector is valued at about USD 65 billion in 2024 and is projected to reach USD 145 billion by 2030, growing at a CAGR of nearly 14.7%. This growing demand underscores a distinct business chance for low-cost, deception-driven endpoint protection customized for small and medium enterprises in areas like Sri Lanka and South Asia.

7.2 Value Proposition

The distinctiveness of this solution stems from the integration of four characteristics that are seldom grouped together:

- Stealth operations, decreasing the chances of being detected or circumvented by intruders.
- Embedded honeypot deception, which attracts opponents and produces useful intelligence.
- Lightweight design, allowing functionality on typical SME-level hardware without any performance concerns.
- Telemetry forwarding, enabling integration with higher-level analytics (e.g., SOAR/AI frameworks)

For small and medium-sized enterprises, this signifies obtaining business-grade features at a small portion of the price, implementable with little technical expertise needed.

7.3 Commercialization Pathway

The path to market acceptance can be imagined in incremental phases:

1. Prototype & Academic Validation
    - Develop a proof-of-concept within regulated SME-style test environments.
    - Verify that the agent can capture and forward telemetry during common SME-relevant attack scenarios.
    - Disseminate results via publications to establish trustworthiness.
2. Pilot Deployment (Proof-of-Concept)
    - Involve a limited group of subject matter experts in the healthcare, retail, and finance industries.
    - Gather practical information regarding usability, detection precision, and effectiveness.
    - Refine based on pilot results.
3. Product Development (Pre-Commercial)
    - Package as an easy-to-install endpoint agent, with data export/integration options that can feed into a unified dashboard (developed at higher framework level)
    - Incorporate APIs to ensure compatibility with SIEM/SOAR platforms.
    - Create user guides and ensure alignment with ISO 27001 compliance documents.
4. Market Introduction
    - Launch as ForLens-HoneyAgent.
    - Disperse via regional IT vendors, small and medium enterprise organizations, and managed service provider affiliates.
    - Provide both on-premise and cloud-ready versions.
5. Scaling & Future Growth
    - Broaden uptake throughout South Asia and global SME markets.
    - Incorporate AI-driven attacker profiling and cross-device correlation.

- Broaden the range to include IoT and IIoT deployments in which deception is essential.

7.4 Revenue Model

The financial approach utilizes various sources of income to enhance adoption:

- SaaS Subscription: $10–$30 for each endpoint each year for cloud management.
- On-Premises Licensing: Yearly or ongoing licenses for small and medium-sized enterprises needing offline options.
- Freemium Tier: The complimentary version includes monitoring, whereas deception and advanced analysis are offered as premium functionalities.
- MSP Collaborations: Collaborative solutions via managed service providers.
- Ecosystem Integration: Modular extension within the wider ForLens security framework.

7.5 Market Viability & Entrepreneurial Potential

Multiple elements strengthen the product's market viability:

- Heightened SME awareness because of increasing cases of ransomware and phishing attacks.
- Regulatory compliance drivers promoting the acceptance of options that include endpoint monitoring and deception-driven forensic assistance.
- Market gap, since existing deceit technologies are frequently demanding in terms of resources or exceed the financial capabilities of SMEs.
- Flexibility and scalability, rendering it appropriate for minor installations or complete SME networks without burdening the infrastructure.

By providing SMEs with a affordable, smart, and implementable endpoint protection, this component demonstrates clear entrepreneurial potential and robust preparedness for market introduction in both domestic and international arenas.

8. BUDGET & BUDGET JUSTIFICATION

Item	Description	Estimated Cost (LKR)	Justification
Development Machine (Personal Use)	Existing laptop/PC with Intel i5/i7, 16GB RAM, 512GB SSD	0 (Already available)	Used for developing and testing the endpoint agent prototype. No additional cost required.
Virtualization Software	VirtualBox / VMware Workstation (free / academic license)	0	Required to run attacker and victim VMs for SMB honeypot validation. No extra cost as free/community editions are available.
Testing Tools	Kali Linux & Metasploitable (open-source)	0	Needed to simulate attacks (SMB exploitation, unauthorized access). No licensing fees.
Storage/Backup	External SSD or allocated lab drive (approx. 500GB)	25,000	Used to store VM snapshots and honeypot telemetry

			securely without impacting the main development machine.
Miscellaneous	Printing, USB drives, cables, contingency	5,000	Printing reports, transporting logs, and other minor project-related needs.

