ROBERT A. KALKA METROPOLITAN SKYPORT EXECUTIVE BRIEFING

PRESENTED BY FINALS-XX

Robert A. Kalka

Metropolitan Skyport

AGENDA

AGENDA

1. INTRODUCTIONS
2. REASSESSMENT SUMMARY
3. COMPLIANCE
4. RECOMMENDATIONS
5. CONCLUSION

INTRODUCTIONS

INTRODUCTIONS

Manager

Senior Consultant

Senior Consultant

Consultant

Consultant

Consultant

REASSESSMENT SUMMARY

RESULTS

REASSESSMENT SUMMARY

RESULTS

Robert A. Kalka

Metropolitan Skyport

33
total vulnerabilities discovered

20
new vulnerabilities discovered

Critical
risk of compromise

130+
regulation violations

100+
employees potentially had exposed data

REASSESSMENT SUMMARY

OBJECTIVES

REASSESSMENT SUMMARY

OBJECTIVES

REASSESSMENT SUMMARY

OBJECTIVES

Security

Assess adherence to general security best practices and defense against specialized threats

Safety

Ensure all testing was performed strategically and safely with explicit approval

Social Engineering

Test the awareness of staff against social engineering tactics

Compliance

Verify compliance with compliance frameworks TSA and FAA.

REASSESSMENT SUMMARY

OBJECTIVES

REASSESSMENT SUMMARY

OBJECTIVES

SCOPE

Corporate Network

Tram Network

Guest Network

User Network

Cloud Infrastructure (AWS)

REASSESSMENT SUMMARY

RISK MATRIX

REASSESSMENT SUMMARY

RISK MATRIX

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 uses a custom heuristic framework for measuring impact, likelihood and overall criticality of technical findings together with the **Common Vulnerability Scoring System 3.1** to gain full coverage of both technical and business risk.

