The Cozy Croissant Executive Briefing

TEAM-XX

CONFIDENTIAL - DO NOT DISTRIBUTE

Agenda

INTRODUCTIONS
01

COMPLIANCE
04

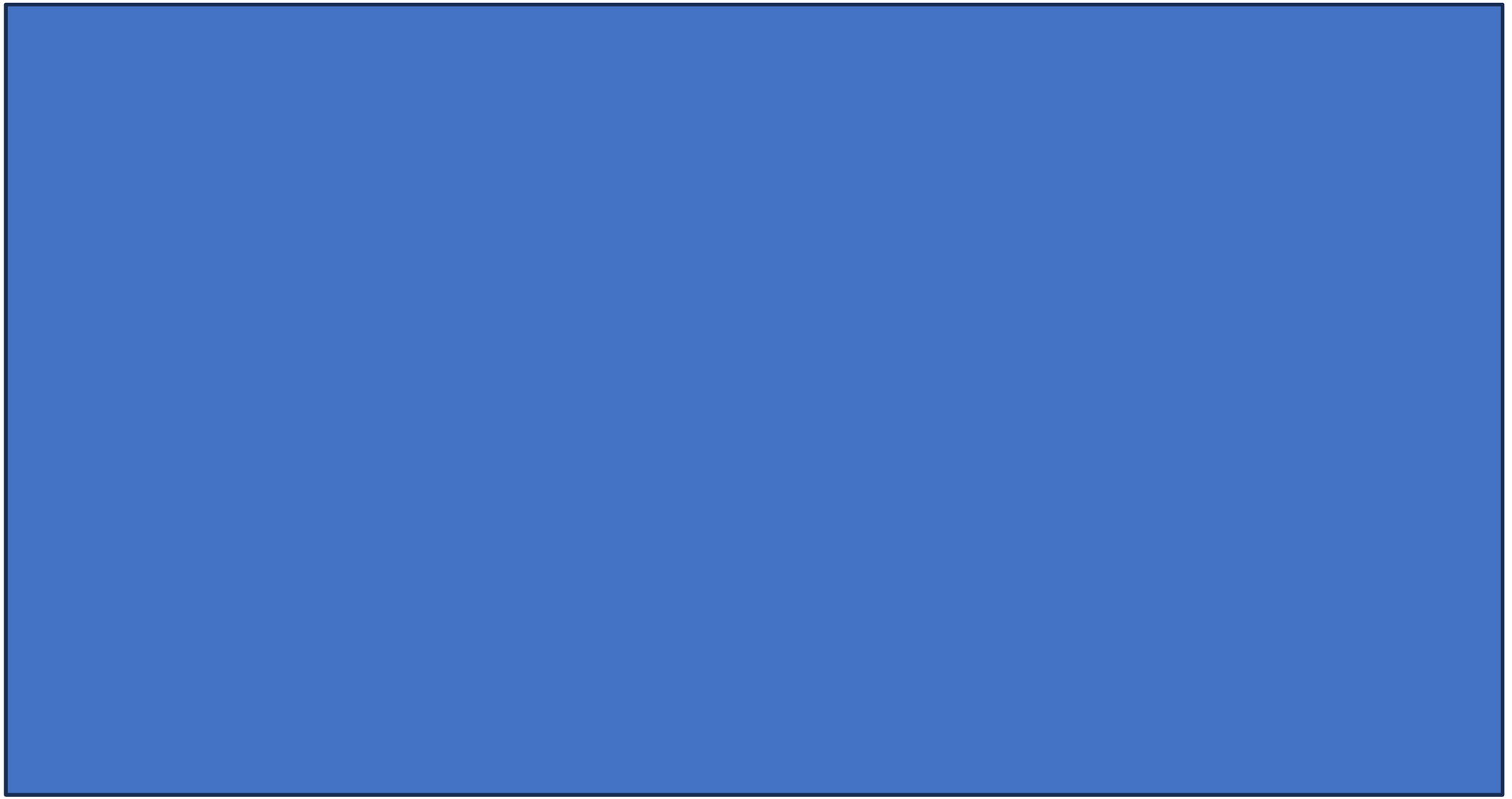
EXECUTIVE SUMMARY
02

RECOMMENDATIONS
05

REASSESSMENT SUMMARY
03

CONCLUSION
06

Introductions



Executive Summary: Results

39

total vulnerabilities discovered

25

new vulnerabilities discovered

100%

of endpoints compromised

$6.56m

potential losses in fines

100

regulation violations

