National College of Ireland

A Novel Mobile Device Security Framework for SMEs

MSc Industrial Internship
MSc in Cybersecurity

Ashok Balaraman Manimaran
Student ID: X21224561

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ashok Balaraman Manimaran		
Student ID:	X21224561		
Programme:	MSc in Cybersecurity	**Year:**	2022/23
Module:	MSc Industrial Internship		
Supervisor:	Prof. Vikas Sahni		
Submission Due Date:	04/09/2023		
Project Title:	A Novel Mobile Device Security Framework for SMEs		
Word Count:	6228	**Page Count:**	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Ashok Balaraman Manimaran
Date:	02/09/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Novel Mobile Device Security Framework for SMEs.

Ashok Balaraman Manimaran
X21224561

Abstract

Mobile devices offer great flexibility and improved productivity for all employees; however, they can also introduce additional security risks. These risks encompass malware infections, phishing attempts, data leakage, network-based attacks, app-based threats, insider threats, device theft or loss, and vulnerabilities associated with jailbreaking or rooting devices. Effectively managing and mitigating these risks has become imperative for enterprises aiming to protect their sensitive information and maintain a secure environment. This research proposes a framework to enhance the mobile device security posture in Small and Medium Enterprises (SMEs) and demonstrates a practical implementation of the framework by incorporating Mobile Application Management (MAM), Endpoint Security, and System Information and Event Management (SIEM) solutions.

Keywords- Mobile device security, Malware, Data theft, MAM, Endpoint security, SIEM

1 Introduction

In today's technology-driven world, mobile devices are vital for individuals and organizations, blurring the lines between personal and business use. This convergence poses cybersecurity risks, as these devices may host sensitive data and third-party apps. The abundance of mobile apps on platforms like Apple's App Store and Google Play adds complexity, with varying levels of security and privacy. Organizations must fully grasp the risks associated with mobile apps, including inadvertent data collection, which can leave individuals susceptible to data breaches. Mobile Device Management (MDM) enhances security in enterprises but has its limitations, leaving both personal and corporate devices vulnerable to malware and phishing attacks. These vulnerabilities can result in data breaches and the exposure of Personal Identifiable Information (PII).Small and medium-sized enterprises (SMEs) benefit from cost-effective and productive Bring Your Own Device (BYOD) practices but face security challenges in safeguarding data and ensuring its integrity.

This research aims to address the security challenges associated with mobile devices in SMEs through a comprehensive approach. It endeavors to enhance mobile device security in the context of Small and Medium-sized Enterprises (SMEs), with a specific focus on those comprising approximately 250 employees. It recognizes that such SMEs often face distinct cybersecurity challenges due to their limited resources and unique operational dynamics.

The proposed solution integrates Mobile Application Management (MAM) alongside Endpoint Security and Security Information and Event Management (SIEM) solutions to enhance threat detection capabilities and streamline incident response processes. Ultimately, this approach aims to bolster mobile device security in SMEs. The research methodology will involve an in-depth review of existing literature on mobile device security, MAM solutions, endpoint protection mechanisms, SIEM integration, and best practices in threat detection and incident response. Furthermore, a practical implementation of the proposed solution will be conducted within an SME environment to validate its effectiveness.

The anticipated outcomes of this research thesis include the development of a novel framework for enhancing mobile device security in SMEs and the demonstration of a corresponding prototype implementation. Moreover, this study will shed light on the benefits and challenges associated with the integrated approach, contributing valuable insights to the existing body of knowledge in mobile device security. Ultimately, the findings will provide actionable recommendations, empowering SMEs to bolster their mobile device security.

1.1 Research Question:

Development of a novel framework for SMEs to enhance their mobile device security posture and demonstrate a practical implementation of the framework.

1.2 Research Objective:

How can SMEs strengthen their mobile device security posture?

1.3 Research Outline:

A thorough examination of this study in comparison to previous review articles is presented in Section 2. Section 3 outlines the techniques and methodologies employed to achieve the research objectives. In Section 4, we provide design specifications used in constructing the framework. Sections 5 and 6 provide insight into the research's implementation, including the tools used and the evaluation process, respectively. The research article concludes with Section 7, which covers conclusions, future research directions, and any identified limitations.

2 Related Work

In today's evolving technology landscape, employees' use of personal devices to access corporate apps brings numerous security risks, especially for SMEs. This research delves deep into these mobile device security issues and presents a comprehensive framework. It integrates MDM, MAM, endpoint protection, and SIEM solutions. By reviewing existing literature and best practices, this study offers practical recommendations for SMEs to secure sensitive data while embracing the benefits of mobile technology. Our literature review explores diverse perspectives on mobile device security, providing insights into the challenges and solutions that shape secure mobile computing for SMEs.

(Weichbroth and Łysik, 2020) analyzes security threats in mobile applications and explores best practices for protection. This study combines a literature review and user survey, emphasizing continuous investment in mobile security. (Wazid, Zeadally and Kumar Das, 2019)highlights user and app developer roles, recommending practical measures and calling for more research on user perceptions and emerging tech risks for improved security. (Abdul

Mutalib, Zainol and Mohamed Halip, 2021) proposes a strategy to tackle malware threats in Small and Medium Enterprises (SMEs) and advocates for proactive measures to safeguard information security. (Emer, Unterhofer and Rauch, 2021)emphasize SME cybersecurity risks due to budget constraints and propose CMERP integration for malware monitoring. Research uses literature review and CMERP implementation but lacks real-world testing. (Vakakis, Nikolis and Ioannidis, 2019) highlights SMEs' need for robust cybersecurity against sophisticated malware. (Mudassar Yamin and Katt, 2019) delves into the realm of Mobile Device Management (MDM) technologies, with a specific focus on addressing security issues and challenges within these systems. The paper explores MDM technologies, their limitations, and remedies, focusing on tools like "MAAS360" and "Airwatch." It raises concerns about user identity, privacy, behavioral data, and GDPR compliance but lacks accessibility for non-experts and practical applications. It sets a foundation for future MDM research in the field. (Aguboshim and Udobi, 2019) presents a comprehensive narrative analysis focusing on the significant security implications associated with the adoption of employee-owned mobile devices in business environments. (Lian, 2020) reviews 51 sources on BYOD policies, emphasizing security limitations and data risks, recommending policy improvements. It lacks quantitative data and real-world cases but offers practical advice for better data management. (Iman Ali, 2021) investigates the safeguarding of critical infrastructure against threats through the implementation of Bring Your Own Device (BYOD) in corporate contexts. The paper emphasizes innovation in securing BYOD traffic, introducing a forensic readiness concept. (Gupta, 2020) proposes a novel framework for detecting malicious BYOD traffic and infrastructure protection but could simplify language and discuss limitations. Overall, it offers a practical BYOD security strategy and inventive threat detection for future research.

(Hayes, Cappa and An Le-Khac, 2020)concludes that mobile applications collect and share a greater amount of personal data than suggested by their permissions and privacy policies, posing significant privacy concerns. (Mutlaq Alnajrani, 2020) give insights about BYOD practices risk security and privacy, prompting future research in PII, DNS, Big Data, and global app studies to enhance data privacy understanding. (R.K.U et al., 2022) introduces a pioneering methodology employing Machine Learning (ML) techniques to identify critical files like .txt, docx, and pdf, based on content categorization and threat levels. Innovative BYOD security approach emphasizes hybrid cryptography, encryption, and automation. Challenges include regulatory compliance and cross-platform use. Future steps involve advanced ML algorithms, expanded compatibility, and real-world testing for practical application. (González-Granadillo, Diaz and González, 2021) assesses current SIEM systems and proposes enhancements. It explores SIEM development, highlights critical applications, and offers insights into commercial solutions. Lacks practical guidance and accessibility for non-technical readers. Emphasizes SIEM's importance for enhanced cybersecurity. (Vakakis et al., 2019) addresses cybersecurity in Smart Home/Office SMEs, stressing the need for stronger security measures Introduces smart home datasets, utilizes LSTM for anomaly detection, highlighting IoT-era SME cybersecurity. (Nespoli, 2021)Lays groundwork for enhanced anomaly detection models. (Dhahi Khaleefah and Al-Mashhadi, 2023) explores modern cybersecurity frameworks (CSFs) in multi-domain, multi-tenancy, and distributed systems, covering IoT security, cyber-attack countermeasures, and machine learning for intrusion detection. It Emphasizes cost-effective cloud computing, addresses security, explores ISO/NIST CSFs, and hints at future research.

