

12/17/2025

Networks and Cyber Security Essentials

Synthesize a solution to a potential real-life scenario

Networks and Cyber Security
Essentials

ACCA 4024

Student Name: Evgeni Veselinov Iliev

Student ID: 2424555

Group: 1

Lecturer's Name: Amit Naik

Table of Contents

1. Introduction and assumptions	2
2. Modern threats facing VTAM.....	2
2.1 External threats (high likelihood/high impact)	2
Ransomware-as-a-Service (RaaS).....	2
AI-powered social engineering (phishing/vishing).....	2
Software supply chain compromises	2
Known exploited vulnerabilities and patch gaps	2
Cloud and hybrid-work risks (misconfigurations + identity attacks)	3
2.2 Internal threats (often underestimated)	3
2.3 Threat mapping to attacker behaviours	3
3. Zero Trust architecture for VTAM (target state).....	3
3.1 Architecture diagram (Zero Trust)	4
4. Security policies aligned to Zero Trust, NIST CSF, and ISO 27001.....	4
5. Technical mitigation measures (feasible and mapped to threats)	5
5.1 Identity protection (top priority)	5
5.2 Endpoint and email controls	5
5.3 Cloud security controls	6
5.4 Network and application controls	6
5.5 Vulnerability management using KEV and real-world exploitation.....	6
6. Proactive monitoring and incident response (24/7)	6
6.1 SIEM + SOAR operating model.....	6
6.2 Diagram: SIEM detection-to-response flow.....	7
6.3 Incident response aligned to NIST guidance.....	7
7. Continuous training and awareness (modern + engaging)	8
8. Mapping recommendations to NIST CSF 2.0 functions	9
Conclusion.....	9
References	9
Presentation.....	10
Cisco Packet Tracer certificate	15

1. Introduction and assumptions

Cybersecurity in 2025 is not just a technical problem; it is a business survival problem. Financial services firms like **Vigilant Trust & Asset Management (VTAM)** are attractive targets because one successful compromise can lead to direct financial theft, extortion, regulatory exposure, and long-term trust damage. The move to **hybrid work** and heavier use of **SaaS and cloud** has expanded VTAM's "attack surface" beyond the traditional office network, meaning attackers now target identities, endpoints, third parties, and misconfigurations as often as they target firewalls.

For this assessment, I assume VTAM is a medium-sized firm with hybrid staff, a mix of managed and unmanaged devices, heavy SaaS usage (email/collaboration/CRM), cloud-hosted workloads, and some legacy on-prem systems. The board requires a **Zero Trust** approach: "never trust, always verify," where access decisions are based on identity, device health, risk, and least privilege rather than location on the network [1].

2. Modern threats facing VTAM

A good security framework starts with a realistic threat picture, including **external** and **internal** threats, and how they hit confidentiality, integrity, and availability (CIA triad).

2.1 External threats (high likelihood/high impact)

Ransomware-as-a-Service (RaaS)

Ransomware is no longer a niche capability. Criminal groups sell access, tooling, and "affiliate programs," which lowers the skill barrier and increases the number of attackers. Europol has described the market for ransomware/malware/phishing-as-a-service as growing and increasingly "industrial" in nature [2]. Even when law enforcement disrupts major groups (e.g., LockBit), the model persists because affiliates migrate and rebrand quickly [3].

AI-powered social engineering (phishing/vishing)

Traditional phishing is evolving into highly convincing campaigns using generative AI and voice cloning. The FBI has warned that criminals use AI to craft believable voice and video messages and to scale fraud against businesses [4]. The risk for VTAM is not only credential theft, but also **helpdesk/social-engineering bypass of MFA**, vendor invoice fraud, and "CEO voice" vishing aimed at urgent transfers or password resets.

Software supply chain compromises

VTAM is exposed through vendors, managed service providers, SaaS integrations, and widely used software. The MOVEit Transfer exploitation shows how a single mass-exploited vulnerability in a common third-party product can lead to widespread data theft and extortion [5]. This is exactly the kind of "blast radius" event financial firms must plan for.