1,000+

customers potentially had exposed data

Executive Summary: Objectives

General Security

Assess adherence to general security best practices and the overall security posture

Integrity

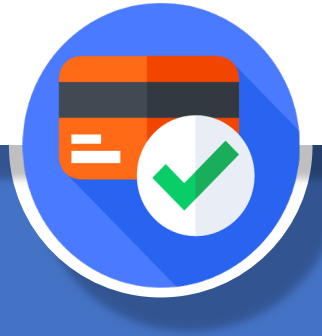
Validate the integrity of custom business processes and customer experience systems

Social Engineering

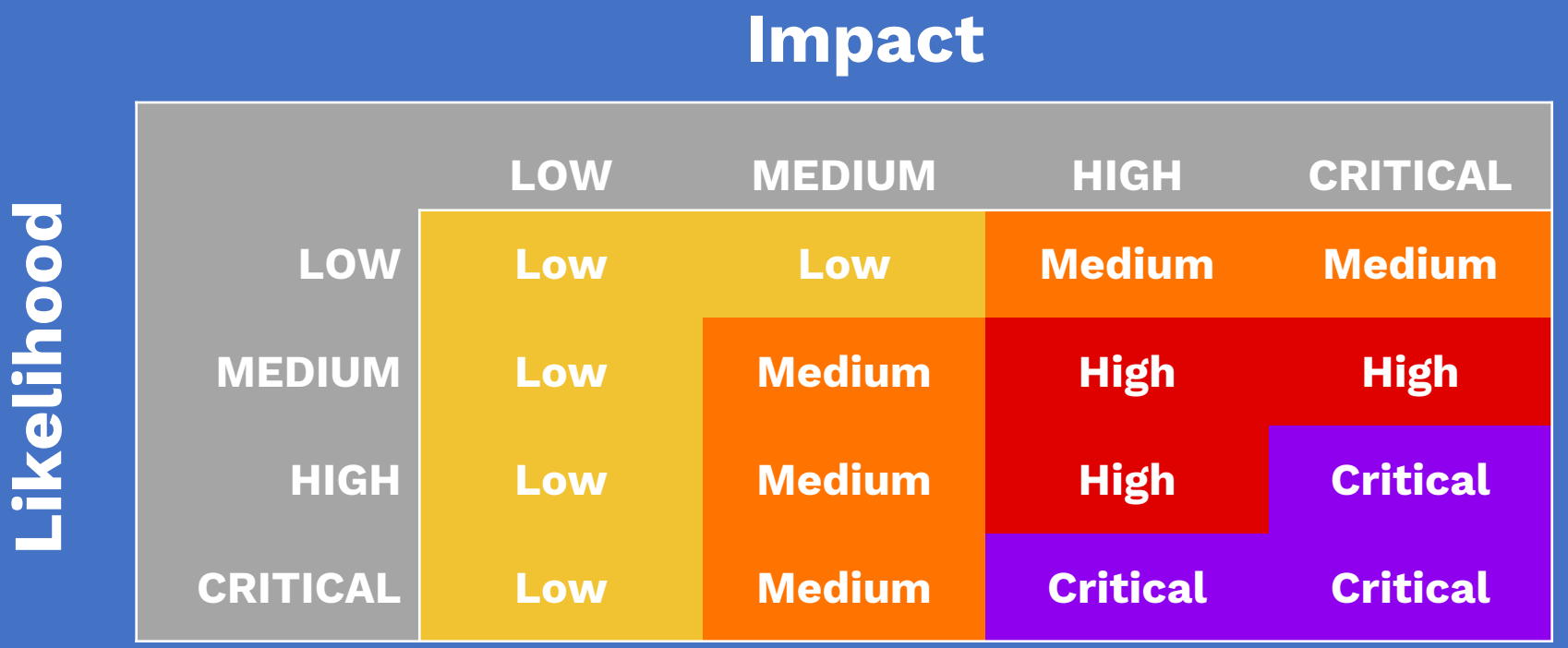
Test the awareness of staff against social engineering tactics

