

11/13/2025

# Networks and Cyber Security

## Assignment 01

"Comprehensive Cybersecurity Framework  
for Vigilant Trust & Asset Management: Zero Trust  
Implementation"

Module Name: Networks and Cyber  
Security

Module Code: ACCA4024

Student Name: Anton Romanov

Student ID: 2430682

Group: 2

Lecturer's Name: Amit Naik

## Contents

|                                                                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----|
| <b>IDENTIFY: Asset Inventory and Threat Landscape Analysis</b> .....                                                                                | 1  |
| Critical Assets and Business Context.....                                                                                                           | 1  |
| Current and Emerging Threat Landscape.....                                                                                                          | 1  |
| External Threats .....                                                                                                                              | 1  |
| Internal Threats .....                                                                                                                              | 2  |
| Risk Assessment and Prioritization .....                                                                                                            | 2  |
| Critical Risks (Immediate Action Required): .....                                                                                                   | 2  |
| High Risks: .....                                                                                                                                   | 3  |
| Regulatory Context .....                                                                                                                            | 3  |
| Key Findings - IDENTIFY Phase:.....                                                                                                                 | 3  |
| <b>PROTECT: Security Policies and Technical Controls</b> .....                                                                                      | 4  |
| Zero Trust Architecture Foundation .....                                                                                                            | 4  |
| 1. Identity and Access Management (IAM) .....                                                                                                       | 6  |
| 2. Network Security and Segmentation .....                                                                                                          | 6  |
| 3. Data Protection .....                                                                                                                            | 7  |
| 4. Cloud Security .....                                                                                                                             | 7  |
| 5. Vulnerability and Patch Management .....                                                                                                         | 8  |
| 6. Backup and Business Continuity.....                                                                                                              | 8  |
| 7. Email and Web Security.....                                                                                                                      | 8  |
| Implementation Summary.....                                                                                                                         | 9  |
| SIEM Diagram .....                                                                                                                                  | 10 |
| <b>DETECT: Proactive Monitoring and Threat Detection</b> .....                                                                                      | 14 |
| Overview .....                                                                                                                                      | 14 |
| SIEM Implementation (Splunk Enterprise Security) .....                                                                                              | 14 |
| Detection Use Cases .....                                                                                                                           | 15 |
| Alert Management and Escalation .....                                                                                                               | 16 |
| 24/7 Security Operations.....                                                                                                                       | 16 |
| <b>NIST CSF Mapping: DETECT</b> (DE.AE: Anomalies and events detected, DE.CM: Security continuous monitoring, DE.DP: Detection processes) [1] ..... | 17 |
| <b>RESPOND: Incident Response and Crisis Management</b> .....                                                                                       | 17 |

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Incident Response Framework .....                               | 17 |
| Response Procedures by Incident Type .....                      | 17 |
| Escalation and Communication .....                              | 18 |
| <b>RECOVER: Business Continuity and Disaster Recovery</b> ..... | 19 |
| Recovery Strategy .....                                         | 19 |
| Recovery Time and Point Objectives .....                        | 19 |
| Backup Architecture (3-2-1-1-0 Rule).....                       | 19 |
| Disaster Recovery Infrastructure .....                          | 20 |
| Recovery Procedures .....                                       | 20 |
| Business Continuity Measures .....                              | 20 |
| Post-Recovery Analysis .....                                    | 21 |
| <b>CONTINUOUS TRAINING AND SECURITY AWARENESS PROGRAM</b> ..... | 21 |
| Overview .....                                                  | 21 |
| Program Components .....                                        | 21 |
| 1. Continuous Simulated Attack Campaigns.....                   | 21 |
| 2. Role-Specific Training Tracks .....                          | 22 |
| 3. Gamification and Engagement .....                            | 22 |
| 4. No-Blame Reporting Culture .....                             | 23 |
| 5. Measurement and Continuous Improvement .....                 | 23 |
| Budget and ROI.....                                             | 24 |
| Creating a Security-First Culture .....                         | 24 |
| Conclusion.....                                                 | 25 |
| References .....                                                | 25 |
| Presentation for board members:.....                            | 27 |

# IDENTIFY: Asset Inventory and Threat Landscape Analysis

## Critical Assets and Business Context

As a medium-sized financial services firm, Vigilant Trust & Asset Management (VTAM) manages sensitive client assets and processes approximately \$500M in daily transactions. The organization's critical assets requiring protection include:

### Digital Assets:

- **Client Data:** PII and financial records of 50,000 clients in AWS cloud databases
- **Trading Systems:** Real-time transaction processing platforms
- **Investment Management:** Portfolio management software with proprietary strategies
- **Communication Systems:** Email, CRM, and secure messaging platforms

### Infrastructure:

- **Hybrid Environment:** Mix of on-premises data centers and cloud services (AWS, Microsoft 365)
- **Endpoints:** 200 workstations, 150 mobile devices (BYOD and corporate)
- **Third-Party Integrations:** Payment processors, regulatory reporting systems, market data providers

The shift to hybrid work (60% remote) has significantly expanded the attack surface, eliminating traditional network perimeters.

## Current and Emerging Threat Landscape

Based on threat intelligence from CISA, NIST, and industry reports [1], [2], [10], VTAM faces sophisticated threats characteristic of financial services targets:

### External Threats

**Ransomware-as-a-Service (RaaS):** Professional criminal platforms (LockBit, BlackCat, ALPHV) enable even low-skilled attackers to deploy sophisticated ransomware with double extortion tactics - encrypting data while threatening to publish stolen client information. Average ransom demands for financial firms exceed \$5M, with total recovery costs reaching \$10M+. The recent ransomware attempt at VTAM demonstrates active targeting.

