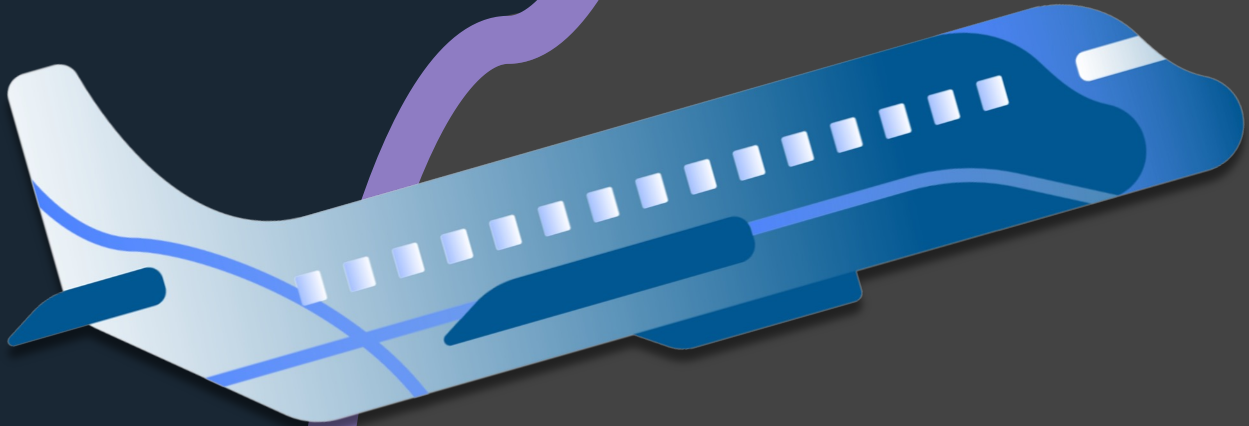
Robert A. Kalka Metropolitan Skyport Executive Debrief

Team XX



CONFIDENTIAL - DO NOT DISTRIBUTE

Introductions

XXXX - Web

XXXX - Windows/AD

XXXX - Linux

XXXXX - Compliance

XXXX - ICS/SCADA

XXXX - Cloud

Agenda

1. Overview
2. Compliance
3. Key Findings
4. Recommendations
5. Closing Remarks
6. Questions

Overview: Findings Summary

36

total vulnerabilities discovered

20

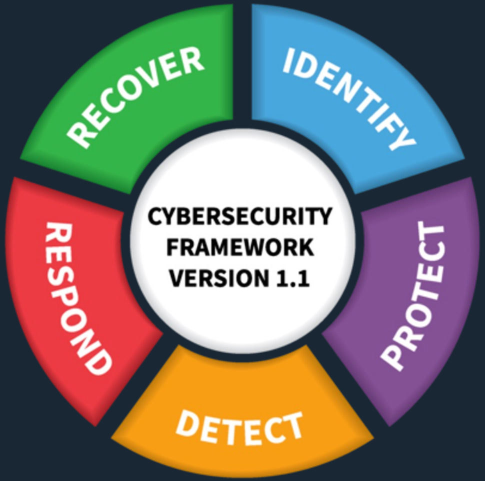
new vulnerabilities discovered

20

regulation violations

Overview: Methodology

TSA Cybersecurity Vulnerability Assessment (Form 3157)



NIST Framework for Improving Critical Infrastructure Cybersecurity

Overview: Risk Matrix

Impact

Likelihood

	0.0	0.1 - 2.9	3.0 - 4.4	4.5 - 6.9	7.0 - 8.9	9.0 - 10.0
Very High	Informational	Medium	High	High	Critical	Critical
High		Medium	Medium	High	High	Critical
Moderate		Low	Medium	Medium	High	High
Low		Low	Low	Medium	Medium	High
Very Low		Low	Low	Low	Medium	Medium

TSA Compliance

- Recent Security Directives (1582-21-01B in Oct. 2023)
- Report incidents
- Cybersecurity Implementation Plan
- Cybersecurity Vulnerability Assessment (Form 3157)
    - Section 2 - Access Management
    - Section 8 - Access Control