Compliance

Verify compliance with various compliance frameworks including PCI-DSS and GDPR.



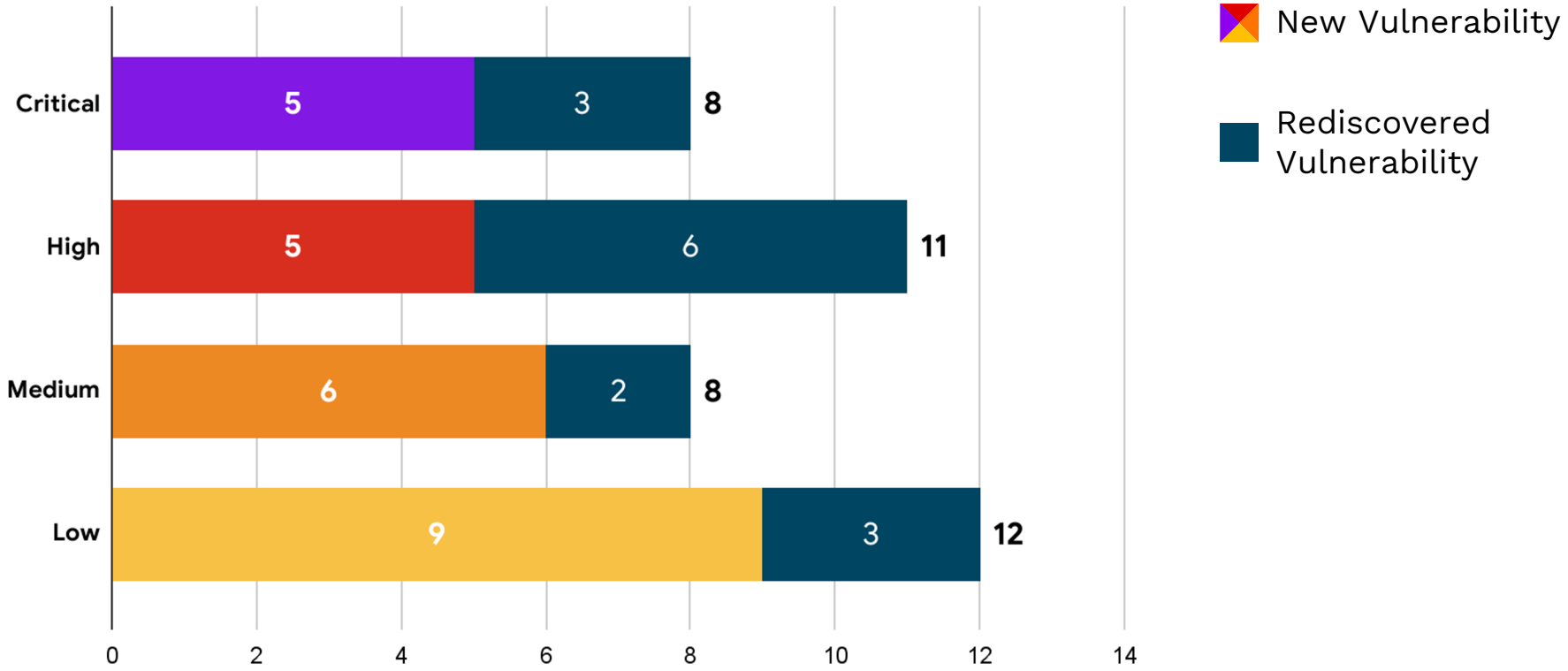
Executive Summary: Risk Metrics



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.

