

A Zero Trust Security Framework for Vigilant Trust & Asset Management: Mitigating Modern Cyber Threats in the Hybrid Cloud Era.

Student name: Yousupha Gaye

Student ID number: 2325927

Programme: CertHE Computing Skills for Workplace

Module: Networks and Cyber Security Essentials

Module code: ACCA4024

Lecturer: Amit Naik, Kwame

Assignment Title: Synthesize a solution to a potential real-life scenario

Table of Contents

Abstract.....	1
1. Introduction.....	2
2. Engagement with Literature.....	3
2.1. The Zero Trust Model	
2.2. The NIST Cyber Security Framework (CSF) and ISO/IEC 27001	
2.3. Contemporary Threat Landscape	
3. Threat Assessment: Internal and External Threats.....	5
3.1. External Threats	
3.2. Internal Threats	
4. Zero Trust Security Model.....	7
5. Recommended Security Policies.....	9
5.1. Access Control Policy (Aligns with NIST CSF, ISO 27001 A.9)	
5.2. Data Security Policy (Aligns with NIST CSF PR.DS, ISO 27001 A.8, A.13)	
5.3. System Acquisition, Development and Maintenance Policy (Aligns with NIST CSF PR.IP, ISO 27001 A.14, A.15)	
5.4. Incident Management Policy (Aligns with NIST CSF RS.RP., ISO 27001 A.16)	
6. Technical Controls and Feasibility Analysis.....	11
6.1. Identity: Multi-Factor Authentication (MFA) and Identity Governance	
6.2. Devices: Endpoint Detection and Response (EDR)	
6.3. Networks: Micro-segmentation	
6.4. Applications & Data: Cloud Security Posture Management (CSPM) and Data Loss Prevention (DLP)	
6.5. Infrastructure: Immutable Backups and Robust Patch Management	
7. Monitoring and Incident Response.....	14
8. Training and Awareness Programme.....	17
9. Conclusion.....	19
10. References.....	20

Abstract

The cyber criminals are currently on a rampage in the financial services industry and this is a factor that is being experienced with trepidation by mid-sized companies such as Vigilant Trust & Asset Management (VTAM).

The recent security breaches, the phishing campaign that was highly sophisticated and a failed ransomware virus attempt strongly highlights the ineffectiveness of conventional perimeter-based security models. The report is a synthesis of an updated, holistic, and current cyber security structure based on the principle of never trust, always verify known as Zero Trust. The report suggests a multi-layered defence approach by examining the existing and future threats, including Ransom-ware-as-a-Service (RaaS), AI-assisted phishing, and supply chain attacks.

This plan is expressed in specific security policies that are in line with the National Institute of Standards and Technology (NIST) Cyber security Framework and the ISO/IEC 27001 and supplemented by practical technical controls such as Multi-Factor Authentication (MFA), Endpoint Detection and Response (EDR), and Cloud Security Posture Management (CSPM). An active monitoring and incident-response strategy based on the use of the technologies of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) is described with the help of the supporting flow chart. Lastly, the report outlines an ongoing, involving security awareness program that would promote a strong human firewall.

The recommendations will also be aimed to improve the security posture of VTAM in a systematic way, safeguard sensitive client data, clarify compliance with regulations as well as provide clear business reasons to the Board to warrant the corresponding investment.

1. Introduction

Vigilant Trust and Asset management (VTAM) is a digital ecosystem that is high and penetrated by diverse and intricate cyber threats. The measured transition to hybrid work arrangements and the growing dependence on cloud-based services have in effect broadened the corporate attack surface, and have rendered outdated the antiquated, perimeter-based security models.

Being a financial services company, VTAM is an excellent target of financially motivated threat actors, who develop their tactics, techniques, and procedures (TTPs) continuously. The latest events, including a phishing attack that has bypassed the old email filters and a ransomware attack that the company has prevented, can be seen as an urgent Board requirement to implement a more resilient, stronger, and more modern security stance.