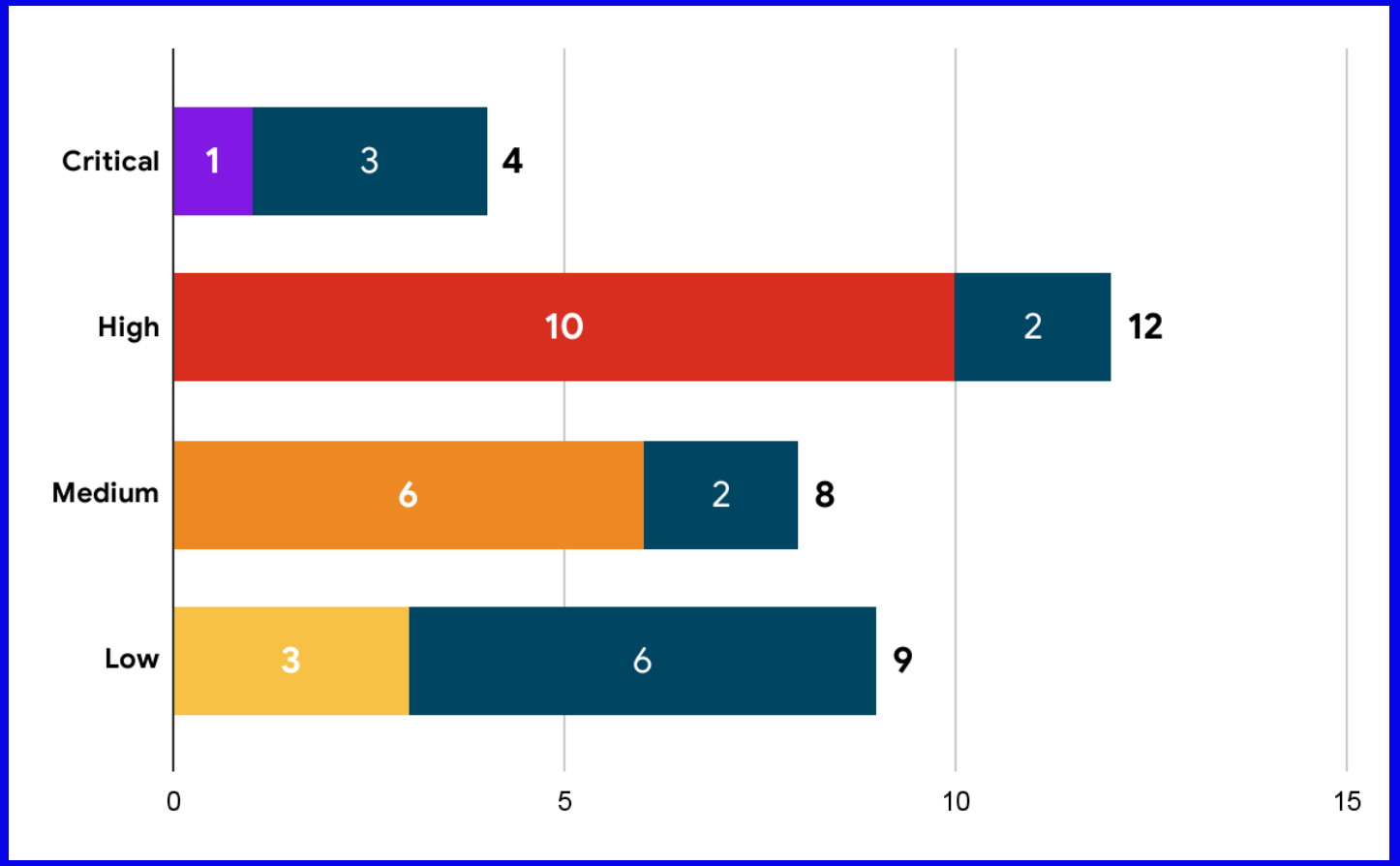
REASSESSMENT SUMMARY

RISK TRENDS

REASSESSMENT SUMMARY

RISK TRENDS

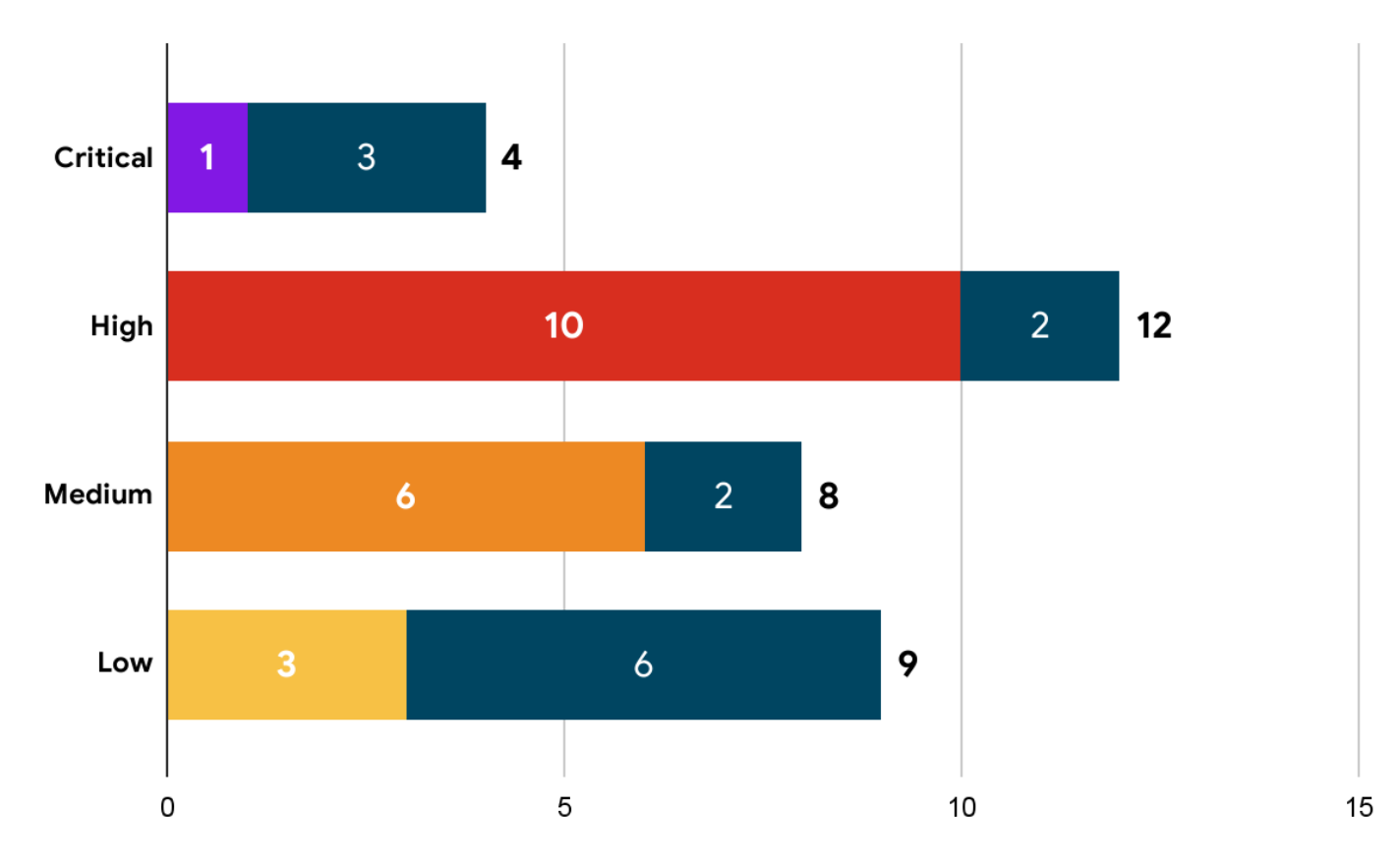
CURRENT VULNERABILITIES



REASSESSMENT SUMMARY

RISK TRENDS

CURRENT VULNERABILITIES

