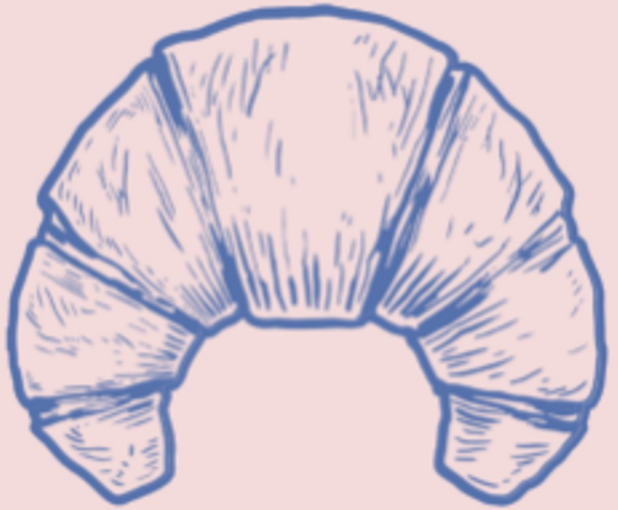
Le Bonbon Croissant Executive Briefing

TEAM-XX



Agenda

INTRODUCTIONS
01

RISK METRICS
02

ENGAGEMENT SUMMARY
03

REASSESSMENT SUMMARY
04

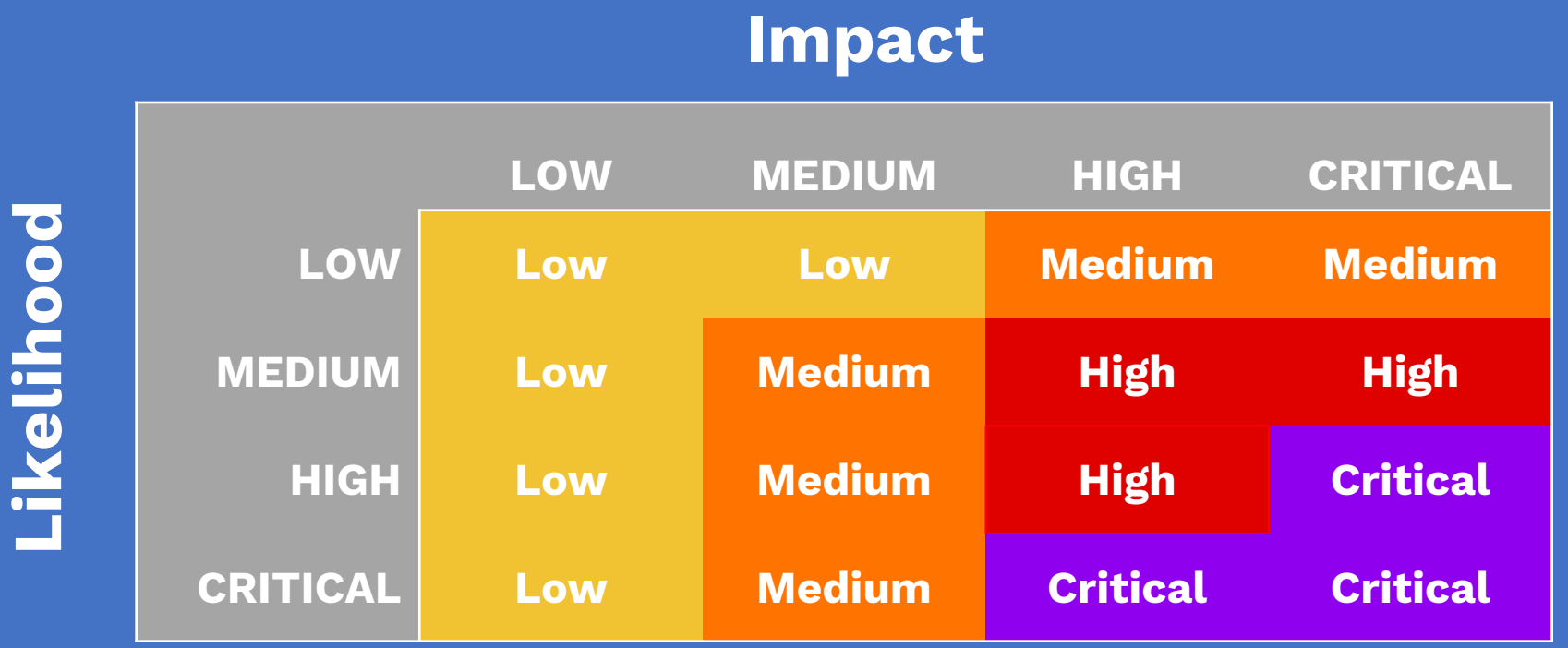
COMPLIANCE
05

RECOMMENDATIONS
06

CONCLUSION
07

Introductions

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.

