OUI CROISSANT

EXECUTIVE BRIEFING

PRESENTED BY FINALS-XX

AGENDA

AGENDA

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

INTRODUCTIONS

INTRODUCTIONS

Captain
Manager

Member
Senior Consultant

Member
Senior Consultant

Member
Consultant

Member
Consultant

Member
Consultant

REASSESSMENT SUMMARY

RESULTS

REASSESSMENT SUMMARY

RESULTS

24
total vulnerabilities discovered

Critical
risk of compromise

8
new vulnerabilities discovered

100+
users potentially had exposed data

REASSESSMENT SUMMARY

OBJECTIVES

REASSESSMENT SUMMARY

OBJECTIVES

REASSESSMENT SUMMARY

OBJECTIVES

Safety

Ensure all testing was performed strategically and safely with explicit approval

Security

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

AI

Evaluate the implementation of AI systems that handle company data

Social Engineering

Test the awareness of staff against social engineering tactics

REASSESSMENT SUMMARY

OBJECTIVES

REASSESSMENT SUMMARY

OBJECTIVES

SCOPE

Production Network

Development Network

yyy.chat

REASSESSMENT SUMMARY

RISK MATRIX

REASSESSMENT SUMMARY

RISK MATRIX

LIKELIHOOD	IMPACT			
	LOW	MEDIUM	HIGH	CRITICAL
LOW	LOW	LOW	MEDIUM	MEDIUM
MEDIUM	LOW	MEDIUM	HIGH	HIGH
HIGH	LOW	MEDIUM	HIGH	CRITICAL
CRITICAL	LOW	MEDIUM	CRITICAL	CRITICAL

FINALS-XX uses a custom heuristic framework for measuring impact, likelihood and overall criticality of technical findings together with the **Common Vulnerability Scoring System 4.0** to gain full coverage of both technical and business risk.