This report answers such a requirement by creating a comprehensive cyber security framework using the Zero Trust architecture. The goal is to systematically define the threat environment, define clear policies based on international standards, adopt layered technical security controls, as well as inculcate a proactive security culture.

The solution is guided by the credible sources of leading governmental and industrial authorities, including the National Institute of Standards and Technology (NIST), Cyber security and Infrastructure Security Agency (CISA), and the European Union Agency for Cyber security (ENISA).

This report will help implement a more realistic, feasible, and reasonable road map to protect critical assets of VTAM and guarantee continuity of the business in the changing cyber environment by aligning with industry-recognized models such as the NIST Cyber security Framework .

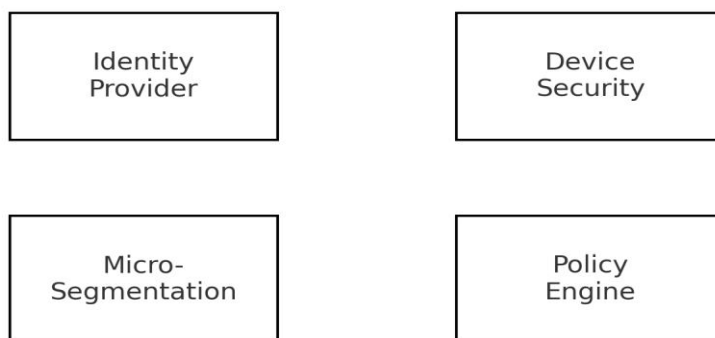
2. Engagement with Literature

This framework is based on a solid background of the modern literature on cyber security, which consists of governmental recommendations, international standards, and the analysis of practical threat intelligence.

2.1. The Zero Trust Model

Zero Trust is the main architectural concept applied in this report. Zero trust is an approach deviating from the classical idea of a castle-and-moat approach, originally introduced by Forrester Research.

Its main principle is never trust, always verify. No user or device, either within or outside corporate network is implicitly trusted. To access allocation the resources are as per-session based, with identity verification, the device health, and finally the least privileged principle. This model directly reacts to the hybrid work environment of VTAM whereby the network perimeter has been dissolved.



2.2. The NIST Cyber security Framework

Zero Trust implementation is designed based on NIST Cyber security Framework (CSF) [3]. The CSF offers a high-level cyber security outcomes taxonomy which it lays into five Functions, namely: Identify, Protect, Detect, Respond and Recover.

This framework is a pragmatic, risk-based way of managing cyber security risk, which is needed to communicate with the Board. Its annex of security controls (Annex A) provides a detailed checklist to develop detailed security policy, to make sure it has a holistic and auditable security program that complies with the international best practices.

2.3. Contemporary Threat Landscape

Threats assessment is informed by actual incidences and CISA and ENISA analysis. The recent supply chain attack that affected various financial institutions serves as the example of the high risk of third-party software compromising.

The Known Exploited Vulnerabilities (KEV) catalog by CISA is an essential element of the patch management strategy of VTAM because it is a list of vulnerabilities actively exploited by attackers and the list is prioritized. Moreover, studies of Ransom ware-as-a-Service (RaaS) services such as LockBit explain how cyber crime can be commoditized so that even less skilled individuals can cause devastating attacks.

According to the latest threat intelligence reports, the development of AI-driven voice phishing (vishing) is also registered, which means that more individualized and persuasive social engineering attacks have begun to emerge .

3. Threat Assessment: Internal and External Threats

VTAM is under the threat of a dynamic set of threats, which pose technological and human weaknesses.

3.1. External Threats

Ransom ware-as-a-Service (RaaS):

RaaS systems have decreased the entry threshold of cyber criminals. A successful attack can encrypt the vital data of VTAM such as client portfolio and transaction records, causing devastating operational impact, loss of money (through extortion) and damage to its reputation that can hardly be salvaged. The latest strike suggests that VTAM is already in the target.