Engagement Summary: Objectives

1. General Security

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

2. Integrity

Validate the integrity of the custom business process and customer experience systems

3. Industrial Systems

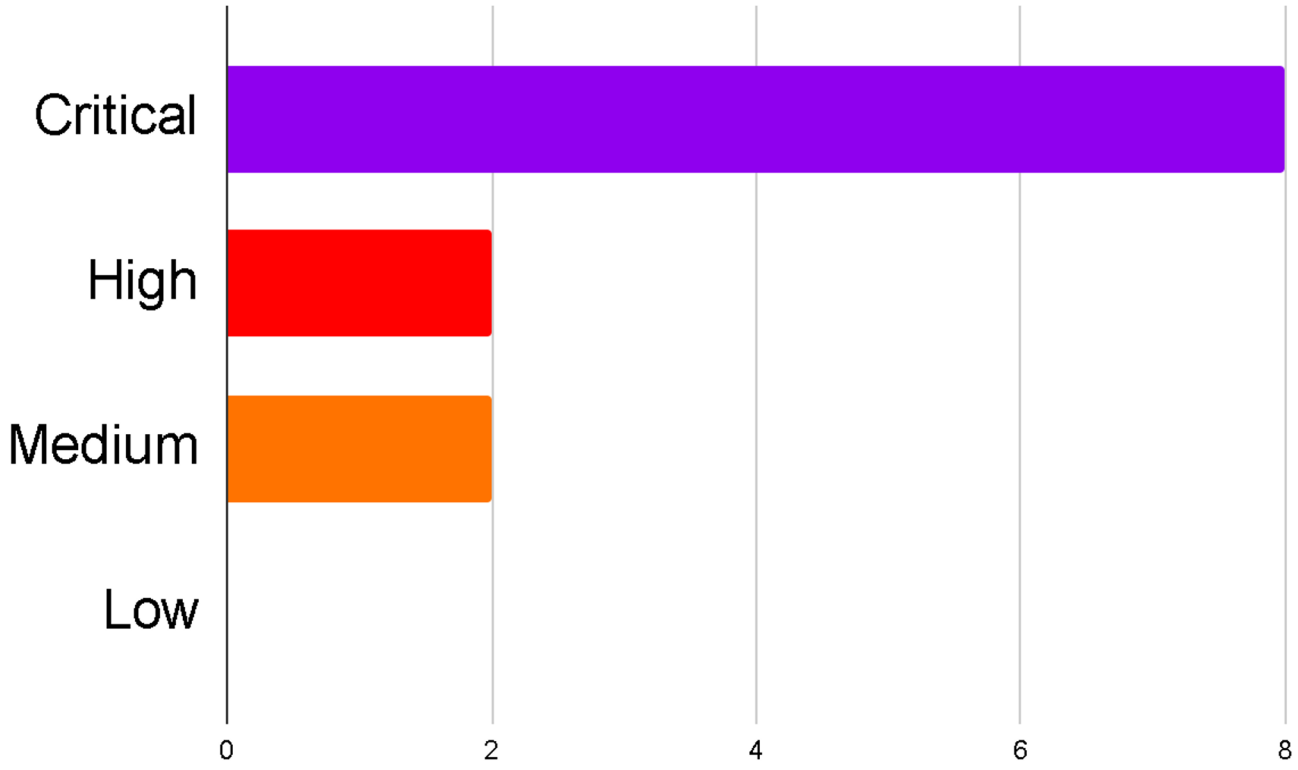
Test the embedded industrial control systems supporting warehouse operations