**AI-Powered Social Engineering:** Artificial intelligence has transformed social engineering attacks. AI voice cloning enables attackers to impersonate executives in

vishing calls requesting fraudulent wire transfers. Deepfake video calls can convincingly impersonate C-suite members. AI-generated phishing emails perfectly mimic writing styles and bypass traditional filters. *Case Study:* A UK financial firm lost \$25M in 2024 following a deepfake video call with an impersonated CFO.

**Supply Chain Compromises:** Attackers increasingly target software vendors and service providers (SolarWinds, MOVEit breaches) to access multiple victims simultaneously. VTAM's reliance on third-party vendors for portfolio management, trading platforms, and cloud services creates multiple attack vectors.

**Cloud-Specific Threats:** With VTAM's AWS and Microsoft 365 adoption: misconfigured S3 buckets accidentally exposing data, compromised cloud credentials providing full environment access, and shadow IT creating security blind spots.

Internal Threats

**Insider Threats:** Malicious insiders with authorized access stealing client data or facilitating external attacks, and negligent employees through poor security practices (weak passwords, clicking phishing links). Verizon's 2024 DBIR reports insider threats account for 20% of financial services breaches [3]

**Weak Access Controls:** Legacy systems with shared credentials, lack of multi-factor authentication, and excessive permissions violating least-privilege principles create vulnerability to both external and internal exploitation.

Risk Assessment and Prioritization

Using the **CIA Triad** (Confidentiality, Integrity, Availability) and **NIST CSF** framework, VTAM's critical risks are:

Critical Risks (Immediate Action Required):

| Threat                  | Likelihood  | Business Impact                                                   |
|-------------------------|-------------|-------------------------------------------------------------------|
| Ransomware Attack       | High        | \$10M+ recovery costs, operational shutdown, regulatory penalties |
| AI-Powered Wire Fraud   | Medium-High | Direct financial loss \$1M-\$25M per incident                     |
| Supply Chain Compromise | Medium      | Client data breach, system compromise, loss of trust              |

| Threat                    | Likelihood | Business Impact                        |
|---------------------------|------------|----------------------------------------|
| Phishing/Credential Theft | Very High  | Unauthorized access, data exfiltration |

### High Risks:

- Cloud misconfigurations leading to data exposure
- Inadequate patch management (CISA KEV vulnerabilities)
- Lack of visibility in hybrid work environment

## Regulatory Context

VTAM must maintain compliance with financial regulations (SOX, GLBA, SEC cybersecurity rules), data protection laws (GDPR for EU clients), and industry standards (PCI-DSS). Recent SEC cybersecurity disclosure rules (2023) require public reporting of material incidents within 4 days, increasing urgency for robust security posture.

### Key Findings - IDENTIFY Phase:

- VTAM has a complex hybrid IT environment with significant cloud adoption expanding the attack surface
- The threat landscape includes sophisticated AI-enhanced attacks specifically targeting financial services
- Recent incidents (phishing, ransomware attempt) confirm VTAM is actively targeted
- Critical risks center on ransomware, social engineering, and supply chain vulnerabilities
- Regulatory requirements demand comprehensive security controls and rapid incident response

**NIST CSF Mapping:** IDENTIFY (ID.AM: Asset Management, ID.RA: Risk Assessment, ID.BE: Business Environment)

**Next Step:** The PROTECT phase details specific security policies and technical controls aligned with principles to mitigate these identified threats.

# **PROTECT: Security Policies and Technical Controls**

## Zero Trust Architecture Foundation

VTAM will adopt a **Zero Trust security model** based on three core principles: (1) verify explicitly - always authenticate and authorize, (2) use least privilege access with Just-In-Time provisioning, and (3) assume breach - minimize blast radius through segmentation. This approach is essential given VTAM's hybrid work environment where traditional perimeter-based security is insufficient.

# VTAM Zero Trust Architecture

Vigilant Trust & Asset Management - Security Framework

✓ Never Trust, Always Verify

 Assume Breach

 Least Privilege



**Employees**  
200+ users  
MFA required



**Executives**  
Hardware tokens  
High privilege



**Partners**  
Limited access  
Monitored



**Devices**  
BYOD+Corp  
EDR protected



## Zero Trust Control Plane

### Identity & Access Control

Azure AD MFA (FIDO2) PAM RBAC JIT Access SSO

### Policy Decision Engine

Conditional Access Risk Assessment Context Analysis Allow/Deny

### Network Security

ZTNA Micro-segmentation SDP Firewalls No VPN

### Data Protection

DLP AES-256 TLS 1.3 Classification Key Mgmt

### Visibility & Analytics

SIEM SOAR UBA Threat Intel 24/7 SOC



**Cloud (AWS)**  
Client DB  
CSPM protected



**Trading**  
\$500M daily  
Hot standby



**SaaS Apps**  
M365, CRM  
CASB control



**On-Premise**  
Legacy  
Segmented

## Encrypted Communication Flow

User Request



Identity



Policy



Tunnel



Access

## Integrated Security Tools



CrowdStrike  
EDR/XDR



Proofpoint  
Email



Zscaler  
ZTNA



Wiz  
CSPM



Splunk  
SIEM



Cortex  
SOAR



CyberArk  
PAM



Veeam  
Backup

Control Plane Security Controls Data Flow Resources

# 1. Identity and Access Management (IAM)

## Multi-Factor Authentication (MFA):

- **Mandatory phishing-resistant MFA** (FIDO2 hardware tokens) for all users
- Hardware security keys (YubiKey) required for privileged accounts, executives, and financial transaction access
- SMS-based MFA prohibited due to SIM-swapping vulnerabilities
- Implementation: Microsoft Entra ID with Conditional Access policies

## Privileged Access Management (PAM):

- **Just-In-Time (JIT) access** - no standing admin privileges, elevated access granted only when needed and auto-expires
- All privileged sessions recorded and monitored
- Separate admin accounts from regular user accounts
- Solution: CyberArk or Microsoft Privileged Identity Management

