Robert A. Kalka METROPOLITAN SKYPORT

Security Re-assessment
Executive Briefing

FINALS-XX

OUR TEAM

PROJECT MANAGER

SECURITY ENGINEER

COMPLIANCE CONSULTANT

LEAD PENETRATION TESTER

CUSTOMER SATISFACTION MANAGER

PENETRATION TESTER

AGENDA

Methodology

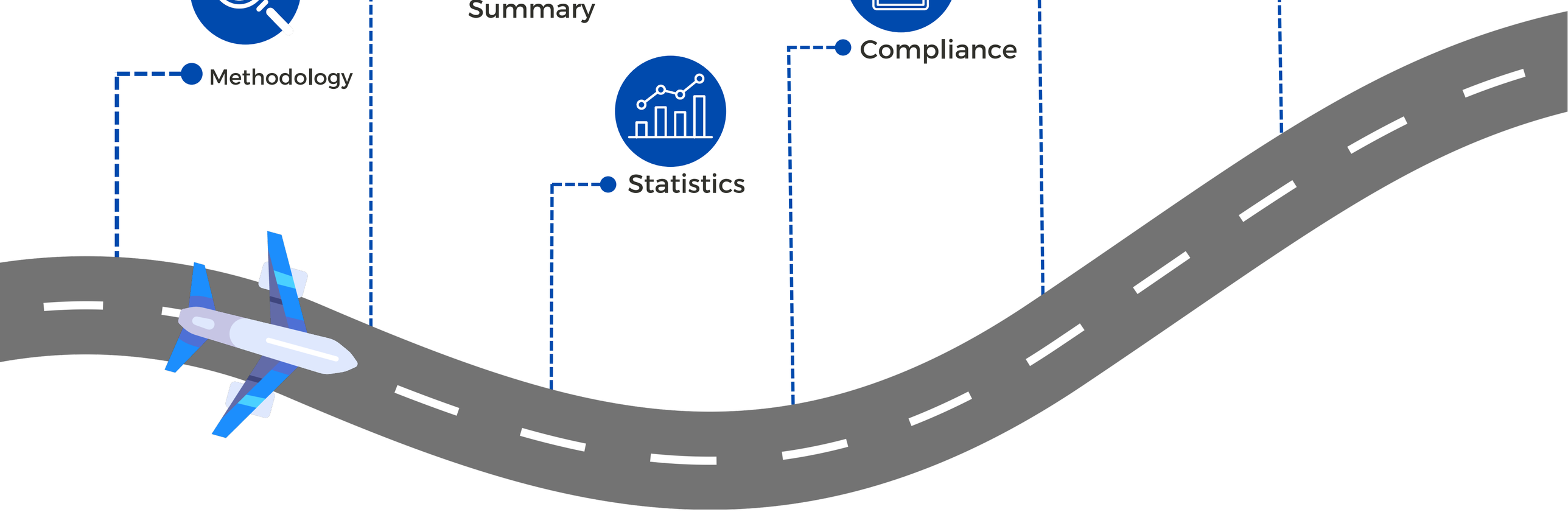
Executive Summary

Statistics

Compliance

Key Strengths

Recommendations



OUR METHODOLOGY

ASSESSMENT OBJECTIVES

General Security

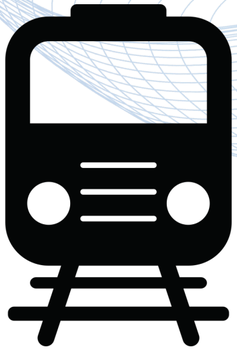
Integrity

Mitigation

Compliance

Assessment Scope

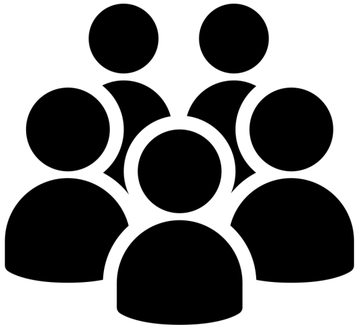
Guest



Train

aws

Cloud



User

Corporate

Executive Summary

Overall Security Posture

CRITICAL

Vulnerabilities Uncovered

42

Estimated Compliance Fines

$8.2M

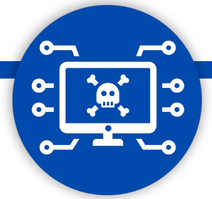