4. Compliance

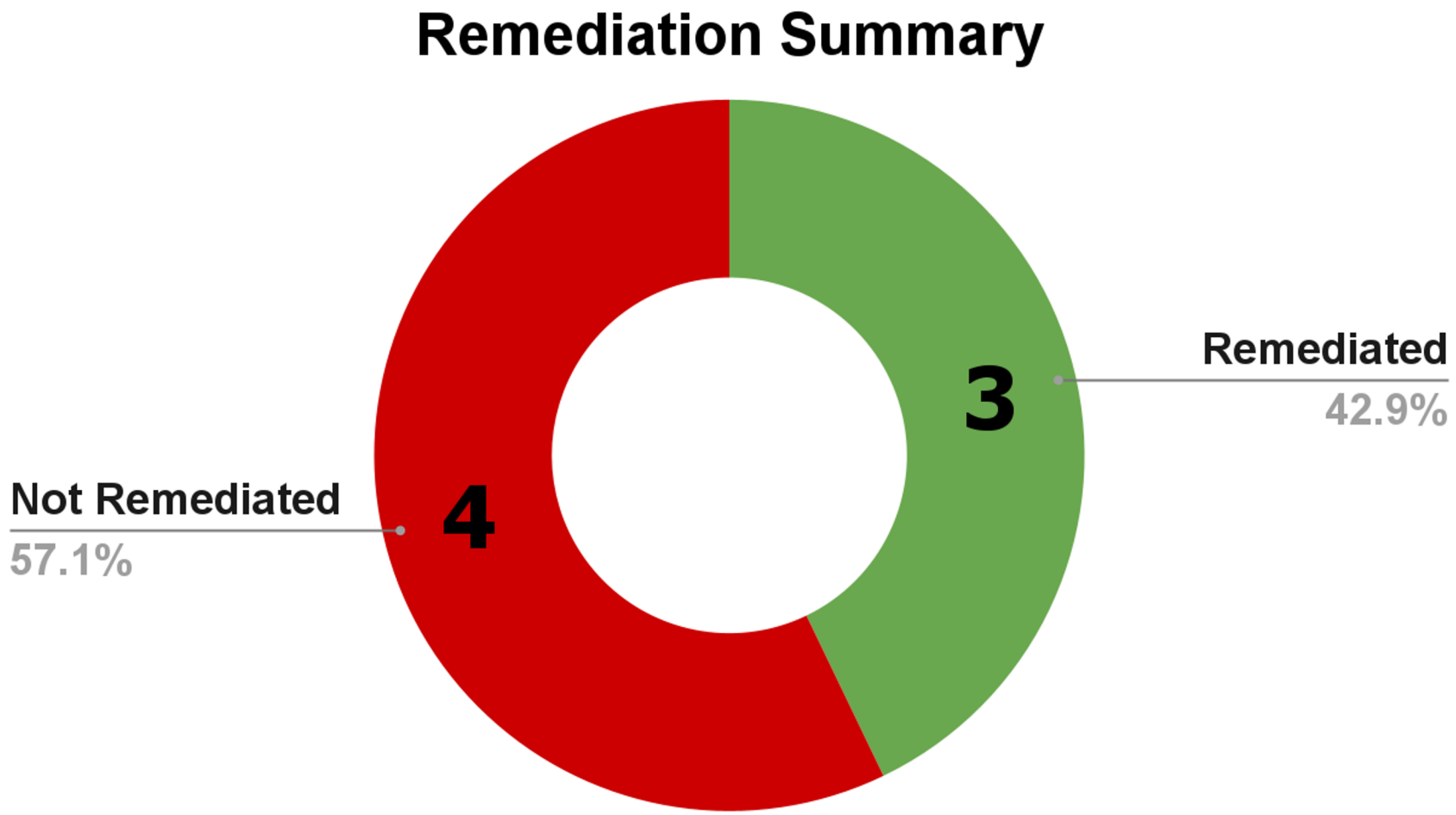
Verify compliance with PCI-DSS and GDPR.