## Least Privilege & RBAC:

- Zero standing privileges - users granted minimum permissions for their role
- Quarterly access reviews and automatic revocation upon role change
- Segregation of Duties (SoD) - no single person can complete critical transactions alone

**NIST CSF Mapping:** PR.AC-4, PR.AC-7

# 2. Network Security and Segmentation

## Zero Trust Network Access (ZTNA):

- Replace traditional VPN with ZTNA (Zscaler Private Access or Palo Alto Prisma Access)
- Micro-segmentation into security zones:
  - **Crown Jewels:** Trading systems, client database (highest restrictions)
  - **Corporate:** Email, collaboration tools
  - **Guest/DMZ:** Isolated networks
- Software-Defined Perimeter (SDP) - resources invisible until identity verified

## Endpoint Protection:

- EDR/XDR platform (CrowdStrike Falcon or Microsoft Defender for Endpoint)
- Automatic threat response: quarantine suspicious files, isolate infected devices
- Disk encryption (BitLocker/FileVault) on all devices
- Mobile Device Management (MDM) with containerization for BYOD

**NIST CSF Mapping:** PR.AC-5, PR.PT-1

### 3. Data Protection

#### **Data Classification & DLP:**

- Four-tier classification: Public, Internal, Confidential, Restricted
- Data Loss Prevention (DLP) prevents:
  - Emailing confidential data to external addresses
  - Uploading sensitive files to unauthorized cloud services
  - Copying client data to USB drives
- Solution: Microsoft Information Protection with automatic labeling

#### **Encryption Standards:**

- **Data at Rest:** AES-256 encryption for all databases and storage
- **Data in Transit:** TLS 1.3 minimum for all communications
- **End-to-End Encryption:** For sensitive client communications
- Key management via Hardware Security Module (HSM)

**NIST CSF Mapping:** PR.DS-1, PR.DS-2

### 4. Cloud Security

#### **Cloud Security Posture Management (CSPM):**

- Continuous monitoring for misconfigurations (Wiz, Prisma Cloud, or Microsoft Defender for Cloud)
- Automated remediation of critical issues:
  - Publicly exposed S3 buckets
  - Overly permissive IAM policies
  - Unencrypted data stores
  - Missing MFA on privileged accounts
- Infrastructure-as-Code (IaC) security scanning in CI/CD pipeline

#### **Cloud Access Security Broker (CASB):**

- All cloud access routed through CASB (Microsoft Defender for Cloud Apps or Netskope)
- Shadow IT discovery and control
- OAuth token management and session controls

**NIST CSF Mapping:** PR.IP-1, PR.DS-6

## 5. Vulnerability and Patch Management

### Prioritized Patching:

- **CISA Known Exploited Vulnerabilities (KEV) catalog** as primary priority
- Critical patches: 72 hours | High-severity: 14 days
- Weekly vulnerability scanning (Tenable or Qualys)
- Virtual patching via Web Application Firewall (WAF) for systems that cannot be immediately patched

### Third-Party Risk Management:

- All vendors undergo security assessment before contract approval
- Request SOC 2 Type II reports from cloud providers
- Monitor vendor security posture (SecurityScorecard or BitSight)
- Contractual requirement: incident notification within 24 hours

**NIST CSF Mapping:** PR.IP-12, PR.PT-4

## 6. Backup and Business Continuity

### Immutable Backup Strategy (3-2-1-1-0 Rule):

- 3 copies, 2 media types, 1 offsite, 1 offline (air-gapped), 0 errors
- **Immutable backups** in AWS S3 with Object Lock - cannot be encrypted by ransomware
- Retention: 30 days daily, 12 months monthly, 7 years compliance data
- Monthly restore drills for critical systems

### Business Continuity:

- **RTO:** 4 hours for critical systems | **RPO:** 1 hour for transaction data
- Hot standby for trading systems (active-active across AWS availability zones)
- Warm standby for databases, cold standby for non-critical systems
- Annual disaster recovery testing and tabletop exercises

**NIST CSF Mapping:** PR.IP-4, PR.IP-9

## 7. Email and Web Security

### Advanced Email Security:

- AI-powered email gateway (Proofpoint or Microsoft Defender for Office 365)

- Detection of phishing, BEC, malicious URLs/attachments, deepfakes
- DMARC reject policy to prevent domain spoofing
- External email warnings and URL sandboxing

#### Secure Web Gateway (SWG):

- Cloud-based SWG (Zscaler or Cisco Umbrella)
- DNS filtering to block malicious domains
- SSL/TLS inspection for encrypted traffic
- Threat intelligence feeds for real-time blocking

#### NIST CSF Mapping: PR.PT-4

### Implementation Summary

| Control Category   | Primary Solutions     | Timeline           | Investment     |
|--------------------|-----------------------|--------------------|----------------|
| Identity & Access  | MFA, PAM, RBAC        | 90 days            | \$100K         |
| Network Security   | ZTNA, EDR/XDR         | 120 days           | \$250K         |
| Data Protection    | DLP, Encryption       | 90 days            | \$75K          |
| Cloud Security     | CSPM, CASB            | 60 days            | \$150K         |
| Vulnerability Mgmt | CISA KEV tracking     | 30 days            | \$50K          |
| Backup & Recovery  | Immutable backups, DR | 90 days            | \$200K         |
| Email/Web Security | Advanced gateways     | 60 days            | \$125K         |
| <b>Total</b>       |                       | <b>6-12 months</b> | <b>~\$950K</b> |

**ROI Justification:** Average ransomware breach cost for financial services: \$10M+ [4] (recovery, ransom, fines, reputation damage). This \$950K investment provides comprehensive protection with estimated 85% risk reduction.

