OuiCroissant Penetration Test Executive Debrief

Finals-XX

Finals-XX

Captain
Manager

Memeber
Technical Lead

Member
Sr. Web Pentester

Member
Sr. Win Pentester

Member
Jr. Web Pentester

Member
Jr. Win Pentester

Assessment Objective

Provide Complete Analysis

- Test fully
- Network visibility
- Current, up-to-date testing

Maintain Perspective

- Slice of the security pie
- Limit assumptions
- Maintain objectivity

Executive Summary

Overall Security Posture

Critical

Vulnerabilities discovered

34

Executive Summary

Remediated Vulnerabilities

33%

Active Directory Domain

Compromised

Business Impact

- Reputational Damage
- Legal Complications
- Business Disruption
- Confidential Information Exposure

Risk Assessment Methodology

- Severity – CVSSv3 (0.00-10.00)
- Risk – NIST SP-800-30 Risk Matrix
    - Likelihood + Impact

∆ LOW ∆

∆∆ MEDIUM ∆∆

∆∆∆ HIGH ∆∆∆

∆∆∆∆ CRITICAL ∆∆∆∆

Risk Assessment Methodology

OVERALL SCORE		SEVERITY LEVEL			
		LOW	MEDIUM	HIGH	CRITICAL
RISK LEVEL	LOW	Δ	Δ	ΔΔ	ΔΔ
	MEDIUM	Δ	ΔΔ	ΔΔΔ	ΔΔΔ
	HIGH	ΔΔ	ΔΔΔ	ΔΔΔ	ΔΔΔΔ
	CRITICAL	ΔΔΔ	ΔΔΔ	ΔΔΔΔ	ΔΔΔΔ

Scope

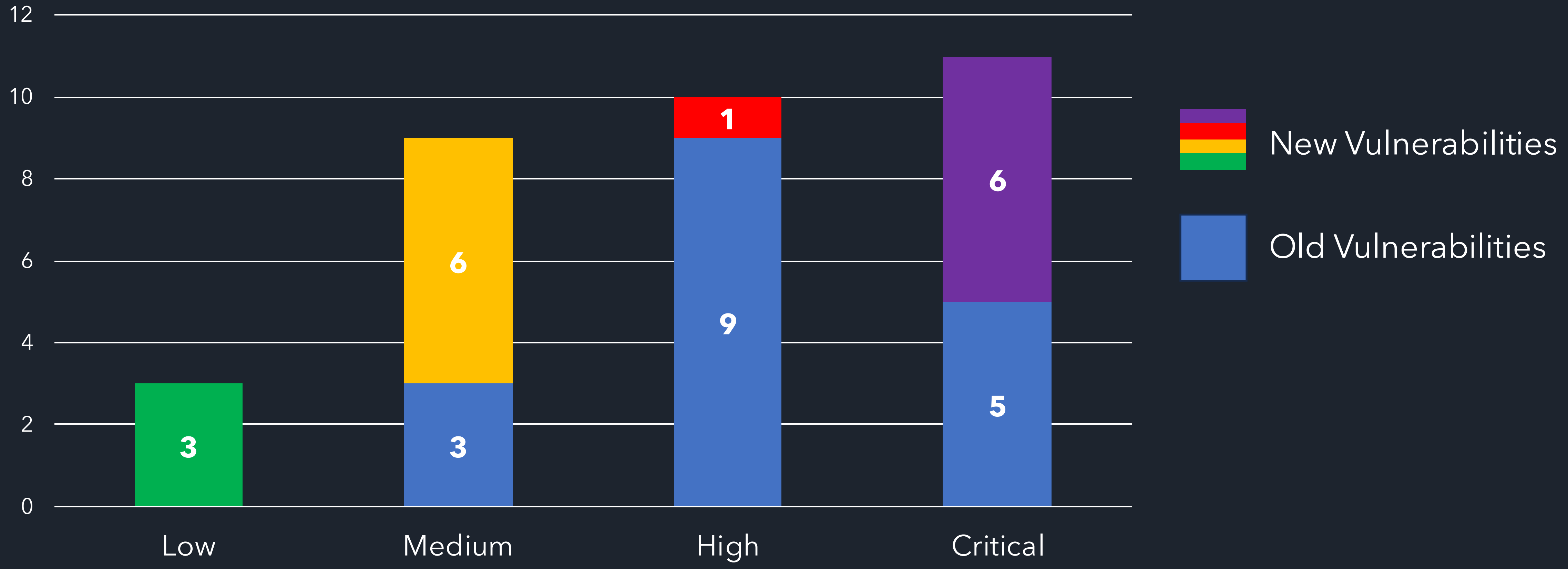
Testing with Intent of Availability & Functionality

