Robert A. Kalka Metropolitan Skyport (RAKMS)

Security Assessment Briefing

Finals-XX

CONFIDENTIAL

Team Introduction

[redacted]

Principal Consultant

Sr. Consultant

Sr. Consultant

[redacted]

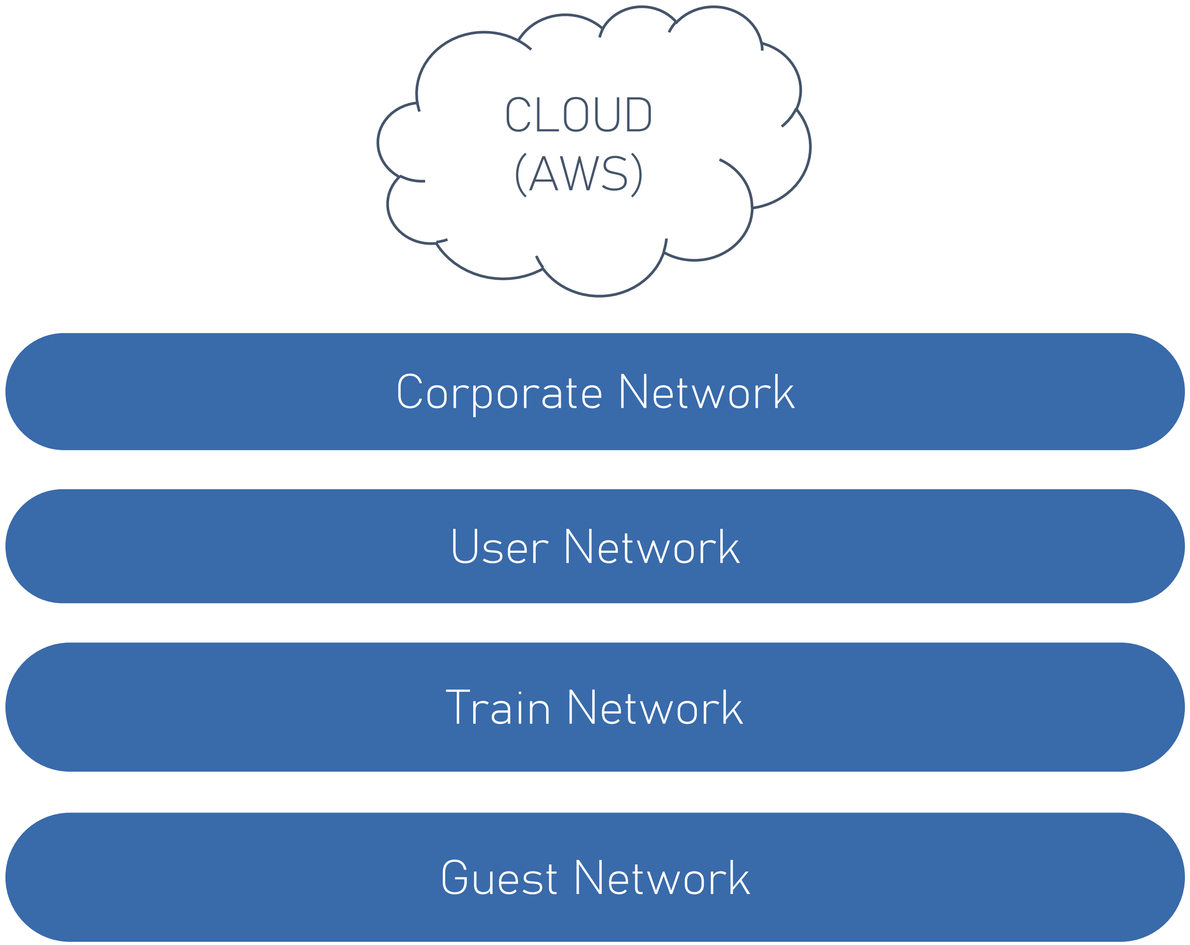
Sr. Consultant

Consultant

Consultant

Assessment Overview

- Finals-XX conducted a penetration test on the following RAKMS assets.
- These assets were tested in two stages:
  - October 2023
  - January 2024