#### Standards Alignment:

- **NIST CSF:** All controls mapped to PROTECT function
- **ISO 27001:** Aligns with Access Control, Cryptography, Operations Security
- **Zero Trust:** Implements explicit verification, least privilege, assume breach
- **CISA Best Practices:** KEV catalog, immutable backups, phishing-resistant MFA

# SIEM Diagram

## SIEM Process Flow Chart

Security Information and Event Management - VTAM 24/7 Monitoring & Detection

**Purpose:** This SIEM system processes 1M+ events daily from all VTAM infrastructure, correlates threat indicators, and enables rapid incident detection and response. Average detection time: <5 minutes | Response time: <15 minutes

### PHASE 1: Data Collection Sources



#### Endpoints

EDR logs  
200+ devices  
CrowdStrike



#### Network

Firewall logs  
IDS/IPS alerts  
NetFlow data



#### Cloud (AWS)

CloudTrail  
VPC Flow Logs  
S3 access logs



#### Email Gateway

Proofpoint logs  
Phishing attempts  
Malware blocks



#### Identity (AD)

Login events  
Failed attempts  
Privilege changes



#### Applications

Trading systems  
CRM logs  
Database audit



### PHASE 2: Log Collection & Normalization

#### Data Processing Pipeline

 Syslog Collection

 API Integration

 Log Parsing

 Field Extraction

 Event Tagging

 Normalization

 Indexing

 Storage (90 days)

## PHASE 3: Intelligent Correlation & Analysis

### ⚡ Real-Time Correlation Engine

#### Threat Intelligence

- MITRE ATT&CK mapping
- IOC feeds (IPs, domains)
- CISA KEV integration
- Threat actor TTPs

#### Event Correlation

- Cross-source analysis
- Time-based clustering
- Pattern recognition
- Multi-stage attack detection

#### Behavioral Analytics

- User behavior (UEBA)
- Anomaly detection (ML)
- Baseline deviation
- Insider threat detection

## PHASE 4: Threat Analysis & Enrichment

### Automated Analysis

**Risk Scoring:** CVSS-based severity calculation

**Asset Context:** Criticality assessment

**Threat Intel:** IOC matching & reputation

**Historical Data:** Previous incident correlation

### Use Case Examples

**Brute Force:** 10+ failed logins in 5 min

**Data Exfiltration:** Large outbound transfers

**Lateral Movement:** Unusual service access

**Ransomware:** Mass file encryption pattern



## PHASE 5: Alert Generation & Prioritization

### CRITICAL

Active Breach  
Ransomware  
Data  
Exfiltration  
Response: <5 min

### HIGH

Malware  
Detection  
Privilege  
Escalation  
Failed MFA  
Response: <15 min

### MEDIUM

Policy Violation  
Suspicious  
Activity  
Config Change  
Response: <1 hour

### LOW

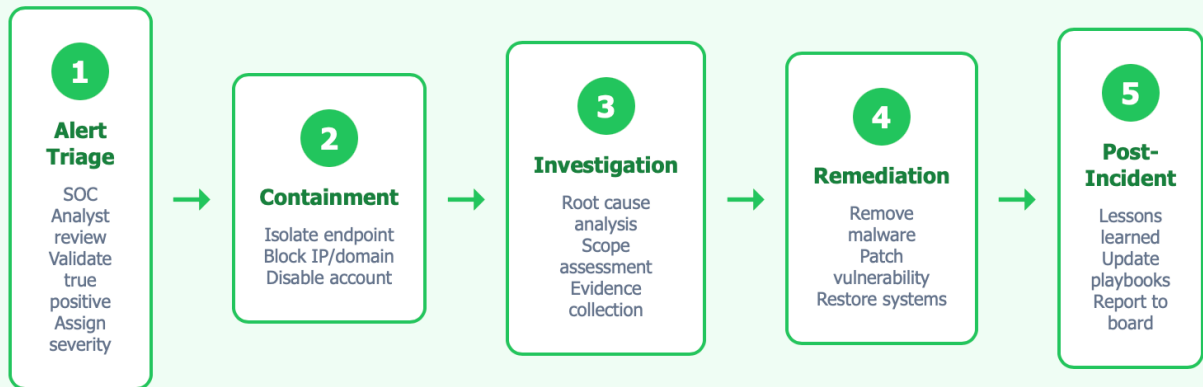
Informational  
Baseline  
Deviation  
Minor Anomaly  
Response: <24 hours

## PHASE 7: SOAR Automation (Palo Alto Cortex)

### Automated Response Actions

## PHASE 6: Incident Response Workflow

### Automated & Manual Response Actions





## Key Performance Indicators (KPIs)

### SIEM Performance Metrics

**1M+**

Events/Day

**<5min**

Mean Detection Time

**<15min**

Mean Response Time

**95%**

Automation Rate

**24/7**

SOC Coverage



### VTAM SIEM Key Features



**Real-time Processing:**

Sub-second log ingestion



**Machine Learning:**

AI-powered anomaly detection



**Integration:**

50+ pre-built connectors



**Dashboards:**

Executive & technical views



**Forensics:**

90-day retention for investigation



**Compliance:**

SOX, GDPR, SEC reporting

## DETECT: Proactive Monitoring and Threat Detection

### Overview

VTAM's detection strategy centers on continuous 24/7 monitoring through an integrated SIEM platform, enabling rapid identification of security incidents before they escalate into major breaches. The system processes over 1 million events daily from all infrastructure components, correlating data to detect sophisticated, multi-stage attacks.