Production Subnet
(10.0.1.0/24)

yyy.chat Web Application
(10.0.1.5)

Development Subnet
(10.0.2.0/24)

Vulnerabilities Found



High Points

Reassessment Improvements

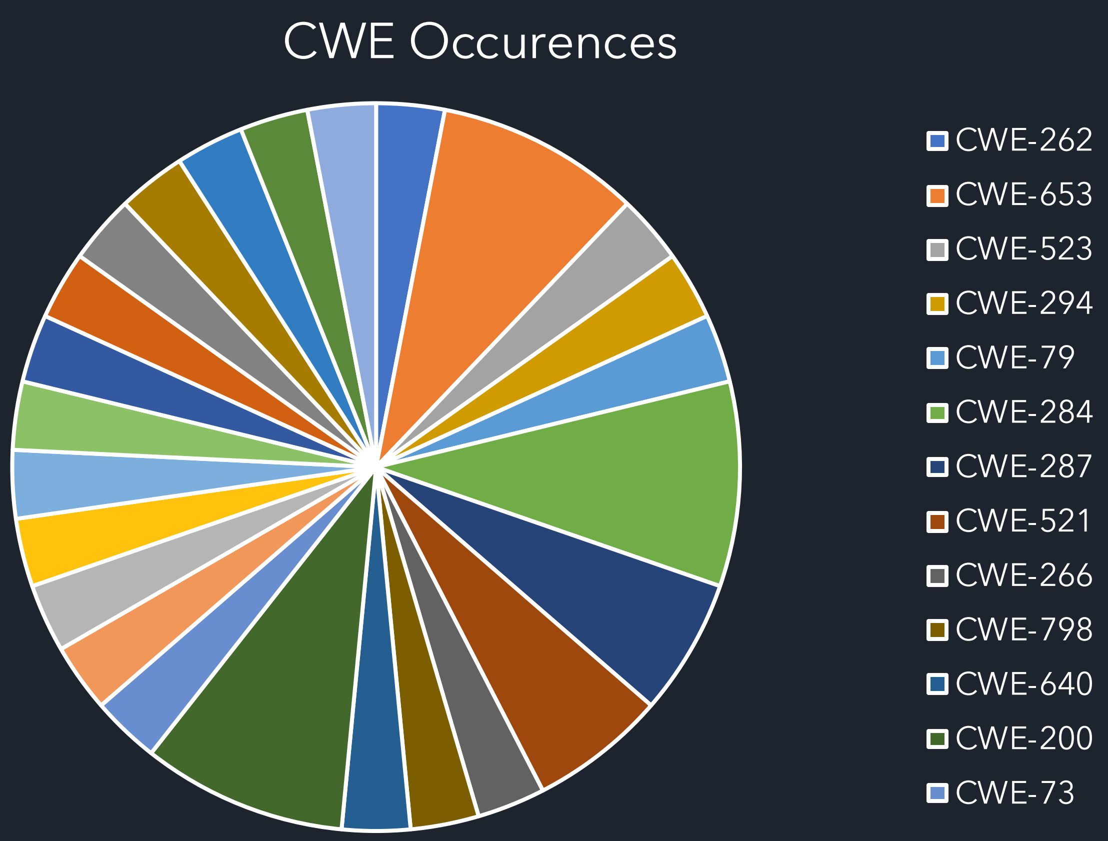
- Improved Database Security
- Enhanced Endpoint Security
- Enforced Principle of Least Privilege

Security Strength Areas

- Automated PII Tooling
- AI Resiliency & Safety

Areas of Improvement

- Improper Isolation or Compartmentalization
- Improper Access Control
- Exposure of Sensitive Information to an Unauthorized Actor



Remediation Recommendation

Authentication and Authorization

- Enforce Centralized Authentication via SAML/SSO
- Validation of authorization based off the principle of least privilege