(P. Roy, 2019) compares two crucial cybersecurity frameworks: NIST's Cyber Security Framework (CSF) and ISO 27001. It advocates a combined approach, emphasizes

complementarity, suggests future research. But it Lacks practical exploration, broader methodology coverage. (Eling, 2021) Proposes framework harmonization and integration with emerging standards. (Benz and Chatterjee, 2020) presents a practical cybersecurity evaluation tool (CET) for SMEs, based on the NIST Cybersecurity Framework (CSF). CET assesses cybersecurity maturity through an online survey, computes scores, identifies gaps, and recommends improvements, considering costs. CET assists in identifying weaknesses, affordable, sector-specific limitations. It is valuable for SME cybersecurity readiness, future directions: broader industry application, automation.

3 Research Methodology

This comprehensive research methodology outlines the stages from problem identification to proposing and evaluating a mobile device security framework for SMEs. It includes the utilization and assessment of Microsoft Intune's MAM policies and Microsoft Defender for Endpoint's alerting policy, integrated into Rapid7 SIEM for centralized alert management and monitoring.

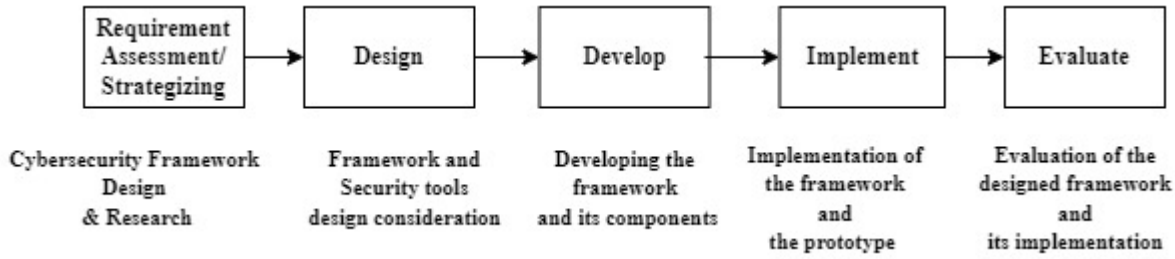


Figure 1: Proposed Research Methodology

- Requirement Assessment/Strategizing:

The process began with a literature review of existing research papers proposing cybersecurity frameworks for SMEs and studying NIST CSF and ISO 27001 standards. A comprehensive literature review covered mobile device security, NIST guidelines, ISO 27001 standards, Microsoft Intune, Windows Defender for Endpoint, and Rapid7 SIEM. Best practices, challenges, and SME cybersecurity gaps were identified. Security tool selection for the framework prototype was followed by researching the license costs, ease of implementation, integration requirements, and steps.

- Design:

A comprehensive framework to enhance mobile device security in SMEs was designed, with a focus on maintaining the Confidentiality, Integrity, and Availability (CIA triad) of data while integrating NIST Cybersecurity Framework and ISO 27001 principles. Microsoft Intune[1] MAM was found to be superior to other similar solutions due to its integration with the Microsoft Ecosystem, wide platform support, the Conditional Access it offers, Application Protection, and various other factors. Microsoft Defender for Endpoint was chosen as the Endpoint protection solution since it is included as a feature in the M365 E3/E5 license. Rapid7 SIEM solution was integrated with MDM for centralized logging and monitoring by the SOC

[1] https://www.scappman.com/post/the-best-mobile-device-management-solution-in-2022-sccm-vs-intune/

team. Rapid7 was selected because the SOC team was already using Rapid7 SIEM[2], and the MSSP (Managed SOC) service provided by Rapid7 is budget-friendly for SMEs. Other SIEM solutions can also be considered when implementing this framework, depending on the requirements of the SMEs.

- Develop:

A comprehensive framework to mitigate mobile device security threats was developed based on the requirements of SMEs, ensuring alignment with the NIST CSF and ISO 27001 standards.

- Implementation:

A prototype of the validated framework was implemented in a real-world SME setting. Microsoft Intune was deployed, and MAM policies were configured for device security and app management. Microsoft Defender for Endpoint was deployed to enable real-time threat detection and response. Rapid7 SIEM was configured and integrated with Microsoft Defender for Endpoint for centralized monitoring and alerting.

- Evaluation:

An evaluation was conducted to determine whether the proposed framework for enhancing mobile device security in the context of SMEs aligns with the NIST Cybersecurity Framework (CSF) and ISO 27001 standards. Each component of the proposed framework was examined, and an assessment was made regarding its alignment with the principles and guidelines outlined in these standards. The policies configured in Intune and the alert policies created in Microsoft Defender were evaluated against the proof of concept.

4 Design Specification

4.1 Design Specification for Comprehensive Mobile Device Security Framework for SMEs

The design of this mobile device security framework is rooted in considerations specific to Small and Medium-sized Enterprises (SMEs), particularly those with approximately 250 employees, acknowledging their resource constraints and operational intricacies. The framework's architecture and policies have been meticulously crafted to align with the unique needs and challenges faced by SMEs of this scale. Technical parameters, such as scalability to accommodate future growth, adaptability to diverse device types, and efficient resource utilization, have been at the forefront of the framework's design, ensuring it effectively addresses the mobile security demands of SMEs in this size range.

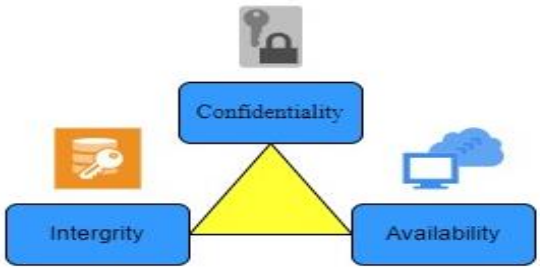


Figure 2: CIA triad.

[2] https://www.rapid7.com/solutions/siem/

The proposed framework to enhance mobile device security in SMEs was meticulously designed with the CIA Triad[3] principles at its core. It prioritizes Confidentiality to safeguard sensitive data, Integrity to ensure data accuracy and trustworthiness, and Availability to maintain consistent access for authorized users. By adhering to these foundational principles, the proposed framework provides a solid defense against mobile device security threats within SMEs.