Assessment Results

Robert A. Kalka

Metropolitan Skyport

Q1 2024
Security Assessment Results

22
Industry & Legal Compliance Findings

$37,500/mo
in potential non-compliance fines

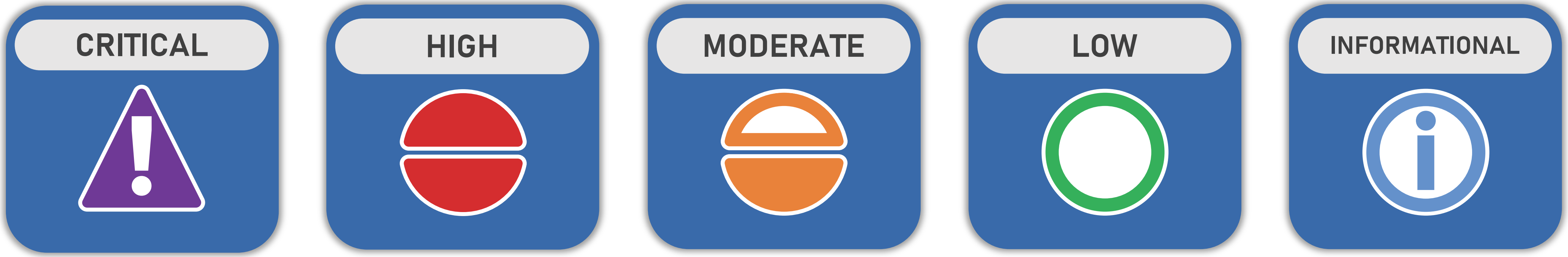
Risk of a potential data breach with PII