$14,950

Maximum fine for noncompliance with a Security Directive

GDPR - Don’t be the next victim

€ 4,372,501

Average GDPR fine in 2023

470

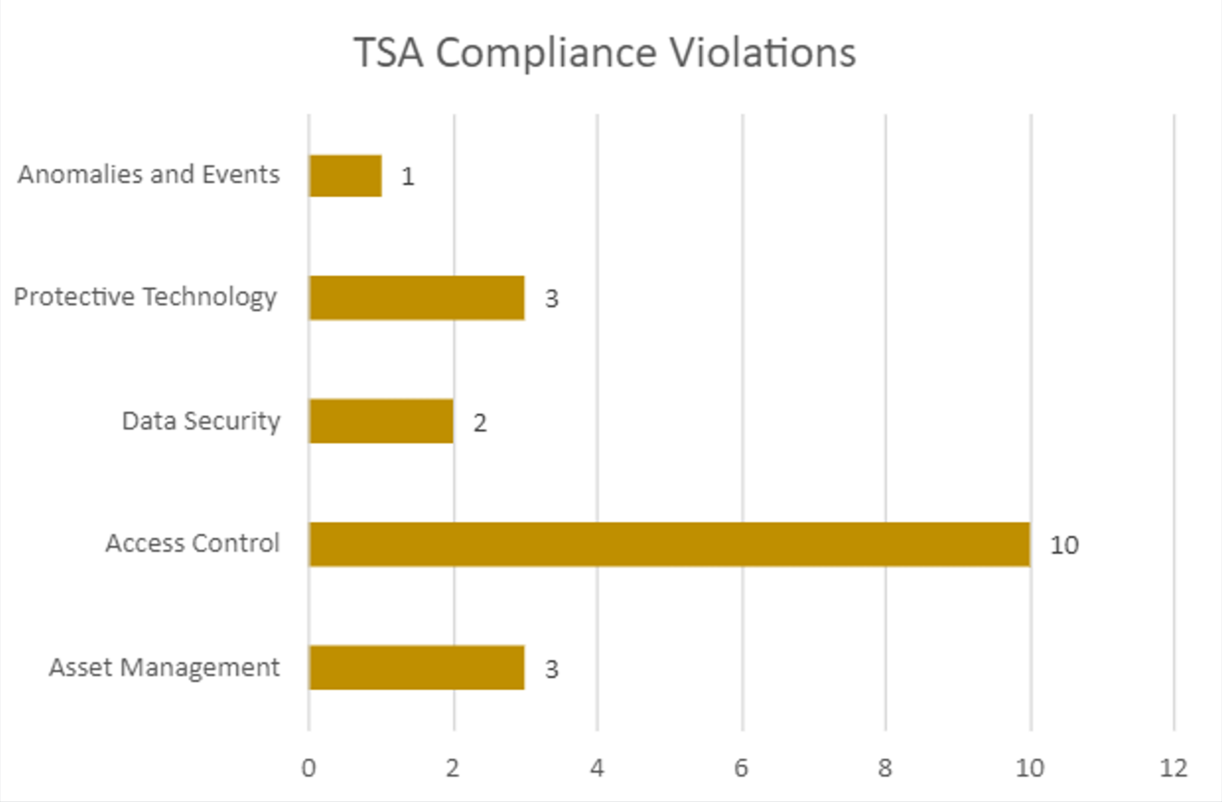
companies fined in 2023

7

GDPR violations that could be remedied

Art. 5 - Storage of Data
Art. 32 - Security of Processing

TSA Compliance Breakdown



Key Strengths

- SSH public key authentication enabled, root login disabled.
- Improvements in network segmentation
- Some mitigations against public vulnerabilities