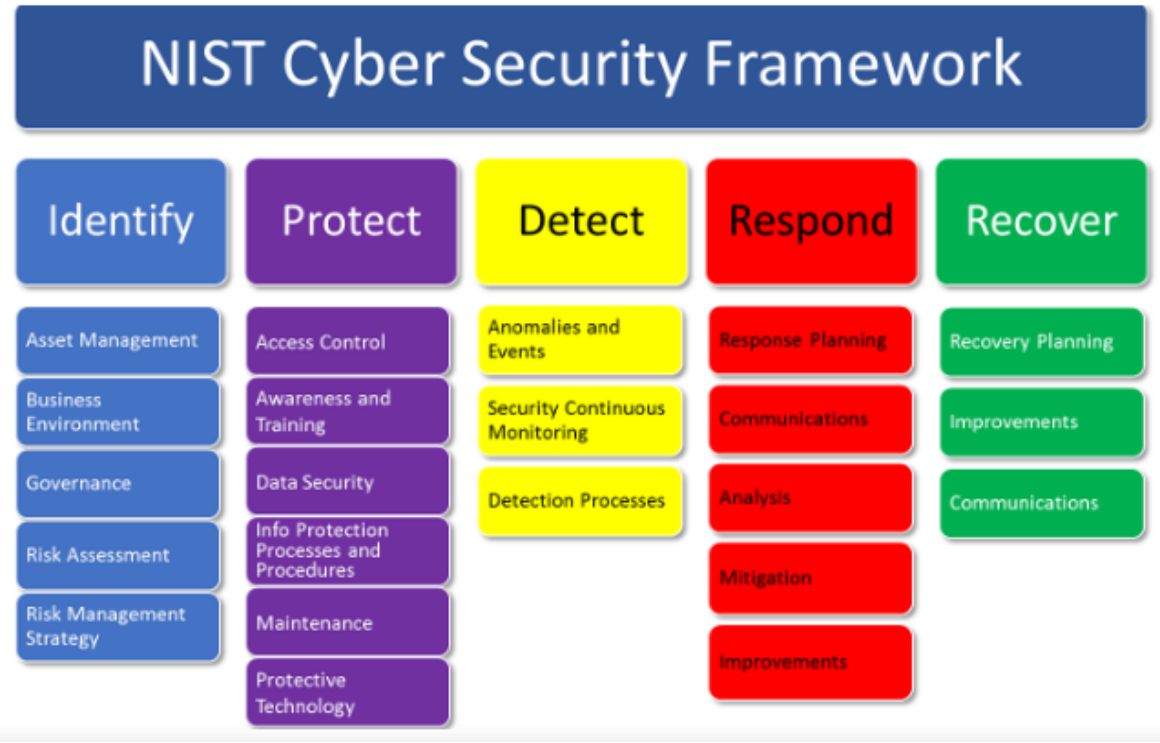


Figure 3: NIST Cyber Security Framework

[3] https://www.fortinet.com/resources/cyberglossary/cia-triad

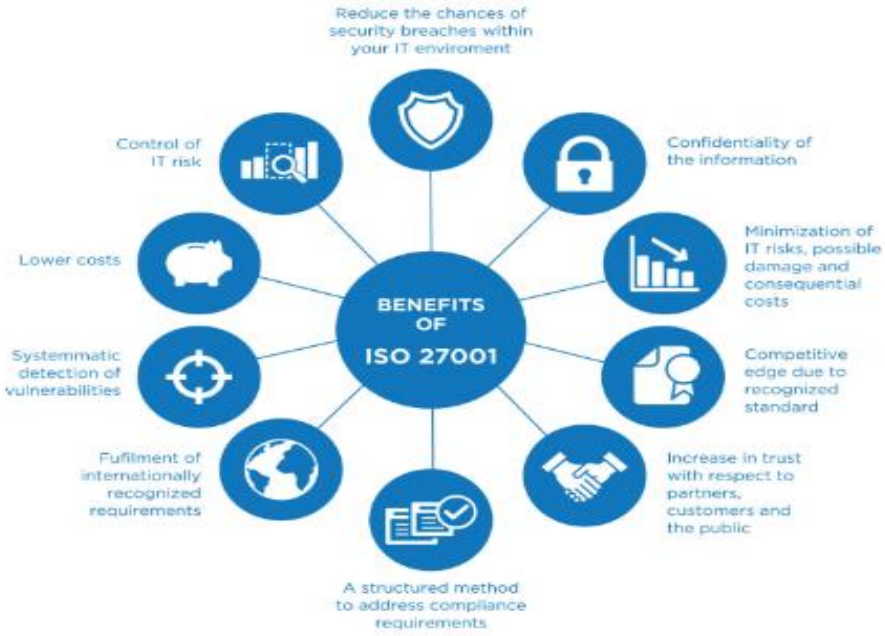
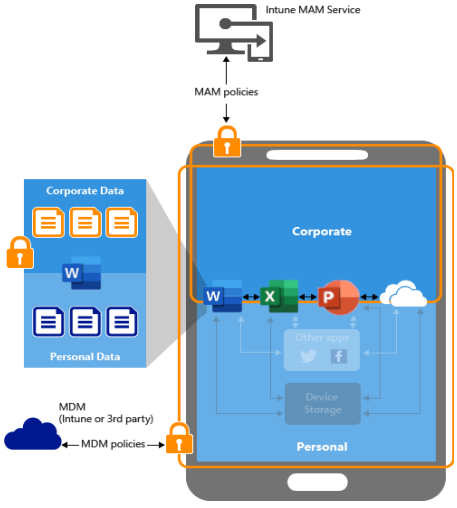


Figure 4: Benefits of ISO 27001

Crafting a comprehensive mobile device security framework for an SME entails careful consideration of effectiveness and budget constraints. This integrated framework was designed by merging NIST CSF[4] and ISO 27001[5] principles to establish a robust mobile device security system for SMEs, ensuring alignment with key controls and requirements from both standards.

4.2 Design Specification for MAM

- Data Protection with MAM and with Device Enrolment.

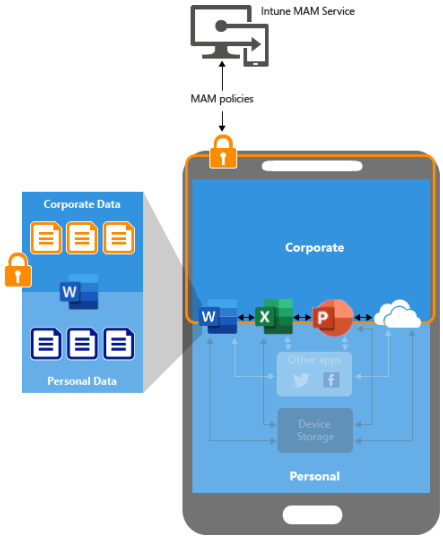


This diagram depicts the functioning of data protection in conjunction with device enrollment. It showcases the safeguarding of the Intune Application Layer, thereby blocking the flow of data to personal apps. However, it enables device management, the ability to push applications to the device, and the collection of compliance data.

Figure 5: With Device Enrolment

[4] https://securityaffairs.com/58163/laws-and-regulations/nist-cybersecurity-framework-2.html
[5] https://hereworks.ie/tech-talk/hereworks-are-iso-27001-accredited/

- Data Protection with MAM but without Device Enrolment.



This diagram demonstrates the operation of data protection in the absence of device enrollment. It exclusively secures apps within the Intune Application Layer while blocking data flow to personal apps. However, it does not support device management.

Figure 6: Without Device Enrolment

- High-level Design:

At a high level, the deployment involved configuring three key components: Microsoft Defender and its associated configuration profiles, Intune App Protection Policies with specified settings, and an Azure AD Conditional Access policy. These measures were implemented to restrict access to corporate data exclusively for authorized users, ensuring a secure mobile device environment within the SME.

- Low-Level Design**:**

The implementation process involved adding the Microsoft Defender Application for iOS to Intune and configuring a VPN Device Configuration Profile for testing purposes. To streamline the deployment, the MDM VPN Test configuration profile was renamed as the 'iOS Defender AutoOnboarding VPN Profile' for production. Additionally, a Dynamic Device Group named 'All iOS iPhone Devices' was created in Azure AD based on device type criteria (iPhone). Both the Microsoft Defender Application and Configuration Profile were assigned as required to this group, encompassing iOS iPhone and Android devices. To facilitate a phased rollout, two distinct groups, 'iOS Devices – Defender Required' and 'iOS Devices – Defender Available,' were established. Devices were allocated accordingly, with the required group enforcing installation, while the available group prompted user action for app installation.

4.3 Design to forward alerts triggered in Windows Defender to Rapid7 SIEM.

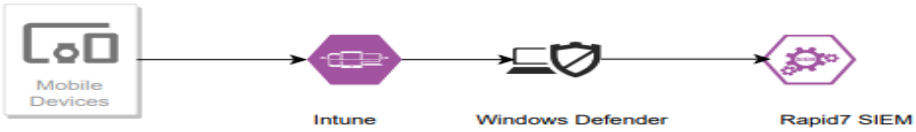


Figure 7: Windows defender and Rapid7 SIEM Integration

As shown in the flow diagram above, the alerts triggered in Microsoft Defender for Endpoint will be forwarded to Rapid7 SIEM for centralized alerting and monitoring. The SOC team will then analyze and investigate the alerts, followed by the incident response process.

5 Implementation

5.1 A novel framework to enhance mobile device security in SMEs.

The following framework outlines a meticulous strategy to enhance mobile device security within the context of small and medium-sized enterprises (SMEs). An assumption made during the creation and implementation of this framework was that the SMEs typically have around 250 employees. By merging the imperatives of robust safeguarding and budgetary prudence, the framework judiciously integrates essential facets while keenly acknowledging the nuanced intricacies inherent to SMEs.