Table 6:Budget & Budget Justification

Total Cost = 30,000 LKR

To reduce overall expenses, the suggested budget mostly makes use of open-source technologies and already-existing hardware. Design and coding are done on a personal development workstation, while testing platforms like Kali Linux and Metasploitable, as well as VirtualBox/VMware, offer free controlled settings that mimic SMB-based assaults. An external SSD is the only major expense required for the safe storing of telemetry and virtual machine snapshots, guaranteeing dependability and avoiding data loss during tests. USB drives, printing, and other modest project requirements are covered by miscellaneous expenses. This allocation maintains affordability and practicality within the parameters of the study while guaranteeing the successful completion of the SMB honeypot endpoint agent prototype.

9. CONCLUSION

This proposal targets a critical need for SMEs: cost-effective, implementable, and robust endpoint security that remains effective even when high-end SIEM/SOAR/EDR solutions are unattainable. Previous efforts offer either effective but resource-intensive honeypots or simple anomaly detection that lacks both deception and stability on the device. To fill this void, the initiative will create and assess a lightweight endpoint agent that integrates a low-interaction honeypot (focused on SMB in the prototype), real-time event forwarding of telemetry and stealth/tamper-resilient operation in a plug-and-play package.

The anticipated result is a functional, SME-prepared agent that persistently observes operations, files, and network activities with little resource consumption, draws in threats to harmless decoys and records malicious behavior, forwards telemetry from honeypot activations and endpoint occurrences for higher-level analysis, and continues to function in adverse situations by avoiding detection and deactivation. Telemetry is transmitted securely for advanced analysis and automated reactions, guaranteeing the component integrates seamlessly within a more extensive AI-powered defense such as ForLens.

By unifying deception with lightweight behavioral monitoring and self-protection, the solution offers business-level capability at small and medium-sized enterprise expense and intricacy. The assessment strategy – addressing resource demands, stealth and tamper-resilience, event forwarding reliability, and robustness against adversarial disruption will showcase viability on standard SME endpoints. If achieved, this initiative will elevate the standard practice for SMEs by transforming deception from a data-center extravagance into a routine endpoint measure.

Reference List

[1] S. Kandanaarachchi, H. Ochiai, and A. Rao, "Honeyboost: Boosting honeypot performance with data fusion and anomaly detection," arXiv preprint arXiv:2105.02526, 2021. [Online]. Available: https://arxiv.org/abs/2105.02526

[2] J. Zou, Z. Sun, C. Ku, X. Li, and A. Dahbura, "WiP: Developing High-Interaction Honeypots to Capture and Analyze Region-Specific Bot Behaviors," in *Proc. Symp. Science of Security (HotSoS '24)*, Virtual, Apr. 2–4, 2024, pp. 1–9.

[3] Y. L. Aung, Y. L. Khoo, D. Y. Zheng, B. S. Duo, S. Chattopadhyay, J. Zhou, L. Lu, and W. Goh, "HoneyWin: High Interaction Windows Honeypot in Enterprise Environment," *arXiv preprint arXiv:2505.00465v1*, May 2025, doi: 10.48550/arXiv.2505.00465.

[4] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Computers & Security*, vol. 140, art. no. 103792, Mar. 2024, doi: 10.1016/j.cose.2024.103792.

[5] M. Raz, P. V. S. Charan, P. Krishnamurthy, F. Khorrami, and R. Karri, "SHIELD: Secure Host Independent Extensible Logging for Tamper Proof Detection and Real Time Mitigation of Ransomware Threats," *arXiv preprint arXiv:2501.16619v2*, Apr. 2025, doi: 10.48550/arXiv.2501.16619.

[6] K. Iyer, "Adaptive Honeypots: Dynamic Deception Tactics in Modern Cyber Defense," *International Journal of Science and Research Archive (IJSRA)*, vol. 4, no. 1, pp. 340–351, 2021, doi: 10.30574/ijsra.2021.4.1.0210.