### SIEM Implementation (Splunk Enterprise Security)

#### Core Capabilities:

VTAM will deploy a centralized SIEM solution that aggregates logs from all critical sources:

- **Endpoints:** EDR telemetry from 200+ devices via CrowdStrike
- **Network Infrastructure:** Firewall logs, IDS/IPS alerts, VPN access logs, NetFlow data
- **Cloud Environments:** AWS CloudTrail, VPC Flow Logs, S3 access logs

- **Identity Systems:** Azure AD authentication events, privilege changes, MFA failures
- **Applications:** Trading platform transactions, database audit logs, email gateway alerts

The SIEM correlation engine applies **machine learning-based behavioral analytics (UEBA)** to establish baseline user and entity behavior, automatically flagging anomalous activities such as:

- Unusual login times or locations
- Abnormal data access patterns
- Privilege escalation attempts
- Lateral movement across network segments

#### **Threat Intelligence Integration:**

The system incorporates real-time threat intelligence feeds mapped to the **MITRE ATT&CK framework**, enabling detection of known adversary tactics, techniques, and procedures (TTPs). Integration with the **CISA Known Exploited Vulnerabilities (KEV) catalog** ensures immediate alerting when vulnerable systems are targeted.

## Detection Use Cases

VTAM has implemented specific detection rules for high-priority threats:

#### **Ransomware Detection:**

- Mass file encryption patterns (multiple files renamed with unusual extensions)
- Shadow copy deletion attempts
- Backup system access anomalies
- Connection attempts to known ransomware C2 servers

#### **AI-Powered Social Engineering:**

- Deepfake detection via email metadata analysis
- Vishing attempts identified through call pattern analysis and voice authentication failures
- Phishing campaigns detected via email header analysis and URL reputation checks

#### **Insider Threats:**

- Large-scale data downloads outside business hours
- Access to unauthorized systems or data
- USB device usage violations
- Attempts to disable security controls

### Supply Chain Compromises:

- Unauthorized software installations
- Suspicious update processes
- Anomalous third-party vendor access patterns

## Alert Management and Escalation

Alerts are automatically classified by severity (Critical, High, Medium, Low) based on asset criticality, threat intelligence, and potential business impact.

### Response Time Objectives:

- **Critical alerts** (active breach, ransomware): <5 minutes
- **High alerts** (malware, privilege escalation): <15 minutes
- **Medium alerts** (policy violations): <1 hour
- **Low alerts** (informational): <24 hours

The **SOAR (Security Orchestration, Automation, and Response)** platform - Palo Alto Cortex - automates initial response actions, including:

- Endpoint isolation for suspected malware infections
- Automatic IP blocking at firewall
- Account suspension for compromised credentials
- Email recall for phishing campaigns
- Ticket generation and stakeholder notification

**Refer to the SIEM Process Flow Chart** (Figure 2) for detailed visualization of the detection and response workflow.

## 24/7 Security Operations

VTAM will establish a **hybrid SOC model**:

- **Tier 1 (Managed SOC Provider):** 24/7 alert monitoring and initial triage
- **Tier 2/3 (Internal Team):** Advanced threat hunting, incident investigation, and response coordination during business hours
- **On-call rotation:** Senior IT security staff available for critical incidents outside business hours

This approach balances cost-effectiveness with the need for deep organizational knowledge during complex incidents.

**NIST CSF Mapping: DETECT** (DE.AE: Anomalies and events detected, DE.CM: Security continuous monitoring, DE.DP: Detection processes) [1]

## **RESPOND: Incident Response and Crisis Management**

### Incident Response Framework

VTAM's incident response capability is built on a structured approach aligned with NIST SP 800-61 guidelines [9], ensuring rapid and effective response to security incidents.

#### **Incident Response Team (IRT):**

- **Incident Commander:** IT Security Manager (leads response, makes decisions)
- **Technical Leads:** Senior system administrators and security analysts
- **Communications Officer:** Coordinates with stakeholders, board, and regulators
- **Legal/Compliance:** Ensures regulatory compliance (SEC, GDPR)
- **Executive Sponsor:** CFO or CEO for critical incidents

### Response Procedures by Incident Type

#### **Ransomware Response:**

1. **Immediate Containment** (0-5 minutes):
  - Isolate infected systems from network via EDR or manual disconnect
  - Disable compromised accounts
  - Block C2 server IPs at perimeter firewall
  - Preserve forensic evidence (memory dumps, disk images)
2. **Assessment** (5-30 minutes):
  - Identify ransomware variant (analyze ransom note, file extensions)
  - Determine scope: how many systems affected?
  - Check if backups are intact and uncompromised
  - Activate crisis management team
3. **Eradication & Recovery** (hours to days):
  - DO NOT pay ransom (VTAM policy, FBI recommendation)
  - Restore from immutable backups
  - Rebuild compromised systems from clean images
  - Apply patches to close entry vectors
4. **Post-Incident** (1-2 weeks):
  - Root cause analysis
  - Update security controls
  - Report to board and regulators (SEC 4-day disclosure rule if material)[5]

#### **Business Email Compromise (BEC) / Vishing:**

1. Immediately freeze wire transfers and contact bank
2. Verify requestor identity through secondary channel (phone call to known number)
3. Review recent email logs for compromise indicators
4. Reset credentials for affected accounts
5. Notify clients if their data potentially exposed

#### **Data Breach:**

1. Contain breach and prevent further data exfiltration
2. Conduct forensic investigation to determine scope
3. Notify affected individuals within regulatory timeframes (GDPR: 72 hours)
4. Engage PR firm for reputation management
5. Offer credit monitoring services to affected clients

## Escalation and Communication

#### **Internal Escalation Path:**

- **Low/Medium incidents:** SOC → IT Security Manager
- **High incidents:** IT Security Manager → CIO → Executive team
- **Critical incidents:** Immediate board notification + emergency meeting

#### **External Communication:**

- **Regulatory bodies:** SEC (4 days for material incidents), state regulators as required
- **Clients:** Transparent communication if their data affected
- **Law enforcement:** FBI Internet Crime Complaint Center (IC3) for major incidents
- **Cyber insurance:** Immediate notification to activate coverage

**Documentation:** All incidents documented in centralized incident management system (ServiceNow) with:

- Timeline of events
- Actions taken
- Evidence collected
- Financial impact assessment
- Lessons learned

**NIST CSF Mapping:** RESPOND (RS.RP: Response planning, RS.CO: Communications, RS.AN: Analysis, RS.MI: Mitigation, RS.IM: Improvements) [1]

# RECOVER: Business Continuity and Disaster Recovery

## Recovery Strategy

VTAM's recovery capability ensures minimal business disruption and rapid restoration of critical services following a cyber incident.

