Robert A. Kalka

Metropolitan Skyport

Security Assessment Briefing

Team XX

January 14, 2024

CONFIDENTIAL - DO NOT DISTRIBUTE

Agenda

01 Introductions

02 Executive Summary

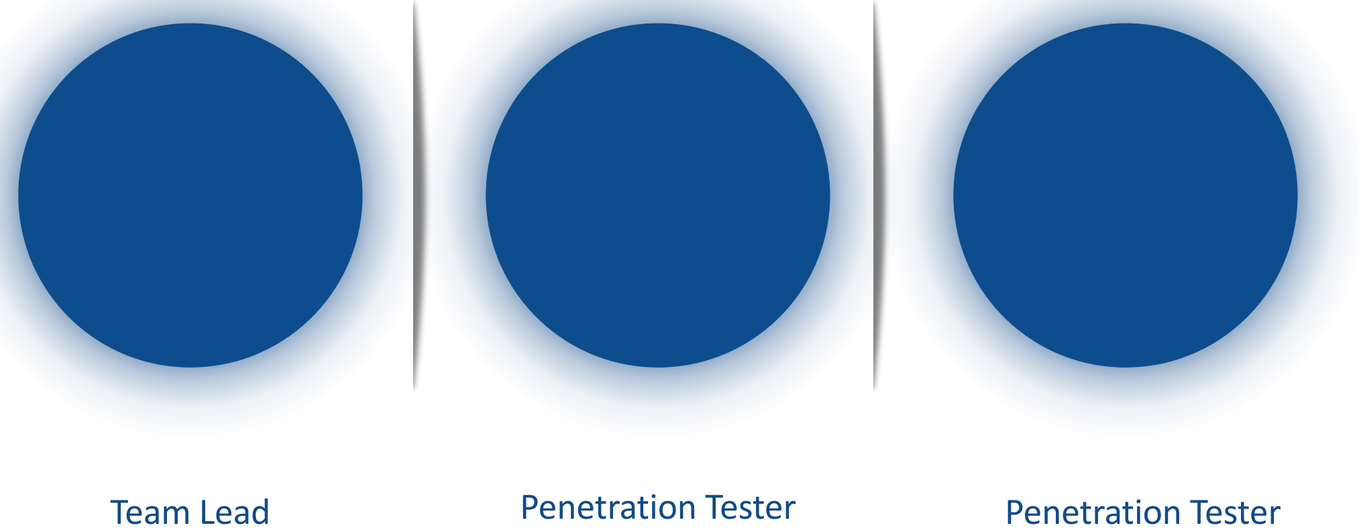
03 Reassessment Overview

04 Compliance

05 Reccomendations

06 Conclusion

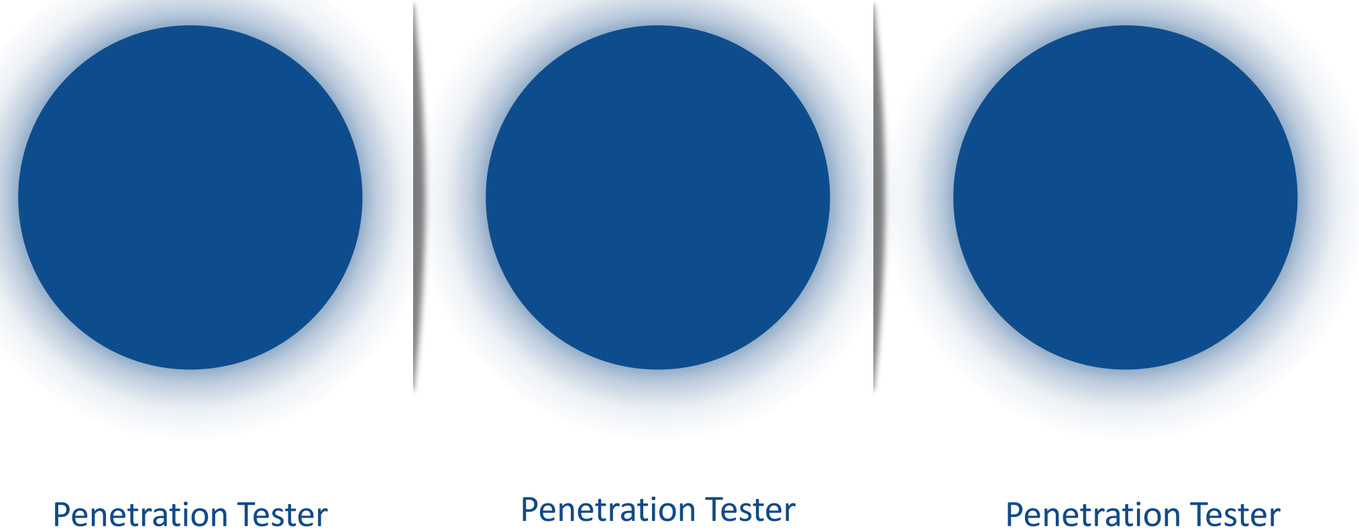
Introductions: Meet Our Team



Team Lead

Penetration Tester

Penetration Tester



Penetration Tester

Penetration Tester

Penetration Tester

EXECUTIVE SUMMARY: RESULTS

30

Total Vulnerabilities Discovered

$50,000 /MONTH

Potential Fines and Loses

100%

Amount of Network with Findings

11

New Vulnerabilities Discovered

10+

Regulations and Compliance Violations

100%

Users with Personal information exposed

EXECUTIVE SUMMARY: OBJECTIVES

Security

Evaluate compliance with commonly recommended security practices and the overall security stance.

Compliance

Validate conformity with compliance frameworks, including PCI-DSS and GDPR.

Social Engineering

Evaluate the staff's recognition and response to social engineering techniques.