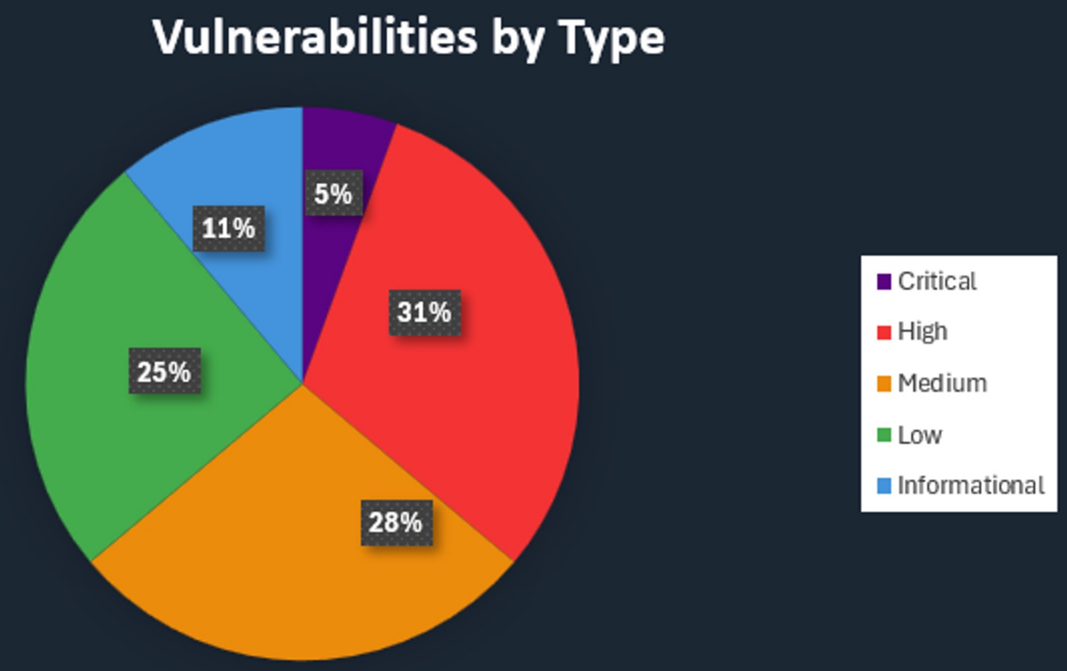
Key Findings

- Broken Access Control on People Mover
- Critical vulnerabilities on the Domain Controller (SkyControl01):
  - Zerologon
  - noPac
- Sensitive Employee Information Disclosure
- Heavily Misconfigured AWS Environment

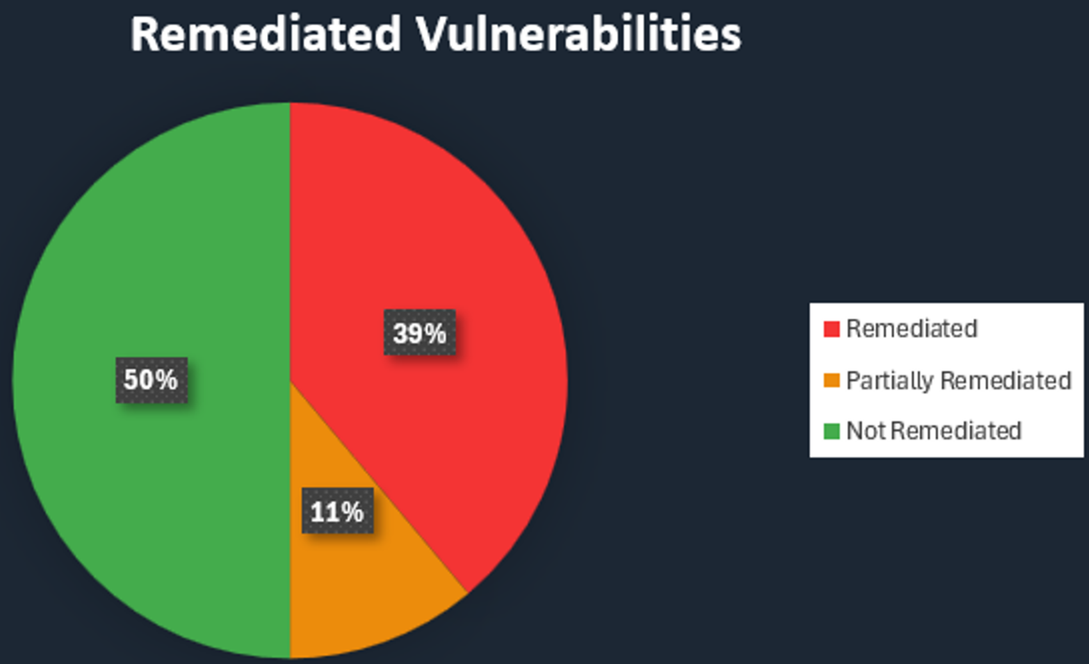
Recommendations

- Update Software
- Improve Access Controls
- Network Segmentation

Vulnerability Breakdown



Remediations



Closing Remarks

Social Engineering

Outdated Systems

Partial Remediation

Questions