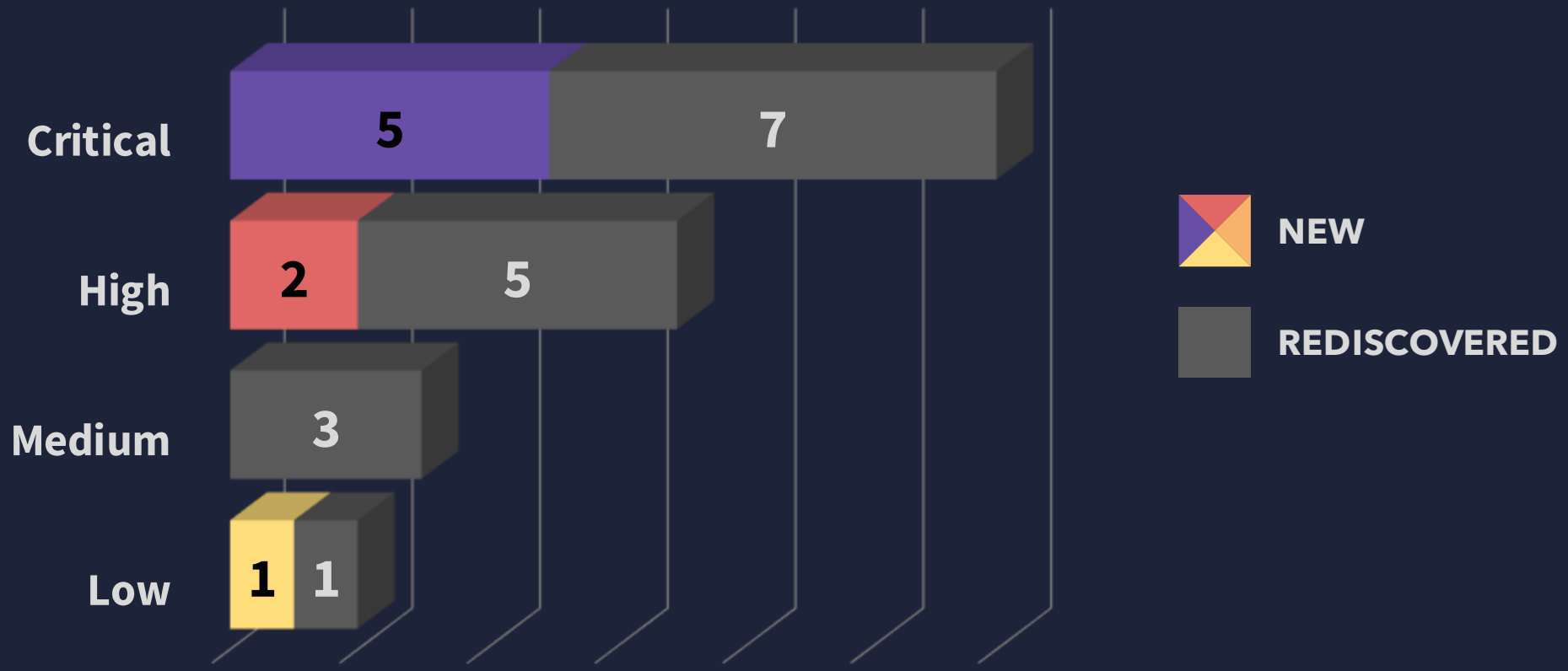
REASSESSMENT SUMMARY

RISK TRENDS

REASSESSMENT SUMMARY

RISK TRENDS