[7] O. Kuznetsov, A. Rusnak, A. Yezhov, K. Kuznetsova, D. Kanonik, and O. Domin, "Evaluating the Security of Merkle Trees: An Analysis of Data Falsification Probabilities," *Cryptography*, vol.8, no. 3, art. 33, Aug. 2024, doi: 10.3390/cryptography8030033.

[8] D. Koisser and A. R. Sadeghi, "Accountability of Things: Large Scale Tamper Evident Logging for Smart Devices," *arXiv preprint arXiv:2308.05557*, Aug. 2023, doi: 10.48550/arXiv.2308.05557.

[9] G. Guardiola Múzquiz and E. Soriano Salvador, "SealFSv2: Combining storage based and ratcheting for tamper evident logging," *International Journal of Information Security*, vol. 22, no. 2, pp. 447–466, 2023, doi: 10.1007/s10207-022-00643-1.

[10] H. Karlzén and T. Sommestad, "Automatic Incident Response Solutions: A Review of Proposed Solutions' Input and Output," in *Proc. 18th Int. Conf. Availability,*

Reliability and Security (ARES 2023), Benevento, Italy, Aug.–Sep. 2023, pp. 1–9, doi: 10.1145/3600160.3605066.

[11] K. R. Ismail, Z. A. Brata, G. A. Nelistiani, S. Heo, H. Kim, and H. Kim, "Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence," *Information*, vol. 16, no. 5, art. 365, 2025, doi: 10.3390/info16050365.

[12] R. Holbel, J. Yerby, and W. Smith, "Utilizing Virtualized Honeypots for Threat Hunting, Malware Analysis, and Reporting," *Issues in Information Systems*, vol. 25, no. 1, pp. 265–278, 2024, doi: 10.48009/1_iis_2024_122.

[13] S. Lanz, S. L.-R. Pignol, P. Schmitt, H. Wang, M. Papaioannou, G. Choudhary, and N. Dragoni, "Optimizing Internet of Things Honeypots with Machine Learning: A Review," *Applied Sciences*, vol. 15, no. 10, art. 5251, 2025, doi: 10.3390/app15105251.

[14] F. Safarov, M. Basak, R. Nasimov, A. Abdusalomov, and Y. Im Cho, "Explainable Lightweight Block Attention Module Framework for Network-Based IoT Attack Detection," *Future Internet*, vol. 15, no. 9, art. 297, Sep. 2023, doi: 10.3390/fi15090297.

[15] S. Roy, J. Li, B.-J. Choi, and Y. Bai, "A lightweight supervised intrusion detection mechanism for IoT networks," *Journal of Parallel and Distributed Computing*, vol. 166, pp. 112–123, 2022, doi: 10.1016/j.jpdc.2021.05.021.

[16] M. Fatima, O. Rehman, I. M. H. Rahman, A. Ajmal, and S. J. Park, "Towards Ensemble Feature Selection for Lightweight Intrusion Detection in Resource-Constrained IoT Devices," *Future Internet*, vol. 16, no. 10, art. 368, Oct. 2024, doi: 10.3390/fi16100368.

[17] V. Pham, E. Seo, and T.-M. Chung, "Lightweight Convolutional Neural Network Based Intrusion Detection System," *Journal of Communications*, vol. 15, no. 11, pp. 808–817, Nov. 2020, doi: 10.12720/jcm.15.11.808-817.

[18] S. T. Muntaha, F. Ashraf, I. Shahzad, and J. Iqbal, "Designing an Adaptive Honeypot for Advanced Cybersecurity Threat Detection," *Spectrum of Engineering Sciences*, vol. 3, no. 5, pp. 816–847, May 2025.

[19] Z. Morić, V. Dakić, and D. Regvart, "Advancing Cybersecurity with Honeypots and Deception Strategies," *Informatics*, vol. 12, no. 1, art. 14, Jan. 2025, doi: 10.3390/informatics12010014.

[20] E. K. Isabirye, "Cloud Adoption and Digital Transformation Cybersecurity Consideration for SMEs," *Iconic Research and Engineering Journals*, vol. 8, no. 7, pp. 453, Jan. 2025.

