Networks and Cyber Security Essentials ACCA4024

SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

Daniel Mark Jones
0300760

Contents

INTRODUCTION 2
IDENTIFICATION OF MODERN THREATS 3
MODERN SECURITY POLICIES 4
TECHNICAL MITIGATION MEASURES 5
PROTECTIVE MONITORING AND INCIDENT RESPONSE 6
CONTINUOUS TRAINING & AWARENESS 7
CONCLUSION 8

INTRODUCTION

Financial institutions remain prime targets for cybercrime due to the high value of financial data and the increasing sophistication of modern threat actors. Hybrid working, cloud adoption, and SaaS applications have significantly expanded the attack surface for organisations such as Vigilant Trust & Asset Management (VTAM), increasing exposure to phishing, ransomware, and unauthorised access attempts. VTAM's recent phishing and ransomware incidents demonstrate the limitations of traditional perimeter-based security models.

To address these risks, VTAM requires a modern security framework based on Zero Trust principles. NIST SP 800-207 defines Zero Trust as a model that requires continuous verification of users, devices, and systems [2]. This approach aligns with frameworks such as the NIST Cybersecurity Framework (CSF) [1] and ISO/IEC 27001:2022 [3]. This report identifies current cyber threats facing VTAM and proposes Zero Trust aligned security policies, technical controls, monitoring strategies, and staff awareness measures to strengthen organisational resilience.

IDENTIFICATION OF MODERN THREATS

Ransomware-as-a-Service (RaaS) enables attackers with limited technical expertise to deploy sophisticated ransomware, increasing the frequency of attacks against financial organisations [4]. Attacks such as the 2023 MOVEit breach demonstrated how vulnerabilities in widely used software can cause large-scale operational disruption and data compromise across multiple sectors [7].

Artificial intelligence has increased the effectiveness of phishing and vishing attacks through realistic emails, deepfake voice impersonation, and automated credential theft [5]. VTAM's recent phishing incident highlights the limitations of traditional email filtering and the growing risk of social engineering within financial environments.

Supply chain compromises and cloud misconfigurations also present significant risks. Reliance on third-party SaaS platforms and cloud services increases exposure to upstream vulnerabilities, while weak identity controls and Shadow IT can result in data leakage and unauthorised access [6].

Internal threats remain equally important. Hybrid working and mobile device usage increase the likelihood of insecure access practices, credential theft, and accidental data disclosure. ISO/IEC 27001 emphasises strict access control and monitoring to reduce insider risks and privilege misuse [3].

MODERN SECURITY POLICIES

VTAM will implement a Zero Trust security framework based on continuous authentication, least privilege access, and strict verification of users, devices, and workloads [2]. Identity and Access Management (IAM) controls including MFA, RBAC, and Privileged Access Management (PAM) will reduce credential theft and privilege escalation associated with AI-powered phishing and RaaS attacks [4][5].

All endpoints will be continuously monitored using EDR/XDR and Mobile Device Management (MDM) solutions to reduce risks associated with hybrid working, insecure personal devices, and cloud-based attacks [6]. Network micro-segmentation and Zero Trust Network Access (ZTNA) curbs lateral movement and lessens the impact of ransomware incidents or supply chain attacks such as MOVEit [7].

VTAM will also implement data classification, encryption, and Data Loss Prevention (DLP) controls in accordance with ISO/IEC 27001:2022 [3]. Cloud Security Posture Management (CSPM) and continuous compliance scanning will reduce cloud misconfiguration and Shadow IT risks [5]. Finally, systems will follow a risk-based patch management policy aligned with the CISA Known Exploited Vulnerabilities (KEV) catalogue to ensure rapid remediation of critical vulnerabilities [4].