Known exploited vulnerabilities and patch gaps

Attackers routinely target vulnerabilities already proven exploited. CISA's **Known Exploited Vulnerabilities (KEV) Catalog** exists to help organizations prioritize patching based on real-world exploitation [6]. In practice, many firms still patch by "CVSS score" alone, which can misallocate effort—high CVSS does not always equal high exploitation risk.

Cloud and hybrid-work risks (misconfigurations + identity attacks)

ENISA continues to highlight ransomware, availability attacks, and threats against data as prime issues, and it emphasizes that real-world incidents increasingly combine technical exploitation with operational weaknesses (like poor configuration control) [7]. For finance specifically, ENISA notes the sector is among the most targeted, with significant potential for disruption and trust impact [8].

2.2 Internal threats (often underestimated)

Insider risk (malicious or negligent): Data mishandling, unauthorized sharing, and “shadow IT” can bypass controls. In financial services, even small leaks (client documents, portfolio data, ID verification scans) can trigger serious compliance consequences.

Compromised internal identities: The most common “internal” threat is an external actor using valid credentials. This is why Zero Trust is identity-centric, and why strong monitoring and conditional access are essential [1].

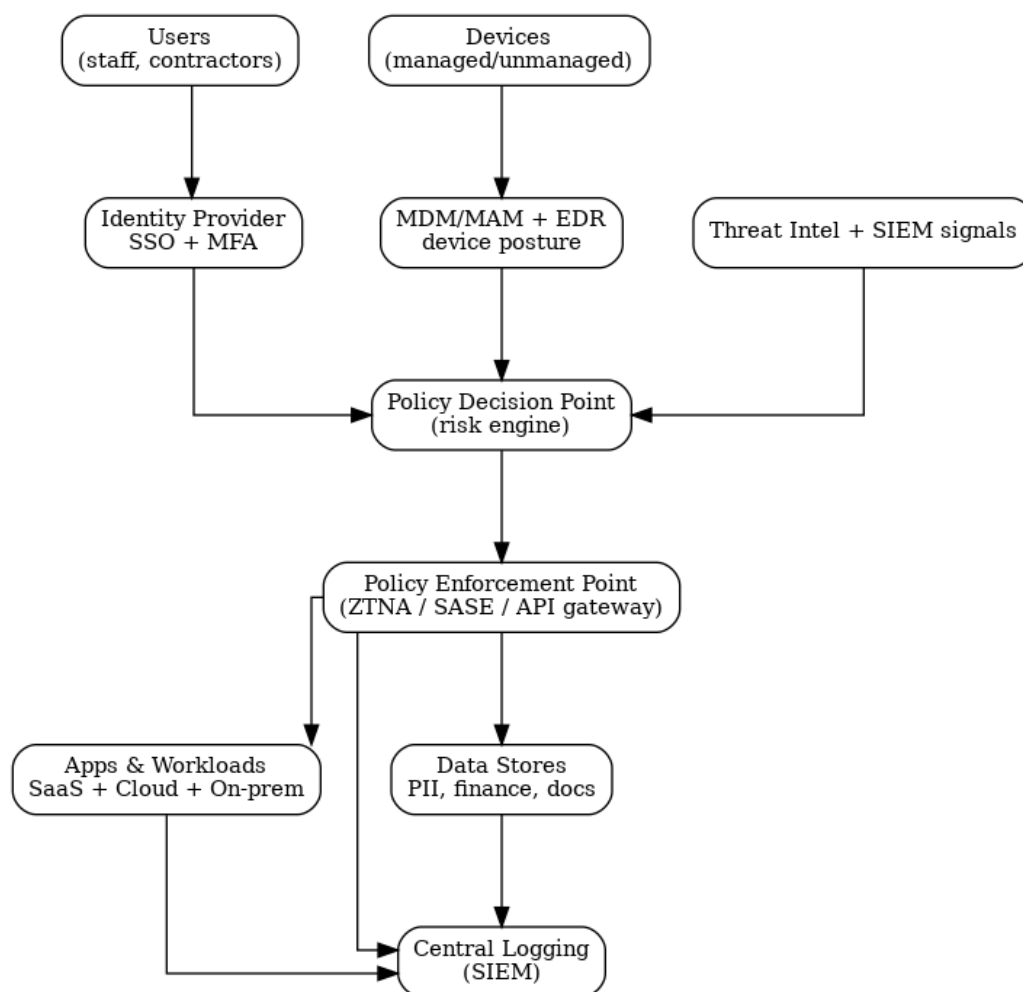
2.3 Threat mapping to attacker behaviours

Using a common language like **MITRE ATT&CK** helps VTAM link threats to detection use-cases (e.g., credential access, lateral movement, data exfiltration, impact) and avoid “checkbox controls” that look good but don’t detect real attacker patterns [9].

