Next Scientists
European International Journal of Multidisciplinary Research and Management Studies

TYPE Original Research
PAGE NO. 48-53

Architecting Resilience: A Design Thinking Approach to Managed Detection and Response (MDR) Service Frameworks for Small and Medium-Sized Enterprises

Dr. Marelia T. Venshiro

School of Cybersecurity & Threat Analytics, National University of Singapore (NUS), Singapore

OPEN ACCESS

SUBMITTED 10 November 2025
ACCEPTED 18 November 2025
PUBLISHED 26 November 2025
VOLUME Vol.05 Issue11 2025

Abstract:

Background: Small and Medium-sized Enterprises (SMBs) increasingly face sophisticated cyber threats previously reserved for large corporations. However, they often lack the financial resources and technical expertise to maintain 24/7 Security Operations Centers (SOCs). Managed Detection and Response (MDR) services offer a potential solution, yet traditional service models are often ill-adapted to the economic and operational realities of SMBs.

Objective: This study aims to design a scalable, profitable, and effective MDR service framework specifically tailored for the SMB market. The research seeks to bridge the gap between high-level enterprise security requirements and the resource constraints of smaller organizations using Design Thinking principles.

Method: Adopting a Design Science Research (DSR) approach, this paper synthesizes literature on cyber situational awareness, Routine Activity Theory, and Industry 4.0 maturity. We utilize a Design Thinking methodology to construct a modular MDR architecture that integrates AI-driven threat detection with human-centric analysis.

Results: The study presents a multi-layered MDR framework. The technological layer leverages hybrid cloud architectures and AI for cost-effective log analysis. The operational layer defines a shared-resource analyst model to reduce overhead. The economic layer proposes a tiered service design that aligns with SMB risk appetites and budgetary limits while ensuring provider profitability.

Conclusion: The proposed framework demonstrates that robust cybersecurity for SMBs is achievable

through the intelligent integration of automation and shared-service models. By shifting from volume-based to value-based detection strategies, MDR providers can offer sustainable protection against modern threats.

Keywords: Managed Detection and Response, SMB Cybersecurity, Design Thinking, Threat Intelligence, Security Operations Center, Cyber Situational Awareness, Routine Activity Theory.

Introduction

The digital ecosystem has undergone a radical transformation over the last decade, shifting the epicenter of cyber risk from exclusively large, multinational corporations to the fragmented and often unprepared sector of Small and Medium-sized Enterprises (SMBs). As organizations increasingly digitize their operations to remain competitive in an Industry 4.0 environment, the attack surface expands, creating new vulnerabilities that malicious actors are eager to exploit. The prevailing assumption that "security by obscurity" protects smaller entities has been decisively debunked by empirical evidence. In reality, SMBs are often viewed as "low-hanging fruit" by cybercriminals due to their valuable data assets paired with historically weak defense mechanisms.

This paper explores the critical necessity of developing specialized Managed Detection and Response (MDR) frameworks. Unlike traditional Managed Security Service Providers (MSSPs), which primarily focus on alert forwarding and device management, MDR services are characterized by their proactive nature, utilizing advanced analytics, threat hunting, and automated response capabilities to contain threats before they result in catastrophic damage. However, a significant gap remains in the literature and practice: the design of MDR services that are robust enough to handle advanced persistent threats (APTs) while remaining economically viable for SMBs.

Current research indicates that while the awareness of cyber risks is growing, the "maturity gap" prevents effective action. Demir, Sariisik, and Ogutlu [7] highlight that while Industry 4.0 awareness is increasing, the maturity level of SMBs often lags, leaving digital integration exposed to exploitation without the requisite security architecture. Furthermore, the nature of threats is evolving. It is no longer sufficient to defend the perimeter; organizations must also account for internal vulnerabilities. As Sylvester [11] notes, a small business's greatest threat often comes from within, whether through malicious intent or negligent error. This internal dimension complicates the security paradigm, requiring monitoring systems that are sensitive to behavioral anomalies as well as external intrusions.

The financial and operational constraints of SMBs create a paradox: they require enterprise-grade security to survive regulatory and criminal pressures but lack the enterprise-grade budget to procure it. Rajgopal [1] addresses this by emphasizing the need for MDR service design that builds profitable 24/7 threat coverage. This requires a fundamental rethinking of how security operations are staffed, priced, and delivered. It is not merely a technical challenge but a service design challenge.

Consequently, this study adopts a Design Thinking approach, as advocated by Bender-Salazar [8], to address this "wicked problem." By empathizing with the SMB context, defining the specific constraints, and ideating on hybrid human-AI models, we propose a framework that leverages the latest advancements in Artificial Intelligence [15] and big data architectures [12] to democratize access to high-level cybersecurity. The objective is to delineate a path toward a resilient digital future for the SMB sector, ensuring that size does not dictate security.

