

Networks and Cyber Security Essentials (ACCA4024)

Marvin Alexander Valencias Alfaro
ID 2501143 | LECTURER: MUNYARADZI N MURIRA

Table of Contents

Introduction: The New Reality of Financial Security	3
1. Understanding the Modern Threat Landscape	4
1.1. Ransomware as a Service (RaaS).....	4
1.2. AI Powered Social Engineering and Vishing.....	4
1.3. Supply Chain Compromises (The MOVEit Scenario).....	4
1.4. Cloud Adoption and the Hybrid Work Dilemma.....	4
2. Modern Security Policies: The Zero Trust Paradigm.....	5
2.1. Embracing Zero Trust Architecture.....	5
2.2. Alignment with the NIST Cybersecurity Framework (CSF) 2.0	6
3. Feasible Technical Mitigation Measures	6
3.1. Phishing-Resistant Multi Factor Authentication (MFA)	7
3.2. Smarter Patch Management via CISA KEV	7
3.3. Cloud Security Posture Management (CSPM)	7
3.4. Immutable Backups for Ransomware Resilience	7
4. Proactive Monitoring and Incident Response	7
4.1. Implementing SIEM and SOAR.....	8
4.2. Visualizing the Modern Security Operations Centre.....	9
5. Cultivating a Security First Human Culture	10
5.1. Engaging, Continuous Simulations	10
5.2. Role Based Security Coaching	10
5.3. Fostering a Blame Free Environment.....	10
6. Conclusion	11
References	12

Introduction: The New Reality of Financial Security

For decades, corporate cybersecurity operated on what we call the "castle and moat" methodology. We built strong firewalls around our headquarters and assumed that anyone inside the building was inherently trustworthy. However, the world has fundamentally changed. The rapid shift to hybrid work models means our employees are now accessing sensitive financial data from their kitchen tables, local coffee shops, and mobile networks. For Vigilant Trust & Asset Management (VTAM), a medium sized firm managing significant wealth, our "castle" is now everywhere, which means our "moat" is effectively gone [3], [8].

Recent security incidents have brought this reality sharply into focus. The sophisticated phishing campaign that recently bypassed our traditional email filters, along with an attempted ransomware infection, were not isolated events. They are stark indicators that threat actors are actively targeting us. The Board of Directors has rightfully mandated a modern, comprehensive security framework to address these vulnerabilities.

This report proposes the adoption of a **Zero Trust** approach. In simple terms, Zero Trust means "never trust, always verify." It is an acknowledgment that threats can originate from anywhere, even from within our own walls. Through this report, we will identify the precise threats targeting our sector, establish clear policies grounded in modern frameworks (NIST CSF and ISO 27001), propose feasible technical solutions, and outline a plan to transform our workforce from our greatest vulnerability into our strongest line of defense.

1. Understanding the Modern Threat Landscape

Before we can build a resilient defense, we must truly understand the adversaries we are facing. Today's cybercriminals are no longer lone hackers operating in basements; they are highly organized, well funded syndicates operating with corporate efficiency [1].

1.1. Ransomware as a Service (RaaS)

In the past, executing a ransomware attack required significant technical skill. Today, developers of malicious software lease their tools to less skilled criminals in exchange for a percentage of the profits [4]. This business model, known as Ransomware as a Service (RaaS), has exponentially increased the volume of attacks. Furthermore, these groups now practice "double extortion." They do not simply lock our files; they steal our sensitive client data first and threaten to publish it online if a ransom is not paid [1]. For VTAM, the financial and reputational devastation of such a leak would be catastrophic.

1.2. AI Powered Social Engineering and Vishing

The recent phishing attack that bypassed our filters succeeded because it was incredibly well crafted. We are entering an era where Artificial Intelligence (AI) can generate flawless, highly persuasive emails. More concerning is "vishing" (voice phishing). Attackers can now use brief audio samples from social media or corporate videos to create convincing "deepfakes" of executive voices [15]. Imagine a scenario where a junior finance officer receives a frantic phone call on a Friday afternoon from a voice that sounds exactly like our CEO, demanding an urgent, confidential wire transfer. Without modern verification protocols, the human instinct to obey authority can override technical safeguards.

1.3. Supply Chain Compromises (The MOVEit Scenario)

We must acknowledge that VTAM could do everything perfectly internally and still suffer a breach due to third-party vendors. The 2023 exploit of the MOVEit file transfer software serves as a sobering case study [2]. Thousands of organizations worldwide, including massive financial institutions, had their data stolen not because their own networks were weak, but because a software tool they trusted contained a critical flaw [5]. This highlights that our risk extends across our entire digital supply chain.