26
Total Findings

6
Critical Findings

Best Practice:
Secure Guest Network

Risk Categorization



CRITICAL

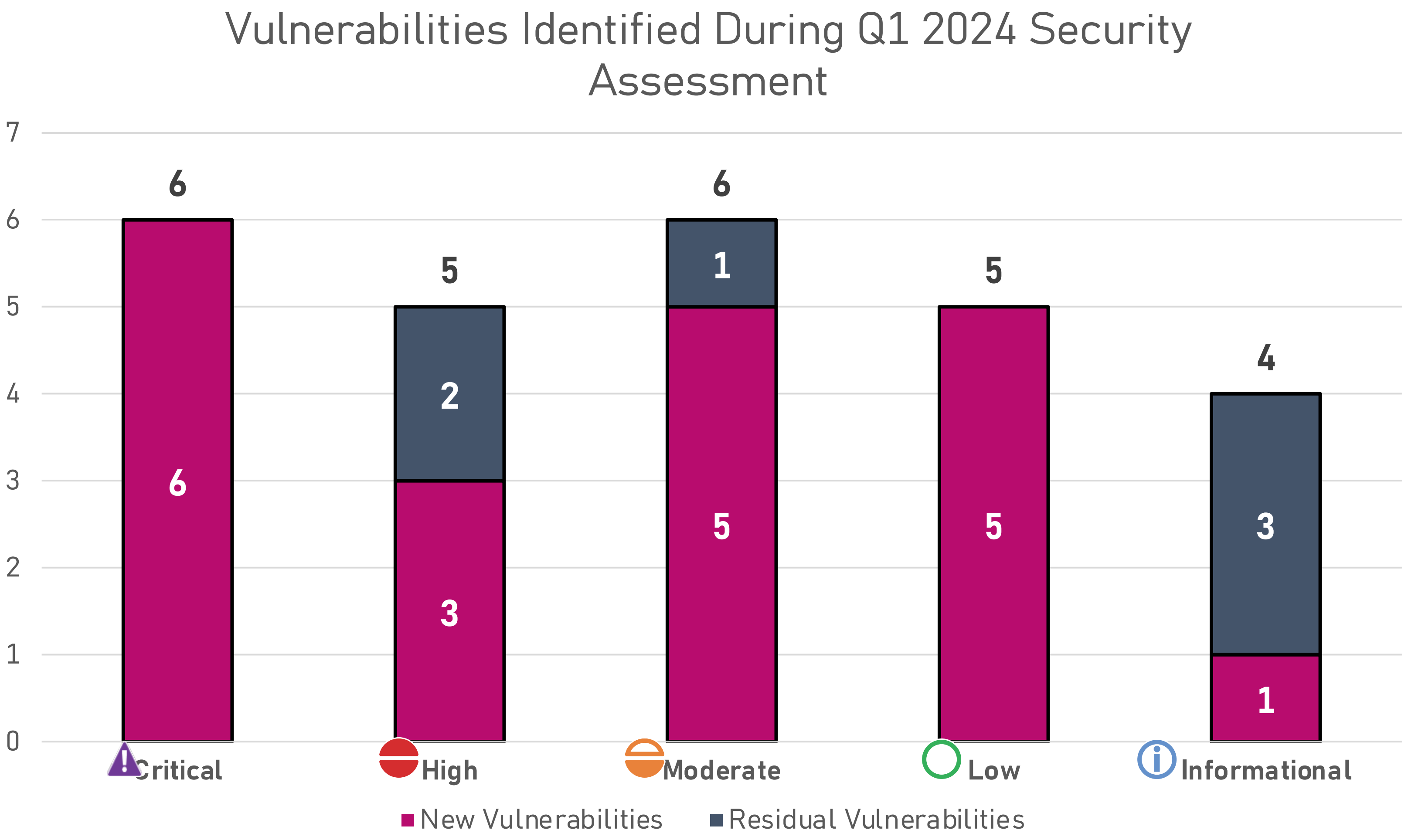
HIGH

MODERATE

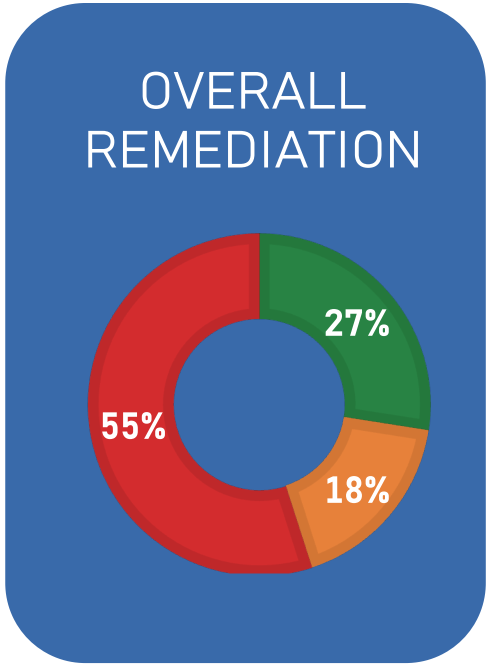
LOW

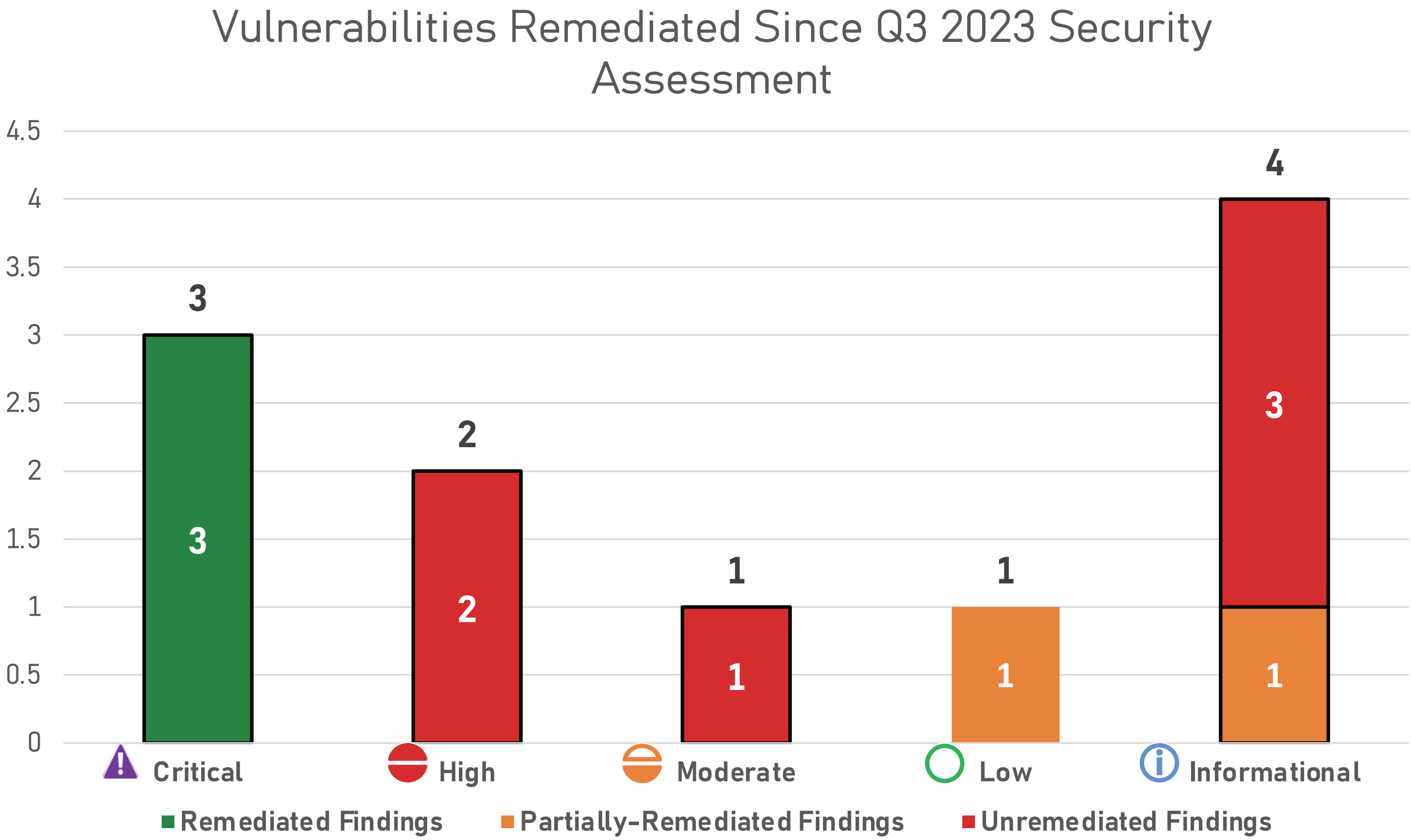
INFORMATIONAL

Findings Distribution



Residual Risk





Additional Items

Social Engineering

Radio Emissions

Security Strengths

Strong Network Segmentation

Active Monitoring and Logging