Executive Summary

Compliance Violations

73

Remediated Vulnerabilities

31%



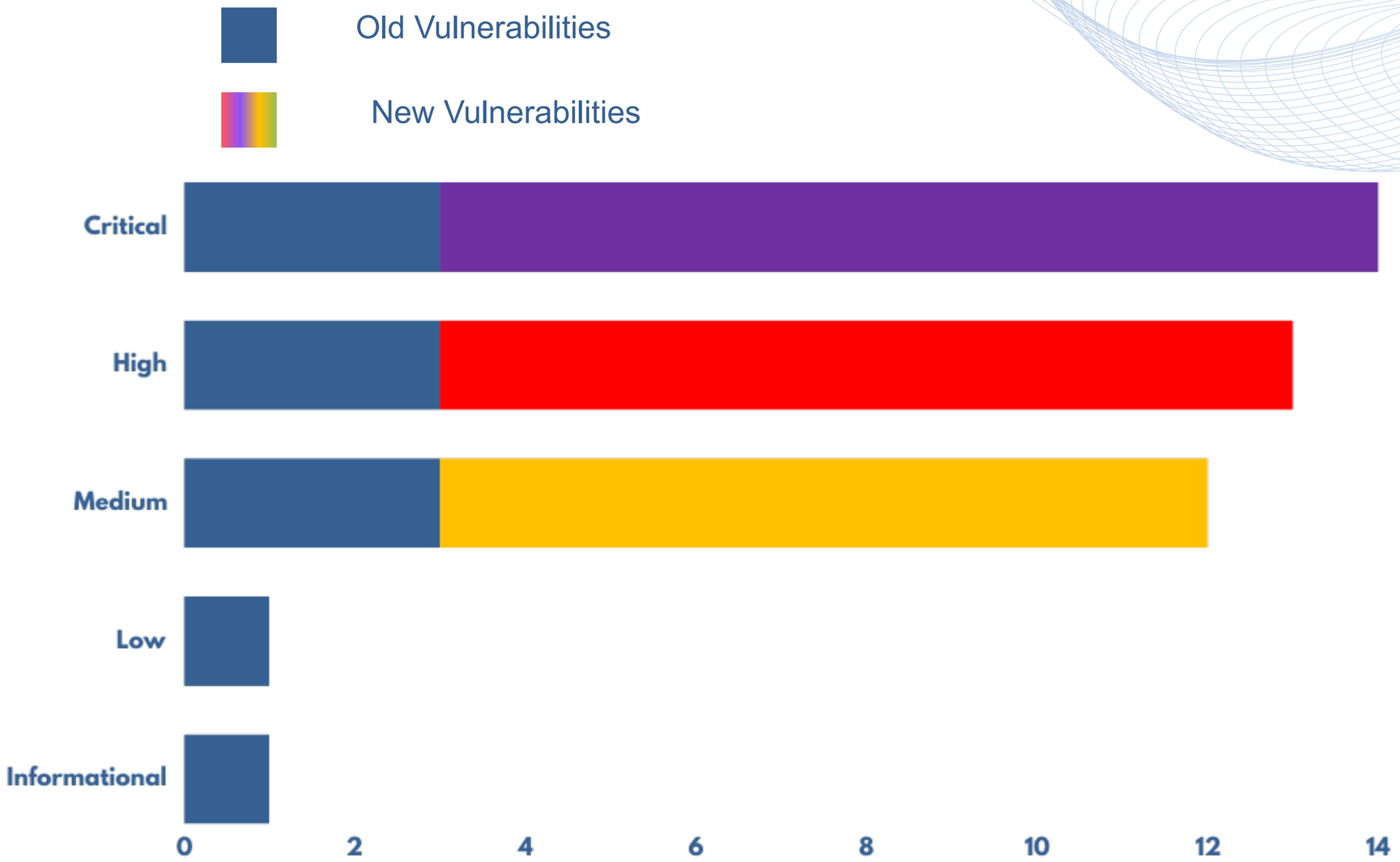
Endpoints Compromised

14

Customers with data breached

6000+

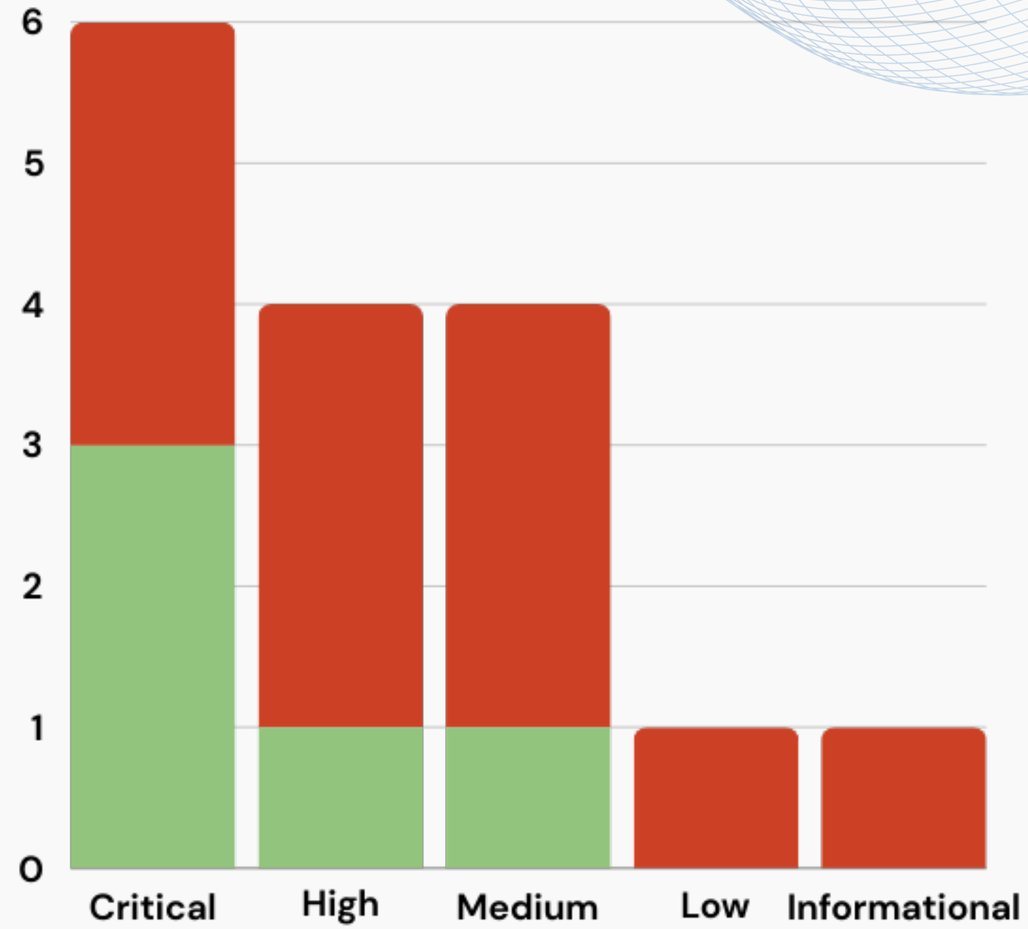
Vulnerabilities Found



Inherent Risk

Unremediated Vulnerability

Patched Vulnerability



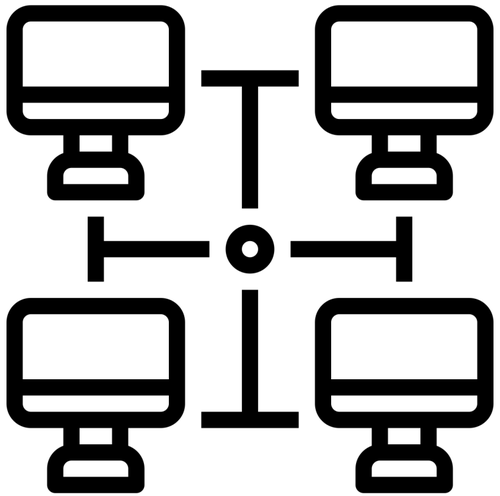
Compliance Overview

PCI-DSS

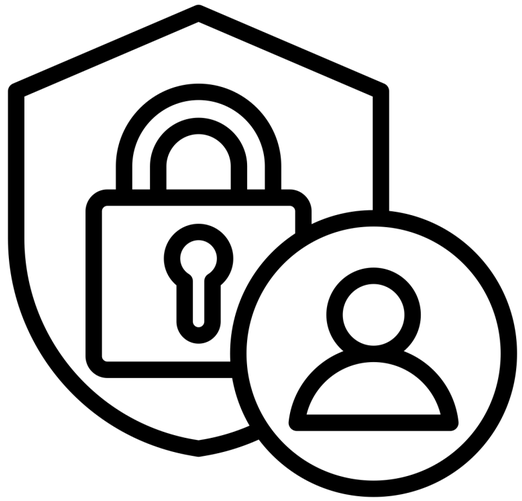
TSA'S CYBER SECURITY REQUIREMENTS

Compliance Review: PCI-DSS & TSA

UNENCRYPTED
CUSTOMER CARD DATA



NETWORK SEGREGATION



ACCESS CONTROL

COMPLIANCE: PCI-DSS

No. of violations

57

Estimated Fines

$7.6M

- Lack of cardholder data protection
- Excessive storage of sensitive cardholder data.

COMPLIANCE: TSA'S CYBER SECURITY REQUIREMENTS