1.4. Cloud Adoption and the Hybrid Work Dilemma

As VTAM has embraced cloud applications (SaaS) to facilitate hybrid work, our data is dispersed across multiple external servers. A single misconfiguration in our cloud storage, or an employee logging in from an unsecured public Wi-Fi network, creates a doorway for

attackers [11]. We can no longer rely on physical office boundaries to protect our digital assets.

2. Modern Security Policies: The Zero Trust Paradigm

To navigate these threats, VTAM requires a robust governance framework. Security policies should not be seen as a set of restrictive rules designed to frustrate employees, but rather as guardrails that allow the business to move quickly and safely [7].

2.1. Embracing Zero Trust Architecture

Under our new Zero Trust Architecture (ZTA), no user, device, or application is trusted by default, regardless of whether they are sitting at a desk in our headquarters or logging in from a hotel abroad [3]. Every request to access VTAM's systems will be evaluated based on context. Who is asking for access? What device are they using? Is the device updated and free of malware? Where are they logging in from? If any of these factors seem suspicious, access is immediately denied or challenged [8].

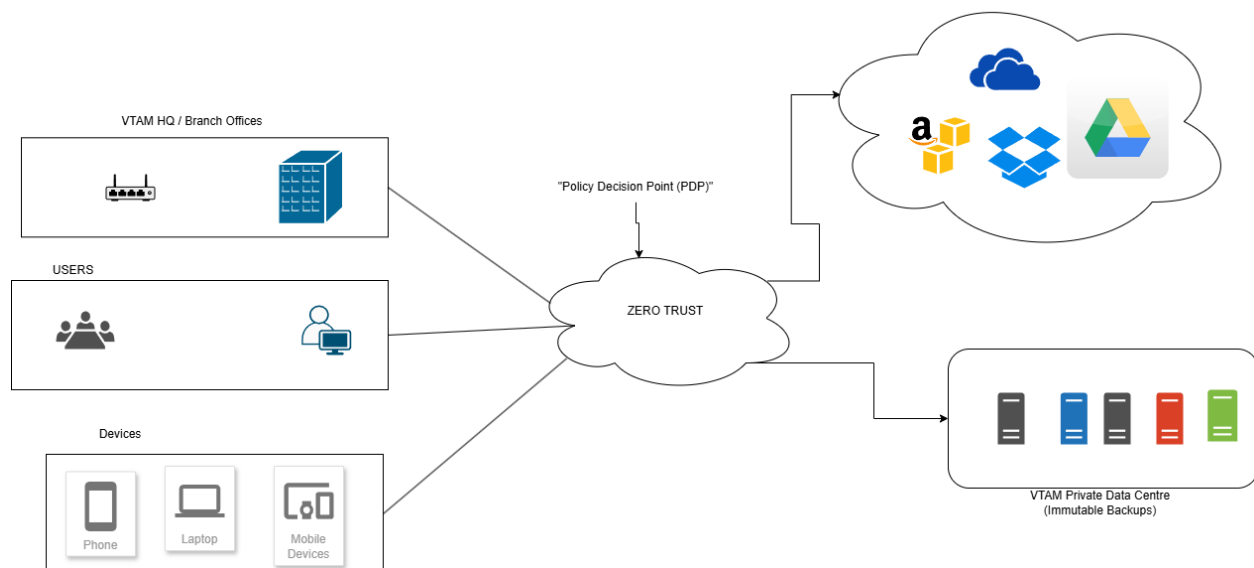


Figure 1: Zero trust diagram

"The architectural shift illustrated in Figure 1 represents the cornerstone of VTAM's new security strategy. Unlike our previous 'castle and moat' model, this **Zero Trust Exchange** acts as a rigorous gatekeeper for every single request. As the diagram shows whether an employee is logging in from our **VTAM Headquarters**, a home office, or a mobile device, their connection is not automatically trusted. Instead, every request is intercepted by the **Policy Decision Point (PDP)**.