## Recovery Time and Point Objectives

| System Category       | RTO      | RPO        | Recovery Priority |
|-----------------------|----------|------------|-------------------|
| Trading Systems       | 2 hours  | 15 minutes | Critical (P0)     |
| Client Database       | 4 hours  | 1 hour     | Critical (P0)     |
| Email & Communication | 8 hours  | 4 hours    | High (P1)         |
| CRM & Internal Apps   | 24 hours | 8 hours    | Medium (P2)       |
| File Servers          | 48 hours | 24 hours   | Low (P3)          |

## Backup Architecture (3-2-1-1-0 Rule)

### Implementation:

- **3 copies** of all data (primary + 2 backups)
- **2 different media types** (disk + tape)
- **1 offsite copy** (AWS S3 in different region)
- **1 offline/air-gapped copy** (monthly tape backups in secure vault)
- **0 errors** (automated verification of all backups)

**Immutable Backups:** All cloud backups stored in AWS S3 with **Object Lock** enabled, preventing deletion or encryption by ransomware for 90-day retention period. This ensures guaranteed recovery even during total infrastructure compromise.

### Backup Schedule:

- **Incremental:** Every 4 hours for critical systems
- **Differential:** Daily at midnight
- **Full backup:** Weekly (Sunday 2 AM)
- **Tape archival:** Monthly for compliance (7-year retention)

### Testing:

- Monthly restore drills for critical systems
- Quarterly full disaster recovery exercise

- Annual tabletop exercise with executive team

## Disaster Recovery Infrastructure

### Hot Standby:

- Trading systems: Active-active configuration across two AWS availability zones
- Automatic failover in <5 minutes if primary site fails

### Warm Standby:

- Client database: Secondary read replica, promoted to primary if needed
- Failover time: ~2 hours (includes DNS updates and testing)

### Cold Standby:

- Non-critical systems restored from backups as needed
- Recovery time: 24-48 hours

## Recovery Procedures

### Ransomware Recovery Workflow:

1. **Verify backups integrity** - Ensure backups not compromised
2. **Clean environment** - Rebuild infrastructure from known-good images
3. **Restore data** - From most recent uninfected backup
4. **Validation** - Test all critical functions before production
5. **Phased return** - Gradual restoration of services to avoid re-infection
6. **Monitoring** - Enhanced surveillance for 30 days post-recovery

### Communication During Recovery:

- Status updates every 2 hours to executive team
- Client communication via website status page and email
- Regulatory updates as required
- Media response coordinated through PR team

## Business Continuity Measures

### Alternative Work Arrangements:

- Critical staff equipped with mobile hotspots for internet redundancy
- Cloud-based systems accessible from any location
- Manual transaction processing procedures documented

### Vendor Contingency:

- Alternative trading platform identified (can activate in 24 hours)
- Backup email gateway available
- Secondary cloud provider evaluated (Azure) for critical system redundancy

## Post-Recovery Analysis

Within 5 business days of major incident:

1. After-Action Review with full IRT team
2. Root Cause Analysis documenting attack vector and control failures
3. Improvement Plan with specific recommendations and timelines
4. Board Report summarizing incident, response, and improvements
5. Insurance Claim if applicable, with full documentation

### Lessons Learned Integration: All findings incorporated into:

- Updated incident response playbooks
- Enhanced security controls (feed into PROTECT phase)
- Modified detection rules (feed into DETECT phase)
- Improved training scenarios

**NIST CSF Mapping:** RECOVER (RC.RP: Recovery planning, RC.IM: Improvements, RC.CO: Communications)[1]

# CONTINUOUS TRAINING AND SECURITY AWARENESS PROGRAM

## Overview

Traditional annual security training videos have proven ineffective - 43% of successful breaches involve human error [3] VTAM will implement a **continuous, engaging training program** that transforms security awareness from a checkbox exercise into an embedded organizational culture, specifically addressing modern threats like AI-powered social engineering.

## Program Components

### 1. Continuous Simulated Attack Campaigns

**Monthly Phishing Simulations:** Using platforms like KnowBe4 or Proofpoint, VTAM will deploy realistic phishing simulations with increasing sophistication:

- **Months 1-3:** Basic phishing (obvious red flags)
- **Months 4-6:** Intermediate (branded emails, urgent requests)
- **Months 7-12:** Advanced (spear phishing, AI-generated, executive impersonation)

**Scenarios include:** fake HR policy updates, spoofed client emails, fraudulent invoices, fake Microsoft/AWS security alerts.

**Immediate Micro-Learning:** When employees click suspicious links, they receive instant 3-minute interactive lessons explaining red flags - **no punishment, only education.**

**Quarterly Vishing Simulations:** Security team conducts simulated voice phishing attacks using AI voice cloning to test verification procedures (callback to known numbers, dual authorization).