Artificial Intelligence Powered Social Engineering (Vishing & Phishing):

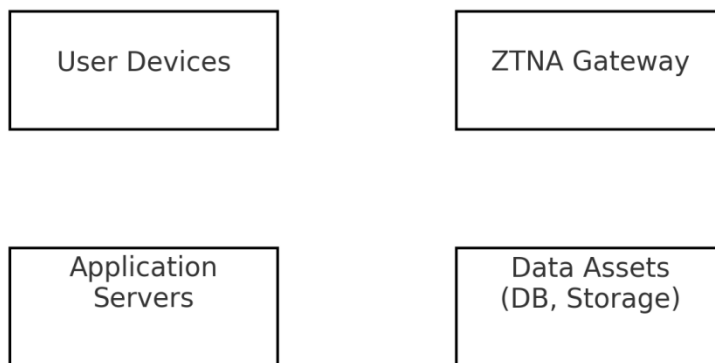
Generative AI enables an attacker to develop more convincing and personalized phishing messages and vishing conversations with senior executives or trusted partners to spook employees into giving money or revealing credentials. This is the bypassing of technical filters by the direct attack on human psychology.

Supply Chain Compromises:

In the case of a breach, attackers attack the software suppliers to get access to a large number of customers. A third-party application vendor of the VTAM, including a cloud service provider or vendor of financial software may offer a trusted entry point into the environment of VTAM.

Cloud Misconfigurations:

The use of cloud services (IaaS, PaaS, SaaS) has started to create the risks of incorrectly set up storage buckets, insecure API endpoints, and excessive user permissions. These misconfigurations are often used in stealing sensitive data straight off the cloud.



3.2. Internal Threats

Negligent Insiders:

The behavior of employees on a hybrid model can result in security incidents accidentally by using unsecured home networks, falling prey to phishing, or poor handling of sensitive data. This is still one of the greatest risk vectors.

Malicious Insiders:

A malicious employee who already has sufficient access may steal sensitive client information or even cause havoc to systems. The concept of least privilege and efficient logging is essential to address this risk.

Bring Your Own Device (BYOD) Risks:

The utilization of personal devices during the work increases the attack area. A personal device with low security might become infected with malware, and it will serve as a pivot point to the corporate network of VTAM.

4. Zero Trust Security Model

The key to the modern security architecture at VTAM is the Zero Trust model. It takes the form of breach and authenticates every request as though it comes out of an untrusted network. This model is developed on the four main pillars of identity, devices, networks, applications, and data.

Zero Trust Architecture Diagram

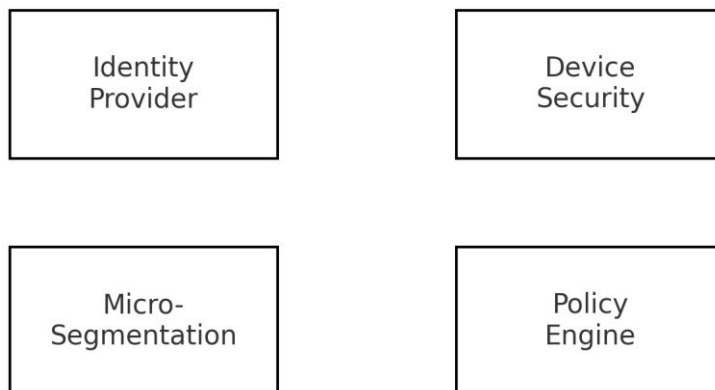


Figure 1: Conceptual Zero Trust Architecture for VTAM, s

Implementation Major Principles of VTAM:

i. Identity as the First Line of Protection:

Any access request should undergo strong MFA authentication, authorization, and encryption. Only users with access can manipulate the data.

ii. Explicit Verification:

Activation is provided according to the dynamic rules which check the identity of a user, the compliance of the device, the place, the application requested, and the sensitivity of the data.

iii. Least Privilege Access:

The minimum access levels of a user are provided to them only to enable them to undertake their job functions. Privileged tasks can have access through Just-in-Time (JIT).

iv. Assume Breach:

Work on the assumption that the internal network is already compromised. Use micro-segmentation to avoid the lateral movement of attackers and make all internal traffic encrypted.