Literature Review

Theoretical Foundations: Routine Activity Theory and Cyber Situational Awareness

To understand the targeting of SMBs, one must look beyond technical vulnerabilities to criminological theories. Bello and Griffiths [9] discuss Routine Activity Theory (RAT) in the context of cybercrime. RAT posits that a crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. In the context of the modern digital economy, SMBs represent "suitable targets" due to the high value of their data (customer records, intellectual property) and often lack "capable guardians" in the form of dedicated security teams or advanced monitoring tools.

This lack of guardianship is often a failure of Cyber Situational Awareness (CSA). Alahmari and Duncan [2] provide a systematic review of risk management in SMEs, noting that a lack of visibility into the network environment is a primary failure point. Without CSA, organizations cannot detect the subtle precursors to an attack. This supports the argument for MDR, which essentially outsources the function of the "capable guardian" to a specialized third party, thereby disrupting the convergence required for successful cybercrime.

The Evolution of Threats and the Insider Dilemma

Bhattacharya [3] traces the evolution of cybersecurity issues, noting that as defensive technologies improve,

attackers pivot to softer targets. The sophistication of automated attacks allows criminals to scan thousands of SMB networks simultaneously, looking for unpatched vulnerabilities. However, the external threat is only half the equation. Sylvester [11] argues that insider threats—employees with legitimate access who misuse that access—are particularly devastating for small businesses where trust models are informal and access controls are often lax.

Back and LaPrade [9] expand on this by examining cyber-situational crime prevention, suggesting that institutions (including higher education and by extension, training bodies) must broaden their understanding of cybercrime to include these behavioral aspects. An effective MDR service, therefore, cannot simply look for malware; it must analyze user behavior, requiring sophisticated logging and correlation capabilities usually found in complex SIEM (Security Information and Event Management) deployments.

Technological Enablers: AI and Big Data Architectures

The feasibility of offering high-end security to low-budget clients hinges on technology. Cloudian [12] outlines the architecture of Splunk and similar big data platforms, which allow for the ingestion and indexing of massive volumes of log data. The challenge has historically been the cost of this data ingestion. However, modern architectures allow for tiered storage and "data-to-the-code" processing, making it possible to monitor SMB environments cost-effectively.

Furthermore, Daniel and Andreas [15] evaluate AI-based use cases for enhancing SMB defense. They conclude that AI is not a luxury but a necessity for scaling security operations. AI algorithms can handle the "noise" of thousands of daily alerts, filtering out false positives and presenting only high-fidelity incidents to human analysts. This symbiotic relationship between AI and human expertise is central to reducing the cost of delivery (CoD) for MDR providers, which in turn lowers the price point for SMB clients.

Regulatory Frameworks and Maturity Models

Compliance is a major driver for SMB security adoption. The Cybersecurity Capability Maturity Model (C2M2) [10] provides a standard against which organizations can measure their security posture. While originally designed for the energy sector, its principles of asset, change, and threat management are universally applicable. Additionally, Chidukwani, Zander, and Koutsakis [5] highlight that adherence to such recommendations is often hindered by complexity. A well-designed MDR service must therefore abstract this complexity, providing not just security, but "compliance-as-a-service." The Australian Government's guidelines on protecting business from cyber threats [6] reinforce this, emphasizing simple, actionable steps that service providers should prioritize in their interactions with non-technical business owners.

Methodology

This research utilizes a Design Science Research (DSR) methodology. DSR is fundamentally a problem-solving paradigm that seeks to enhance human knowledge via the creation of innovative artifacts—in this case, a service framework. The artifact is the MDR Service Architecture. The process follows the Design Thinking phases described by Bender-Salazar [8]: Empathize, Define, Ideate, Prototype, and Test (validated through theoretical application).

1. Empathize: We analyzed the constraints of SMBs through the lens of Alahmari and Duncan [2] and Demir et al. [7], focusing on budget limitations, lack of in-house expertise, and the psychological burden of compliance.

2. Define: The core problem was defined as the "Service Delivery Gap"—the inability of current MSSP models to provide genuine detection and response capabilities at an SMB price point.

3. Ideate: We synthesized technical capabilities (Splunk architecture [12], AI optimization [15]) with operational theories (RAT [9]) to brainstorm a modular service structure.

4. Prototype: The resulting framework (detailed in the Results section) conceptualizes the interaction between technology, people, and process.

Results: The Integrated MDR Framework

The proposed framework consists of three integrated layers: The Technological Aggregation Layer, the Operational Analysis Layer, and the Service Delivery Layer.