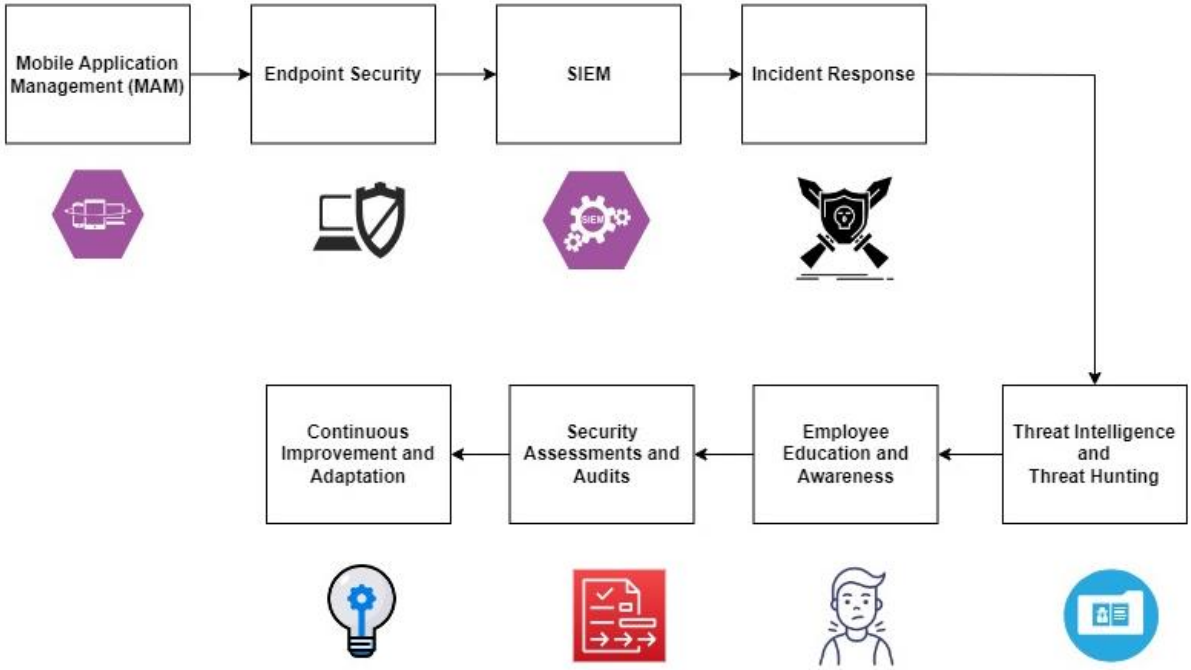


Figure 8: Mobile device security framework for SME

1. Mobile Application Management (MAM):

Deploying Microsoft Intune as an MAM solution strategically addresses SME budget constraints, prioritizing cost-effectiveness while enforcing critical security policies such as encryption, screen locks, and passcodes. Meticulous app whitelisting guidelines ensure precise data control, harmonizing security with usability. Thoughtful implementation of remote wipe capabilities minimizes disruption, aligning with SMEs' resource optimization goals. Timely updates and patches are synchronized with SMEs' financial considerations, fostering a comprehensive yet budget-conscious mobile security approach.

2. Endpoint Security:

Tailoring Microsoft Defender for Endpoint to the financial context of SMEs is crucial, while retaining robust threat detection mechanisms. Policy configurations strike a balance between security and financial viability. Emphasizing behavioral-based detection and cloud-enabled safeguards enhances real-time threat vigilance. Diligent patch management bolsters endpoint protection within SMEs' budgets, fostering resilient cybersecurity.

3. SIEM:

Integrating Microsoft Defender for Endpoint and Microsoft Intune into Rapid7 SIEM aligns with the financial strategy of SMEs, centralizing vigilance. This streamlines the propagation of security incidents and alerting, optimizing resource efficiency in line with the practical approach of SMEs. The formulation of rules and correlations in the SIEM architecture offers tailored defense, meeting the contextual needs of SMEs. Automated incident handling and predefined alerts strengthen the cybersecurity posture of SMEs, aligning with their operational efficiency goals.

4. Incident Response:

Creating a budget-conscious incident response plan ensures efficient security incident management for SMEs. Roles and responsibilities are clearly defined with a focus on cost-effective containment and resolution. The plan incorporates budget-friendly incident detection tools and regular, resource-adjusted simulation exercises to enhance incident handling within financial constraints, strengthening the cybersecurity readiness of SMEs.

5. Threat Intelligence and Threat Hunting:

By subscribing to economical threat intelligence services, SMEs can enhance their vigilant awareness within the constraints of their financial resources. Implementing periodic threat hunting, adjusted to the available resources, enables proactive identification of potential threats. Furthermore, strategically utilizing threat intelligence to shape security policies ensures that SMEs can maintain their effectiveness while fulfilling their fiscal responsibilities.

6. Employee Education and Awareness:

Disseminating concise yet impactful security awareness modules integrate seamlessly with SMEs' operational culture. Customized instructional materials clarify mobile phishing risks and app vulnerabilities, aligning with SMEs' specific context. Cultivating a culture of prompt security incident reporting reinforces a harmonious balance between operational pace and security prudence, strengthening SMEs' overall cybersecurity posture.

7. Security Assessments and Audits:

Periodic security assessments systematically uncover vulnerabilities within the digital landscape of SMEs. Swiftly addressing identified vulnerabilities exemplifies SMEs' unwavering commitment to operational resilience and security.

8. Continuous Improvement and Adaptation:

Sustained vigilance against evolving threats complements SMEs' discernment in navigating dynamic security scenarios. Collaborative ties with cost-effective security networks and SME-focused communities form a harmonious symphony of cutting-edge security expertise.

5.2 Intune Mobile Application Management Policies

- iOS Mobile App Protection Policy

The "iOS Mobile App Protection Policy" is designed for iOS and iPadOS devices, focusing on mobile application protection. It applies to all device types and includes a selection of public apps like Adobe Acrobat Reader and Microsoft Office applications. The policy ensures data security by blocking backups and allowing data transfer only to policy-managed apps. It exempts specific apps and universal links while preventing data copies and limiting cut, copy, and paste actions. Organizational data encryption is required, along with the use of a numeric PIN. Biometric authentication options like Touch ID and Face ID are permitted, with a PIN fallback after inactivity. There's a maximum of 5 PIN attempts before a reset, and the policy addresses jailbroken/rooted devices with data wiping. It sets OS version requirements and actions, and disabled accounts result in blocked access. This comprehensive policy strikes a balance between security and usability for iOS devices, aligning with organizational standards and user convenience. The complete list of policies configured is given in the configuration manual.

- Android Mobile App Protection Policy

The "Android Mobile App Protection Policy" aims to enhance Android device and application security for all device types. It covers popular public apps like Adobe Acrobat Reader and Microsoft Office tools, prioritizing data security by blocking backups and restricting data transfer to policy-managed apps. Users can save data copies to specified services like OneDrive for Business and SharePoint. The policy controls telecommunication data transfer to authorized dialer apps and data reception from all apps. It tightly regulates cut, copy, and paste actions, blocks screen capture and Google Assistant, and allows only approved keyboards. Data encryption is mandatory for organizational data on enrolled devices. Policy-managed app data can't sync with native apps or add-ins, printing org data is blocked, and web content transfer is limited to Microsoft Edge. The policy enforces PIN access, rechecking after inactivity, and limits PIN attempts to five with a reset option. It includes offline grace periods, rooting detection, and app threat scans, ensuring comprehensive Android device security.

5.3 Microsoft Defender for Endpoint alerts in Rapid7 SIEM

Given below is a test alerting policy created in Microsoft defender for which when the configured policy condition matches, an incident would be created in Defender which would be forwarded to Rapid7 SIEM for centralized logging and monitoring by the SOC team.

- Alert Policy to detect malicious files:

This Policy detects when a malicious file is found in a mobile device or uploaded to the cloud.