Engagement Summary: Vulnerabilities

Total Vulnerabilities Found:



Reassessment Summary: Remediations



Compliance

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**.

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.**

Compliance: PCI DSS

PCI DSS Violations

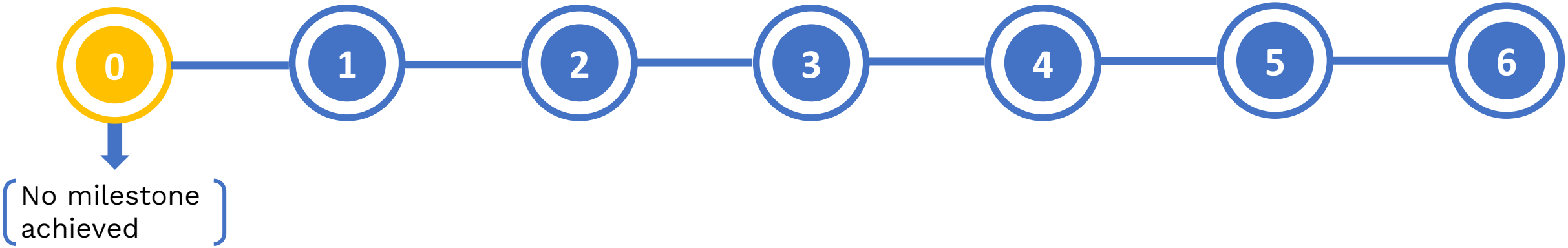
72

Estimated Fines

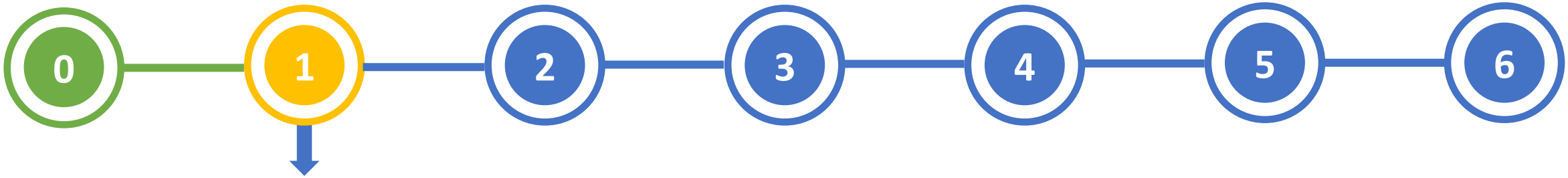
€300,000 - €600,000

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

Compliance: PCI DSS



Compliance: PCI DSS



Remove sensitive cardholder data and limit data retention.

Compliance: GDPR

GDPR Violations

14

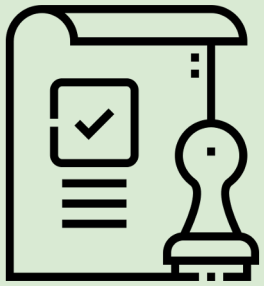
Typical Range

€100,000 - €600,000

LBC is in violation of not encrypting passwords and implementing sufficient access control measures.

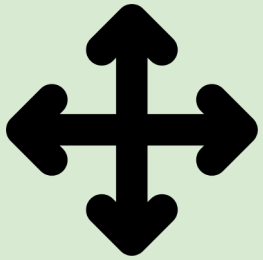
Additionally, LBC does not meet the mandatory requirements to document information about the data being collected and transparently inform consumers about LBC's data privacy policy.