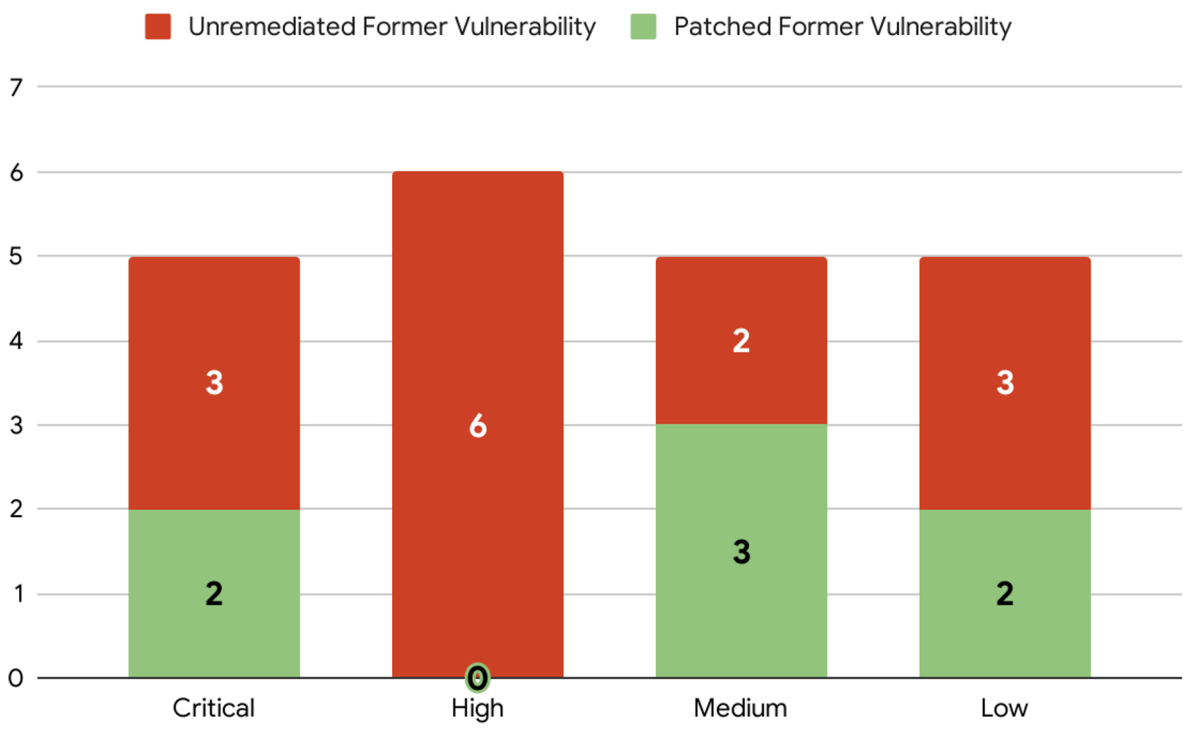
Reassessment Summary:

Current Vulnerabilities Found



Reassessment Summary: Residual Risk

Vulnerabilities Remediated



Estimated Impact

- Compromise is highly likely due to unremediated password vulnerabilities
- Future data breaches of customer data and can lead to fines
- Vulnerabilities may lead to prevention of revenue generation

Compliance

GDPR

A European law to ensure that personal data is collected, handled, and protected under stringent law. **All organizations** which interact with any EU citizen's data **must be compliant.**

PCI DSS

A set of standards that ensures companies process, store, and transmit cardholder data securely. All major credit card companies **require PCI DSS compliance**.