EXECUTIVE SUMMARY: RISK METRICS

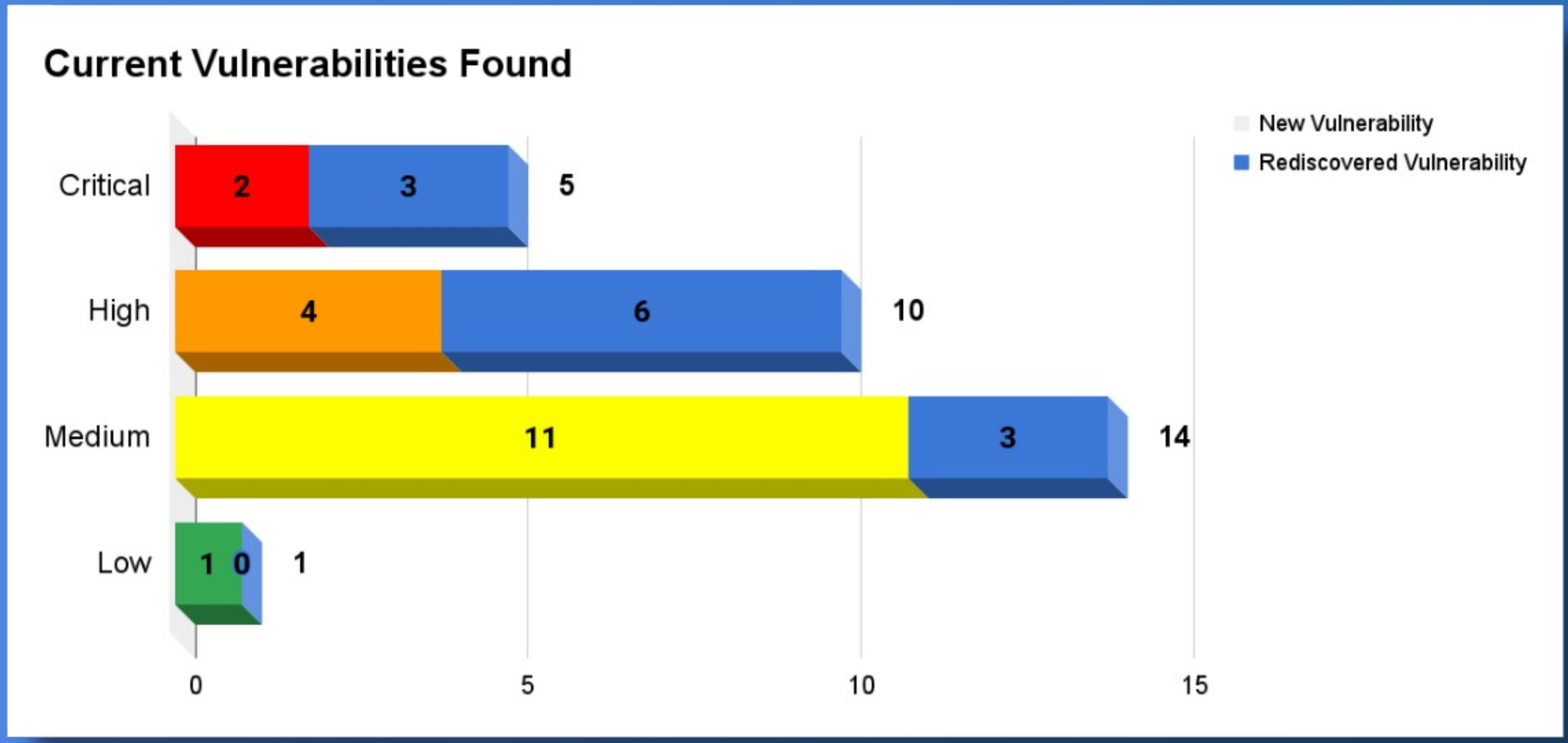
IMPACT

LIKELIHOOD

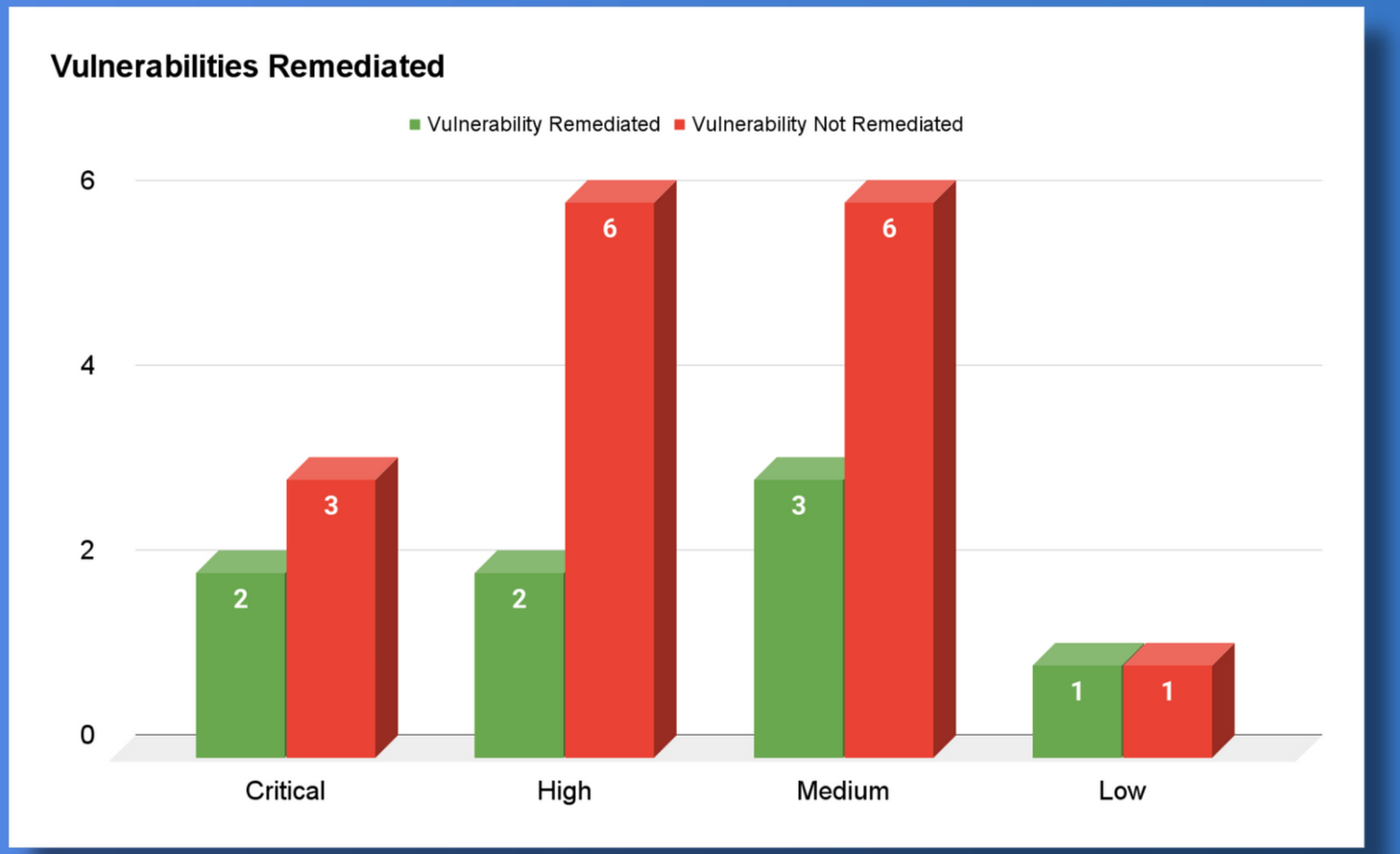
	Low	Medium	High	Critical
Low	Low	Low	Medium	Medium
Medium	Low	Medium	High	High
High	Low	Medium	High	Critical
Critical	Low	Medium	Critical	Critical