[21] H. Maosa, K. Ouazzane, and M. C. Ghanem, "A Hierarchical Security Event Correlation Model for Real-Time Threat Detection and Response," *Network*, vol. 4, no. 1, pp. 68–90, 2024, doi: 10.3390/network4010004.

[22] Q. Wang, W. Ul Hassan, D. Li, K. Jee, X. Yu, K. Zou, J. Rhee, Z. Chen, W. Cheng, C. A. Gunter, and H. Chen, "You Are What You Do: Hunting Stealthy Malware via Data Provenance Analysis," in *Proc. 27th Network and Distributed System Security Symp. (NDSS)*, San Diego, CA, USA, Feb. 23–26, 2020, doi: 10.14722/ndss.2020.24167.

[23] H. A. Balan and B. Agarwal, "Comparative Performance Evaluation of Modern Container Security Agents: Red Hat ACS, Wiz, SentinelOne, and Tenable," *Int. J. Computer Trends and Technology (IJCTT)*, vol. 73, no. 5, pp. 113–124, May 2025. [Online].Available:https://www.ijcttjournal.org/2025/Volume-73%20Issue-5/IJCTT-V73I5P115.pdf

[24] M. AlKhanafseh and O. Surakhi, "Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography," *Electronics*, vol. 13, no. 18, p. 3729, Sep. 2024, doi: 10.3390/electronics13183729.

Appendices

Appendix A : Scope of The Study

- The project focuses on SMEs with restricted financial resources and technical knowledge.
- The scope is restricted to endpoint-level protection utilizing surveillance and honeypot trickery.
- Only low-interaction honeypots are executed (not high-interaction, because of resource expenses).
- The research assesses resilience, stealth, and user-friendliness in simulated SME testbeds (e.g., VirtualBox/VMware).
- Integration with sophisticated AI/response frameworks (e.g., SOAR) is being evaluated, but implementation of full SOAR orchestration is beyond the range of this component.

Appendix B : Limitations

- Resource Limitation: Testing is restricted to a virtualized SME-style lab environment; real-world SME deployments may reveal additional performance challenges
- Prototype Scope: Focus is only on the lightweight endpoint agent with SMB honeypot functionality; integration with AI-driven analysis and dashboards belongs to other ForLens components.
- Attack Scope: Prototype validation is limited to common SME-relevant attacks (e.g., SMB exploitation attempts, unauthorized file access). Broader attack classes (e.g., nation-state APTs, large-scale DDoS) are outside scope.
- No Dataset Use: Evaluation relies on telemetry generated from honeypot engagements and simulated attacks in the lab; no external datasets are used.
- Time Constraint: The progression and assessment are limited to the duration of the project (approximately 8 months).

- Single Component Focus: Only the endpoint honeypot agent has been developed; more advanced AI modules are part of other team elements.

Appendix C : Risks and Mitgations

Technical Risks

- Risk: Detection of honeypots by sophisticated attackers.
  Mitigation: Utilize covert operations, unpredictable services, and ongoing enhancements.
- Risk: Limited coverage of attack types beyond SMB-based deception.
  Mitigation: Focus prototype on SMB exploitation attempts, while leaving extension to other services for future work.
- Risk: Performance burden on SME equipment.
  Mitigation: Aim for ≤10% CPU and ≤150 MB RAM consumption.

Operational Risks

- Risk: SMEs might not have personnel with the expertise to set up solutions.
  Mitigation: Provide plug-and-play deployment and simple configuration
- Risk: Intruders interfering with the agent.
  Mitigation: Implement Self-recovery and tamper-resistant features.

Project Risks

- Risk: Limited real-world test data.
  Mitigation: Utilize regulated ransomware/lateral movement exercises.
- Risk: Time constraints on development.
  Mitigation: Break tasks into phases with clear deliverables (design, prototype, testing).

Appendix D : Ethical Considerations

- All evaluations are conducted in controlled lab environments using legal datasets (e.g., Metasploitable, Kali Linux).
- No genuine SME production systems or actual customer data will be utilized.
- Any collected telemetry will remain anonymized and securely stored.

- The research complies with IEEE Code of Ethics and institutional research policies.