Risk Assessment Report

Cyber Threat Intelligence Dashboard

Prepared by: Yarin Hazan

Date: May 2025

Framework: ISO 27001:2022 & NIST CSF

Executive Summary

Project Overview

This comprehensive risk assessment was conducted on the Cyber Threat Intelligence (CTI) Dashboard system, a custom-built application that integrates with external threat intelligence APIs (VirusTotal, AbuseIPDB) to provide IP and domain reputation analysis. The assessment follows ISO 27001:2022 methodology and incorporates NIST Cybersecurity Framework principles.

Key Findings

- Total Risks Identified 25

- Critical Risks 3

- High Risks 8

- Medium Risks 10

- Low Risks 4

- Overall Risk Level Medium-High

Critical Risks Requiring Immediate Attention

1. Data Breach (OPS-001) Unauthorized access to sensitive information

2. Natural Disasters (ENV-002) Complete service disruption from physical events

3. Malicious Insiders (HUMAN-001) Intentional harm by authorized personnel

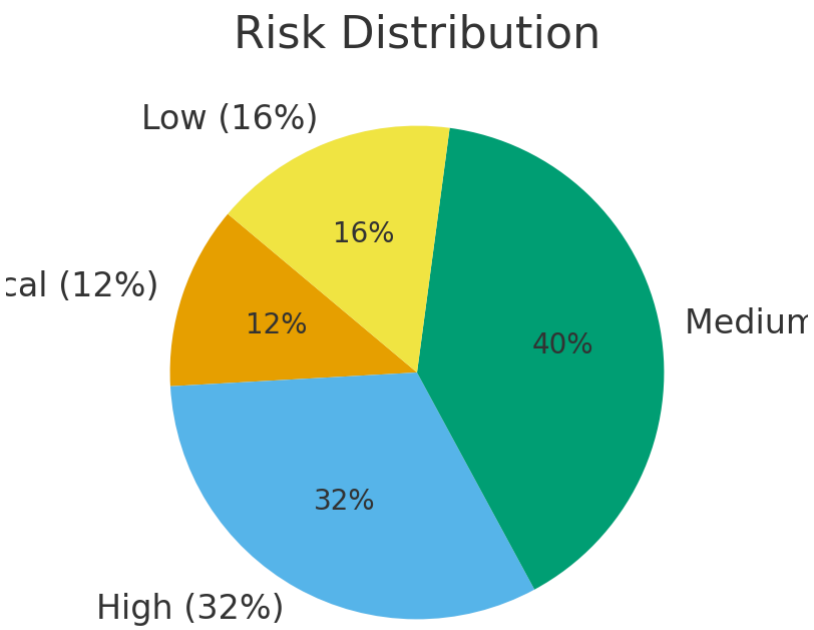
Risk Treatment Strategy

- Risk Mitigation 18 risks (72%)

- Risk Transfer 4 risks (16%)

- Risk Acceptance 2 risks (8%)

- Risk Avoidance 1 risk (4%)


Risk Distribution
Low (16%)
16%
cal (12%)
12%
Medium
40%
32%
High (32%)

Introduction

Purpose and Scope

This risk assessment evaluates the security posture of the CTI Dashboard system, identifying potential threats, vulnerabilities, and risks to enable informed decision-making for risk treatment and control implementation.

Methodology

- Framework ISO 27001:2022 Information Security Management System

- Threat Modeling STRIDE methodology

- Risk Assessment FAIR (Factor Analysis of Information Risk)

- Asset Classification Based on confidentiality, integrity, and availability requirements

System Description

The CTI Dashboard is a web-based application consisting of

- Backend FastAPI application hosted on Render

- Frontend React application hosted on Vercel

- External APIs VirusTotal and AbuseIPDB for threat intelligence

- Data Storage Cloud-based storage for user queries and results

Asset Inventory and Classification

Asset Classification Framework

Assets are classified based on

- Criticality High, Medium, Low

- Confidentiality Public, Internal, Confidential, Restricted

- Integrity Critical, Important, Standard

- Availability 24/7, Business Hours, Non-Critical

Asset Summary

- Infrastructure Assets 7 (3 High Criticality, 4 Medium Criticality)