Layer 1: Technological Aggregation and Hybrid Architecture

The foundation of the framework is a cloud-native, multi-tenant architecture. Citing Cloudian's analysis of Splunk architecture [12], the system utilizes heavy forwarders deployed in the SMB environment to compress and encrypt logs before transmission. To manage costs, the framework utilizes a "Data Lake" approach where logs are stored in low-cost object storage, and only metadata or active alerts are ingested into the high-speed analysis engine.

This layer relies heavily on the integration of Artificial Intelligence. As noted by Daniel and Andreas [15], rule-

based detection is insufficient for modern threats. The framework incorporates Machine Learning (ML) models trained on aggregated datasets from multiple SMB tenants. This "community immunity" approach means that a threat detected in one client's environment immediately updates the detection logic for all other clients. This creates a network effect that increases the value of the service as the subscriber base grows.

Layer 2: Operational Analysis and the "Human-in-the-Loop"

Technology alone cannot solve the problem; the interpretation of data is crucial. The framework proposes a shared-analyst model. Instead of dedicating specific analysts to specific accounts (which is cost-prohibitive), the SOC operates on a queued model. Tier 1 analysis is entirely automated by the AI engine, which handles 90% of incoming signals (noise reduction). Tier 2 analysts review high-fidelity alerts.

This structure addresses the "capability" aspect of Routine Activity Theory [9]. By pooling resources, the MDR provider acts as the "capable guardian" for multiple entities simultaneously. Crucially, this layer also integrates Insider Threat protocols [11]. By establishing baselines of normal user behavior (time of login, file access patterns), the system triggers alerts not just on malware signatures, but on anomalous human behavior, addressing the risk of negligent or malicious insiders.

Layer 3: Profitable Service Design and Financial Modeling

Rajgopal [1] emphasizes the necessity of "Building profitable 24/7 threat coverage." The framework addresses this through a tiered pricing model based on "Asset Criticality" rather than raw data volume.

1. Bronze (Perimeter Watch): Monitoring of firewalls and external-facing IPs.
2. Silver (Endpoint Visibility): Addition of EDR (Endpoint Detection and Response) agents on workstations.
3. Gold (Full Context): Full log ingestion, insider threat monitoring, and compliance reporting (C2M2 alignment).

This tiered approach allows SMBs to enter the security ecosystem at a price point they can manage and scale up as their digital maturity [7] increases.

Discussion

Democratizing Cyber Resilience

The primary contribution of this framework is the democratization of cyber resilience. By leveraging the economies of scale inherent in multi-tenant cloud architectures and AI, the cost barrier to entry is significantly lowered. This aligns with the Australian Government's mandate [6] to make cyber protection accessible. The shift from "time-and-materials" pricing to "outcome-based" subscriptions aligns the incentives of the provider and the client: the provider is incentivized to automate and prevent threats to maintain their own margins, while the client receives continuous protection.

The Critical Role of AI and Automation in Modern MDR

Expanding on the technological layer, it is imperative to understand that the integration of Artificial Intelligence is not merely a feature but the structural backbone of modern MDR for SMBs. Daniel and Andreas [15] provide critical insights into the evaluation of AI use cases. In the context of this framework, AI serves three distinct functions: Prevention, Detection, and Response recommendation.

First, in Prevention, predictive modeling analyzes vulnerability scan data against global threat intelligence feeds. If a specific vulnerability in a Windows Server version is being actively exploited globally, the AI prioritizes this patch recommendation for the SMB client, effectively acting as a virtual CISO (Chief Information Security Officer). This moves the service from reactive to proactive.

Second, in Detection, Unsupervised Learning algorithms are deployed to establish a baseline of "normalcy" for the specific SMB network. Unlike rule-based systems that look for known bad signatures, unsupervised learning looks for deviations. For example, if a marketing employee suddenly utilizes PowerShell scripts at 3:00 AM—an action theoretically possible but historically unprecedented for that user—the system flags this anomaly. This directly addresses the insider threat concerns raised by Sylvester [11].

Third, in Response, the framework utilizes SOAR (Security Orchestration, Automation, and Response) logic. When a threat is confirmed, the system can automatically isolate the infected host from the network to prevent lateral movement. This speed is critical. Human reaction time is measured in minutes or hours; automated response is measured in milliseconds. For an SMB, where a ransomware attack can lead to bankruptcy, this speed is vital.

Ethical Governance and Regulatory Compliance

However, the introduction of extensive monitoring and AI raises ethical and regulatory questions. When implementing such a framework, adherence to governance standards is paramount. The C2M2 model [10] serves as a guideline here. The framework must ensure that the data collected (especially regarding

employee behavior for insider threat detection) is handled in compliance with privacy laws (like GDPR or local equivalents).

Furthermore, the concept of "Algorithmic Accountability" becomes relevant. If an AI model automatically shuts down a business's e-commerce server due to a false positive, the financial damage could be significant. Therefore, the "Human-in-the-Loop" remains essential not just for technical verification, but for accountability. The service design must include "break-glass" procedures where human analysts can override automated containment decisions.