3. Zero Trust architecture for VTAM (target state)

Zero Trust is not a single product. It is an operating model where every access request is continuously evaluated using identity, device posture, and risk signals, enforced through strong policy controls [1].

3.1 Architecture diagram (Zero Trust)



Why this matters for VTAM:

1. It reduces reliance on “being inside the network” as a trust factor.
2. It makes access decisions risk-based (e.g., deny impossible travel, block unmanaged devices from finance apps).
3. It supports hybrid work without opening wide VPN tunnels that attackers love to abuse.

4. Security policies aligned to Zero Trust, NIST CSF, and ISO 27001

Policies are how the board’s intent becomes day-to-day behaviour. VTAM should develop a concise policy set that aligns with **NIST CSF 2.0** (Govern, Identify, Protect, Detect, Respond, Recover) [10] and can be supported by an ISO 27001-style management system (risk assessment, scope, auditability) [11].

Recommended core policies:

1. **Identity & Access Management Policy:** SSO for all apps, MFA everywhere, least privilege, periodic access reviews, privileged access management (PAM) for admins.
2. **Device Security & Remote Work Policy:** baseline hardening, encryption, EDR required, clear rules for BYOD, device compliance checks before access.
3. **Data Classification & Handling Policy:** classify client/PII/financial data, define approved storage/sharing, enforce retention and secure disposal.
4. **Vulnerability & Patch Management Policy:** risk-based patching with KEV priority; defined SLAs for critical exploited issues [6].
5. **Logging & Monitoring Policy:** what logs must be collected, retention periods, and escalation rules.
6. **Incident Response Policy:** roles, decision authority, evidence handling, communications, and post-incident learning, aligned to NIST incident guidance [12].
7. **Third-Party Risk Management Policy:** supplier onboarding, security requirements, contracts (logging, breach notification SLAs), and periodic reassessments—especially for SaaS and MSPs.

Policies should not be written as “perfect rules” that nobody follows. VTAM should keep them short, measurable, and enforceable through technical controls (e.g., conditional access enforcing remote-work rules).

5. Technical mitigation measures (feasible and mapped to threats)

5.1 Identity protection (top priority)

1. **Phishing-resistant MFA** for privileged users and finance workflows (e.g., FIDO2). This directly reduces account takeover and MFA fatigue attacks.
2. **Conditional access:** block high-risk logins, require compliant devices for sensitive apps, step-up authentication for unusual behaviour.
3. **PAM:** separate admin accounts, just-in-time access, session recording for critical systems.
CIA impact: increases confidentiality and integrity by reducing unauthorized access.

5.2 Endpoint and email controls

1. **EDR** on endpoints + server workloads; centralized alerting into SIEM.
2. **MDM/MAM** for mobile; block copy/paste or downloads from sensitive apps to unmanaged spaces.
3. **Hardened email posture:** stronger filtering, attachment sandboxing, DMARC alignment (where possible), and disabling legacy authentication.
Why: phishing is still the “front door,” even when the real target is ransomware or data theft.

5.3 Cloud security controls

1. **CSPM (Cloud Security Posture Management)**: continuous checks for misconfigurations (public storage, overly permissive IAM, insecure security groups).
2. **CASB/SaaS security posture**: monitor risky sharing, OAuth app abuse, and unusual downloads.
3. **Key management + encryption**: enforce encryption at rest and in transit; protect secrets using a vault/HSM approach for critical keys.

5.4 Network and application controls

1. **ZTNA/SASE** to replace broad VPN access; micro-segment access by application rather than network.
2. **Web application firewall (WAF) + API gateway controls** for customer-facing services.
3. **Secure SDLC and dependency controls**: software supply chain scanning and approval gates, reflecting MITRE supply chain techniques [9].