Recommendations: Key Strengths



User Input Validation

Logging and Monitoring

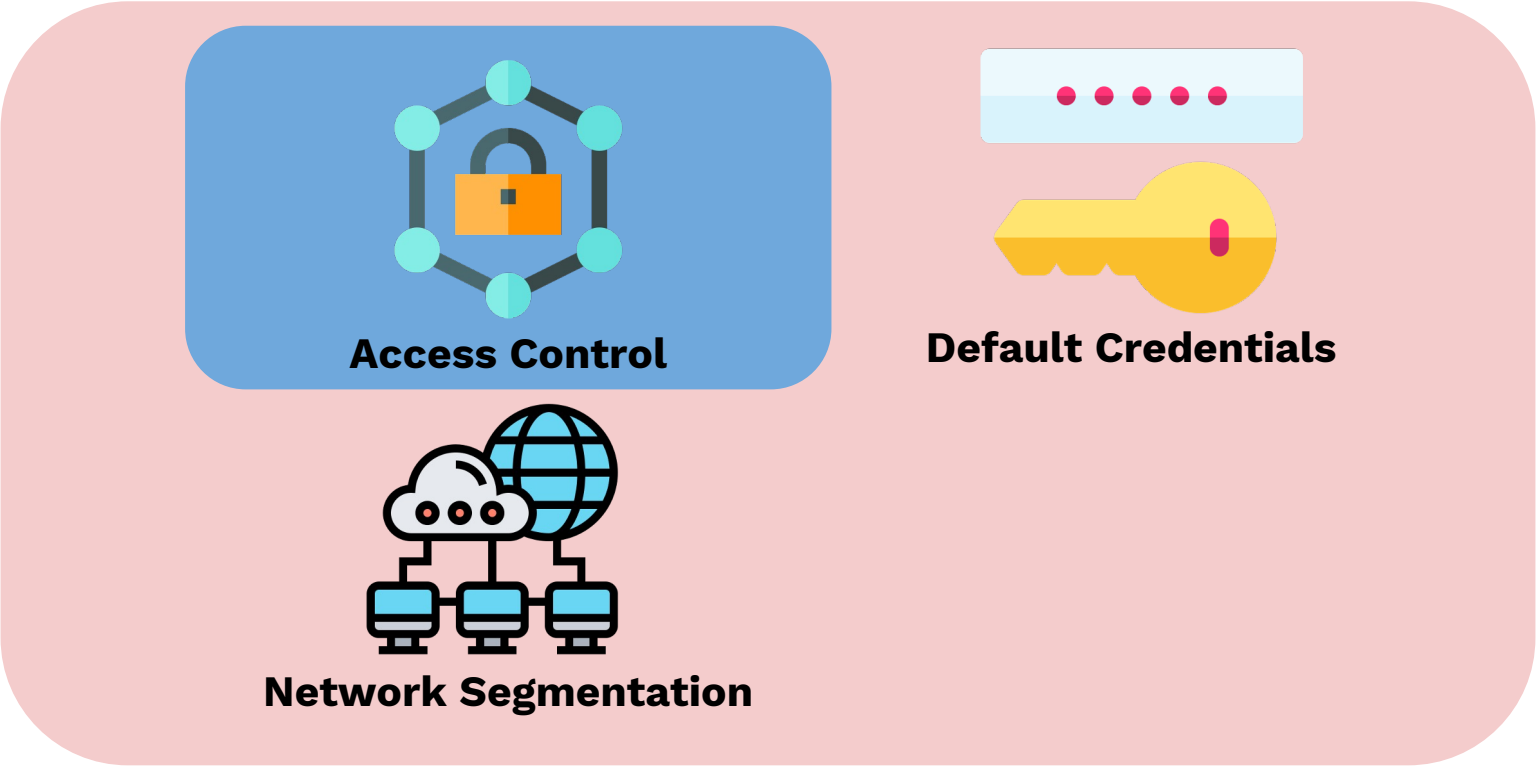


Lateral Movement

Team XX found LBC's security policy to excel in certain areas.