#### **Target Metrics:**

- Phishing click rate: <5% within 12 months (industry average: 15-20%)
- 90% reduction in repeat offenders quarter-over-quarter

## **2. Role-Specific Training Tracks**

**Executives & Board (Quarterly - 60 min):** CEO fraud, BEC schemes, deepfake detection, social media oversharing risks

**Finance Team (Monthly - 30 min):** Wire fraud verification procedures, invoice scams, dual authorization protocols

- *Monthly drill:* Security team sends fake wire transfer requests

**IT Staff (Monthly - 60 min):** Advanced TTPs from MITRE ATT&CK, incident response tabletops, hands-on malware analysis labs

**Client-Facing Staff (Bi-Monthly - 30 min):** Protecting client PII, secure communications, social engineering scenarios

**General Employees (Monthly - 15 min):** Rotating topics: password security, MFA, phishing recognition, mobile device security, remote work best practices

- *Format:* 5-7 minute videos + 5-question quiz

## **3. Gamification and Engagement**

### **Security Champions Program:**

- Each department nominates a "Security Champion" who receives advanced training
- Monthly recognition for highest phishing detection rates
- Quarterly prizes: gift cards, extra PTO, "Cyber Defender" trophy
- **Anonymous Department Leaderboard:** Dashboard displays department performance (not individuals) - friendly competition

**Annual "Cyber Security Awareness Week":** Lunch-and-learns, live hacking demonstrations, escape room challenges, executive participation

#### 4. No-Blame Reporting Culture

**"See Something, Say Something":**

- One-click "Report Phishing" button in email
- Anonymous reporting hotline
- **No punishment policy** - mistakes are learning opportunities
- Monthly recognition for employees reporting legitimate threats

**Target:** 100+ security reports per month

#### 5. Measurement and Continuous Improvement

**Key Performance Indicators:**

| Metric                   | 12-Month Target |
|--------------------------|-----------------|
| Phishing Click Rate      | <5%             |
| Training Completion Rate | 98%             |
| Incidents Reported/Month | 100+            |
| Repeat Offenders         | <2%             |
| Time to Report Incident  | <15 min         |

### Quarterly Reviews:

- Analyze simulation results and real incident trends
- Update content based on emerging threats
- Report metrics to board with improvement recommendations

## Budget and ROI

### Annual Investment: \$40,000

- Training platform (200 users): \$15,000
- Content development: \$10,000
- Gamification/incentives: \$5,000
- External speakers: \$10,000

### ROI Calculation:

- Average phishing attack cost: \$500,000+
- Program reduces success rate by ~80%
- Expected annual savings: \$400,000+
- **ROI: 10:1**

## Creating a Security-First Culture

Beyond technical training, VTAM fosters security awareness through:

- **Leadership Commitment:** CEO and executives visibly participate in training
- **Positive Reinforcement:** Celebrate security successes, share near-miss stories
- **Continuous Communication:** Monthly newsletters, posters, all-hands mentions
- **Integration:** Security metrics in management dashboards

### Alignment with Standards:

- **NIST CSF: PROTECT (PR.AT: Awareness and training) [1]**
- **ISO 27001: Clause 7.2 (Competence), 7.3 (Awareness) [6]**
- **CISA Best Practices: Security awareness as foundational control [2]**

## Conclusion

VTAM's training program transforms security awareness from annual compliance into **continuous practice**. By combining realistic simulations, role-specific content, gamification, and no-blame reporting culture, every employee becomes an active defender against modern threats. This human firewall, combined with technical controls, positions VTAM for resilience against evolving cyber threats.

## References

[1] National Institute of Standards and Technology (NIST), "Cybersecurity Framework," NIST Cybersecurity Framework, 2023. [Online]. Available: <https://www.nist.gov/cyberframework>. [Accessed: Nov. 13, 2025].

[2] Cybersecurity and Infrastructure Security Agency (CISA), "Known Exploited Vulnerabilities Catalog," CISA.gov, 2024. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>. [Accessed: Nov. 13, 2025].

[3] Verizon, "2024 Data Breach Investigations Report," Verizon Enterprise, 2024. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>. [Accessed: Nov. 13, 2025].

[4] IBM Security, "Cost of a Data Breach Report 2024," IBM Corporation, Aug. 2024. [Online]. Available: <https://www.ibm.com/security/data-breach>. [Accessed: Nov. 13, 2025].

[5] U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Federal Register, vol. 88, no. 149, pp. 51896-51933, July 2023.

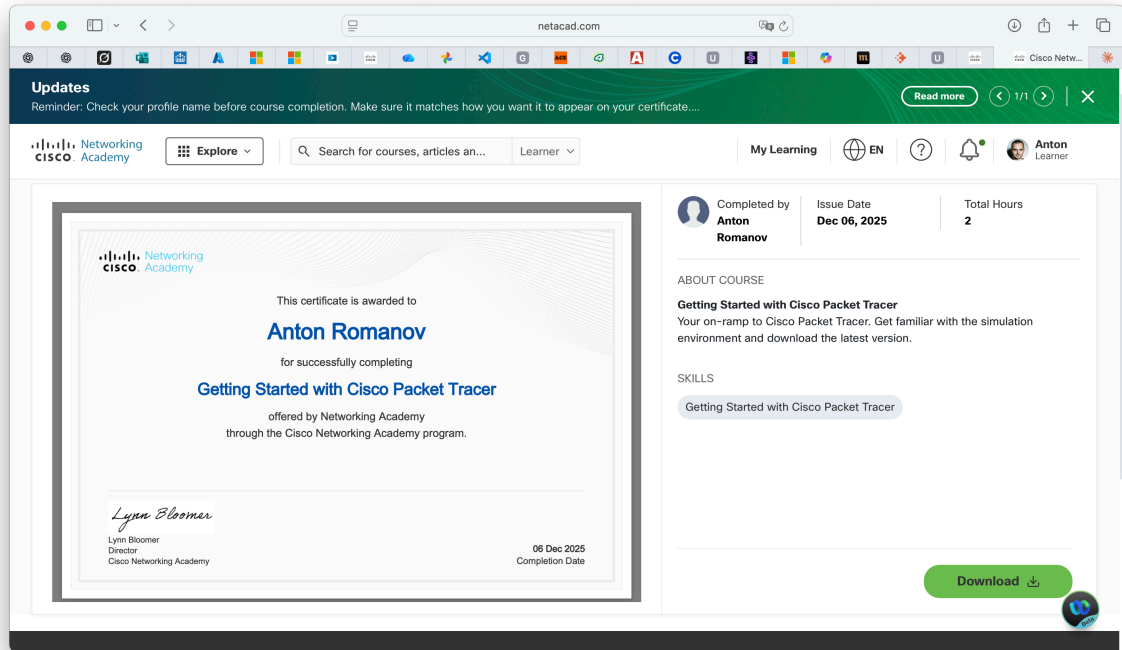
[6] International Organization for Standardization (ISO), "ISO/IEC 27001:2022 Information Security Management Systems — Requirements," ISO/IEC, Oct. 2022.