Bridging the Maturity Gap through Education

The framework also serves an educational function. By providing regular, simplified reports that map technical events to business risks, the MDR service helps elevate the "Industry 4.0 Awareness" and maturity of the client, as discussed by Demir et al. [7]. Over time, the client moves from a passive consumer of security to an active participant in their own defense strategy. This educational component is reinforced by the findings of Back and LaPrade [9], who suggest that institutions must play a role in broadening the understanding of cybercrime. In this model, the MDR provider effectively becomes the institution of learning for the SMB.

Financial Viability and the "Profitability Paradox"

A critical discussion point derived from Rajgopal [1] is the "Profitability Paradox." SMBs generate less revenue per unit for the provider than enterprise clients, yet often require more hand-holding due to lower technical literacy. The traditional "high touch" model of consultancy is unsustainable here. The proposed framework solves this through "Tech-Touch." Routine interactions (reporting, basic queries, ticketing) are handled through a self-service portal powered by the same data structures that drive the security backend.

This allows the high-cost human analysts to focus solely on "moments of truth"—critical security incidents or complex architectural changes. By stripping away the administrative overhead through design thinking (Bender-Salazar, [8]), the provider allows the margins to remain healthy even at lower price points. This economic sustainability is the linchpin of the entire model; without it, the market will naturally revert to serving only the enterprise elite, leaving the SMB sector exposed.

Limitations

While the framework is robust, it relies on the availability of cloud infrastructure and a minimum level of digitisation within the SMB. "Analog" businesses may find the integration challenging. Additionally, the reliance on AI introduces the risk of "adversarial AI," where attackers specifically design malware to evade machine learning models. Future research must focus on "adversarial robustness" in the SMB context.

Conclusion

The cybersecurity divide between large enterprises and SMBs is a critical vulnerability in the global economic infrastructure. This paper has argued that bridging this divide requires more than just scaled-down enterprise tools; it requires a fundamental redesign of the service delivery model. By applying Design Thinking principles, we have proposed an MDR framework that integrates advanced AI architectures with profitable, tiered service models.

The synthesis of Routine Activity Theory [9] with technical architectures [12] and maturity models [7, 10] provides a holistic path forward. The result is a system where the "capable guardian" is restored to the digital environment of the small business. As the threat landscape continues to evolve, with attackers utilizing automation and AI, the defense mechanisms must evolve in parallel. The future of SMB cybersecurity lies not in buying more boxes, but in subscribing to intelligent, resilient, and empathetic service ecosystems. This framework represents a significant step toward that resilient future, ensuring that the benefits of the digital age are not outweighed by its risks.

References

1. Rajgopal, P. R. (2025). MDR service design: Building profitable 24/7 threat coverage for SMBs. International Journal of Applied Mathematics, 38(2s), 1114-1137.
2. ALAHMARI, A. & DUNCAN, B. (2020). Cybersecurity risk management in small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In Int. Conf. on Cyber Situational Awareness, Data Analytics and Assessment.
3. BHATTACHARYA, D. (2015). Evolution of cybersecurity issues in small businesses, Technology. In 4th Annual Conference on Research in Information.
4. CAMBRIDGE DICTIONARY. (2023). Retrieved 7 October 2023, from https://dictionary.cambridge.org/tr/
5. CHIDUKWANI, A., ZANDER, S., & KOUTSAKIS, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10.
6. Australian Government. (2021, August 3). Protect your business from cyber threats. Business.gov.au.

7. DEMİR, S., SARIIŞIK, G., & ÖĞÜTLÜ, A. S. (2022). KOBİ lerin Endüstri 4.0 Farkındalık ve Olgunluk Seviyesinin Belirlenmesi. Journal of Business Research - Turk, 14(4).

8. Bender-Salazar, R. (2023). Design thinking as an effective method for problem-setting and needfinding for entrepreneurial teams addressing wicked problems. Journal of Innovation and Entrepreneurship, 12(1).

9. Bello, M., & Griffiths, M. (2020). Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable Are Law Enforcement Agencies? Rethinking Cybercrime.

10. CESER (2021). C2M2, version 2.0. Department of Energy.

11. Chris Sylvester (2018). Your Small Business's Greatest Cybersecurity Threat Comes from Inside. Network Depot.

12. Cloudian. (n.d.). Splunk Architecture: Components and Best Practices. Cloudian.

13. CYBERSECURITY. (2023). Retrieved 8 October 2023, from https://business.defense.gov/Work-with-us/Cybersecurity/

14. Back, S., & LaPrade, J. (2020). Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions. International Journal of Cybersecurity Intelligence & Cybercrime.

15. Daniel, K., & Andreas, J. (2022). Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). Electronic Imaging, 34(3).