Figure 1: Zero Trust Security Architecture for VTAM

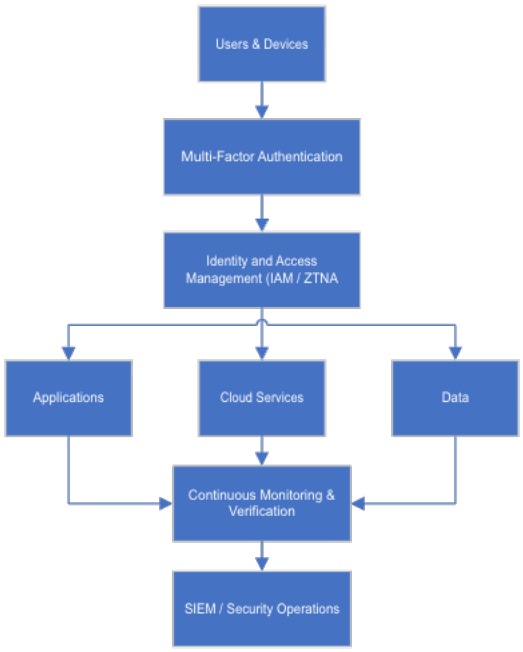

Figure 1 presents VTAM's Zero Trust architecture, in which users and devices are continuously verified through MFA and IAM controls before any access to applications, cloud platforms, or sensitive information is permitted. Ongoing activity monitoring, combined with SIEM integration, enables rapid identification of anomalous behaviour and helps prevent unauthorised access and lateral movement [2].

TECHNICAL MITIGATION MEASURES

VTAM will implement layered technical controls aligned with Zero Trust principles, the NIST CSF [1], and ISO/IEC 27001:2022 [3]. MFA, conditional access, and Privileged Access Management (PAM) will reduce credential theft, privilege escalation, and AI-powered phishing attacks by enforcing continuous identity verification [2][5].

Endpoint Detection and Response (EDR/XDR) solutions will provide behavioural monitoring and automated isolation of compromised devices, reducing ransomware propagation and hybrid work risks. SIEM and SOAR platforms will support continuous monitoring, threat detection, and automated incident response by correlating events across endpoints, cloud services, and network infrastructure [8][10].

To reduce cloud and supply chain risks, VTAM will implement Cloud Security Posture Management (CSPM), compliance scanning, and Zero Trust Network Access (ZTNA). Micro-segmentation will restrict lateral movement within the network, limiting the impact of ransomware or supply chain compromise [7]. Finally, immutable backups and ransomware-resilient storage will support rapid recovery and business continuity during cyber incidents [1].

Figure 2: Technical security controls implemented within VTAM's Zero Trust architecture.

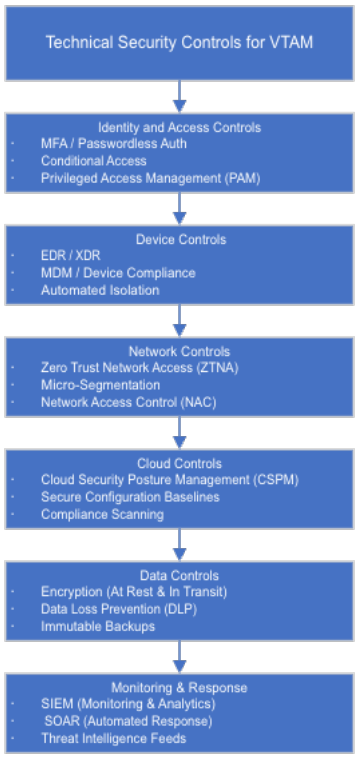

Figure 2 illustrates the layered technical controls used to protect VTAM's infrastructure. Identity, endpoint, network, cloud, and monitoring controls work together to reduce ransomware, phishing, insider, and supply chain threats through continuous verification and monitoring.

PROTECTIVE MONITORING AND INCIDENT RESPONSE

VTAM will implement continuous monitoring through SIEM, SOAR, and threat intelligence integration to support rapid detection and containment of cyber threats. SIEM platforms provide centralised log collection and real-time analytics across endpoints, cloud services, identity systems, and network traffic, supporting the NIST CSF Detect function [1]. Integration with threat intelligence feeds from CISA and ENISA improves detection of ransomware, phishing, and supply chain attacks [4][5][10].

SOAR enables automated response actions such as endpoint isolation, account suspension, and phishing triage, reducing response times during large-scale attacks. VTAM's incident response process follows the NIST SP 800-61 lifecycle [9], including detection, containment, eradication, recovery, and lessons learned. This structured approach improves resilience against ransomware, insider threats, and cloud-based attacks while supporting continual improvement aligned with ISO/IEC 27001:2022 [3].