Proof of Concept: A test file was renamed with a malicious extension ‘.TheTrumpLockerf’ which is a malicious extension for a malware. The file was uploaded to OneDrive from the Test

IOS device. Defender detected this activity and created an incident which in turn created an investigation in Rapid7 SIEM since we have integrated it in Microsoft defender for endpoint.

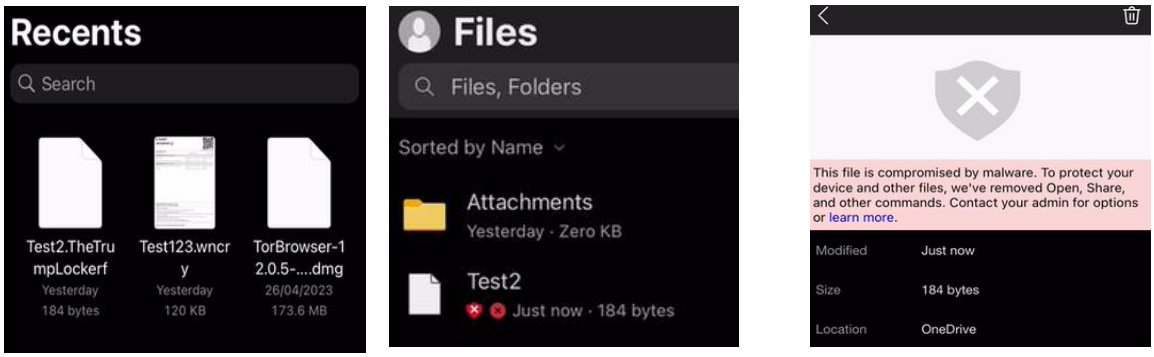


Figure 9: Malicious file uploaded to OneDrive.

- Alert Policy created in Defender:

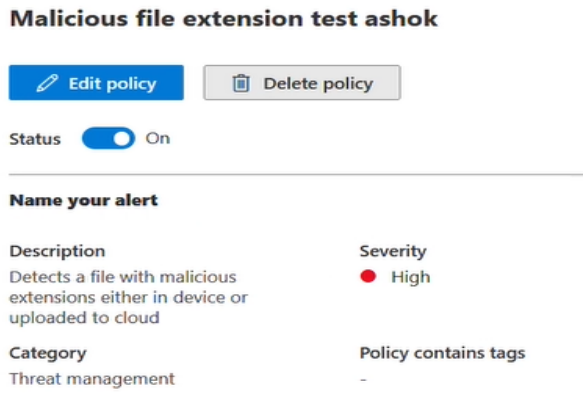


Figure 10: Defender alert policy

- Incident triggered in Defender after the created Alert Policy:

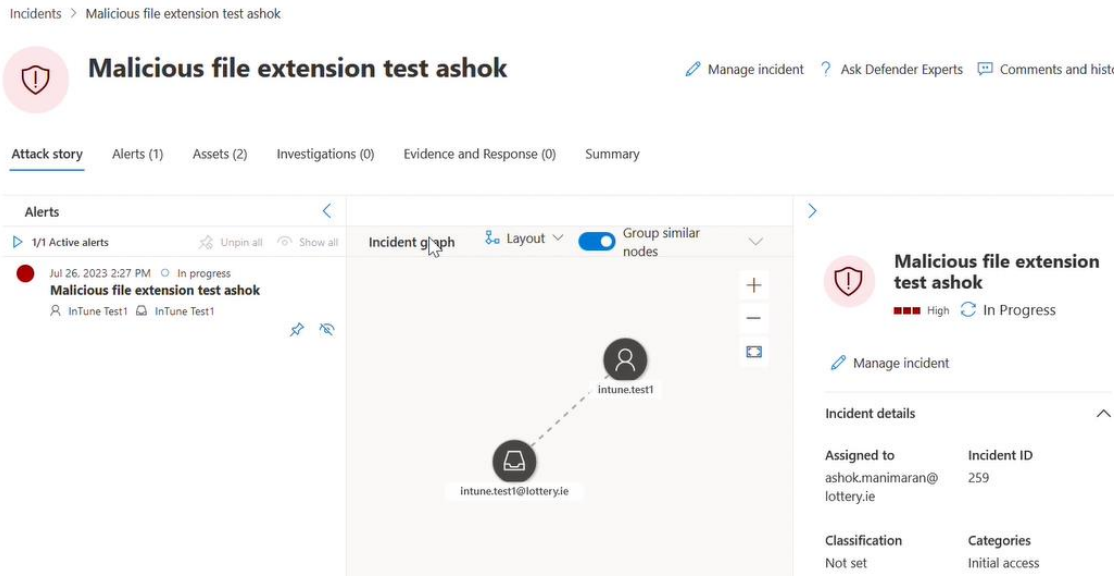


Figure 11: Incident created for the alert policy in defender.

- Investigations created in Rapid7 SIEM

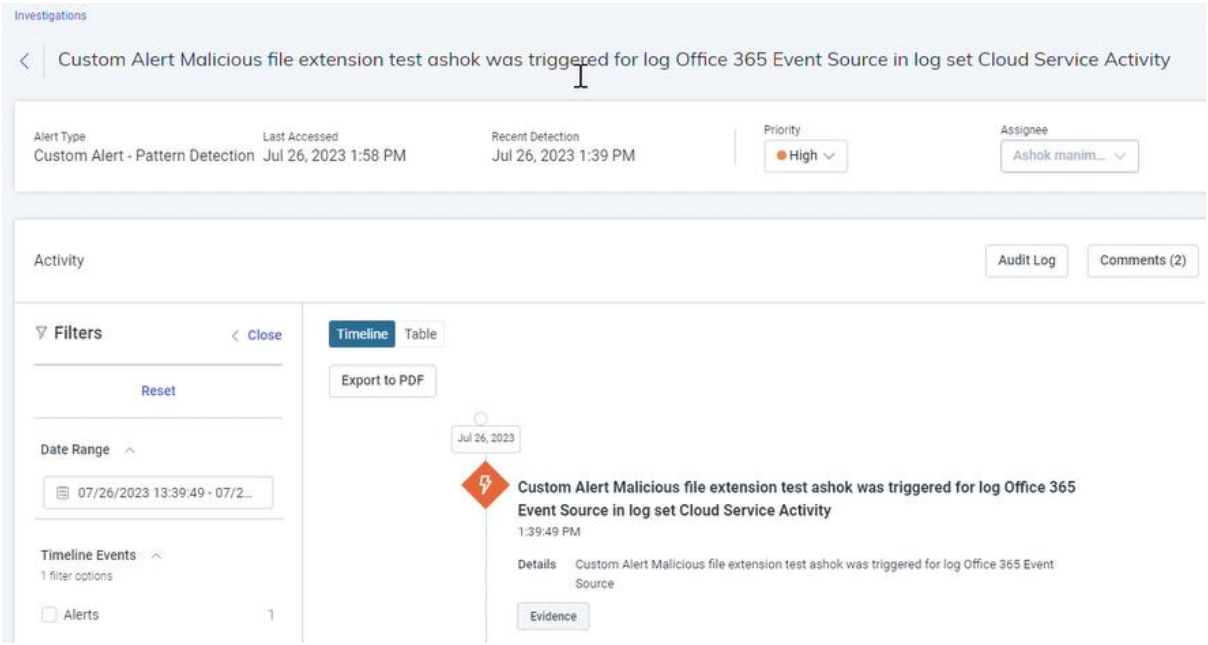


Figure 12: Investigation created for the incident in Rapid7 SIEM

- Microsoft Defender VPN:

A mobile device with Microsoft Defender installed can initiate a local VPN connection. This is a loopback VPN, unlike traditional VPNs, and it does not route network traffic outside of the device. This VPN creates a safer browsing environment, providing web protection, scanning for malicious links, and offering anti-phishing capabilities.