- Application Assets 10 (4 High Criticality, 6 Medium Criticality)

- Data Assets 11 (3 High Criticality, 8 Medium Criticality)

- Human Assets 7 (2 High Criticality, 5 Medium Criticality)

Critical Assets

- Web Server (FastAPI) - INF-001

- Database Server - INF-002

- FastAPI Main Application - APP-001

- User Accounts - DATA-005

- API Keys - DATA-008

- System Administrators - HUMAN-001

- Security Engineers - HUMAN-002

Asset Valuation

- Total Replacement Cost $850,000 - $3,700,000

- Business Impact $10,000 - $50,000 per day of downtime

- Reputation Value Priceless (requires continuous protection)

Threat and Vulnerability Analysis

Threat Modeling Methodology

STRIDE Framework

- Spoofing Impersonation of legitimate users or systems

- Tampering Unauthorized modification of data or systems

- Repudiation Denial of actions or transactions

- Information Disclosure Unauthorized access to sensitive information

- Denial of Service Disruption of system availability

- Elevation of Privilege Unauthorized access to higher-level permissions

Risk Assessment Matrix

Impact Level Likelihood Level Risk Rating

Low Low Low

Low Medium Low

Low High Medium

Medium Low Low

Medium Medium Medium

Medium High High

High Low Medium

High Medium High

High High Critical

Threat Categories Identified

Technical Threats (7 threats)

- SQL Injection (SQLi) - TECH-001

- Cross-Site Scripting (XSS) - TECH-002

- API Abuse and Rate Limiting - TECH-003

- Distributed Denial of Service (DDoS) - TECH-004

- Man-in-the-Middle (MITM) Attacks - TECH-005
- Credential Stuffing - TECH-006
- Privilege Escalation - TECH-007

Operational Threats (4 threats)

- Data Breach - OPS-001
- Data Loss - OPS-002
- Configuration Drift - OPS-003
- Patch Management Failures - OPS-004

Environmental Threats (3 threats)

- Power Outages - ENV-001
- Natural Disasters - ENV-002
- Cloud Provider Outages - ENV-003

Human Threats (4 threats)

- Malicious Insiders - HUMAN-001
- Accidental Insiders - HUMAN-002
- Phishing Attacks - HUMAN-003
- Pretexting - HUMAN-004

Third-Party Threats (2 threats)

- Compromised Dependencies - THIRD-001
- Vendor Security Failures - THIRD-002

Vulnerability Assessment

- High Priority Input validation, authentication controls, encryption implementation
- Medium Priority Logging, monitoring, backup procedures, configuration management
- Low Priority Documentation, non-critical features, legacy components

Control Framework and ISO 27001 Mapping

Control Framework Overview

ISO 27001:2022 Control Categories

- A.5 - Organizational Controls
- A.6 - People Controls
- A.7 - Physical Controls
- A.8 - Technological Controls

Control Implementation Status

- Implemented Controls currently in place

- Planned Controls scheduled for implementation
- Recommended Controls recommended for future implementation
- Not Applicable Controls not relevant to current system

Control Implementation Status

- Implemented 7 controls (37%)
- Planned 11 controls (58%)
- Not Applicable 1 control (5%)

NIST CSF Alignment

- Identify Function 60% implemented
- Protect Function 70% implemented
- Detect Function 20% implemented
- Respond Function 10% implemented
- Recover Function 15% implemented

Risk Evaluation and Treatment

Risk Distribution

- Critical Risk (9) 3 risks (12%)
- High Risk (6) 8 risks (32%)
- Medium Risk (4) 10 risks (40%)
- Low Risk (1) 4 risks (16%)

Top Risks by Category

Technical Risks

1. SQL Injection (TECH-001) High Risk
2. API Abuse (TECH-003) High Risk
3. DDoS Attacks (TECH-004) High Risk

Operational Risks

1. Data Breach (OPS-001) Critical Risk
2. Patch Management Failures (OPS-004) High Risk

Environmental Risks

1. Natural Disasters (ENV-002) Critical Risk
2. Cloud Provider Outages (ENV-003) High Risk

Human Risks

1. Malicious Insiders (HUMAN-001) Critical Risk
2. Phishing Attacks (HUMAN-003) High Risk

Risk Treatment Strategies

Risk Mitigation (18 risks - 72%)