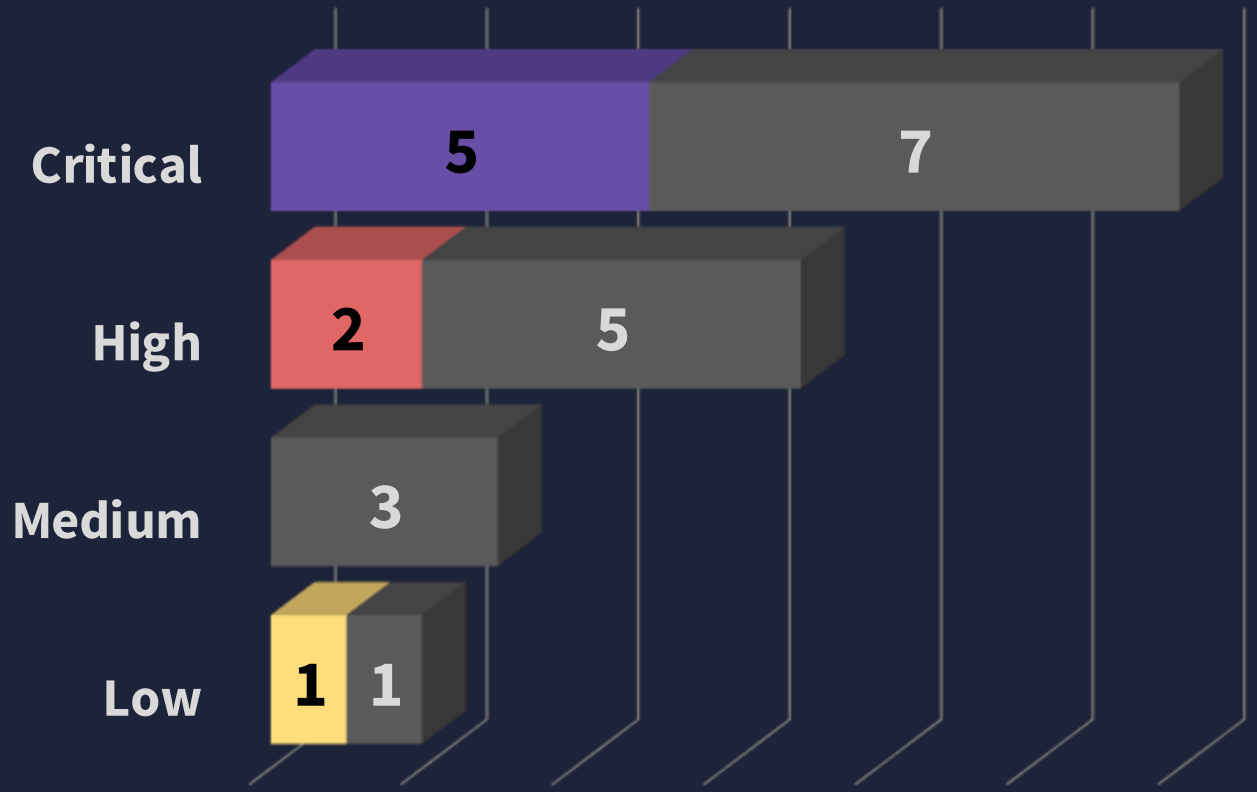
CURRENT VULNERABILITIES



REASSESSMENT SUMMARY

RISK TRENDS

CURRENT VULNERABILITIES