5. Suggested Security Policies

The policy below transforms the Zero Trust principles into the governance.

5.1. Access Control Policy

Purpose: To enforce and allow only the authorized users and devices to manipulate VTAM resources. Only users with permission to access this can manipulate the VTAM resources.

Policy Statements:

- **Multi-Factor Authentication (MFA)** is compulsory to all the users when they gain access to any system of VTAM, irrespective of the location.
- **The least privilege policy will be applied;** user accounts will be audited after every quarter.
- **Role-based Access Control (RBAC)** will be incorporated in order to simplify the process of managing permissions. . All distance access will be bridged by a Zero Trust Network Access (ZTNA) answer, as compared to a customary VPN.

5.2. Data Security Policy

Purpose: To ensure that the data of VTAM is secured in terms of confidentiality, integrity and availability.

Policy Statements:

- I. The encryption of all sensitive data, both in transit and at rest, should be done using strong and industry level algorithms. II.This will be done through the introduction of
- II. Data classification into different categories to inform the rules of handling and access.
- III. The Data Loss Prevention (DLP) software is going to be installed to detect and prevent the illegal exit of the sensitive data.

5.3. System Acquisition Development and Maintenance Policy.

Purpose: To provide security is pervasive in terms of systems and software.

Policy Statements:

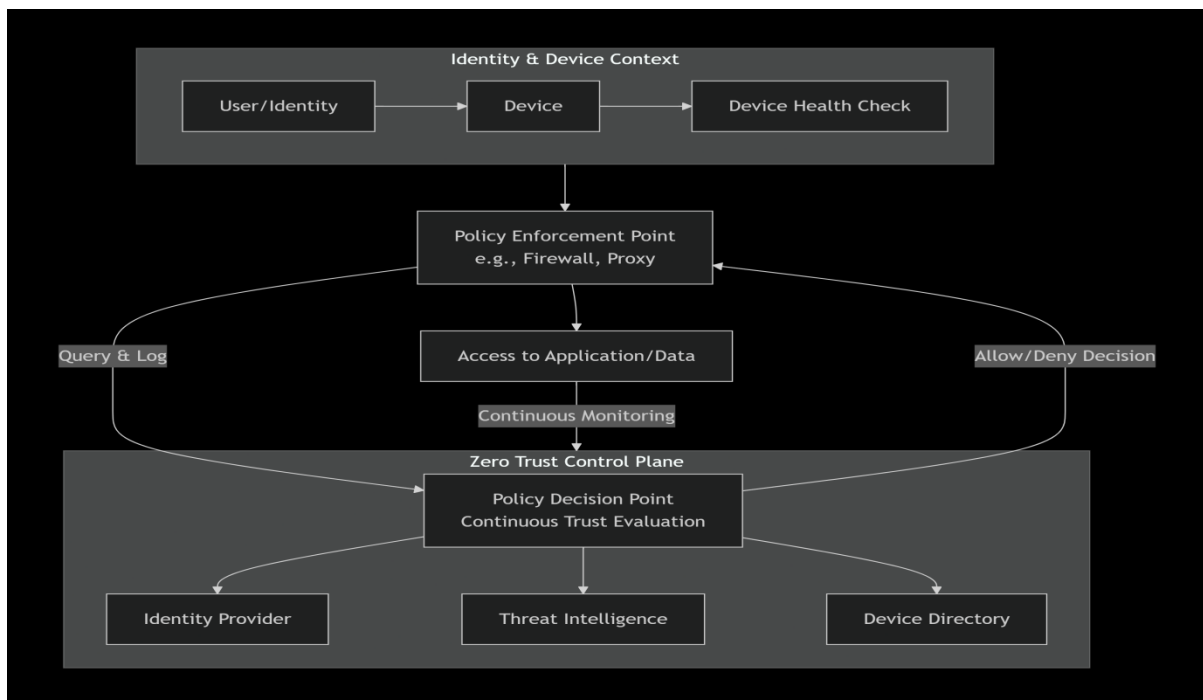
- i. The third-party vendors should uphold security requirements of VTAM and perform security assessment on an annual basis.
- ii. An official Secure Software Development Lifecycle (SDLC), which incorporates both the static and dynamic application security testing (SAST/DAST), will be embraced.
- iii. The patch management processes will focus on the remediation of the vulnerabilities listed in the CISA KEV catalog in 48 hours of their publication.