Team XX employs the **Common Vulnerability Scoring System (CVSS) 4.0**, a widely recognized standard for assessing the severity of security vulnerabilities. Utilizing CVSS 4.0, we meticulously evaluate and prioritize potential risks, enabling a data-driven approach to address and remediate vulnerabilities within the Robert A. Kalka Metropolitan Skyport's aviation infrastructure.

REASSESSMENT SUMMARY: VULNERABILITIES



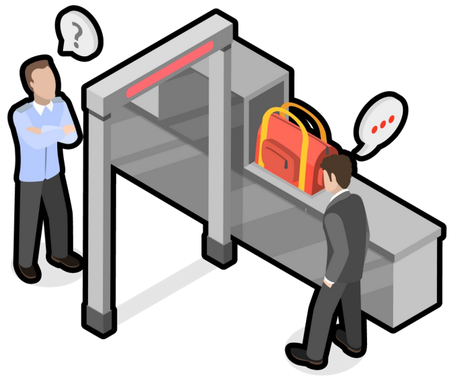
REASSESSMENT SUMMARY: RISK



Estimated Impact

- Many improvements have been made to the network
- Previous findings leave RAKMS open to continued exploitation
- Continued fines due to compliance violations

COMPLIANCE



TSA Cybersecurity Requriements

This amendment underscores the critical need for heightened cybersecurity measures in the aviation sector, particularly in light of persistent threats against U.S. critical infrastructure.

PCI DSS

PCI DSS is a security standard that ensures safe handling of credit card information during transactions to prevent data breaches in organizations dealing with credit card data.

GDPR

GDPR is a set of rules ensuring that companies handle personal information of European citizens with care, giving individuals control over how their data is collected and used.

COMPLIANCE: TSA REQURIEMENTS

TSA Cybersecurity Violations

7

The most common issue was the amount of cool cats we had within the network. They were so cool omg!

COMPLIANCE: PCI DSS

PCI DSS Violations

3

Estimated Fines

$10,000/month

The most common issue was the amount of cool cats we had within the network. They were so cool omg!

COMPLIANCE: GDPR

GDPR Violations

2

Estimated Fines

$40,000

The most common issue was the amount of cool cats we had within the network. They were so cool omg!