Figure 3: Incident Response Workflow for VTAM

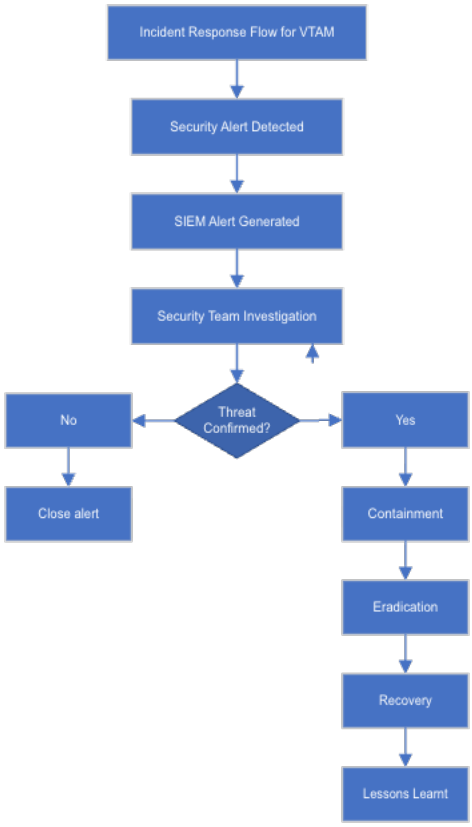

Figure 3 illustrates VTAM's incident response workflow aligned with NIST SP 800-61. SIEM monitoring, investigation, containment, eradication, and recovery processes support rapid detection and response to cyber incidents.

CONTINUOUS TRAINING & AWARENESS

VTAM will implement a continuous security awareness programme to reduce human-factor risks, which remain a leading cause of breaches [11]. Monthly micro-training sessions will focus on AI-powered phishing, vishing, cloud security, and hybrid work risks, reinforcing Zero Trust principles of continuous verification and identity security [2][5].

Regular phishing and vishing simulations will test staff readiness and identify high-risk users, complementing technical controls such as MFA and SIEM monitoring [4]. VTAM will also establish a Security Champions programme to promote secure behaviour, improve incident reporting, and support organisational awareness requirements within ISO/IEC 27001:2022 [3].

Gamified training methods and clear reporting channels will encourage employee engagement and rapid reporting of suspicious activity. KnowBe4's 2023 report found that gamified awareness training improves long-term retention and reduces phishing susceptibility [12]. This strengthens VTAM's ability to detect and respond to ransomware, insider threats, and social engineering attacks in alignment with the NIST CSF Detect and Respond functions [1].

CONCLUSION

VTAM faces increasing cyber threats including Ransomware-as-a-Service, AI-powered phishing, supply chain compromise, and cloud-based attacks [4][5][7]. These risks demonstrate the limitations of traditional perimeter-based security and highlight the need for a Zero Trust approach based on continuous verification and monitoring. By aligning with NIST SP 800-207 [2], the NIST Cybersecurity Framework [1], and ISO/IEC 27001:2022 [3], VTAM can strengthen protection across its identity, endpoint, network, cloud, and data environments.

The proposed security policies, technical controls, monitoring capabilities, and awareness programme collectively improve VTAM's ability to detect, contain, and recover from modern cyber threats. This Zero Trust framework enhances organisational resilience, reduces operational risk, and supports long-term business continuity within an evolving threat landscape.

References

[1] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. Gaithersburg, MD, USA: NIST, Apr. 2018. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207

[3] International Organization for Standardization, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. Geneva, Switzerland: ISO, 2022.

[4] Cybersecurity and Infrastructure Security Agency, *Ransomware Guide*. Washington, DC, USA: CISA, 2023. [Online]. Available: https://www.cisa.gov/stopransomware/ransomware-guide

[5] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2023*. Heraklion, Greece: ENISA, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[6] IBM Security, *Cost of a Data Breach Report 2023*. Armonk, NY, USA: IBM Corporation, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

[7] Progress Software, *MOVEit Transfer Vulnerability Analysis*. Burlington, MA, USA: Progress Software, 2023. [Online]. Available: https://www.progress.com/blogs

[8] Splunk, *What is SIEM?,* Splunk, San Francisco, CA, USA, 2023. [Online]. Available: https://www.splunk.com/en_us/data-insider/what-is-siem.html

[9] K. Scarfone, P. Mell, T. Grance, and K. Masone, *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Rev. 2. Gaithersburg, MD, USA: National Institute of Standards and Technology, Aug. 2012. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-61r2

[10] IBM Security, *Security Intelligence and SIEM Guide*. Armonk, NY, USA: IBM Corporation, 2022. [Online]. Available: https://www.ibm.com/topics/siem

[11] Verizon, *2023 Data Breach Investigations Report*. New York, NY, USA: Verizon, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[12] KnowBe4, *Security Awareness Training Report 2023*. Clearwater, FL, USA: KnowBe4, 2023. [Online]. Available: https://www.knowbe4.com