This PDP is the 'brain' of our infrastructure. It doesn't just check if a password is correct; it evaluates a range of contextual signals such as the health of the laptop, the geographical location of the user, and the sensitivity of the data being requested. For instance, a financial analyst accessing a public cloud application like **Google Drive or Dropbox** from an unrecognized public Wi-Fi will be met with an immediate challenge for biometric authentication

2.2. Alignment with the NIST Cybersecurity Framework (CSF) 2.0

To structure our policies logically, we will adopt the globally respected NIST CSF 2.0, which breaks cybersecurity down into easily understandable core functions [6]:

- **Identify & Govern:** We cannot protect what we do not know we have. VTAM will implement a dynamic inventory of all hardware, software, and data repositories. Our access policy will strictly enforce the *Principle of Least Privilege* (PoLP) employees will only have access to the data absolutely necessary to perform their specific roles [6].
- **Protect:** We will mandate the encryption of all sensitive client data, both when it is stored on our servers ("at rest") and when it is being transmitted across the internet ("in transit").
- **Detect, Respond, and Recover:** Policies will be established to ensure continuous monitoring of our networks, ensuring that when an anomaly occurs, we have clear, rehearsed protocols to isolate the threat and recover operations without paying ransoms [12].

3. Feasible Technical Mitigation Measures

Policies are only effective if backed by solid, practical technology. The following technical measures are specifically chosen for their feasibility and high impact in mitigating the threats identified earlier.

3.1. Phishing-Resistant Multi Factor Authentication (MFA)

Traditional passwords are no longer sufficient. While VTAM currently uses some forms of Multi-Factor Authentication (like receiving a code via SMS), these are vulnerable to interception or "SIM swapping" attacks. We will upgrade to phishing-resistant MFA based on the FIDO2 standard [10]. This involves using physical security keys or biometric markers (like Windows Hello or Touch ID). Because this technology mathematically ties the authentication to the specific, legitimate website, an employee cannot be tricked into giving their credentials to a fake login page.

3.2. Smarter Patch Management via CISA KEV

IT departments are often overwhelmed by "patch fatigue," desperately trying to update software to fix thousands of theoretical vulnerabilities. To be efficient, VTAM will align its patching strategy with the **CISA Known Exploited Vulnerabilities (KEV) Catalog** [9]. Instead of guessing what to fix first, we will prioritize the specific vulnerabilities that intelligence agencies have confirmed are actively being used by hackers in the real world right now.

3.3. Cloud Security Posture Management (CSPM)

To secure our hybrid work environment, we will deploy CSPM tools. Think of CSPM as an automated auditor that constantly scans our cloud environments (like Microsoft 365 or AWS) looking for human errors such as a folder full of client financial records accidentally set to "public." It automatically corrects these misconfigurations before attackers can find them [11].

3.4. Immutable Backups for Ransomware Resilience

Our ultimate safety net against Ransomware as a Service is our backup infrastructure [4]. We will implement "Write Once, Read Many" (WORM) immutable backups. This technology creates a digital vault. Once data is written to this backup, it cannot be altered, encrypted, or deleted by anyone not even a system administrator, for a set period. If ransomware strikes VTAM, we will not need to negotiate with criminals; we will simply wipe the infected systems and restore pristine data from our immutable backups.

4. Proactive Monitoring and Incident Response

A modern security strategy assumes that, eventually, a breach will occur. The difference between a minor IT inconvenience and a catastrophic headline is how quickly we detect and respond to the intrusion [14].

4.1. Implementing SIEM and SOAR

To achieve 24/7 visibility, VTAM will deploy a **Security Information and Event Management (SIEM)** platform. The SIEM acts as the central brain of our security operations, collecting millions of event logs from our firewalls, antivirus software, and cloud applications every day. It uses machine learning to connect the dots and identify subtle patterns of a cyberattack that a human would miss.

However, detecting a threat is only half the battle. We will pair our SIEM with **Security Orchestration, Automation, and Response (SOAR)** technology [13]. SOAR acts as our automated first responder. If the SIEM detects ransomware attempting to encrypt a laptop at 3:00 AM, the SOAR platform will automatically execute a pre-written playbook to instantly disconnect that laptop from the network, preventing the infection from spreading, all before the IT team even wakes up [13].