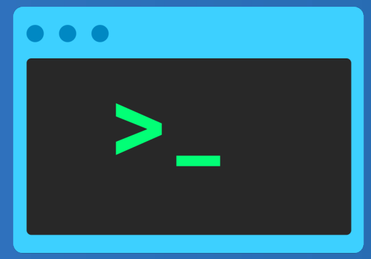
RECOMMENDATIONS: PRINCIPAL STRENGTHS

Robert A. Kalka

Metropolitan Skyport

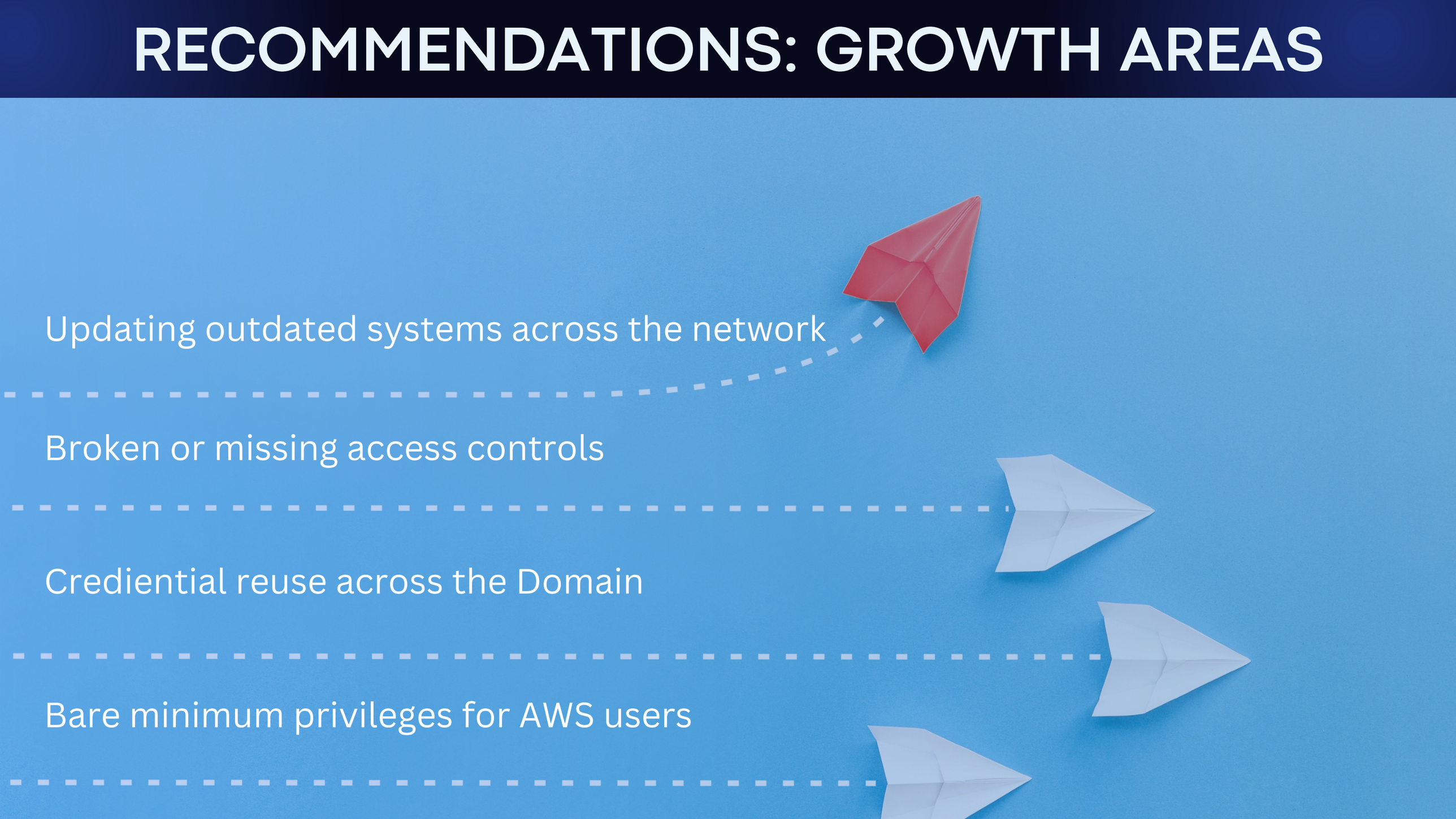
Social Engineering Awareness

Strong Lockout Policy



Secure Linux Hosts

RECOMMENDATIONS: GROWTH AREAS



Updating outdated systems across the network

Broken or missing access controls

Crediential reuse across the Domain

Bare minimum privileges for AWS users

Conclusion

Robert A. Kalka

Metropolitan Skyport

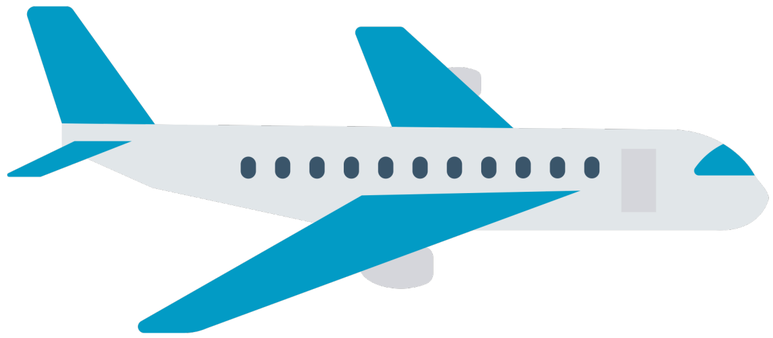
Showed Improvement

Less vulnerable

Password Reuse

Compliance Violations

Thank you for your time.



Robert A. Kalka

Metropolitan Skyport

Questions?

finals-xx@cptc.team