Credential Security

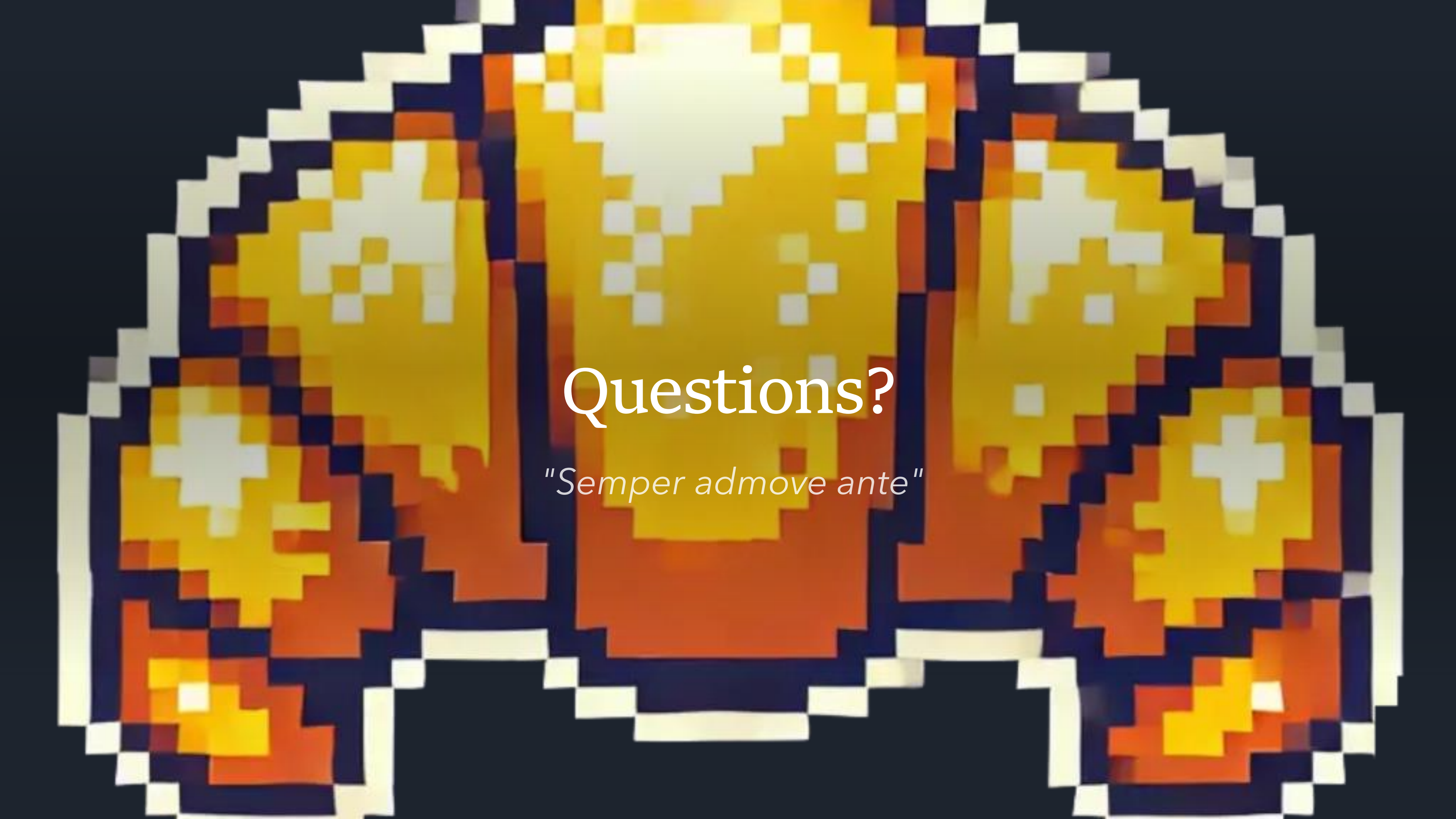
- Centralized Identity and Credential Management through password managers
- Re-enforce industry standard 2FA/MFA

AI Resiliency and Safety

- Develop continuous AI resiliency and compliance processes
- Research latest models and RAG implementations

Key Takeaways

- Proactive Secure Software Development Lifecycle
- Follow industry standard (NIST, DISA, Mozilla) security practices for configuration and implementation
- Employee security awareness and preparedness



Questions?

"Semper admove ante"