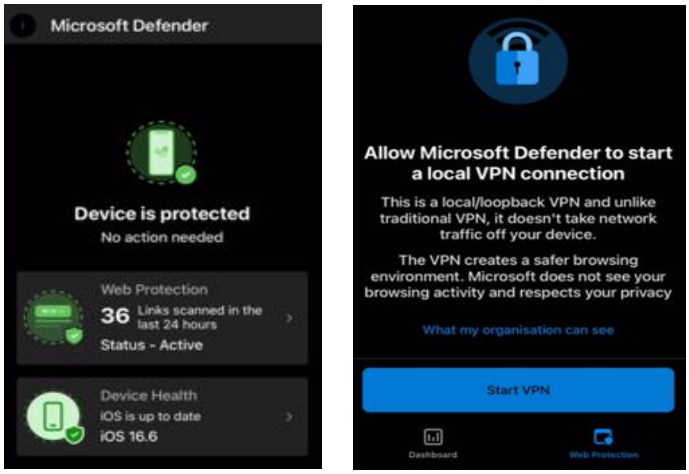


Figure 13: Defender VPN for Web protection

6 Evaluation:

6.1 Framework Evaluation:

Below is the detailed evaluation of the proposed framework for enhancing mobile device security in the context of SMEs while aligning it with the NIST Cybersecurity Framework (CSF) and ISO 27001 standards.

1. Mobile Device Management (MDM) and Mobile Application Management (MAM):
- Implementation: Microsoft Intune was adopted as the MDM/MAM solution, aligning with NIST's emphasis on controlling and managing mobile devices and applications.
- NIST Alignment: The MAM component enforces device encryption, screen locks, and passcodes (NIST controls AC-3, AC-11, AC-12) to protect against data loss or theft.
- ISO 27001 Alignment: Regular updates and patches to Intune ensure the framework's adherence to ISO 27001's requirement for ongoing risk management and improvement (A.12.6).
2. Endpoint Security:
- Implementation: Microsoft Defender for Endpoint was deployed, aligning with NIST's focus on continuous monitoring, detection, and response.
- NIST Alignment: Defender's policies for identifying and blocking phishing attempts, malware, and malicious files (NIST control SI-7) enhance threat detection capabilities.
- ISO 27001 Alignment: Regular software updates and patches adhere to ISO 27001's requirement for managing technical vulnerabilities (A.12.6).
3. SIEM for Centralized Monitoring and Alerting:
- Integration: Microsoft Defender for Endpoint and Microsoft Intune was integrated with Rapid7 SIEM, meeting NIST's recommendation for centralized monitoring and alerting.
- NIST Alignment: Centralized monitoring and incident response automation correspond to NIST's guidelines for real-time threat detection and response.
- ISO 27001 Alignment: Centralized monitoring aligns with ISO 27001's emphasis on information security event monitoring (A.12.4).
4. Incident Response:
- NIST CSF Alignment: This corresponds to the "Response" category by establishing a plan for effectively responding to security incidents.
- ISO 27001 Alignment: It supports "Information Security Incident Management" by ensuring a structured approach to incident response.
5. Threat Intelligence and Threat Hunting:
- Subscription to Feeds: Subscribing to threat intelligence feeds aligns with NIST's proactive approach to security awareness and continuous monitoring.
- NIST Alignment: Regular threat hunting exercises support NIST's proactive stance on detecting and mitigating emerging threats.
- ISO 27001 Alignment: Threat intelligence-driven policy refinement enhances ISO 27001's requirement for monitoring and reviewing the effectiveness of security controls (A.12.6).
6. Employee Education and Awareness:
- Security Awareness Training: Conducting regular security awareness training complies with NIST's recommendation for training and awareness programs.
- NIST Alignment: Educating employees about mobile device security best practices (NIST control AT-3) is aligned with NIST's focus on workforce training.

- ISO 27001 Alignment: Employee education enhances ISO 27001's requirement for security awareness (A.7.2.2).

7. Regular Security Assessments and Audits:

- Periodic Assessments: Performing security assessments and audits meets ISO 27001's requirement for regular security reviews and compliance checks (A.18).
- ISO 27001 Alignment: Addressing identified vulnerabilities and implementing improvements aligns with ISO 27001's risk treatment process (A.12).

8. Continuous Improvement and Adaptation:

- Ongoing Monitoring: Continuously monitoring the threat landscape aligns with NIST's recommendation for continuous monitoring and adaptation.
- NIST Alignment: Collaboration with vendors and security communities to stay informed about the latest security developments corresponds to NIST's guidance for staying current with emerging threats.
- ISO 27001 Alignment: The framework's adaptation to address emerging challenges supports ISO 27001's emphasis on continual improvement (A.18).

6.2 Testing Incident-to-Investigation Flow from Microsoft Defender to Rapid7 SIEM

Proof of concept: The intention behind this alert policy was to identify instances where a user clicks on a potentially malicious url while using a mobile device with Microsoft Defender for Endpoint installed. When such an event occurs, an alert policy has been created in defender to create an incident. This incident is forwarded to Rapid7 SIEM, where an investigation is created and subsequently examined by the SOC team. The evaluation process involved cross-referencing the incident details in Defender with those in the Rapid7 investigation to verify their accuracy.

Original mail containing the malicious url clicked by the user:

Figure 14: Original phishing mail

When the user clicked on the malicious URL, an incident was created in Defender for Endpoint, where it was observed that the user who clicked on the malicious URL is Paul Dervan, the same user who received the malicious email. The URL displayed in the incident was also found to be the same URL that was present in the email. Now, this incident has been forwarded to Rapid7 SIEM due to the integration with Defender to initiate an investigation. As we can see I the investigation created in Rapid7, the events source for the created investigation is given as Office 365. Hence, we can conclude that the investigation.

Incident created in defender for endpoint:

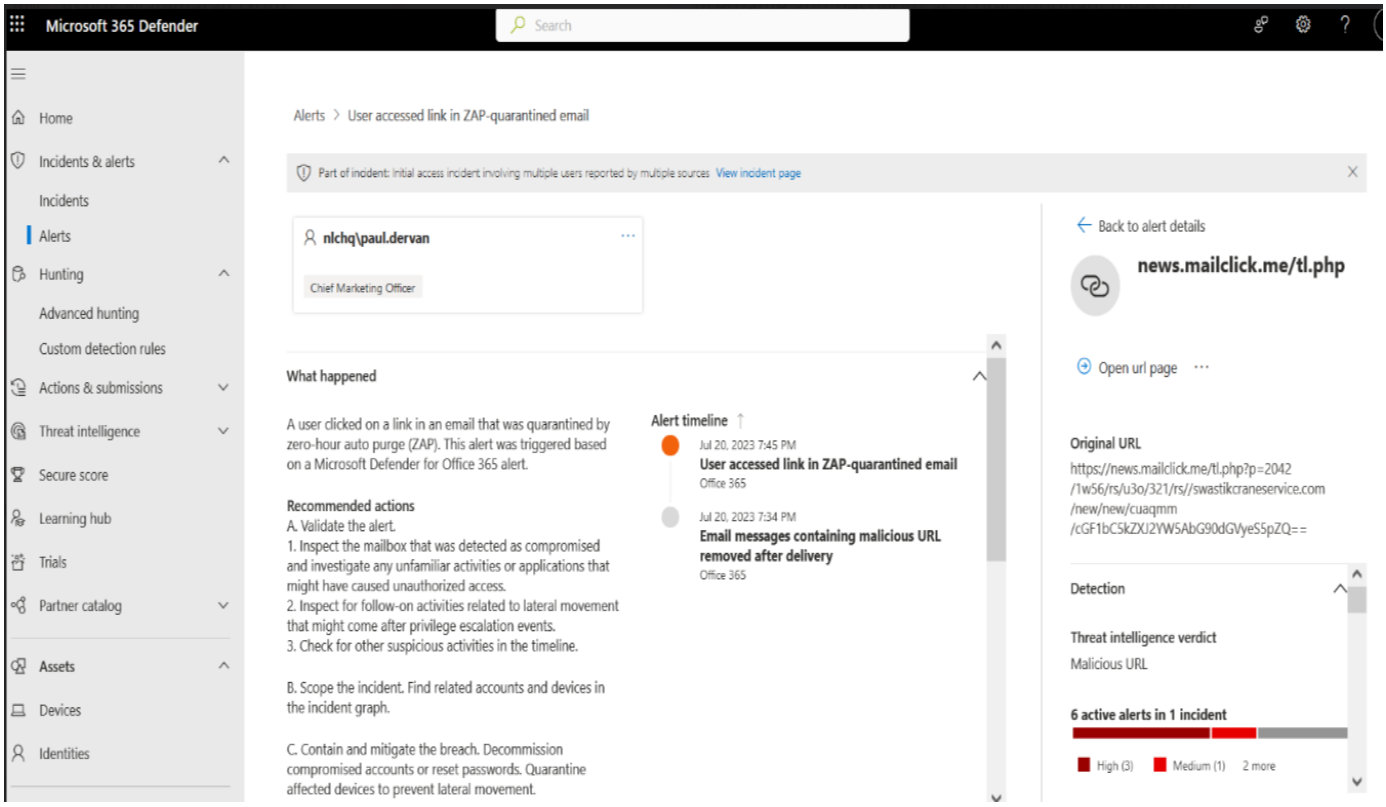


Figure 15: Incident created in Defender for Malicious link clicked by the user.


```
"AlertType": "System",
"Category": "ThreatManagement",
"Comments": "New alert",
"Data": "{\"ts\":\"2023-07-21T21:13:31.1510962Z\",\"te\":\"2023-07-21T21:13:31.1510962Z\",\"tid\":\"910757d4-7f42-4cda-b0a2-b78bdde4c812\",\"tdc\":\"1\",\"tht\":\"MaliciousUrlClick\",\"a
"Name": "A potentially malicious URL click was detected",
"PolicyId": "a74bb32a-541b-47fb-adfd-f8c62ce3d59b",
"Severity": "High",
"Source": "Office 365 Security & Compliance",
"Status": "Active"
```


Figure 16: Evidence in the investigation created in Rapid7.

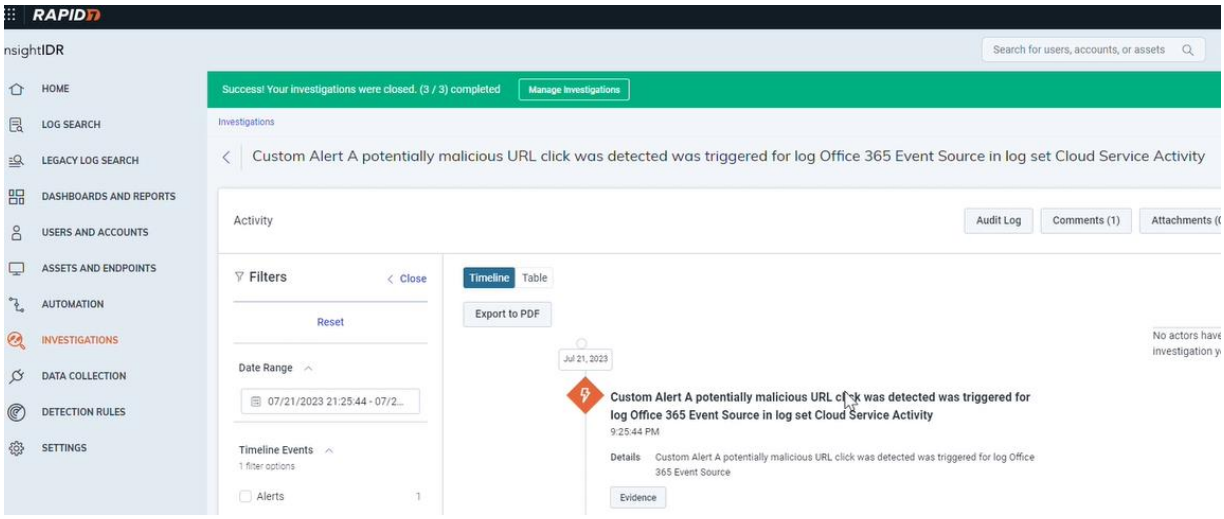


Figure 17: Investigation created in Rapid7.

6.3 Discussion

- Strengths of the framework:

The framework's strengths lie in its foundation with Microsoft Intune, offering adaptable MAM capabilities ideal for SMEs. Leveraging Microsoft's ecosystem, including O365 Azure integration and Defender, allows for cost-effective yet comprehensive device security. It boasts features like device encryption and app whitelisting while considering user needs. Additionally, it prioritizes threat intelligence and hunting for proactive threat detection and integrates with SIEM (Rapid7) for swift incident response. Therefore, the framework provides a holistic approach to SME mobile security, aligning with practicality and robustness.

- Comparison with CMERP Framework.(Abdul Mutalib, Zainol and Mohamed Halip, 2021)

1. Targeted Approach: The framework presented I this paper focuses specifically on mobile device security, a critical area often overlooked. Mobile devices are often subject to distinct vulnerabilities. CMERP, on the other hand, is a general framework for malware management, not especially focused on mobile security.
2. Centralized Monitoring and Alerting: The framework presented in this paper has SIEM (Rapid7) for centralized monitoring and alerts. This real-time threat monitoring is a proactive and comprehensive strategy, giving an overview of your systems. The CMERP framework does offer analysis and collection stages, but there's no mention of a centralized, real-time monitoring system.
3. Employee Education and Awareness: Humans are often the weakest link in cybersecurity. The presented framework includes a very important component of employee education and awareness, which directly addresses this issue. CMERP does not explicitly mention addressing human factors.
4. Regular Security Assessments and Audits: The presented framework includes regular security assessments and audits, which can help detect vulnerabilities before they're exploited. While the CMERP framework does highlight ongoing analysis and collection, there is no explicit mention of regular assessments and audits.

5. Adaptation: The framework presented in this paper emphasizes continuous improvement and adaptation. While CMERP also likely assumes this, this framework makes this process clear, suggesting an ongoing commitment to staying current with evolving threats.

These attributes make the proposed framework in this paper more comprehensive, targeted, and potentially more effective at addressing today's cybersecurity threats in the SME environment.

- Selection of MAM, Endpoint Security and SIEM solutions based on budget and features.

In our framework's current implementation, Microsoft Intune was strategically chosen as the Mobile Application Management (MAM) solution, while Microsoft Defender for Endpoint was selected as the endpoint security solution. This decision was primarily based on the cost-efficiency and integration advantages offered by these solutions within the Microsoft 365 E3 license.

The Microsoft 365 E3[6] license provides a comprehensive package, including access to Microsoft 365 apps, Windows for Enterprise, collaboration tools, ample cloud storage, and robust security and identity management features. Importantly, it covers the usage of both Microsoft Intune and Microsoft Defender for Endpoint, eliminating the need for additional expenditures. This approach significantly optimizes the budget for SMEs as it eliminates the extra cost burden associated with standalone MAM and endpoint security solutions. Moreover, the seamless integration of Microsoft Intune and Microsoft Defender for Endpoint with Azure AD and the broader Microsoft environment streamlines implementation, making it an efficient choice for SMEs. This strategic selection not only enhances security but also contributes to substantial cost savings, simplifying the adoption and management of these critical security components. Rapid7 SIEM is the ideal choice for SMEs with limited resources and budget constraints. It provides a comprehensive solution by combining advanced technology, security specialists, and cutting-edge solutions. This ensures thorough vulnerability assessments, efficient threat hunting, and prioritized action plans for swift remediation. Rapid7's anytime access to technology and expertise offers SMEs a strategic advantage, delivering cost-effective, expert-backed security solutions tailored to their specific needs.

- Modification and improvements that can be made to the design of the framework:

While the framework provides a solid foundation, there are areas where it could be improved. It would benefit from placing a greater emphasis on Identity and Access Management (IAM) to strengthen access controls and implement comprehensive encryption measures. Expanding encryption beyond the device level is essential to ensure data security during transit and while at rest. Furthermore, the framework's effectiveness hinges on the security solutions chosen by SMEs, such as MDM, Endpoint protection, and SIEM, which are influenced by budget constraints. To ensure complete GDPR compliance, adjustments to the framework and its implementation may be necessary, as compliance currently depends on how each organization implements it. Flexibility and a commitment to continuous improvement are crucial in the ever-evolving landscape of cybersecurity.