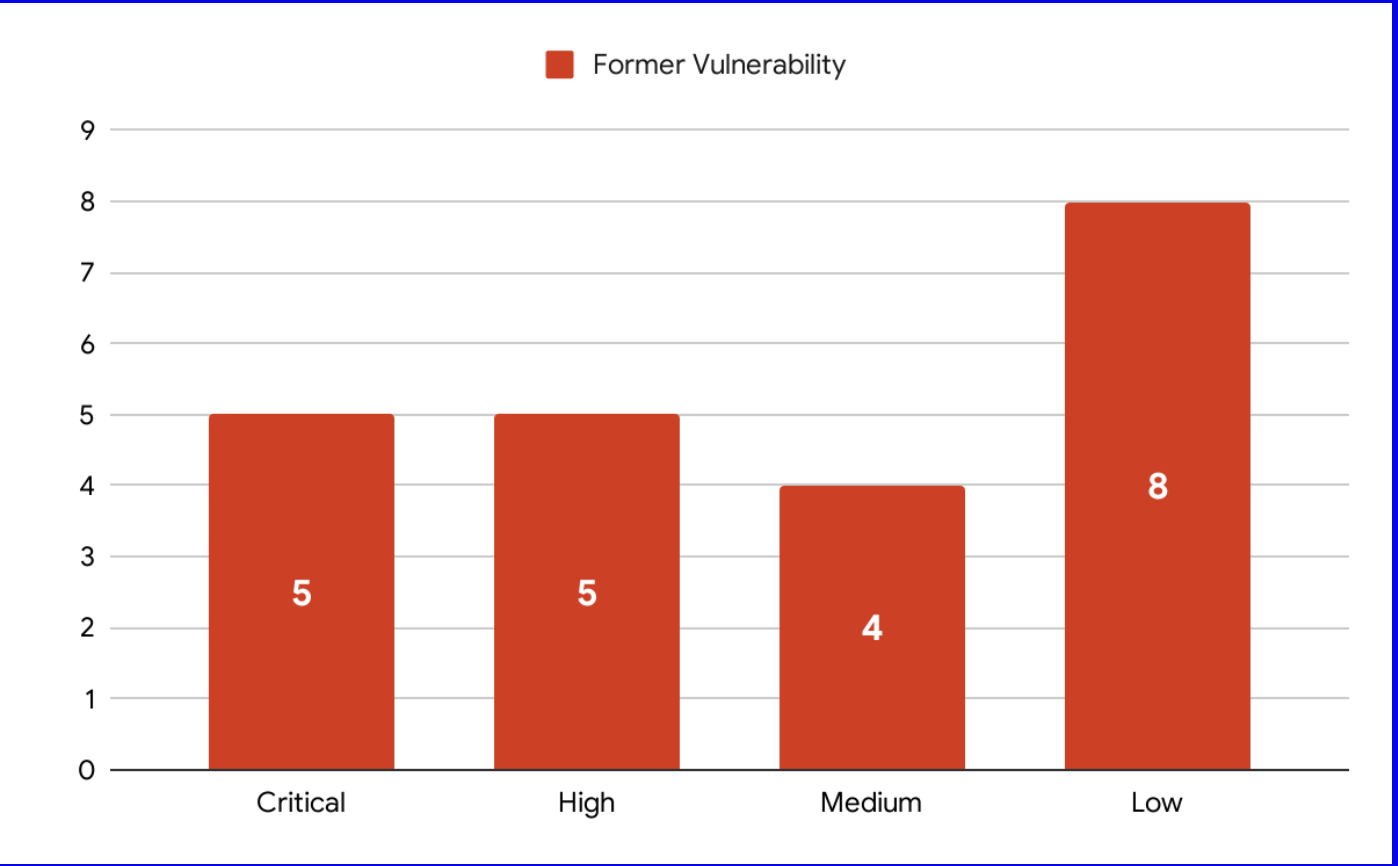


KEY TRENDS IN VULNS

- Incompletely patched systems (4)
- Access control misconfigurations (8)
- Publicly facing beta internal tools (3)
- Lacking baked-in security processes

