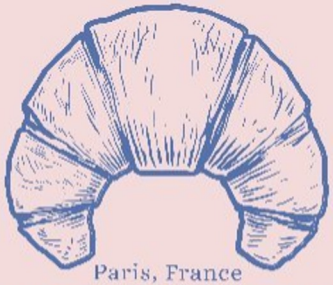
PENETRATION TEST & RISK ASSESSMENT DEBRIEF

TEAM XX



MEET THE TEAM

XXXX XXXXX, *Project Manager*
XXXX XXXXX, *Senior Security Analyst*
XXXX XXXXX, *Senior Security Analyst*
XXXX XXXXX, *Senior Security Analyst*
XXXX XXXXX, *Jr. Security Analyst*
XXXX XXXXX, *Jr. Security Analyst*

AGENDA

- **OVERVIEW**
  - METHODOLOGY
  - SCOPE
  - RISK CLASSIFICATION
  - COMPLIANCE
- **FINDINGS**
  - TOTAL FINDINGS
  - POSITIVE SECURITY CONTROLS
  - HIGH-LEVEL RECOMMENDATIONS
- **CONCLUSION**

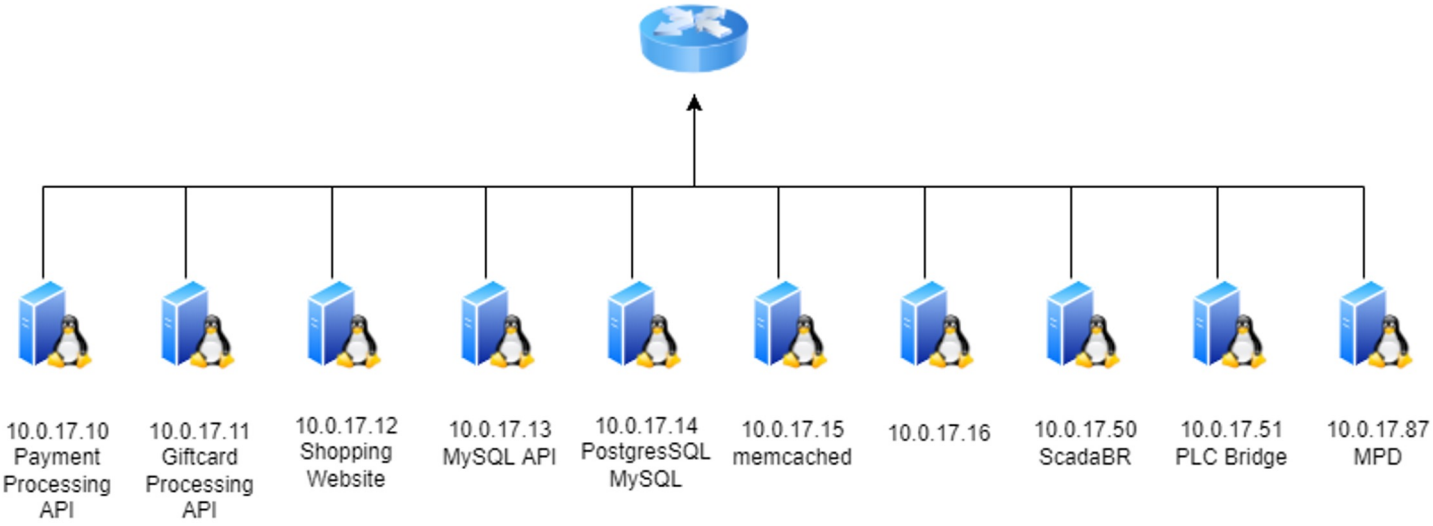
OVERVIEW

SCOPE

IP range 10.0.17.0/24

- Initially excluded hosts 10.0.17.50 and 10.0.17.51
- Later expanded to include hosts 10.0.17.50 and 10.0.17.51

SCOPE (CONT.)


10.0.17.10
Payment
Processing
API
10.0.17.11
Giftcard
Processing
API
10.0.17.12
Shopping
Website
10.0.17.13
MySQL API
10.0.17.14
PostgresSQL
MySQL
10.0.17.15
memcached
10.0.17.16
10.0.17.50
ScadaBR
10.0.17.51
PLC Bridge
10.0.17.87
MPD

COMPLIANCE

PCI DSS

A set of security standards designed to ensure that companies that handle credit card information maintain a secure environment