4.2. Visualizing the Modern Security Operations Centre

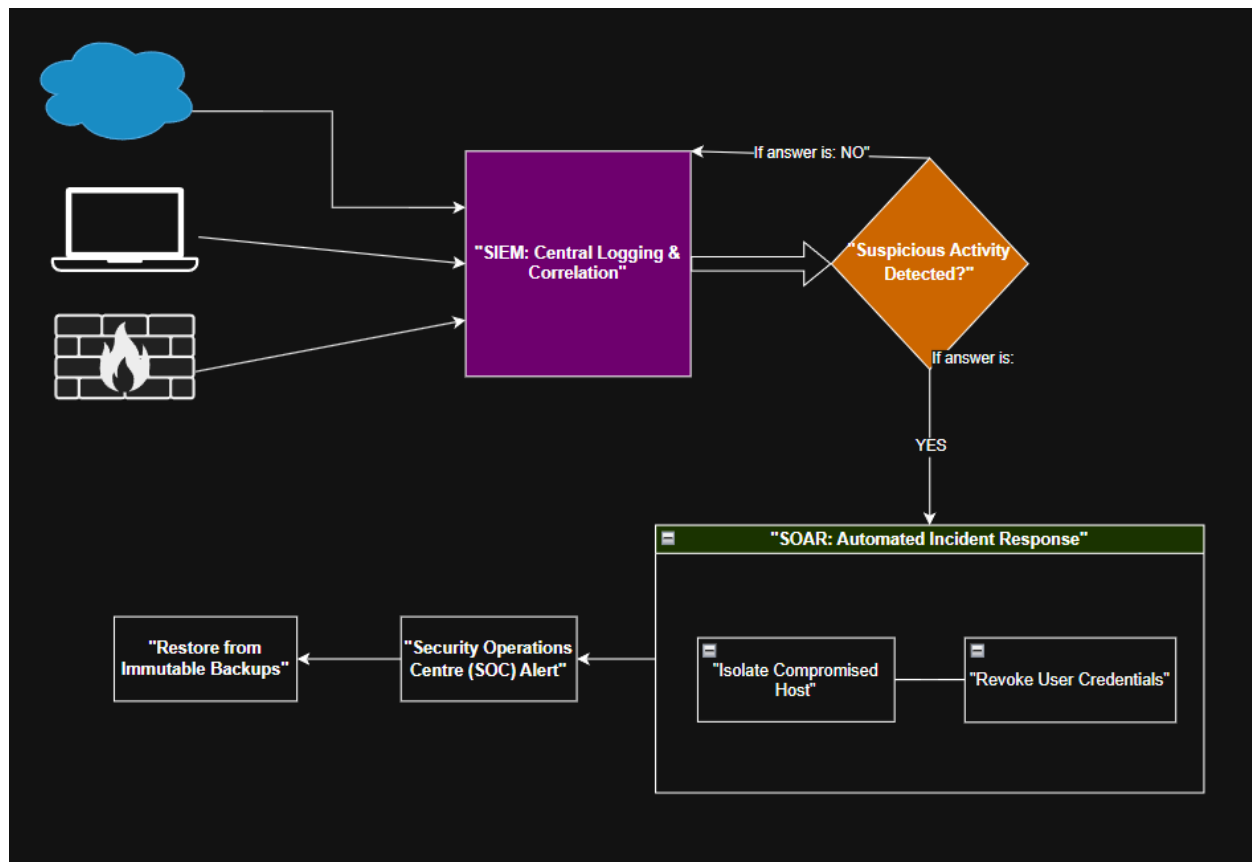


Figure 2: Automated Incident Response Flowchart illustrating the integration of SIEM for detection and SOAR for rapid containment.

To truly appreciate the value of our security model, we must look at how it handles the high-pressure reality of a cyberattack. In a traditional office environment, a 'Suspicious Activity' alert is often like a distress signal sent to an empty room it might sit unnoticed in a busy inbox for hours while a threat spreads. At VTAM, we have eliminated that dangerous silence.

As illustrated in the workflow of **Figure 2**, our SIEM and SOAR engines act as a tireless, 24/7 digital first responder. The moment a high-risk threat like ransomware is detected, the system doesn't wait for a human to clock in; it triggers an **Automated Incident Response** instantly. By isolating compromised computers and revoking access in mere seconds, we effectively quarantine the virus, keeping the 'blast radius' small and our financial data centers safe. This automation doesn't just stop the clock on an attack; it gives our human experts the breathing room they need to focus on a calm, professional recovery. By leveraging our **Immutable Backups**, we can restore business as usual with almost no disruption to our clients' day to day operations.

5. Cultivating a Security First Human Culture

For too long, the cybersecurity industry has viewed human employees as the "weakest link." At VTAM, we must shift this paradigm and empower our staff to become an active, intelligent human firewall. Traditional, compliance-driven annual training videos are ineffective against modern, emotionally manipulative attacks [15].