5.5 Vulnerability management using KEV and real-world exploitation

1. Integrate scanners with asset inventory; tag internet-facing assets; patch **KEV-listed vulnerabilities first** with strict timelines [6].
2. Maintain an “exposure list” for third-party products commonly exploited (like file transfer platforms), with emergency patch procedures informed by lessons from MOVEit-type events [5].

This is where many firms fail—patching is treated as routine IT work rather than an urgent risk control tied to exploitation reality.

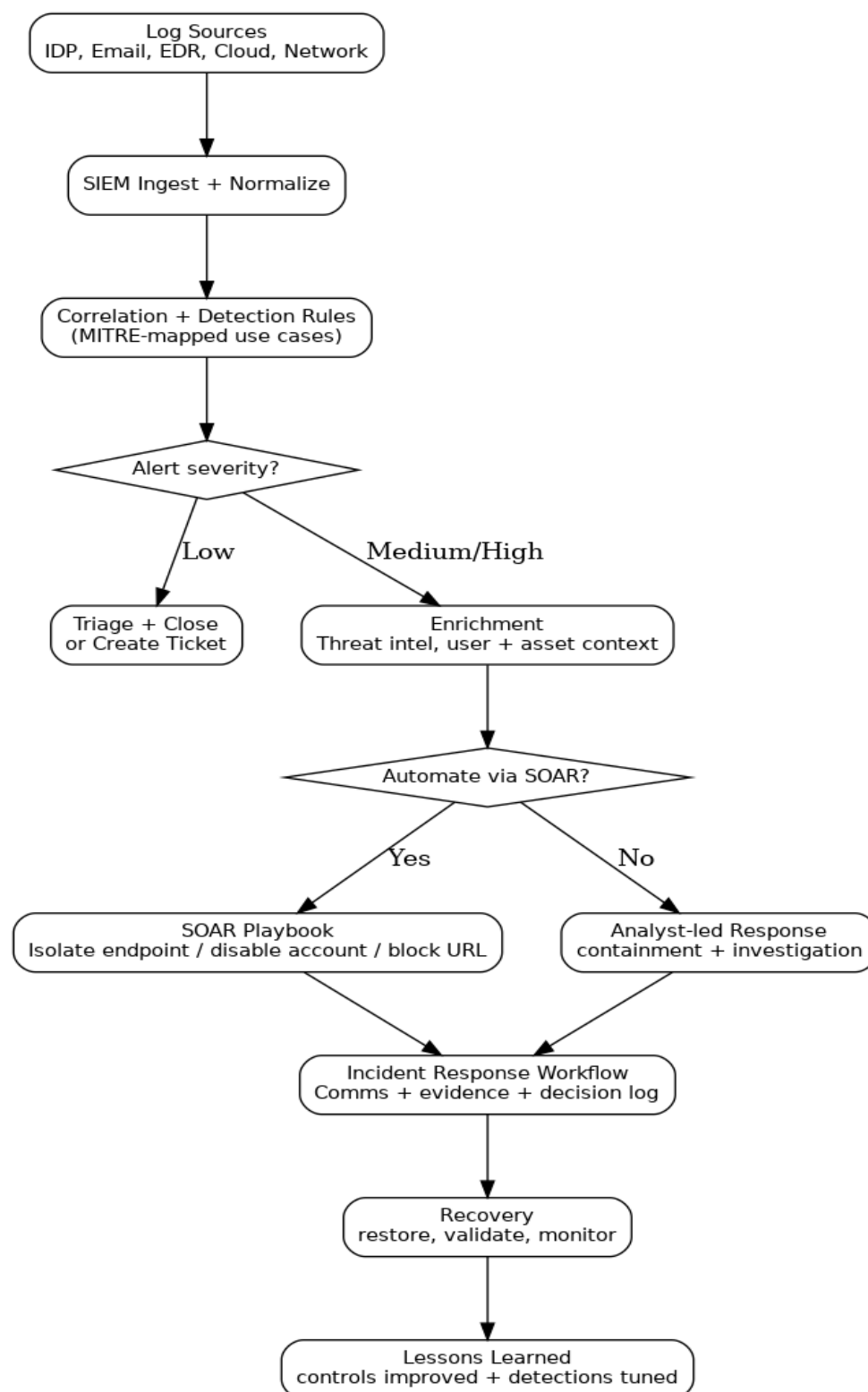
6. Proactive monitoring and incident response (24/7)

If VTAM only focuses on prevention, it will eventually lose. The goal is to detect quickly, contain faster, and recover cleanly.