REASSESSMENT SUMMARY

RISK TRENDS

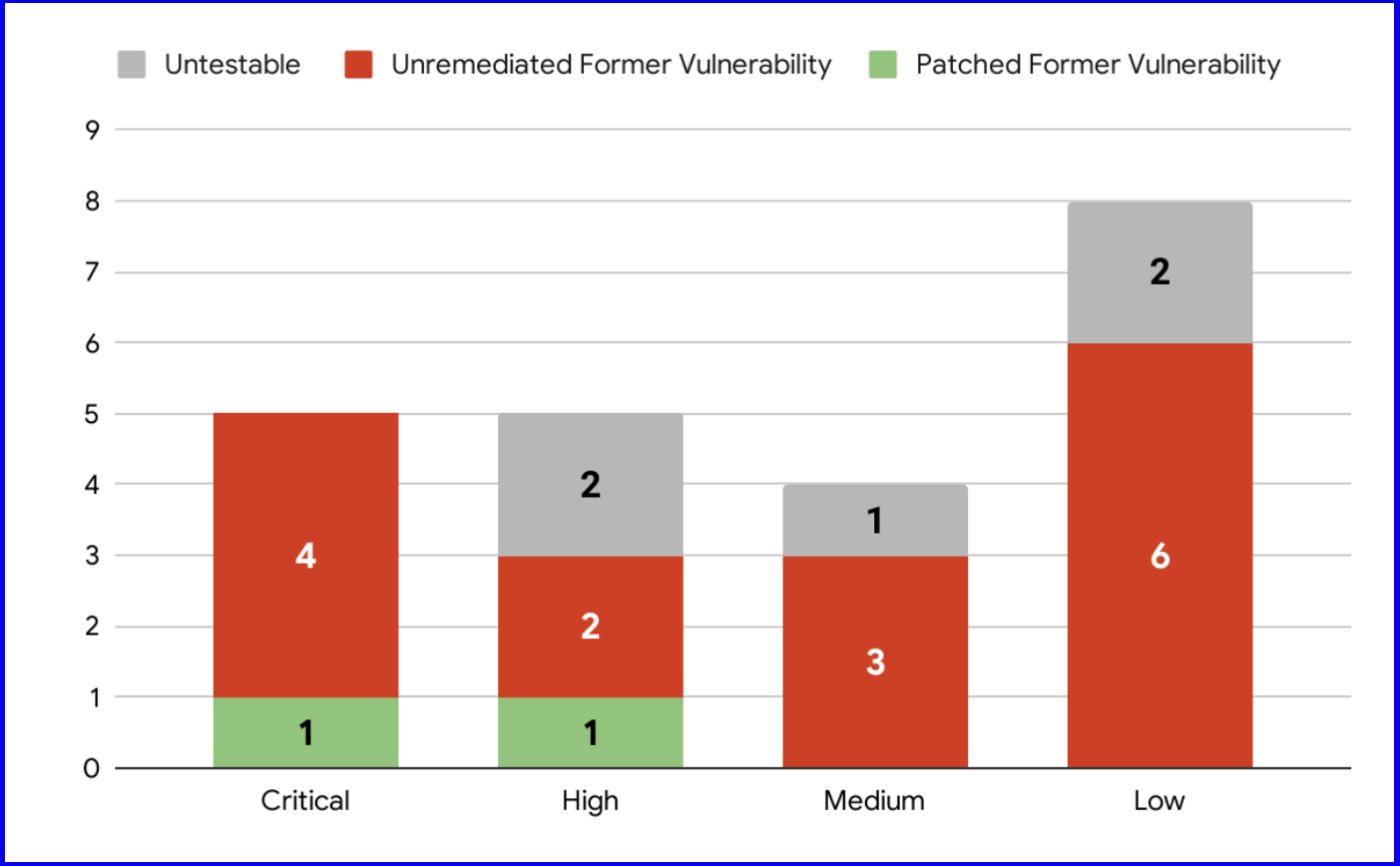


RESIDUAL RISK: BEFORE

- Vulnerable corporate network
- Exposed internal beta tools on public cloud infrastructure
- Insecurely designed tram network

REASSESSMENT SUMMARY

RISK TRENDS



RESIDUAL RISK: AFTER

- Vulnerable corporate network
- Exposed internal beta tools on public cloud infrastructure

REASSESSMENT SUMMARY

SPECIALIZED THREATS

REASSESSMENT SUMMARY

SPECIALIZED THREATS

RF ATTACKS

2

Investigations of RF signals

1

benign signal found

1

unidentifiable signal found

REASSESSMENT SUMMARY

SPECIALIZED THREATS

RF ATTACKS

SOCIAL ENGINEERING

1
vhishing assessment

1
phishing assessment

0
employees caught

COMPLIANCE

COMPLIANCE

FAA AIP

A FAA funded grant provided to improve airport infrastructure. Airport projects vying for the grant must comply with the cybersecurity requirements.

