

# Building a Modern Zero Trust Security Framework for VTAM

---

## ***Protecting VTAM Against Modern Cyber Threats***

- *Prepared for the Board of Directors*
- *Networks & Cyber Security Essentials*
- *Based on NIST CSF 2.0, ISO/IEC 27001:2022 and CISA guidance*

# Why This Matters

Why VTAM Is at Risk:

## **Current Threat Landscape**

- Hybrid working has expanded the attack surface
- Heavy cloud and SaaS adoption increases exposure
- Financial firms are prime ransomware targets
- AI-powered phishing and vishing attacks are increasing
- Supply chain breaches now affect thousands of organisations at once

## **Recent VTAM Incidents**

- Sophisticated phishing campaign bypassed filters
- Attempted ransomware infection

## **Business Impact**

- GDPR and FCA penalties
- Financial losses
- Reputational damage

# Key Threats Facing VTAM

Modern Internal & External Threats

## **External Threats**

- Ransomware-as-a-Service (LockBit, BlackCat)
- AI-generated voice cloning attacks
- Supply chain compromise (MOVEit breach)
- Cloud misconfiguration
- Credential theft

## **Internal Threats**

- Human error
- Phishing link clicks
- Shadow IT usage
- Weak password practices
- Privileged access misuse



# Zero Trust Architecture

## Why Zero Trust?

### Traditional Security No Longer Works

- The firewall is no longer enough
- Users work remotely from unmanaged locations
- Attackers exploit stolen credentials

### Zero Trust Principles

- Never trust, always verify
- Continuous authentication
- Least privilege access
- Device verification before access
- Application-level segmentation

# Security Policies & Governance

## Governance and Security Policies

### Governance

- C-suite IT Steering Committee
- Quarterly risk reviews
- Alignment with NIST CSF 2.0 Govern Function

### Core Policies

- Identity & Access Management
- Data Classification
- Remote Access Policy
- Supplier Security Policy
- Incident Response Policy

### ISO/IEC 27001 Alignment

- A.5.12 Data Classification
- A.5.15 Access Control
- A.5.10 Security Policy

# Technical Mitigation Measures

## Technical Security Controls

### Identity Protection

- FIDO2 hardware-based MFA
- Role-based access control
- Just-in-time privileged access

### Cloud & Endpoint Security

- CSPM monitoring for AWS and Azure
- MDM/UEM device management
- Network Access Control checks

### Vulnerability Management

- Patching prioritised using CISA KEV catalogue
- Critical vulnerabilities fixed within 15 days

### Data Protection

- TLS 1.3 encryption in transit
- AES-256 encryption at rest
- Immutable 3-2-1-1 backups

# 24/7 Monitoring & Incident Response

## **Detection and Response Strategy**

### **Hybrid SOC Model**

- Internal security team
- MDR provider covers nights/weekends

### **SIEM & SOAR**

- Microsoft Sentinel or Splunk
- MITRE ATT&CK aligned detections
- Automated ransomware containment

### **Automated Response Actions**

- Isolate infected endpoint
- Disable compromised account
- Snapshot affected host

### **Incident Response Framework**

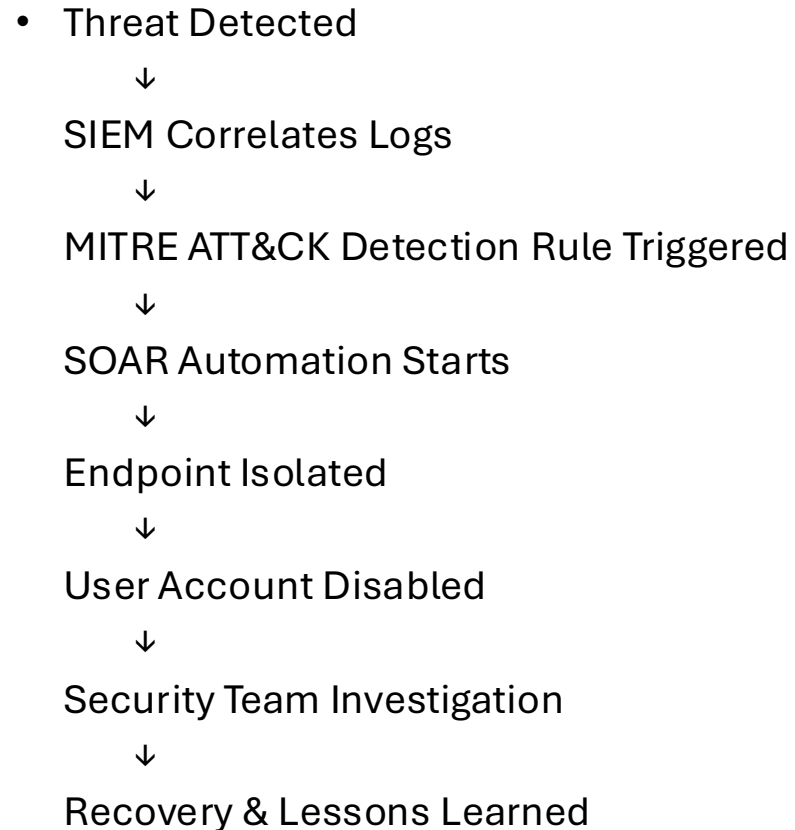
Based on NIST SP 800-61r2:

1. Preparation
2. Detection & Analysis
3. Containment
4. Recovery
5. Post-Incident Review

# Incident Response Flowchart

## SIEM and SOAR Response Flow

### **SIEM and SOAR Response Flow**



# Security Awareness & Training

- **Continuous Training Programme**

## **Monthly Activities**

- Phishing simulations
- AI-powered vishing simulations
- Micro-learning sessions

## **Role-Specific Training**

- Finance: BEC awareness
- IT: Secure configuration
- Executives: Deepfake recognition

## **Security Culture**

- Security Champions programme
- Non-punitive learning approach
- Quarterly KPI dashboard to board

## **Key Metrics**

- Click rate
- Time-to-report
- Training completion rate

# Business Benefits & Conclusion

## **Strategic Benefits for VTAM**

### **Outcomes**

- Reduced ransomware risk
- Faster threat detection
- Stronger regulatory compliance
- Improved cyber resilience
- Better protection of customer trust

### **Strategic Message**

This is not just a compliance exercise.

The proposed framework:

- Reduces operational risk
- Strengthens resilience
- Protects VTAM's reputation
- Supports long-term business continuity

## **Final Recommendation**

Adopt a Zero Trust security framework aligned with:

- NIST CSF 2.0
- ISO/IEC 27001:2022
- CISA guidance and KEV catalogue

# References

- **Key References**

- [1] NIST SP 800-207, Zero Trust Architecture, 2020
- [2] NIST Cybersecurity Framework 2.0, 2024
- [3] ISO/IEC 27001:2022
- [4] CISA Known Exploited Vulnerabilities Catalogue
- [5] ENISA Threat Landscape 2023
- [6] FBI IC3 PSA on AI Voice Cloning Fraud, 2024
- [7] Verizon 2024 Data Breach Investigations Report
- [8] CISA Insider Threat Guidance
- [9] CISA Zero Trust Maturity Model 2.0
- [10] CISA MFA Best Practices Guidance
- [11] MITRE ATT&CK Framework
- [12] NIST SP 800-61r2 Incident Handling Guide
- [13] IBM Cost of a Data Breach Report 2024