5.4. The policy of incident management

Purpose: To develop an efficient and precise system of response to the cybersecurity incidents.

Policy Statements:

- I. A specialized Incident Response Team (IRT) with well-defined roles and duties will be created.
- II. All incidents should be communicated as fast as possible through a special channel and will be handled based on a formal playbook.
- III. Internal stakeholders, clients, and regulators communication plans will be maintained and tested on a yearly basis.



6. Technical Control and Feasibility Analysis.

This section presents the specific, achievable technologies to implement the policies and curb the mentioned threats.

6.1. Identity:

Identity Security Governance and Multi-Factor Authentication (MFA).

Control: Introduce security protocols such as phishing resistance MFA (FIDO2 security keys) on all users. For instance the administrative and access to the financial systems of critical concern.

Feasibility: Cloud-based Multi-Factor Authentication services (Azure AD MFA, Okta) are affordable and they support medium-sized business including VTAM. The implementation process is easy and it gives an immediate and high security boost. NIST CSF Mapping: Identities and credentials are controlled on authorized users and devices.

6.2. Devices: Endpoint Detection and Response (EDR).

Control: Implement an EDR on all corporate users and owner endpoints. EDR is also superior to traditional antivirus in that it applies to behavioural analytics in order to identify and act upon advanced threats.

Feasibility: EDR has become a common industry control. There are a number of vendors that provide the solutions that apply to a mid-market company. Combat with RaaS and other malware is a mandatory investment. The principle of least privilege is included in the design of access controls and malicious codes are easily identified.

6.3. Networks: Micro-segmentation

Control: Enact micro-segmentation in the internal network to form separated areas. This will make sure that an attacker who has compromised on one system (e.g. the laptop of a user) cannot make a lateral movement to any part of the critical servers (e.g. database servers).

Feasibility: With software-defined networking (SDN) available in both a current firewall and a cloud platform, micro-segmentation is not possible without a complete network overhaul. It can be staged with those that are most critical being done first.

6.4. Applications & Data Cloud Security Posture Management (CSPM) and Data Loss Prevention (DLP).

Control: Deploy a CSPM tool to maintain constant cloud environments (e.g., AWS, Azure) checks to determine misconfigurations. Implement a DLP solution to detect, track and secure sensitive data.

Feasibility: CSPM is mandatory to all cloud adoption and is a characteristic of most cloud security providers. DLP solutions are full-fledged and can be combined with email and endpoint channels. These are both possible and essential to a financial services company.

6.5. Infrastructure: Immutable Back-ups and Strong Patch Management.

Control: Have immutable (can neither be modified nor removed) and isolated backups of all critical data. Implement a strict patch management procedure; it is based on the CISA KEV catalog.

Feasibility: Immutable backup storage is a service that is provided by most backup vendors and is a very low-cost ransomware recovery tool.

7. Monitoring and Incident Response

The development of a proactive security stance requires 24/7 round-the-clock surveillance and a well-planned response.