Secure Guest Network

Key Finding: **Unpatched Critical Infrastructure**

Impact

- Complete Disruption of Skyport Functionality
- Significant Financial Loss and Loss of Customer Trust

Recommendation

Regularly Patch and Update Critical Systems

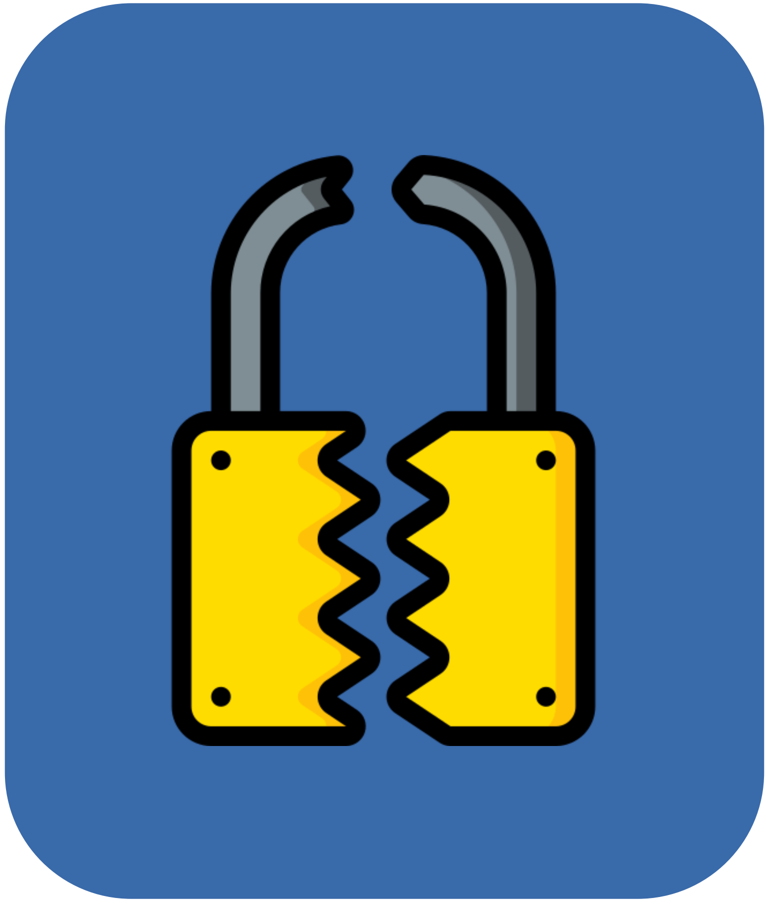
Key Finding: Weak Password for Services

Impact

- Significant Risk to Human Life and Public Endangerment
- Complete Operational Disruption