- Applications securely handle user input
- Environment implements effective logging and monitoring
- Limited lateral movement between machines

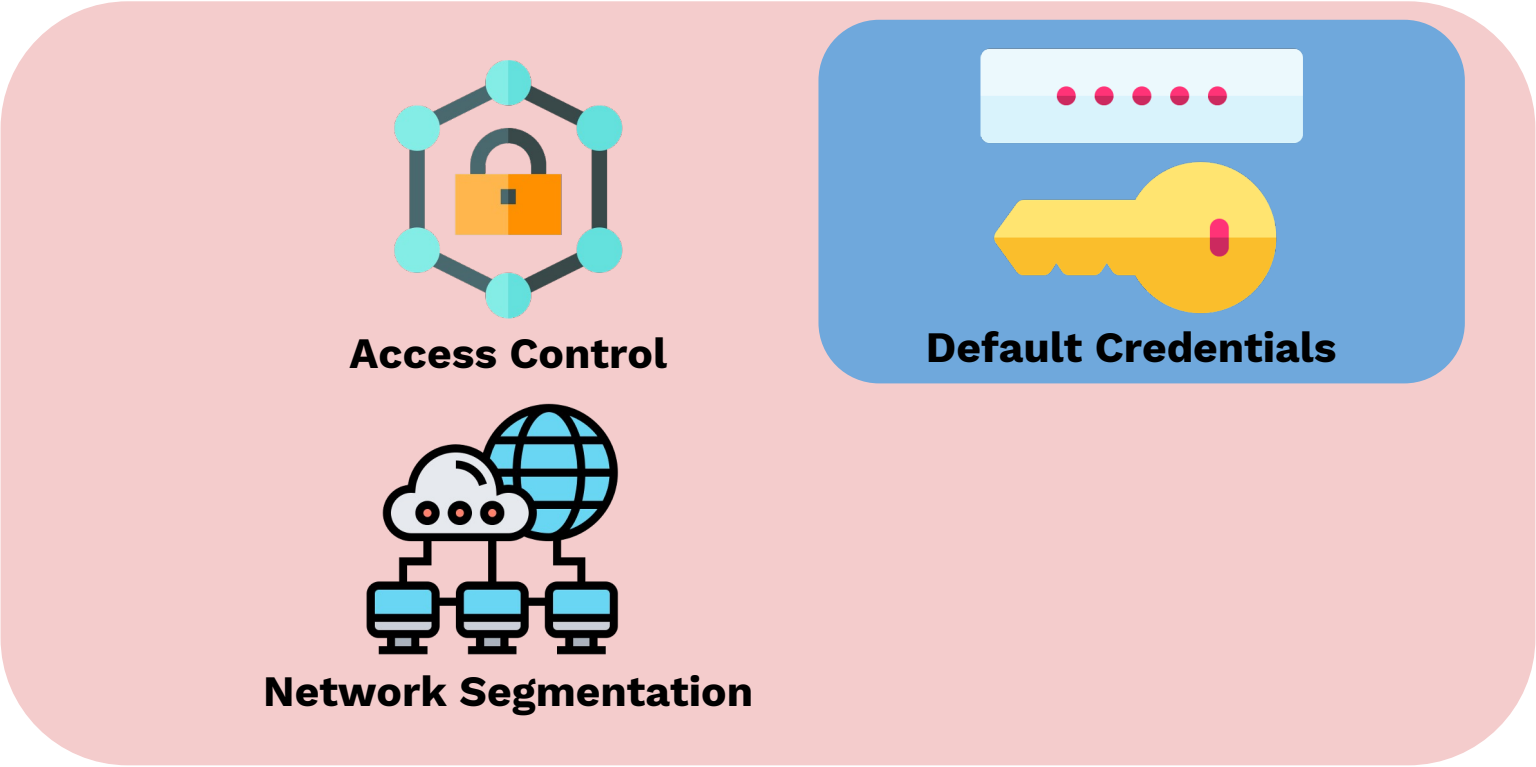
Recommendations: Areas of Improvement



Team XX found LBC's access controls to be insufficiently protecting company assets.

