OUICROISSANT EXECUTIVE PRESENTATION

Finals-XX

OUR TEAM

Captain

Project Lead

Member

Senior Penetration Tester

Member

Senior Penetration Tester

Member

Penetration Tester

Member

Penetration Tester

Member

Penetration Tester

AGENDA

01 OBJECTIVES

02 SCOPE

03 SUMMARY

04 STRENGTHS

05 FINDINGS

06 RECOMMENDATIONS

OBJECTIVES AND GOALS

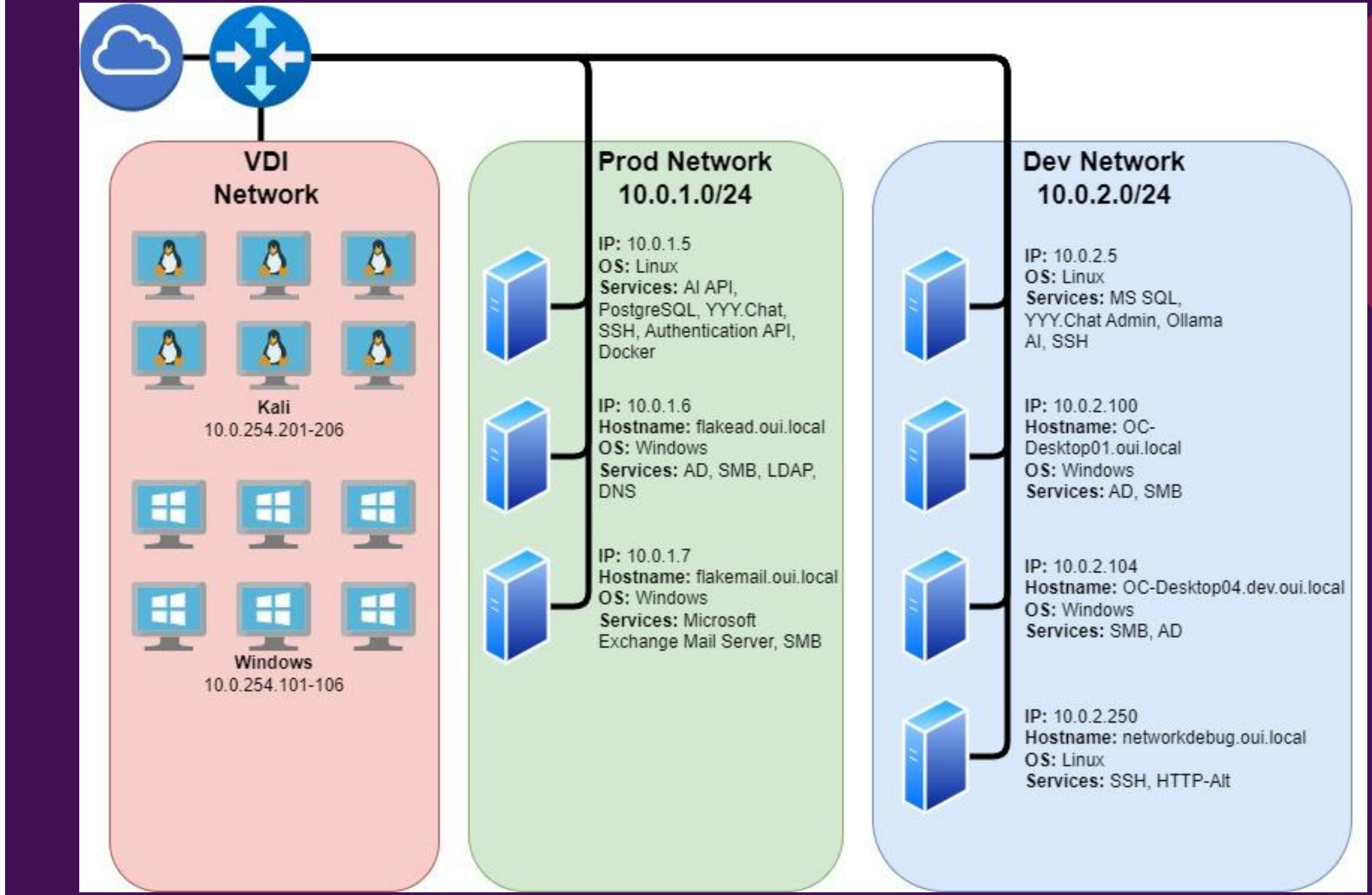
IDENTIFY REMEDIATIONS

TEST EXPANDED SCOPE

ELEVATE AI UNDERSTANDING

SCOPE

- Access through VDI network
- Production Network
  - Yyy.chat
- Development Network
- Scale AI
- AI Vishing through ScamGuardian.ai