- Implementation of security controls
- Process improvements and training
- Technology enhancements and monitoring

Risk Transfer (4 risks - 16%)

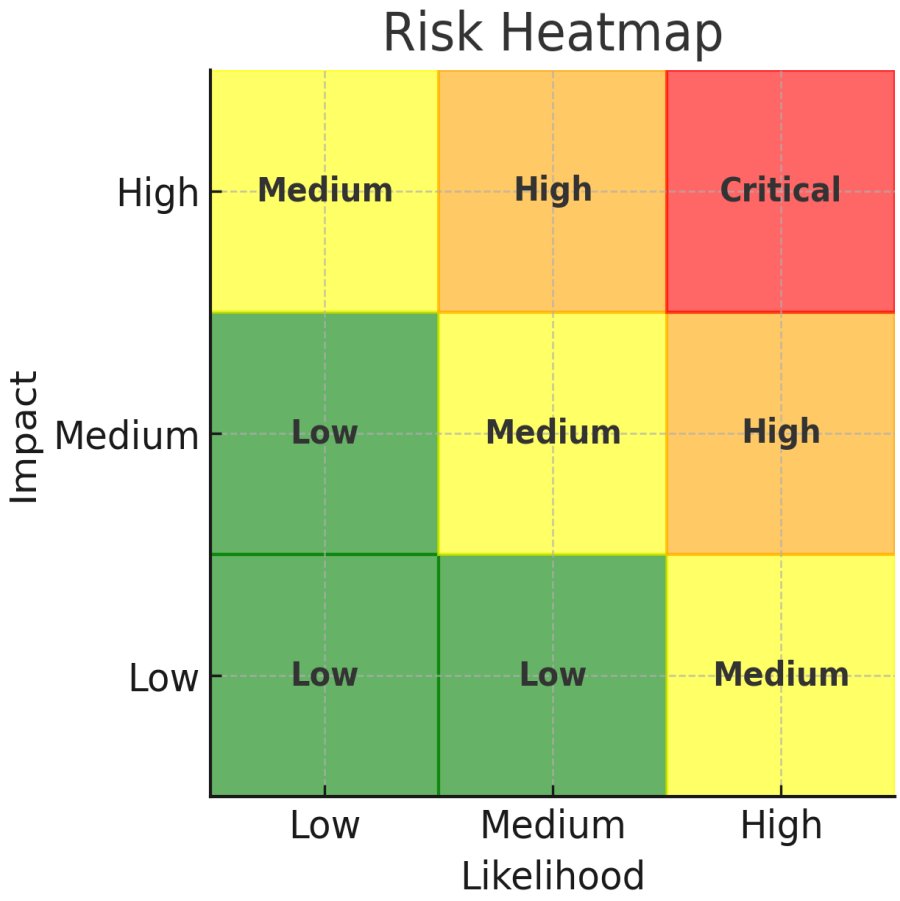
- Cloud service dependencies to providers
- Insurance coverage for business interruption
- Vendor management for supply chain risks

Risk Acceptance (2 risks - 8%)

- Low-risk threats with high mitigation costs
- Environmental threats with low likelihood

Risk Avoidance (1 risk - 4%)

- Discontinuation of high-risk services



Implementation Roadmap

Phase 1 (Q1 2026) - Foundation

- Information security policies
- Authentication and access controls
- Basic monitoring and logging
- Security awareness training

Phase 2 (Q2 2026) - Enhancement

- Advanced monitoring and detection
- Incident response procedures
- Security testing and assessment
- Business continuity planning

Phase 3 (Q3 2026) - Maturity

- Advanced threat detection
- Automated response capabilities
- Continuous improvement processes
- Compliance monitoring and reporting

Immediate Actions (Next 30 Days)