- Ensure all services require valid credentials
- Implement the principle of least privilege
- Restrict unauthenticated access

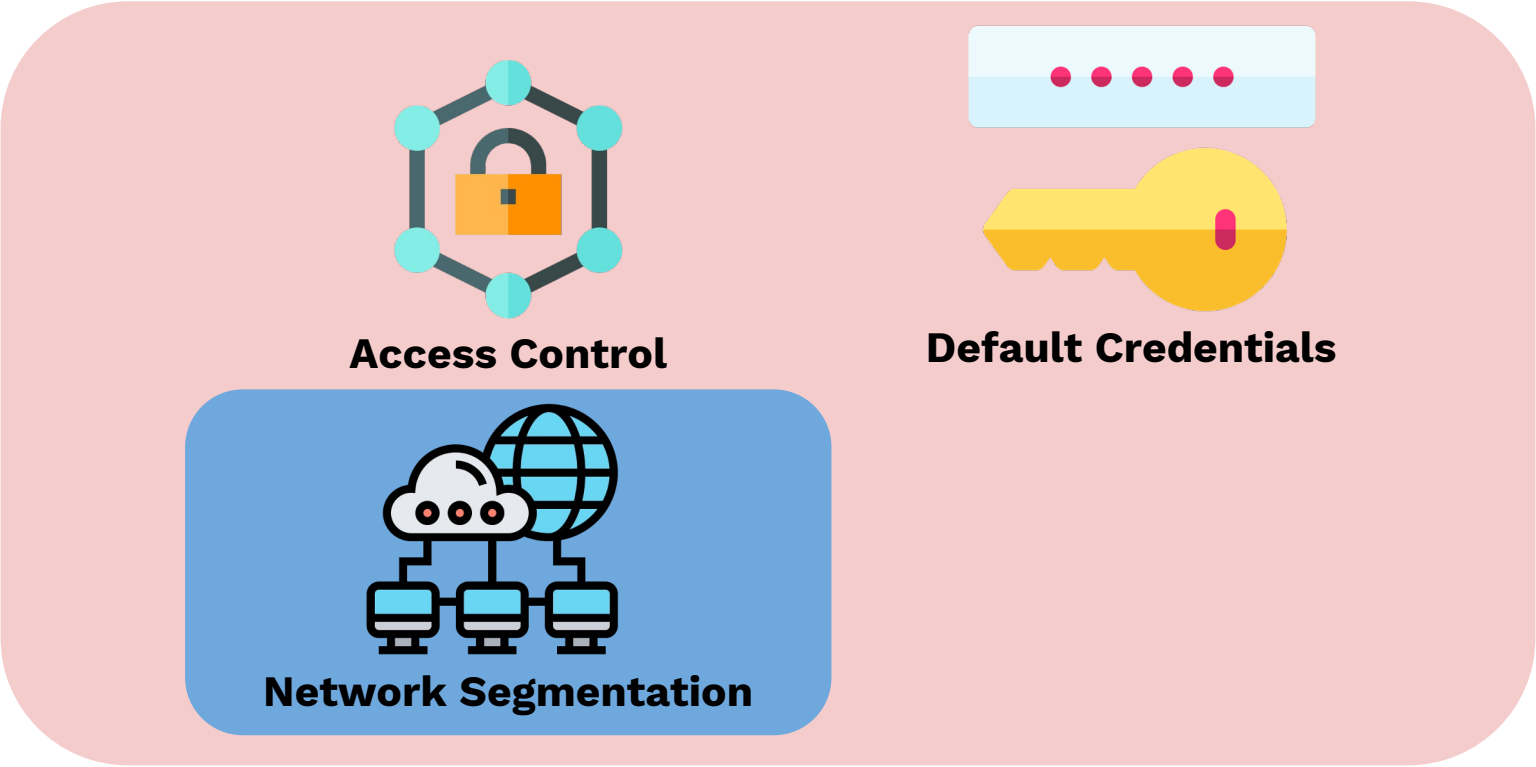
Recommendations: Areas of Improvement



Team XX found LBC's services to be using default credentials

- Change default credentials for all deployed services
- Ensure all passwords are sufficiently complex and securely stored
- Implement Multi-Factor Authentication

Recommendations: Areas of Improvement



Team XX identified poor network segmentation of LBC's systems.

- Implement security zones for the network
- Implement system isolation as outlined in compliance guidelines
- Implement network-based firewalls between subnetworks

Less Secure

Less Compliant

Vulnerable ICS

Access Control

Conclusion

Questions?

finals-xx@cptc.team

Thank you for your time.