[6] (*Microsoft 365 E3 License*, 2023)

7 Conclusion and Future Work

The research successfully addressed its objectives by presenting a novel mobile device security framework for SMEs. This framework strengthens the mobile device security posture of SMEs through proactive threat detection and incident response. Its practical implementation demonstrates its viability for safeguarding against mobile device security threats, offering a multi-layered security approach. A Mobile Application Management (MAM) like Microsoft Intune, protects mobile devices by addressing threats like data leakage, unauthorized access, malware, and data loss. It enforces strong authentication, detects jailbroken/rooted devices, and controls app permissions to ensure corporate data and apps remain secure. and protection against security threats like malware, phishing. Microsoft Defender for Endpoint, when integrated with Mobile Application Management (MAM) solutions, helps protect mobile devices from threats like malware, phishing, data leakage, unauthorized access, and app security risks. It enforces security policies, monitors device health, and ensures data protection on mobile devices. Defender integration with Rapid7 SIEM enables centralized security threat monitoring and incident response by the SOC team.

The framework's effectiveness depends on the Security tools chosen by the SMEs during the implementation, with alternatives offering varying results. SMEs may face challenges in configuring and managing components due to a lack of expertise, potentially leading to complications. Initial licensing costs may appear manageable, but hidden expenses like training, consulting, integration, and infrastructure upgrades could strain budgets. Aligning the framework with specific regulations, such as GDPR, may require additional customization to ensure compliance.

In the future, enhancing GDPR compliance can be a valuable modification to this framework. The research provides a foundation for potential commercialization, enabling security consultancies or solution providers to offer tailored services to SMEs Further validation through practical implementation in SMEs of varying sizes and industries would provide valuable insights. Additionally, diverse security tools and industry-specific customization offer opportunities for tool vendors to enhance their offerings.

8 References

Abdul Mutalib, M.M., Zainol, Z. and Mohamed Halip, M.H. (2021) 'Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework', *IEEE* [Preprint]. Available at: https://ieeexplore.ieee.org/abstract/document/9703991 (Accessed: 19 August 2023).

Aguboshim, Felix.C. and Udobi, Joy.I. (2019) 'Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD).' Available at: https://core.ac.uk/download/pdf/234677445.pdf (Accessed: 19 August 2023).

Benz, M. and Chatterjee, D. (2020) 'Calculated risk? A cybersecurity evaluation tool for SMEs'. Available at: https://www.sciencedirect.com/science/article/pii/S0007681320300392?casa_token=ovYhTB81ha4AAAAA:wkg6S4Tl9KMRKdA-apfJhc5m7tODZF8dCaYELD0QobUIy1m5-6mAoUO5q6jrNg3HyTPsXXz8amoQ (Accessed: 20 August 2023).

CIA Triad (2023) *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,and%20methods%20for%20creating%20solutions. (Accessed: 26 August 2023).

Daly, A. (2022) *ISO270001 benefits*, *hereworks*. Available at: https://hereworks.ie/tech-talk/hereworks-are-iso-27001-accredited/ (Accessed: 26 August 2023).

Dhahi Khaleefah, A. and Al-Mashhadi, H.M. (2023) 'Methodologies, Requirements and Challenges of Cybersecurity Frameworks: A Review'. Available at: https://www.mecs-press.org/ijwmt/ijwmt-v13-n1/IJWMT-V13-N1-1.pdf (Accessed: 20 August 2023).
Eling, M. (2021) 'Cyber risk management: History and future research directions'. Available at: https://onlinelibrary.wiley.com/doi/epdf/10.1111/rmir.12169 (Accessed: 20 July 2023).
Emer, A., Unterhofer, M. and Rauch, E. (2021) 'A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises'. Available at: https://ieeexplore.ieee.org/document/9424999 (Accessed: 10 August 2023).
González-Granadillo, G., Diaz, R. and González, S. (2021) 'Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures'.
Gupta, D. (2020) 'Security Challenges and Cyber Forensic Ecosystem in IoT Driven BYOD Environment', *IEEE* [Preprint]. Available at: https://ieeexplore.ieee.org/document/9199866 (Accessed: 1 July 2023).
Hayes, D., Cappa, F. and An Le-Khac, N. (2020) 'An effective approach to mobile device management: Security and privacy issues associated with mobile applications'. Available at: https://www.sciencedirect.com/science/article/pii/S2666954420300016 (Accessed: 19 August 2023).
Iman Ali, M. (2021) 'BYOD Cyber Threat Detection and Protection Model', *IEEE* [Preprint]. Available at: https://ieeexplore.ieee.org/abstract/document/9397105 (Accessed: 19 August 2023).
Intune vs SCCM (2022). Available at: https://www.scappman.com/post/the-best-mobile-device-management-solution-in-2022-sccm-vs-intune/ (Accessed: 22 August 2023).
Lian, J.-W. (2020) 'Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value', *Taylor & Francis online* [Preprint]. Available at: https://www.tandfonline.com/doi/full/10.1080/17517575.2020.1791966 (Accessed: 2 July 2023).
Microsoft 365 E3 License (2023) *Microsoft*. Available at: https://www.microsoft.com/en-ie/microsoft-365/enterprise/microsoft365-plans-and-pricing (Accessed: 27 August 2023).
Mudassar Yamin, M. and Katt, B. (2019) 'Mobile device management (MDM) technologies, issues and challenges'. Available at: https://dl.acm.org/doi/abs/10.1145/3309074.3309103 (Accessed: 19 August 2023).
Mutlaq Alnajrani, H. (2020) 'The Effects of Applying Privacy by Design to Preserve Privacy and Personal Data Protection in Mobile Cloud Computing: An Exploratory Study', *MDPI* [Preprint]. Available at: https://www.mdpi.com/2073-8994/12/12/2039 (Accessed: 1 July 2023).
Nespoli, P. (2021) 'Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices', *ScienceDirect* [Preprint]. Available at: https://www.sciencedirect.com/science/article/pii/S2214212621001058?via%3Dihub (Accessed: 11 August 2023).
P. Roy, P. (2019) 'A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard', *IEEE* [Preprint]. Available at: https://ieeexplore.ieee.org/abstract/document/9119914 (Accessed: 20 August 2023).
Paganini, P. (2017) *NIST Cyber Security framework*, *Securityaffairs*. Available at: https://securityaffairs.com/58163/laws-and-regulations/nist-cybersecurity-framework-2.html (Accessed: 26 August 2023).
Rapid7 SIEM (2023). Available at: https://www.rapid7.com/solutions/siem/ (Accessed: 22 August 2023).
R.K.U, M. *et al.* (2022) 'CYBER THREAT DETECTION, SECURING AND STORING CONFIDENTIAL FILES IN BYOD', *CYBER THREAT DETECTION, SECURING AND STORING CONFIDENTIAL FILES IN BYOD* [Preprint]. Available at: https://www.icisc-conf.org/wp-content/uploads/2023/05/CYBER-THREAT-DETECTION-SECURING-AND-STORING-CONFIDENTIAL-FILES-IN-BYOD-1.pdf (Accessed: 19 August 2023).
Vakakis, N. *et al.* (2019) 'Cybersecurity in SMEs: The Smart-Home/Office Use Case'. Available at: https://ieeexplore.ieee.org/abstract/document/8858471 (Accessed: 19 August 2023).
Vakakis, N., Nikolis, O. and Ioannidis, D. (2019) 'Cybersecurity in SMEs: The Smart-Home/Office Use Case', *IEEE* [Preprint]. Available at: https://ieeexplore.ieee.org/document/8858471 (Accessed: 10 July 2023).
Wazid, M., Zeadally, S. and Kumar Das, A. (2019) 'Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions', *IEEE* [Preprint]. Available at: https://ieeexplore.ieee.org/document/8634991 (Accessed: 31 August 2023).
Weichbroth, P. and Łysik, Ł. (2020) 'Mobile Security: Threats and Best Practices', *Hindawi* [Preprint]. Available at: https://www.hindawi.com/journals/misy/2020/8828078/ (Accessed: 19 August 2023).