6.1 SIEM + SOAR operating model

1. Centralize logs from: identity provider, email, endpoints, cloud, network devices, key applications, and critical databases.
2. Build detection rules mapped to MITRE techniques (e.g., impossible travel, token theft, mass file encryption, suspicious OAuth grants).
3. Use **SOAR** for repeatable containment actions: isolate endpoint, disable account, block URL/domain, revoke sessions, quarantine mailbox.

6.2 Diagram: SIEM detection-to-response flow



6.3 Incident response aligned to NIST guidance

VTAM should align its IR lifecycle to recognized guidance (preparation → detection/analysis → containment/eradication/recovery → lessons learned), using NIST's incident handling recommendations as a baseline [12].

Key components:

1. **Playbooks** for phishing/BEC, ransomware, cloud credential compromise, and third-party breach notification.
2. **Evidence handling and decision logs** (important for financial regulators and legal defensibility).
3. **Backup strategy**: immutable backups, periodic restore testing, and defined RTO/RPO for critical services (because ransomware recovery often fails due to untested restores).

24/7 reality: VTAM can combine a small internal security team with an MDR/MSSP for round-the-clock monitoring. What matters is not the org chart, but the SLA: who acknowledges alerts, how quickly containment happens, and how escalation works.

7. Continuous training and awareness (modern + engaging)

Security culture is built the old-fashioned way: repetition, clarity, and accountability—yet it must match modern threats.

A strong VTAM program should include:

1. **Monthly micro-learning** (5–10 minutes) tied to real attacker methods (credential phishing, MFA fatigue, invoice fraud, vishing).
2. **Phishing simulations** with targeted coaching (not shame).
3. **Vishing drills**: scripted “helpdesk reset” attempts and “urgent payment” calls—because AI voice fraud is rising and feels more real than email [4].
4. **Tabletop exercises** quarterly: MOVEit-style supplier breach, ransomware outbreak, cloud token theft. The goal is to train decisions, not just tools.
5. **Metrics that matter**: click rate, reporting rate, time-to-report, time-to-contain, and repeated-risk users supported by additional coaching.

Awareness training fails when it becomes a box-ticking exercise. VTAM should reward reporting and transparency, because early reporting is often the difference between a contained incident and a full-scale breach.

8. Mapping recommendations to NIST CSF 2.0 functions

NIST CSF 2.0 provides a practical structure to ensure the framework is balanced, not overly focused on “Protect” only [10].

1. **GOVERN:** policies, risk ownership, supplier standards, security KPIs for the board.
2. **IDENTIFY:** asset inventory, data classification, third-party mapping, exposure list.
3. **PROTECT:** MFA, ZTNA, EDR, encryption, secure configuration baselines.
4. **DETECT:** SIEM coverage, MITRE-mapped detections, anomaly monitoring, threat intel.
5. **RESPOND:** SOAR playbooks, IR procedures, comms plan, evidence handling [12].
6. **RECOVER:** tested backups, recovery validation, post-incident improvements.

Conclusion

VTAM’s most realistic risk is not a single “super-hacker,” but the steady pressure of scalable cybercrime: RaaS affiliates, AI-boosted social engineering, exploitation of known vulnerabilities, and third-party compromise. A **Zero Trust** approach gives VTAM a defensible, modern foundation because it treats identity, device trust, and risk signals as the real perimeter [1]. However, Zero Trust only works when it is paired with disciplined basics: KEV-driven patching [6], strong monitoring and incident response [12], and continuous training that reflects how attacks happen today [4].

In short: VTAM should build a security program that is measurable, enforceable, and practiced—because in financial services, resilience is not optional; it is the price of trust.