COMPLIANCE

FAA AIP

TSA

A set of United States security directives managing airport cybersecurity to ensure national, economic, and public security. All United States airports **must follow the directives.**

COMPLIANCE

FAA AIP

14

violations

$10,000-$500,000

in estimated losses

TSA

120

violations

$1,742,500-$4,485,240

in estimated fines

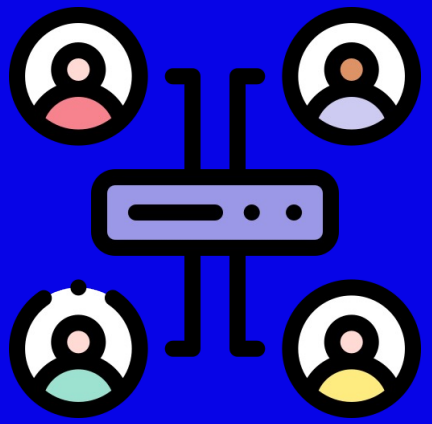
RECOMMENDATIONS

KEY STRENGTHS

RECOMMENDATIONS

KEY STRENGTHS

Social Engineering Awareness



Network Segmentation

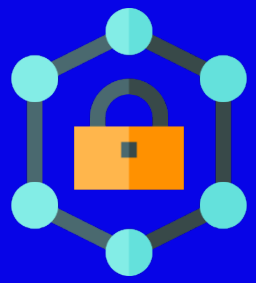
Logging and Monitoring

RECOMMENDATIONS

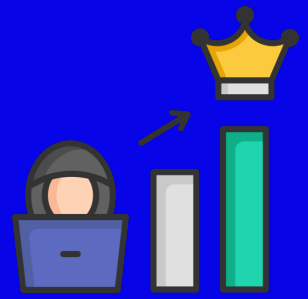
AREAS OF IMPROVEMENT

RECOMMENDATIONS

AREAS OF IMPROVEMENT



ACCESS CONTROLS

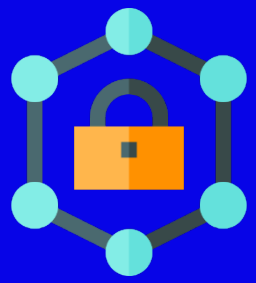


EXCESSIVE PRIVILEGES

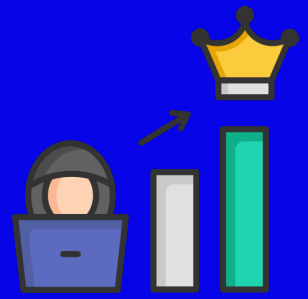
FULLY UPDATE SYSTEMS

RECOMMENDATIONS

AREAS OF IMPROVEMENT



ACCESS CONTROLS

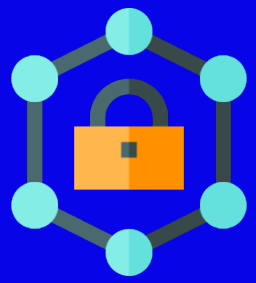


EXCESSIVE PRIVILEGES

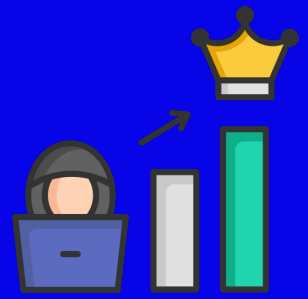
FULLY UPDATE SYSTEMS

RECOMMENDATIONS

AREAS OF IMPROVEMENT



ACCESS CONTROLS



EXCESSIVE PRIVILEGES

FULLY UPDATE SYSTEMS

CONCLUSION

CONCLUSION

1. GOOD PROGRESS
2. CONTINUED PROGRESS
3. SOCIAL ENGINEERING AWARENESS
4. BAKED-IN SECURITY

Robert A. Kalka

Metropolitan Skyport

THANK YOU FOR YOUR TIME

QUESTIONS?

finals-xx@cptc.team

Robert A. Kalka

Metropolitan Skyport