Architecture:

A Security Information and Event Management (SIEM) will be implemented to consolidate and correlate any logs generated by all the critical systems, including Endpoint Detection and Response (EDR), firewalls, Multi-Factor Authentication (MFA), cloud platforms and other relevant assets. This will be followed by integration with a Security Orchestration, Automation, and Response (SOAR) platform that will be used to automate response activities.

SIEM/SOAR Incident Response Flow Chart



Figure 2: Incident Response Process Flow, illustrating the integration of SIEM detection and SOAR automation for rapid containment and eradication.

The Incident Response Plan (Based on NIST CSF Respond Function):

Preparation :

The Incident Response Team (IRT) will ensure that it will have detailed playbooks and communication plans. Tabletop drills, imitating ransomware attacks and Business Email Compromise (BEC) attacks, will be performed on a regular basis.

Detection and Analysis (SIEM/SOAR):

The SIEM system relates events (e.g. a user clicking on a phishing link and then malicious outbound traffic is detected to have been generated by the same device). An alarm is then raised and sent to the security staff. The SOAR platform is able to query the EDR automatically to get some context information.

SOAR-enhanced: Containment, Eradication & Recovery:

Short-term:

The playbook SOAR automatically de-escalates the concerned endpoint of the network to the infected endpoint, preventing subsequent lateral motion.

Long-term:

The IRT determines the root cause (e.g. a specific malware variant). The infected system is then wiped and re-constructed. The immutable backups are used to restore critical data.

Communication:

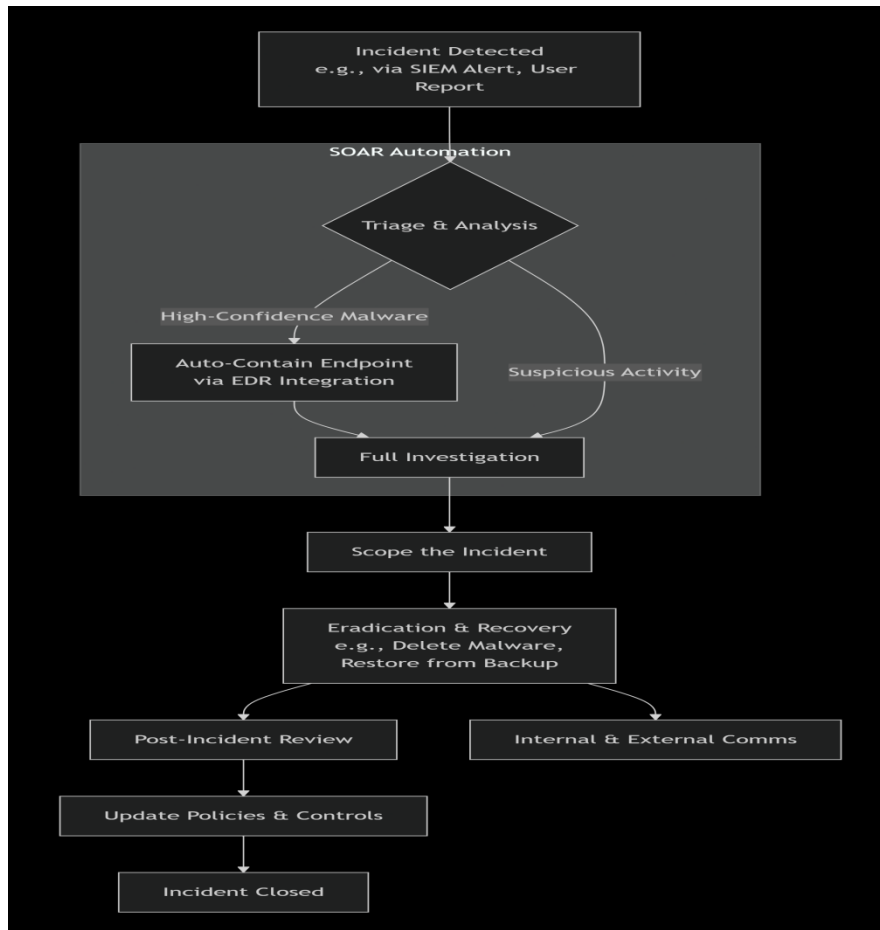
The IRT implements the communication plan that has been planned and in the case of a breach of client data, relays the information to the relevant regulators as required by financial compliance regulations.