VDI Network

Kali
10.0.254.201-206

Windows
10.0.254.101-106

Prod Network 10.0.1.0/24

IP: 10.0.1.5
OS: Linux
Services: AI API, PostgreSQL, YYY.Chat, SSH, Authentication API, Docker

IP: 10.0.1.6
Hostname: flakead.oui.local
OS: Windows
Services: AD, SMB, LDAP, DNS

IP: 10.0.1.7
Hostname: flakemail.oui.local
OS: Windows
Services: Microsoft Exchange Mail Server, SMB

Dev Network 10.0.2.0/24

IP: 10.0.2.5
OS: Linux
Services: MS SQL, YYY.Chat Admin, Ollama AI, SSH

IP: 10.0.2.100
Hostname: OC-Desktop01.oui.local
OS: Windows
Services: AD, SMB

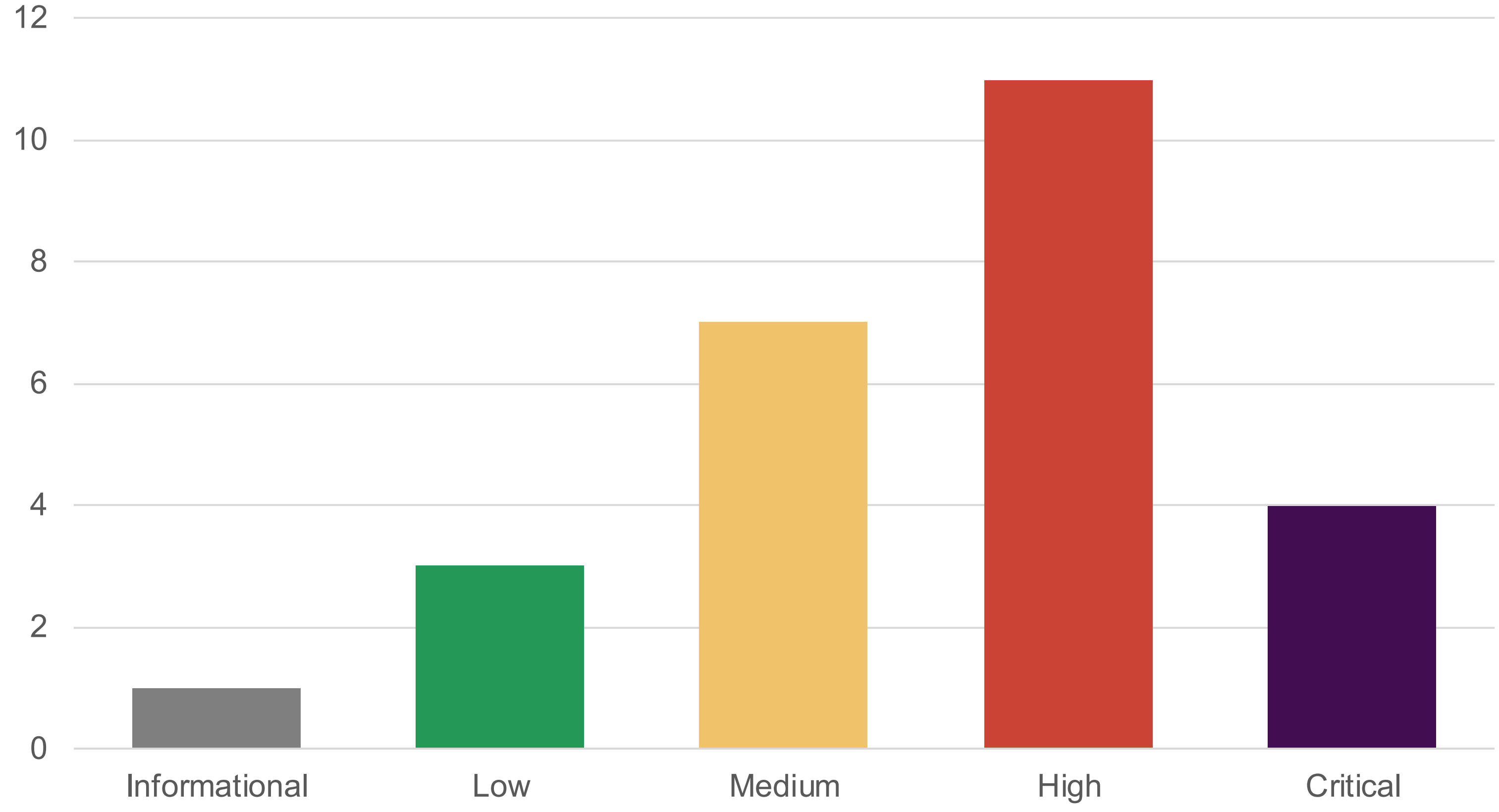
IP: 10.0.2.104
Hostname: OC-Desktop04.dev.oui.local
OS: Windows
Services: SMB, AD