1. Implement Multi-Factor Authentication (MFA)

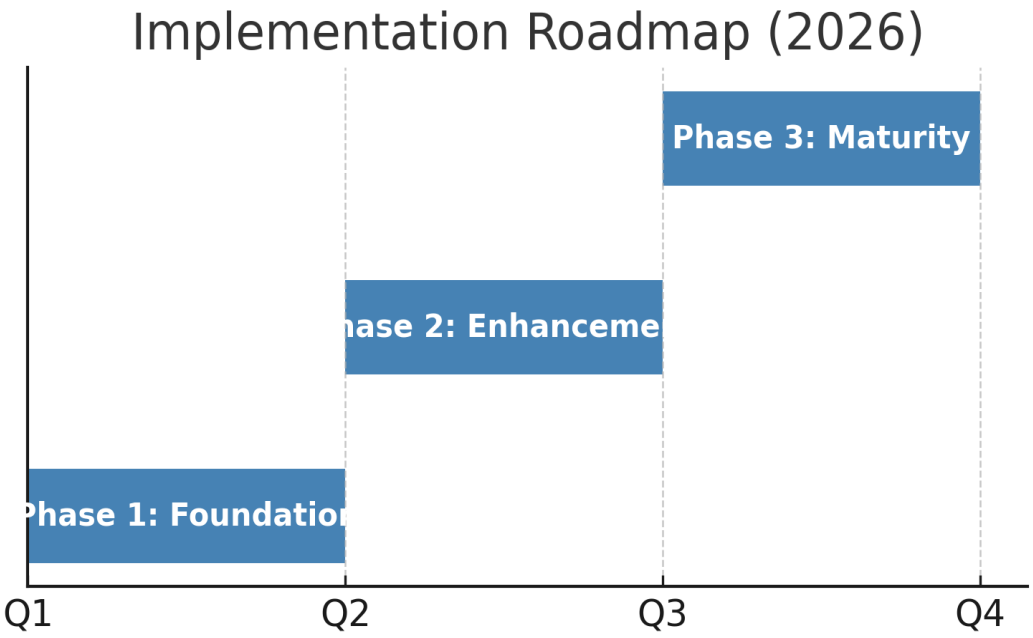
- Priority Critical
- Impact Reduce credential-based attacks
- Effort Medium
- Timeline 30 days

2. Deploy Web Application Firewall (WAF)

- Priority High
- Impact Protect against common web attacks
- Effort Low
- Timeline 14 days

3. Implement Rate Limiting

- Priority High
- Impact Prevent API abuse and DDoS
- Effort Medium
- Timeline 21 days



Compliance and Regulatory Considerations

ISO 27001:2022 Compliance

- Current Status 37% compliant
- Target Status 80% compliant by end of year
- Gap Analysis Major gaps in people controls and process documentation

NIST Cybersecurity Framework

- Current Tier Tier 1 (Partial)
- Target Tier Tier 3 (Repeatable)
- Key Improvements Implement continuous monitoring and incident response

Additional Frameworks

- GDPR Basic compliance through data classification
- SOC 2 Not currently pursued
- PCI DSS Not applicable (no payment processing)