References

- [1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” *NIST Special Publication 800-207*, 2020. nvlpubs.nist.gov
- [2] Europol, “Internet Organised Crime Threat Assessment (IOCTA) 2024,” 2024. [Europol+1](https://www.europol.europa.eu)
- [3] Europol, “Law enforcement disrupts world’s biggest ransomware operation (LockBit),” 2024. [Europol](https://www.europol.europa.eu)
- [4] Federal Bureau of Investigation (FBI), “FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence,” 2024. [Federal Bureau of Investigation](https://www.fbi.gov)
- [5] CISA, “#StopRansomware: CL0P Ransomware Gang Exploits MOVEit Transfer Vulnerability,” 2023. [cisa.gov+2](https://www.cisa.gov)[cisa.gov+2](https://www.cisa.gov)
- [6] CISA, “Known Exploited Vulnerabilities (KEV) Catalog,” ongoing. [cisa.gov+1](https://www.cisa.gov)
- [7] ENISA, “ENISA Threat Landscape 2024,” 2024. [enisa.europa.eu+1](https://www.enisa.europa.eu)
- [8] ENISA, “ENISA Threat Landscape: Finance Sector (Finance TL 2024),” 2025. [enisa.europa.eu](https://www.enisa.europa.eu)
- [9] MITRE, “MITRE ATT&CK® Enterprise Matrix,” ongoing. attack.mitre.org
- [10] NIST, “The NIST Cybersecurity Framework (CSF) 2.0,” 2024. nvlpubs.nist.gov
- [11] ISO, “ISO/IEC 27001:2022 — Information security management systems,” 2022. [ISO](https://www.iso.org)
- [12] NIST, “Computer Security Incident Handling Guide (SP 800-61 Rev. 3),” 2025. [nvlpubs.nist.gov+1](https://nvlpubs.nist.gov)

Presentation

Cyber Resilience Program for VTAM

Zero Trust roadmap - translating technical risk into business impact

Financial

- Losses from fraud and extortion
- Regulatory penalties and remediation
- Higher insurance and capital drag

Operational

- Outages in servicing
- Delayed settlements and reporting
- Incident-driven staff diversion

Reputational

- Client trust erosion
- Brand damage from data leaks
- Partner and auditor scrutiny

Prepared for: Board of Directors | Prepared by: IT Security Manager | Date: Dec 2025

Confidential - Vigilant Trust & Asset Management (VTAM)

Executive takeaway

10-minute board brief

What the board needs to know (in one slide)

RISK POSTURE

High exposure: identity + ransomware

PRIMARY PATHWAY

Phishing/vishing -> stolen identity

STRATEGIC RESPONSE

Zero Trust + 24/7 response

Bottom line

- Our controls were bypassed (phishing) and ransomware was attempted - this will happen again.
- The business risk is client harm, regulatory exposure, and operational disruption - not just IT downtime.
- A phased Zero Trust program reduces likelihood and blast radius, and improves recovery speed (resilience).

What you will be asked to approve today

- Sponsor Zero Trust as the enterprise security strategy (12-month roadmap).
- Fund the 90-day priority controls (identity, endpoint, patching, backups, monitoring).
- Hold leadership accountable through KPIs (MTTD/MTTR, patch SLA, training effectiveness).

Confidential - Vigilant Trust & Asset Management (VTAM)

Modern threats (and why they matter to the business)

Threat landscape

Threats impacting financial firms are scaling - especially identity, ransomware, and supply-chain events.

Ransomware-as-a-Service (RaaS)

- Affiliate model increases attacker volume
- Disruption and extortion costs (including recovery)
- Often paired with data theft (double extortion)

AI-powered phishing and vishing

- More believable lures and voice impersonation
- Targets helpdesk resets and finance approvals
- Scales social engineering at low cost

Supply chain compromise (example: MOVEit)

- Single vendor flaw can enable mass data theft
- Third-party incident becomes our incident
- Regulatory and client notification exposure

Cloud and hybrid-work misconfigurations

- Identity becomes the new perimeter
- Misconfigured access can expose sensitive data
- Shadow IT and unmanaged devices increase risk

Confidential - Vigilant Trust & Asset Management (VTAM)