5.1. Engaging, Continuous Simulations

We will replace annual training with a continuous, engaging programmed [16]. Employees will receive periodic, unannounced simulated phishing emails and vishing calls based on real-world trends [15]. Crucially, the goal is not to punish employees who "fail." If an employee clicks a simulated malicious link, they are immediately presented with a brief, two-minute interactive lesson explaining what red flags they missed. This "just in time" training ensures the lesson is highly relevant and memorable.

5.2. Role Based Security Coaching

Security is not one size that fits all. Different departments face different risks, and our training will reflect this:

- **The Finance Team:** Will receive deep-dive training on Business Email Compromise (BEC) and how to verify urgent payment requests out of band (e.g., verifying an email request via a known phone number).
- **The IT Department:** Will participate in advanced tabletop exercises simulating a ransomware outbreak, testing our incident response plan under pressure.
- **The Board of Directors:** Will receive tailored briefings on regulatory compliance, the business impacts of cyber risk, and strategic crisis communication [17].

5.3. Fostering a Blame Free Environment

Finally, we must create a psychological environment where employees feel safe reporting mistakes. If an employee genuinely clicks a malicious link, hiding it out of fear of being fired allows the attacker to dwell in our systems. We will gamify cybersecurity, create leaderboards and reward departments that consistently report suspicious emails. By celebrating vigilance rather than punishing errors, we build a genuine culture of security [17].

6. Conclusion

The cyber threat landscape facing Vigilant Trust & Asset Management is formidable, but it is not insurmountable. The recent incidents serve as a timely catalyst for necessary change.

By migrating to a Zero Trust Architecture, we remove the outdated assumption of inherent trust. By aligning with the NIST CSF and prioritizing real world vulnerabilities through the CISA KEV catalog, we ensure our technical investments are highly efficient. By implementing automated SIEM/SOAR monitoring, we guarantee that our response to threats is measured in milliseconds, not days. Most importantly, by treating our employees with empathy and providing continuous, engaging education, we build a resilient organizational culture.

This proposed strategy represents a critical strategic investment. It protects not only our data and financial assets but also the foundational pillar of VTAM's business: the enduring trust of our clients.

References

- [1] ENISA, "ENISA Threat Landscape 2023," Oct. 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [2] Cybersecurity & Infrastructure Security Agency (CISA), "CISA and FBI Release Advisory on MOVE Transfer Vulnerability Exploited by CL0P Ransomware Gang," Jun. 2023. [Online].
- [3] National Institute of Standards and Technology (NIST), "Zero Trust Architecture," NIST SP 800-207, Aug. 2020. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- [4] C. J. Deepu and A. P. Vijayaraghavan, "Ransomware as a Service (RaaS): A New Dimension of Cybercrime," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, Noida, India, 2021, pp. 1-6.
- [5] CISA, "CISA and FBI Release Advisory on MOVEit Transfer Vulnerability," Jun. 2023. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>
- [6] NIST, "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024. [Online]. Available: <https://www.nist.gov/cyberframework>
- [7] International Organization for Standardization, "Information security, cybersecurity and privacy protection Management systems Requirements," ISO/IEC 27001:2022, Oct. 2022.
- [8] CISA, "Zero Trust Maturity Model Version 2.0," Apr. 2023. [Online]. Available: <https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model>
- [9] CISA, "Known Exploited Vulnerabilities Catalog," 2026. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- [10] FIDO Alliance, "FIDO2: Moving the World Beyond Passwords," 2024. [Online]. Available: <https://fidoalliance.org/fido2/>
- [11] NIST, "Guide to Adopting the Zero Trust Architecture," NIST SP 1800-35, 2024.
- [12] NIST, "Computer Security Incident Handling Guide," SP 800-61 Rev. 2, 2023. [Online].
- [13] Gartner, "Market Guide for Security Orchestration, Automation and Response (SOAR) Solutions," 2024. [Online].
- [14] CISA, "Incident Response Plan (IRP) Basics," 2025. [Online]. Available: <https://www.cisa.gov/resources-tools/resources/incident-response-plan-basics>

[15] S. J. Dodge, "Beyond the Annual Video: Effective Security Awareness Training," *Journal of Cybersecurity Education*, vol. 12, no. 2, pp. 45-58, 2024.

[16] CISA, "Security Awareness Training for Financial Institutions," 2025. [Online].

[17] NIST, "Building a Cybersecurity Culture," NIST SP 800-50 Rev. 1, 2024.