Nevada Breach Disclosure

A **state law** which requires companies to **report data breaches** to affected customers as quickly as possible.

Compliance: GDPR

GDPR Violations

45

Estimated Fines

$6,440,000

The overall most prevalent issue was insecure processing of customer data.

Compliance: PCI DSS

PCI DSS Violations

53

Estimated Fines

$5,000-
$10,000/month

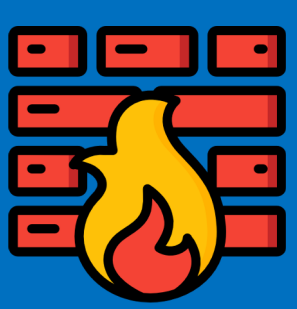
The most prevalent issues were a lack of cardholder data protection, and the excessive storage of sensitive cardholder data.

Compliance: Nevada Privacy Law

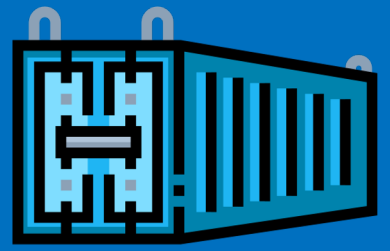
Nevada Privacy Law Violations

The most prevalent issues were services vulnerable unauthorized access which lead to unauthorized access of PII and user credentials.

Recommendations: Key Strengths



Network Segmentation



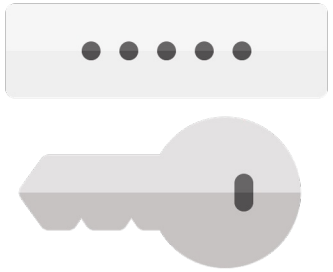
Containerized Services

Logging and Monitoring

Recommendations: Areas of Improvement

Active Directory

Social Engineering

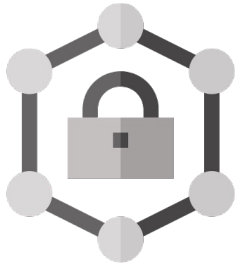


Password Policy

Team XX found TCC's Active Directory implementation to be insufficiently protecting company assets.

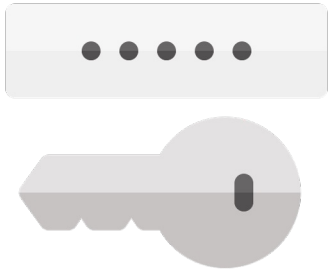
Recommendations
Ensure all systems are up to date
Implement the principle of least privilege
Improve existing configurations to be more secure

Recommendations: Areas of Improvement



Active Directory

Social Engineering

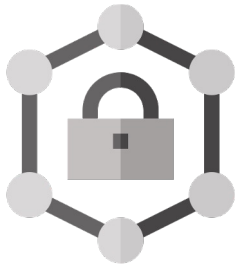


Password Policy

Team XX identified TCC employees were vulnerable to social engineering attacks.

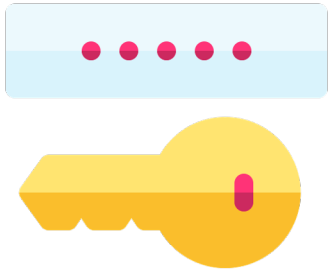
Recommendations
Implement social engineering awareness training
Ensure processes are in place for escalating potentially harmful communications
Mandate identity verification before disclosing information

Recommendations: Areas of Improvement



Active Directory

Social Engineering



Password Policy

Team XX found TCC's services reused credentials across multiple services and systems

Recommendations
Ensure passwords for Administrator accounts are rotated
Ensure all passwords are unique, complex, and securely stored
Implement Multi-Factor Authentication

Less Secure

Less Compliant

Social Engineering

Password Reuse

Conclusion

Questions?

finals-XX@cptc.team

Thank you for your time.