IP: 10.0.2.250
Hostname: networkdebug.oui.local
OS: Linux
Services: SSH, HTTP-Alt

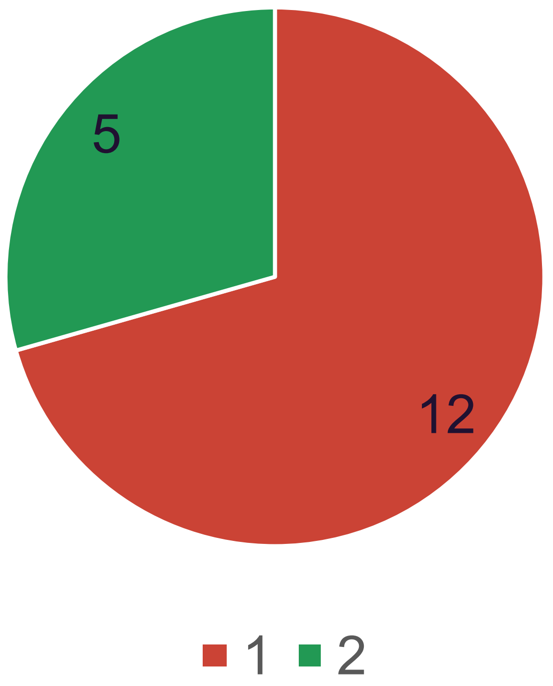
EXECUTIVE SUMMARY

- 4 Critical, 11 High, 7 Medium, 3 Low, 1 Informational
- 17 previously identified vulnerabilities
  - 5 remediated
  - 12 still present
- Allows for:
  - Complete domain takeover
  - Exfiltration of customer data
  - Compromise of user integrity and confidentiality

Findings



Previously Identified Vulnerabilities



KEY STRENGTHS

LACK OF DEFAULT CREDENTIALS

Remediated issue from last assessment

GOOD INPUT SANITIZATION

Could not perform common web attacks

STRONG OPERATIONAL SECURITY

Removed domain access for terminated employee

KEY FINDINGS

INSECURE NETWORK CONFIGURATION

WEAK SECURITY POLICIES

IMATURE SOFTWARE SECURITY

KEY RECOMMENDATIONS

TOP FIXES

Should be remediated
as soon as possible

SHORT TERM

Can be remediated in ~3
months or less

LONG TERM

Will take longer than 3
months to remediate

CYBERSECURITY TRAINING

- Implement a SETA program to educate employees about secure passwords and spotting social engineering attempts
- Level of effort: High/Med**/Low**
- Impact: **High**/Med/Low

SECURE DEVELOPMENT PROCESSES

- Consider security throughout the entire development pipeline. (ex: encrypt traffic, safeguard sensitive information)
- Level of effort: High/**Med/**Low
- Impact: High/**Med**/Low

CENTRALIZED LOGGING

- Consider adding centralized logging to monitor for security incidents and to conduct investigations
- Level of effort: High/**Med**/Low
- Impact: **High**/Med/Low

ENDPOINT DETECTION & RESPONSE

- Implement an EDR solution to protect against malware and undetected security incidents
- Level of effort: **High**/Med/Low
- Impact: High/**Med**/Low

CONCLUSIONS

CONTINUE IMPROVEMENTS

KEEP SECURITY AT TOP OF MIND

PROTECT Y CUSTOMERS

THANK YOU!

We would love to take your questions