Resource Requirements and Budget

Implementation Costs

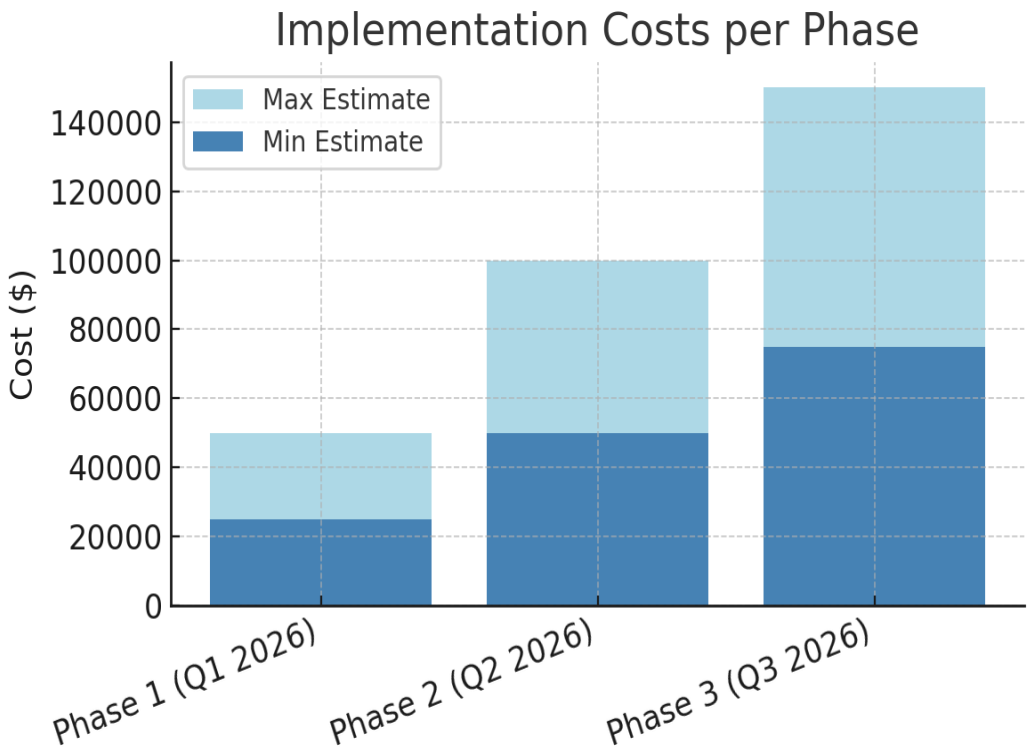
- Phase 1 (Q1 2026) $25,000 - $50,000
- Phase 2 (Q2 2026) $50,000 - $100,000
- Phase 3 (Q3 2026) $75,000 - $150,000
- Total Investment $150,000 - $300,000

Resource Requirements

- Security Engineer 1 FTE (Full-Time Equivalent)
- Security Analyst 0.5 FTE
- Developer Support 0.25 FTE
- Management Oversight 0.1 FTE

Return on Investment

- Risk Reduction 60-80% reduction in high and critical risks
- Compliance Benefits ISO 27001 certification readiness
- Business Continuity Improved resilience and customer trust
- Cost Avoidance Prevention of potential $500,000+ security incidents



Conclusion and Recommendations

Overall Assessment

The CTI Dashboard system presents a medium-high risk profile with several critical and high-risk areas requiring immediate attention. While the system has good foundational security controls, significant gaps exist in people controls, process documentation, and advanced threat detection capabilities.

Strategic Recommendations

1. Prioritize Critical Risks Focus resources on data breach prevention and insider threat mitigation

2. Implement People Controls Establish comprehensive security awareness and training programs

3. Enhance Detection Capabilities Deploy advanced monitoring and threat detection systems

4. Build Incident Response Develop comprehensive incident response and business continuity capabilities

5. Achieve Compliance Work toward ISO 27001 certification and NIST CSF Tier 3

Success Metrics

- Reduce critical and high risks by 60% within 12 months

- Achieve 80% ISO 27001 control coverage within 18 months

- Implement comprehensive incident response within 6 months

- Establish continuous monitoring capabilities within 9 months

Next Steps

1. Immediate Implement MFA and WAF protection

2. Short-term Develop security policies and training programs

3. Medium-term Conduct penetration testing and implement advanced controls

4. Long-term Achieve ISO 27001 certification and establish continuous improvement

Appendices

Appendix A Detailed Risk Register

See separate Risk-Register.xlsx file for comprehensive risk details.

Appendix B Asset Inventory Details

Complete asset classification and business impact analysis.

Appendix C Control Framework Details

ISO 27001 control mapping and implementation status.

Appendix D Methodology Details

- Risk assessment methodology and criteria

- Asset valuation methodology

- Control effectiveness measurement approaches

This risk assessment report should be reviewed and updated annually or following significant system changes.

Report Version 1.0

Date MAY 2025

Prepared By Yarin Hazan

Review By Yarin Hazan

Next Review December 2025