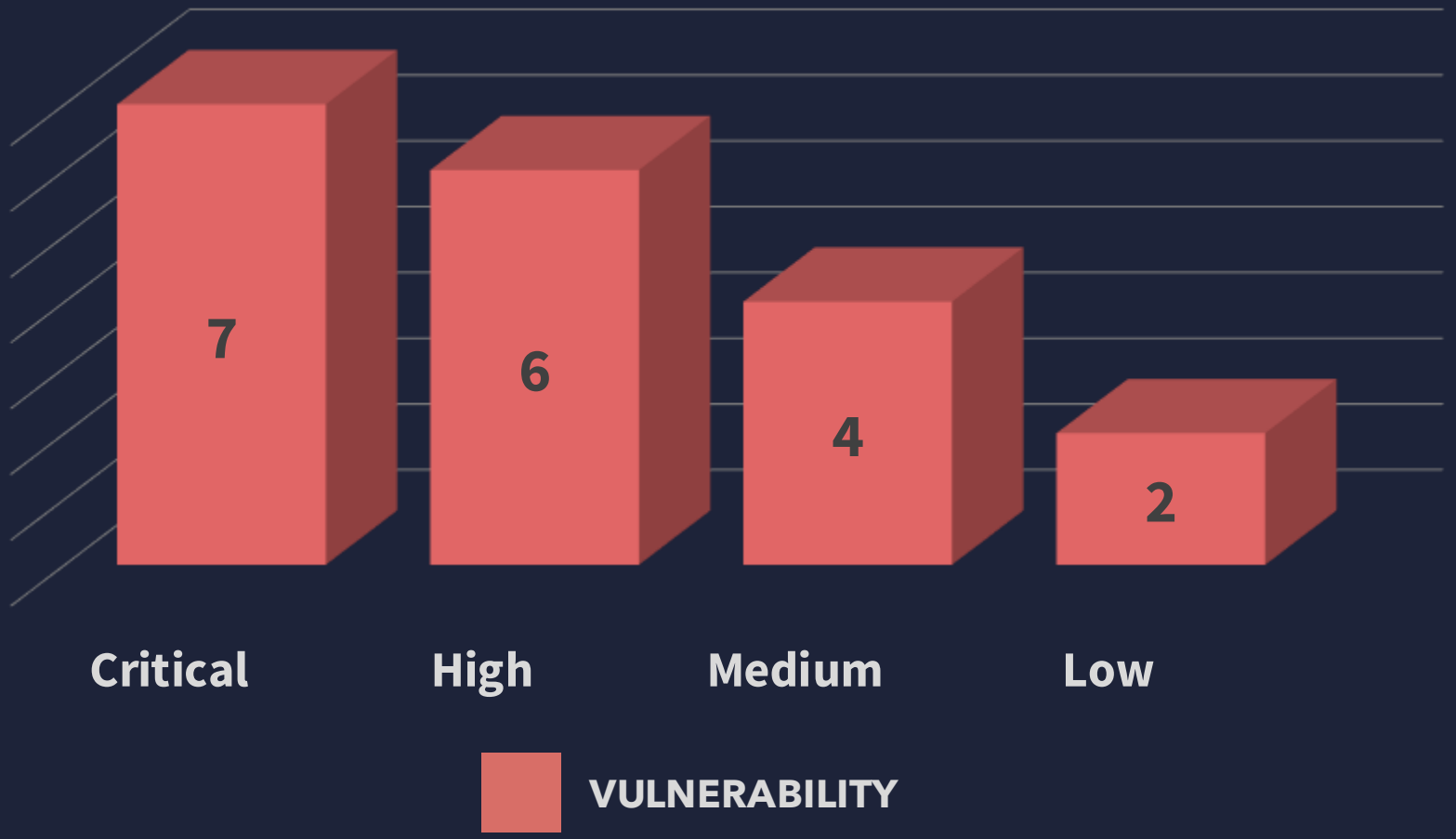


KEY PATTERNS

- Access control misconfigurations (9)
- Incompletely patched systems (3)