GDPR

A legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union

NON-COMPLIANCE RESULTS IN FINES AND PENALTIES

ISO

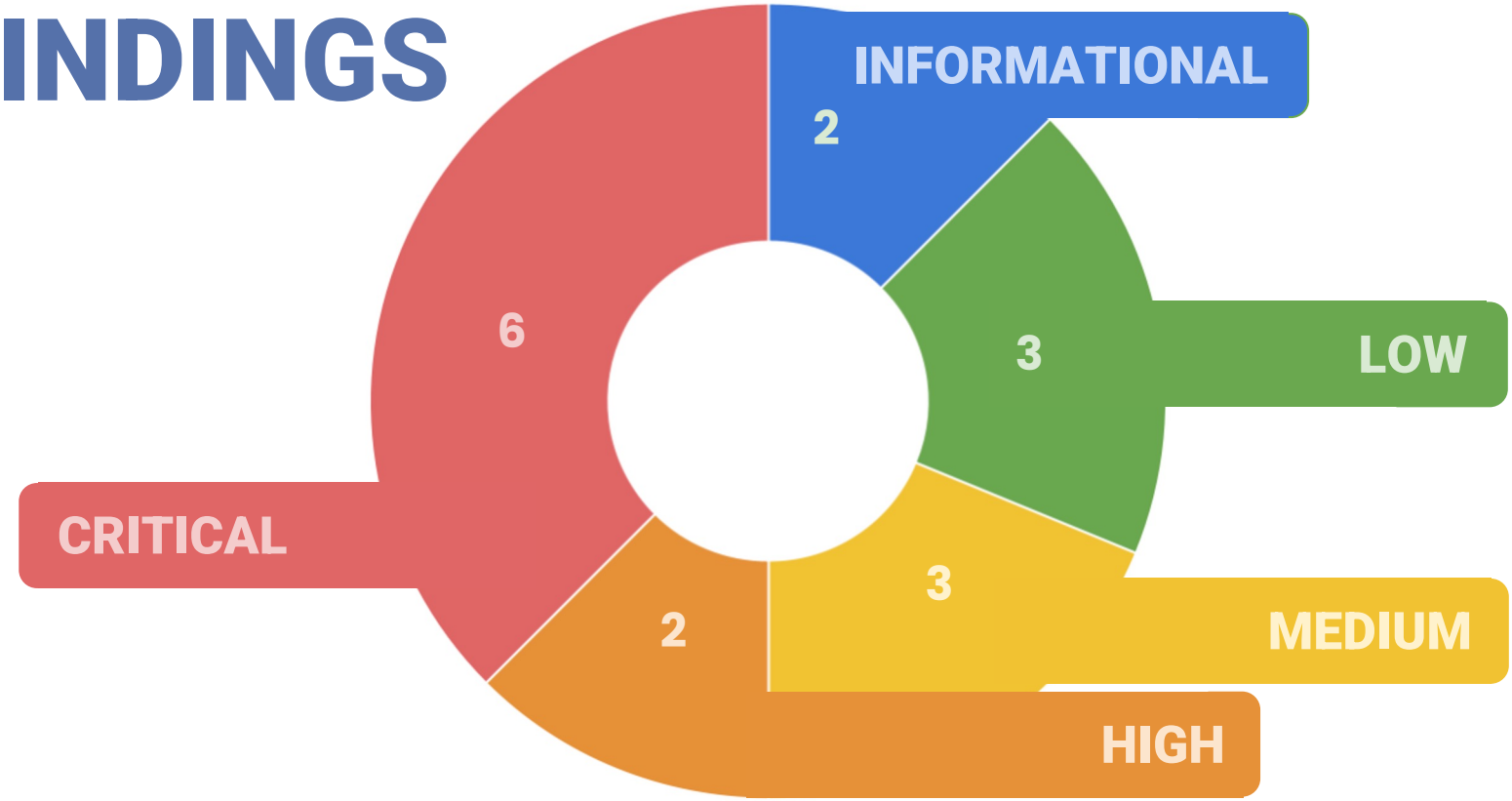
An international non-governmental organization made up of national standards bodies

RISK FRAMEWORK

IMPACT x LIKELIHOOD = RISK

FINDINGS

TOTAL FINDINGS



POSITIVE SECURITY CONTROLS

LBC exhibited many positive security controls including:

- Public-facing LBC website is segmented from the internal network
- Security-forward thinking after cyber attack and data breach
- LBC practices secure communication over their network by rerouting port 80 traffic through port 443 to enforce HTTPS.

HIGH-LEVEL RECOMMENDATION:

Restructure network to incorporate segmentation

An unsegmented network could allow a malicious actor to move laterally, compromising the systems and services vital to LBC’s operations including LBC’s production control systems.

HIGH-LEVEL RECOMMENDATION:

Create and implement an acceptable use policy (AUP)

Enforcing an AUP ensures that employees are not misusing organizational resources or systems.

HIGH-LEVEL RECOMMENDATION:

Implement a password policy compliant with industry standards

Follow best security practices and industry standards to develop and implement a password policy that ensure user credentials are computationally strong and secure.

HIGH-LEVEL RECOMMENDATION:

Change default credentials

Default credentials present organizational risk as default credentials are widely-known and can be easily exploited by a malicious actor.

HIGH-LEVEL RECOMMENDATION:

Develop and enforce policies for protecting sensitive customer data at rest, and encrypting sensitive customer data in transit

Compliance organizations and standards such as PCI DSS and GDPR outline policies for securing data at rest and in transit.

CONCLUSION

- LBC exhibits strong potential in regards to network security.
- Our security firm found security vulnerabilities ranging in severity from low to critical.
- The recommendations provided will help LBC increase their security posture and reduce any potential impact in the case of a compromise.

QUESTIONS?

Feel free to reach out to us at finals-xx@cptc.com