[7] MITRE Corporation, "ATT&CK Framework for Enterprise," MITRE ATT&CK, 2024. [Online]. Available: <https://attack.mitre.org/>. [Accessed: Nov. 13, 2025].

[8] Cybersecurity & Infrastructure Security Agency, "Zero Trust Maturity Model," CISA, ver. 2.0, Apr. 2023. [Online]. Available: <https://www.cisa.gov/zero-trust-maturity-model>. [Accessed: Nov. 13, 2025].

[9] NIST, "Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide," National Institute of Standards and Technology, Aug. 2012.

[10] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," ENISA, Oct. 2024. [Online]. Available: <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>. [Accessed: Nov. 13, 2025].



Presentation for board members:

# VTAM Cybersecurity Strategy

## Zero Trust Investment Proposal

Presented to: Board of Directors

Vigilant Trust & Asset Management

Anton Romanov, IT Security Manager

November 2025

# The Problem: VTAM Under Active Attack

⚠️ Recent incidents: Sophisticated phishing + ransomware attempt

| Threat                | Likelihood  | Potential Financial Impact             |
|-----------------------|-------------|----------------------------------------|
| Ransomware Attack     | HIGH        | \$10M+ (recovery, downtime, penalties) |
| AI-Powered Wire Fraud | MEDIUM-HIGH | \$1M - \$25M per incident              |
| Data Breach           | MEDIUM      | \$5M+ (fines, lawsuits, reputation)    |
| Supply Chain Attack   | MEDIUM      | \$3M+ (system rebuild, lost trust)     |

## What We're Protecting



**Financial Assets**

\$500M daily transactions  
50,000 client portfolios  
Proprietary strategies



**Regulatory Compliance**

SEC 4-day disclosure  
GDPR €20M fines  
SOX, GLBA requirements



**Client Trust**

Decades of reputation  
Competitive advantage  
Market confidence

**\$10M+**

Avg Breach Cost

**43%**

Breaches via Human Error

**4 Days**

SEC Disclosure Deadline

**\$25M**

Largest Deepfake Fraud

# The Solution: Zero Trust Security



## Investment Required: \$950K

| Security Component               | Investment       | Timeline           |
|----------------------------------|------------------|--------------------|
| Network Security (ZTNA, EDR/XDR) | \$250,000        | 120 days           |
| Backup & Disaster Recovery       | \$200,000        | 90 days            |
| Cloud Security (CSPM, CASB)      | \$150,000        | 60 days            |
| Email/Web Security               | \$125,000        | 60 days            |
| Identity & Access Management     | \$100,000        | 90 days            |
| Data Protection & Encryption     | \$75,000         | 90 days            |
| Vulnerability Management         | \$50,000         | 30 days            |
| <b>TOTAL INVESTMENT</b>          | <b>\$950,000</b> | <b>6-12 months</b> |

+ \$200K annual operating costs (24/7 monitoring, training, maintenance)

## Return on Investment: 10:1

**\$10M+**

Average Breach Cost  
(Industry Data)

**\$950K**

Our Investment  
(One-Time Capital)

Preventing ONE major breach pays for the ENTIRE program

### Financial

Prevent \$10M+ losses  
Avoid regulatory fines  
Lower insurance premiums

### Operational

4-hour recovery vs weeks  
No trading disruptions  
Business continuity

### Reputational

Maintain client trust  
Avoid headlines  
Competitive edge

## 12-Month Implementation Roadmap

### Quick Wins (30 days)

MFA rollout for all users, critical vulnerability patching, baseline phishing test, 24/7 monitoring activation

### Foundation (90 days)

SIEM deployment, EDR on all endpoints, immutable backups, continuous training program launch

### Advanced (180 days)

Zero Trust Network Access, cloud security (CSPM/CASB), privileged access management

### Mature Security (365 days)

<5% phishing rate achieved, ISO 27001 ready, quarterly board reporting, 85% risk reduction

**85%**

Risk Reduction Target

**<5%**

Phishing Click Rate Target

# VTAM vs Industry Standard

| Metric              | VTAM Proposed        | Industry Average |
|---------------------|----------------------|------------------|
| Initial Investment  | \$950,000            | \$1.2M - \$1.5M  |
| Implementation Time | 12 months            | 18-24 months     |
| Threat Detection    | <5 minutes           | 15-30 minutes    |
| Security Training   | Monthly (continuous) | Annual           |
| Recovery Time (RTO) | 4 hours              | 24-48 hours      |

More cost-effective AND faster than industry standard

Positions VTAM as security leader in mid-sized financial services

# Requesting Board Approval

**We request the Board to approve:**

- **✓ \$950,000** capital expenditure for security infrastructure
- **✓ \$200,000** annual operating budget for 24/7 monitoring and training
- **✓ Zero Trust** as VTAM's strategic security direction
- **✓ Executive participation** in security awareness initiatives

Timing is critical: We are actively targeted NOW

This is not just IT infrastructure - it's strategic business resilience

# Questions?

Thank You  
Anton Romanov