REASSESSMENT SUMMARY

RISK TRENDS

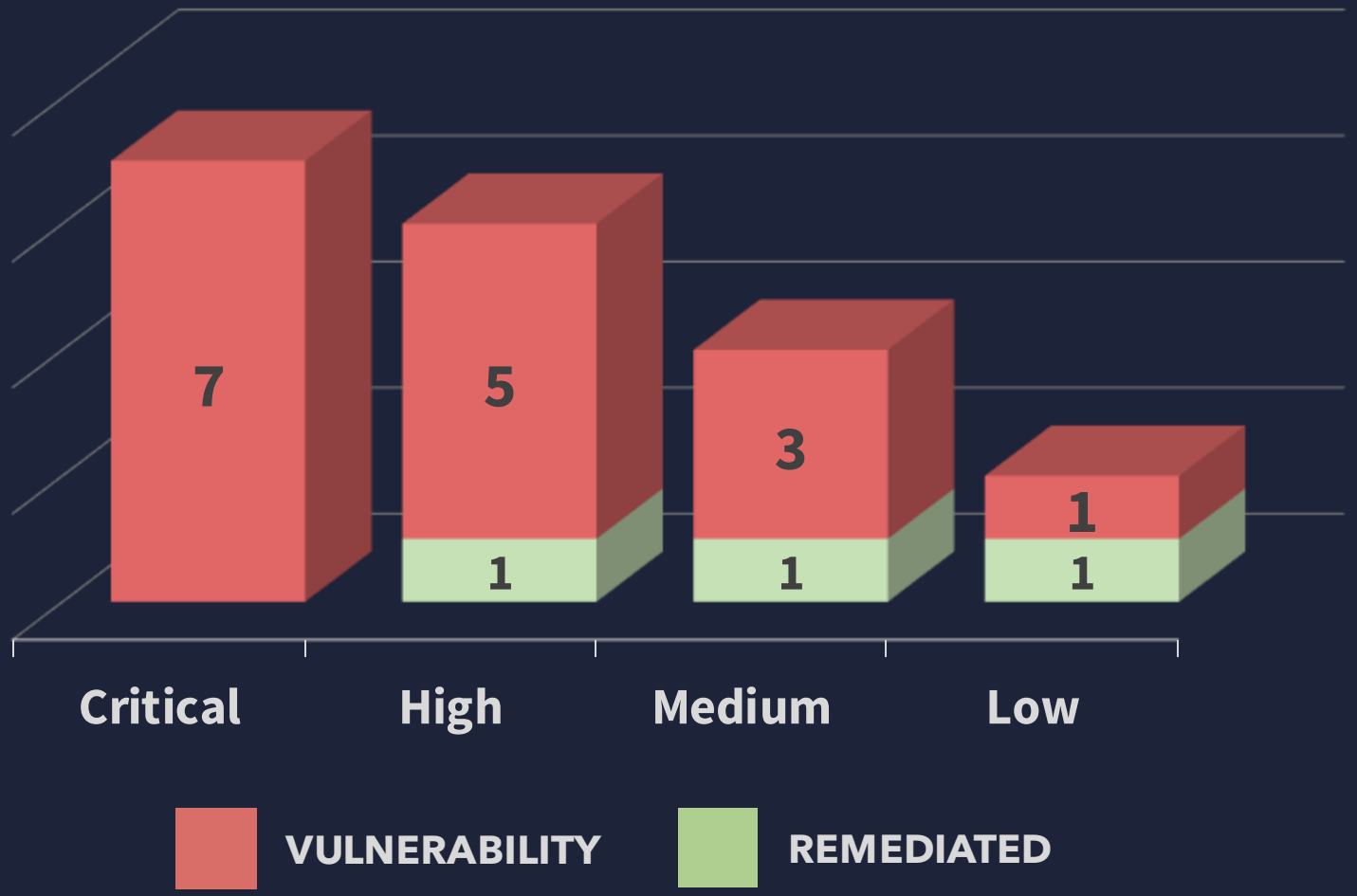


RESIDUAL RISK: BEFORE

- Vulnerable production network
- Exposed development projects

REASSESSMENT SUMMARY

RISK TRENDS



RESIDUAL RISK: AFTER

- Vulnerable corporate network
- Exposed sensitive customer data

REASSESSMENT SUMMARY

SPECIALIZED THREATS

REASSESSMENT SUMMARY

SPECIALIZED THREATS

AI PROMPT INJECTION RETEST

INITIAL ASSESSMENT	REASSESSMENT
4	7
AIs tested	AIs tested
3	7
compromised	compromised

REASSESSMENT SUMMARY

SPECIALIZED THREATS

SOCIAL ENGINEERING

INITIAL ASSESSMENT

3
phishing

33%
compromised

REASSESSMENT

1
vhishing

1
phishing

0%
compromised

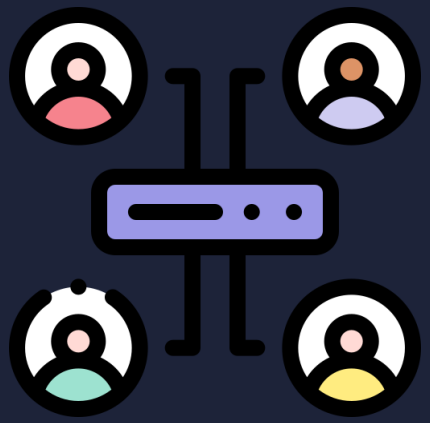
RECOMMENDATIONS

KEY STRENGTHS

RECOMMENDATIONS

KEY STRENGTHS

Social Engineering Resilience



Exposed Credential Scanning

Product Containerization

RECOMMENDATIONS

AREAS OF IMPROVEMENT

RECOMMENDATIONS

AREAS OF IMPROVEMENT

ACCESS CONTROLS

EXCESSIVE PRIVILEGES

DEVELOPMENT SECURITY

RECOMMENDATIONS

AREAS OF IMPROVEMENT

ACCESS CONTROLS

EXCESSIVE PRIVILEGES

DEVELOPMENT SECURITY

RECOMMENDATIONS

AREAS OF IMPROVEMENT

ACCESS CONTROLS

EXCESSIVE PRIVILEGES

DEVELOPMENT SECURITY

CONCLUSION

CONCLUSION

1. CURRENT PROGRESS
2. AI THREAT MODELING
3. PRIVILEGE AUDITING
4. SECURE BY DESIGN

THANK YOU FOR YOUR TIME

QUESTIONS?

finals-XX@cptc.team