Recommendation

Strong Password Policy Implementation for Service Accounts



Key Finding: Unencrypted Sensitive Data

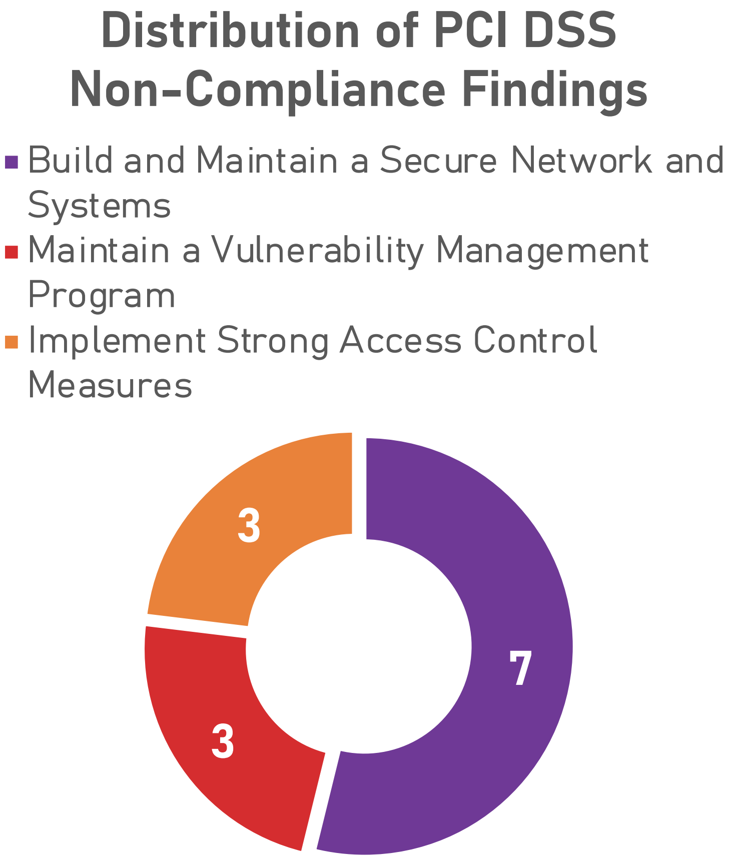
Impact

- Affects Passenger Boarding Passes
- Leads to Customer Distrust and Potential Forgery

Recommendation

Ensure all internal services are not publicly exposed

PCI DSS Compliance

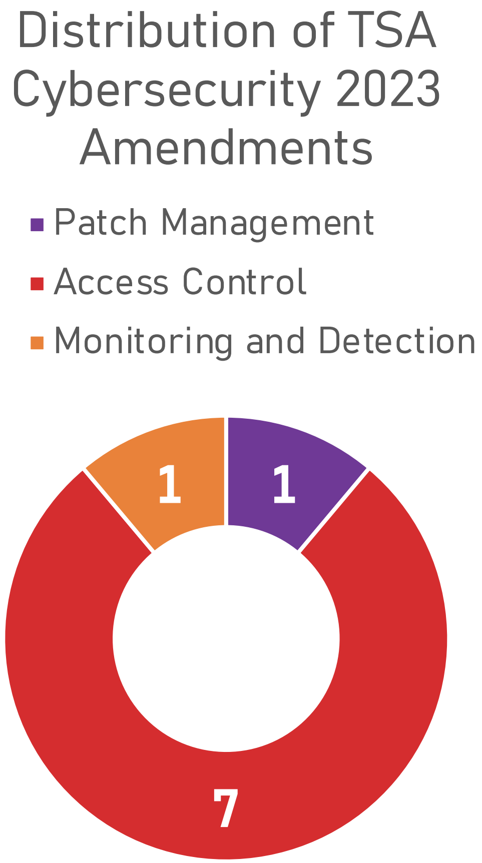


- Payment Card Industry Data Security Standard
- 13 Related findings in total
- Estimated Cost of Monthly Fines
    - $37,500/month

49 CFR § 1520 – Protection of SSI

- Sensitive Security Information (SSI)
  - Includes documents provided by TSA/DHS relating to the security of airports

TSA Cybersecurity 2023 Amendment



- An amendment aimed towards reducing cybersecurity risks & improving cyber resilience

- 9 Related findings in total
  - 7 Relating towards access control policies
  - 1 Relating to patch management
  - 1 Relating to monitoring and detection

Conclusion

Authentication

Implement multi-factor authentication where possible

Configuration

Configure software according to vendor-specific security recommendations

Patching

Implement regular updates to all software, services, and operating systems.

Policies/Compliance

Implement a strong password policy and encryption of sensitive data

Robert A. Kalka

Metropolitan Skyport

Any Questions?
Thank You!