No. of violations

16

Estimated Fines

$650k

- Lack of Proper Network Segmentation
- Unpatched Software

Key Strengths

Firewall

- 90% of reported vulnerabilities were found after taking down the firewall during the assessment

Key Strengths

Operational Security Awareness

- None of the publicly available info found impacted RAKMS' security in a critical manner

Key Areas For Improvement

Security Solutions

Access Control Mechanisms

Operational Security

- Malicious software was not detected by Anti-Viruses
- Implementing advanced malware detection software

Key Areas For Improvement

Access Control Mechanisms

- Authentication best practices were not followed in storage and processing
- Educate technical staff about authentication best practices

Operational Security

Key Areas For Improvement

Social Engineering

- Convinced a staff member to execute malicious software on RAKMS systems
- Conduct an operational awareness training for all employees

Conclusion

Less Secure

Less Compliant

Huge Room for Improvement

Questions & Answers

Thank you for your time!

Don’t hesitate to contact us, if you have any questions:
Finals-XX@cptc.team

Let's Fly Together
Safeguarding Every Journey, Every Day

Appendix I

CVSS 3.1 Scoring	
Severity	**Score**
Informational	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

RISK MATRIX		IMPACT			
LIKELIHOOD		LOW	MEDIUM	HIGH	CRITICAL
	RARE	LOW	LOW	MEDIUM	MEDIUM
	UNLIKELY	LOW	MEDIUM	HIGH	HIGH
	POSSIBLE	LOW	MEDIUM	HIGH	CRITICAL
	PROBABLE	LOW	MEDIUM	CRITICAL	CRITICAL