What this means for VTAM

From incidents to exposure

Recent events are signals, not anomalies

A sophisticated phishing campaign bypassed controls, and ransomware was attempted. The same pathway can lead to:

Material business impact if the chain completes: client data exposure • disruption • financial loss • regulatory action



Where Zero Trust helps

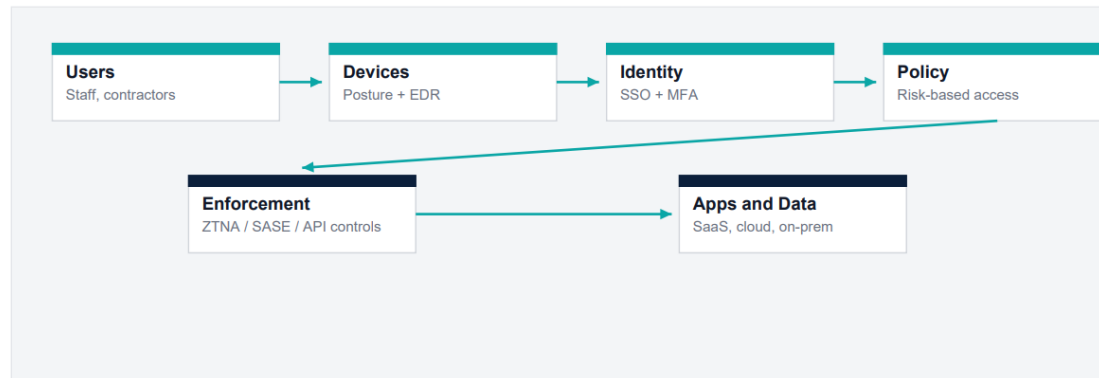
- Stops trusted-network assumptions; every request is verified.
- Reduces blast radius through least privilege and segmentation.
- Detects faster and recovers cleaner (resilience).

Confidential - Vigilant Trust & Asset Management (VTAM)

Zero Trust strategy (how we reduce risk)

Architecture overview

Zero Trust is a strategy: verify explicitly, use least privilege, assume breach.



Core pillars (what we invest in)

Identity	Device	Access	Data
MFA - least privilege	EDR - compliance gates	ZTNA - segmentation	DLP - encryption - backups

Confidential - Vigilant Trust & Asset Management (VTAM)

90-day priorities (fast risk reduction)

Actions + business outcomes

These controls reduce the probability of a material incident and limit blast radius if one occurs.

Investment	Risk reduced	Business outcome	Early KPI
Phishing-resistant MFA + conditional access	Account takeover, vishing helpdesk bypass	Fewer successful identity compromises	MFA coverage > 98% (privileged)
Endpoint hardening + EDR everywhere	Ransomware execution, lateral movement	Stops and contains malware earlier	EDR coverage 100% corp devices
KEV-driven patching + external exposure review	Exploitation of known-vulnerable systems	Closes the known-open-door class of risk	KEV patches within SLA (e.g., 7-14)
Immutable backups + recovery tests	Extortion + prolonged outages	Faster restore; stronger negotiating position	Quarterly restore tests for Tier-1 apps
Email + SaaS posture (DMARC, sandbox, OAuth controls)	Phish delivery + SaaS account abuse	Reduces phishing success and data leakage	High-risk OAuth apps blocked; DLP

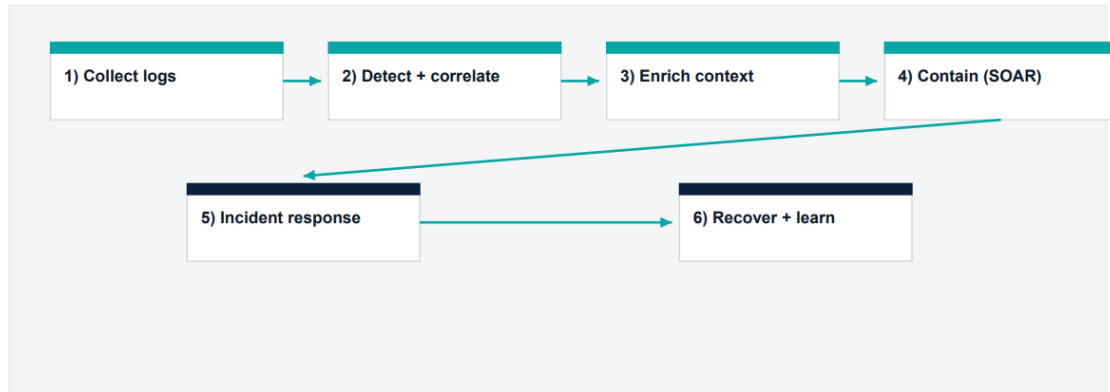
Prioritization is driven by real-world exploitation (CISA KEV) and our incident pattern (phishing/ransomware).