Post-Incident Activity:

This is a comprehensive review to come up with lessons learned. The security controls and playbooks are updated to prevent repeat occurrence.

8. Training and Awareness Programme

It is during the training that the participants will be sensitised on the importance of food safety. Technology cannot be used in isolation, developing a security-conscious culture is the final line of offense. The VTAM programme should go beyond annual and training based on compliance.



Constant, Interactive Security Culture Programme:

i. Phishing and Vishing Simulation Platform:

It will have a platform where simulated phishing emails and vishing calls are released to employees regularly and randomly. Those users which fail these simulations will be automatically registered on a short and targeted training module, hence supplying constant reinforcement and measurable measures in terms of the vulnerability of the organisation.

ii. Role-Based Training:

Training information will be role based:

iii. Executive Training:

Focuses on the financial and reputational consequences of cyber threats, BEC, and executive at governance.

iv. Training on Finance Department:

Gives an insight into wire fraud, vendor email compromise and process of verifying payment.

v. IT & Development Training:

Focuses on secure coding methods, cloud design, and incident reporting.

vi. Gamification and Positive Reinforcement:

The employees will be encouraged to report suspicious emails, do training modules and keep a perfect simulation record to be rewarded by a points based system to encourage positive competition and interaction.

vii. Microlearning:

Every once in a while, training is reinforced with a short video or newsletter on one topic, e.g., on how to spot AI-generated phishing or how to secure your home router.

viii. Measures of Success:

Program effectiveness will be assessed using the click-through rate on phishing simulations, the response time of the incident report, and the results of annual knowledge tests. The goal is a measurable annual reduction of human-risk measures.

9. Conclusion

The advanced cyber threats that face Vigilant Trust and Asset Management (VTAM) require a radical change in the approach of its security. The old model of perimeter based no longer works, as it has been shown by the recent cases. This report provides a highly detailed, practical, and supported model based on the principle of Zero Trust, which is to never trust, always verify. The layered approach outlined in the present work can assist VTAM in becoming significantly more resilient through adopting the modern policies, aligned with NIST and ISO 27001, applying viable technical controls, including MFA, EDR, and SIEM/SOAR, and upholding the culture of continuous security awareness. This plan is in line with the Board mandate, which protects the most crucial assets of the firm and this is client data, financial

stability and hard-earned reputation. Investment in this new security model is not only an IT investment, but a key business requirement that must pass to maintain client confidence and help VTAM remain sustainable in an ever-increasing unfriendly digital environment.

References

- [1] ENISA. (2023). ENISA Threat Landscape 2023. European Agency on Cybersecurity.
- [2] Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology.
- [3] NIST. (2018). Cybersecurity of Critical Infrastructure Framework Version 1.1. National Institute of Standards and Technology.
- [3] ISO/IEC. (2022). Information security, cybersecurity and privacy protection — Information security management systems- Requirements, ISO/IEC 27001:2022. International Organization Standardisation.
- [4] CISA. (2023). CISA Alert: Threat Actors Play on MOVEit Vulnerability. Cybersecurity and Infrastructure Security Agency. AA23-158A.
- [5] CISA. (2023). Exploited Vulnerabilities Known Catalog. Cybersecurity and Infrastructure Security Agency. <https://known-exploited-vulnerabilities-catalog>.
- [6] NCSC-UK & CISA. (2023). Joint Cybersecurity Advisory: Critical Infrastructure Ransomware Foundation. AA23-129A.
- [8] proofpoint. (2023). 2023 Social Engineering Report. Proofpoint, Inc.