Confidential - Vigilant Trust & Asset Management (VTAM)

24/7 monitoring and rapid response

SIEM + SOAR

Goal: detect fast, contain faster, recover cleanly - minimizing downtime and client impact.



Operating model (practical)

- Hybrid SOC: internal team + MDR partner (24/7)
- SOAR playbooks: phishing, ransomware, cloud compromise
- Monthly board metrics: MTBD/MTTR and trends

Board KPIs (examples)

- MTBD / MTTR trending down
- Percent critical log sources onboarded
- High-severity incidents contained within SLA

Confidential - Vigilant Trust & Asset Management (VTAM)

People + governance (making resilience stick)

Training & accountability

Technology reduces risk; culture determines whether it stays reduced.

Continuous training program (modern + engaging)

- Monthly micro-learning (5-10 min) tied to current scams
- Quarterly phishing simulations with coaching (no blame)
- Vishing drills: helpdesk reset and urgent payment scenarios
- Tabletop exercises: ransomware, cloud compromise, vendor breach
- Report-and-reward culture: fast reporting is a control

Governance guardrails

- Clear data classification
- Third-party security requirements
- Access reviews for critical systems
- Policy and audit readiness

Success metrics

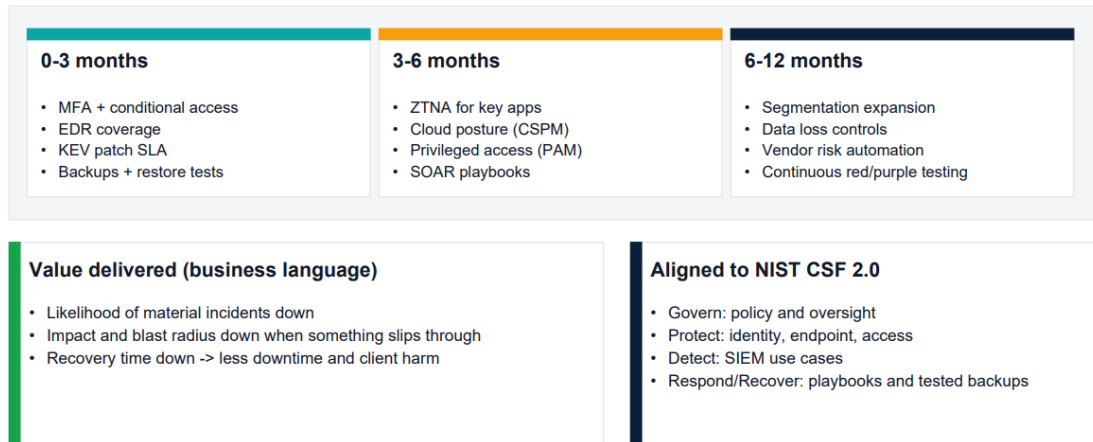
- Reporting rate up; click rate down
- Time-to-report improves
- Repeat-risk users coached
- Audit findings trend down

Confidential - Vigilant Trust & Asset Management (VTAM)

12-month roadmap (phased investment in resilience)

Strategy -> execution

We deliver value in phases: reduce the most likely risks first, then harden and mature.



Confidential - Vigilant Trust & Asset Management (VTAM)

Board decisions & oversight

What we need from you

Requested approvals



Strategic intent: reduce the likelihood, impact, and duration of cyber incidents - protecting clients, operations, and trust.
Thank you. Questions?

Confidential - Vigilant Trust & Asset Management (VTAM)

Cisco Packet Tracer certificate

