

# Le Bonbon Croissant Penetration Test Debrief

Team Finals-xx



# Agenda

- ★ Engagement Overview
- ★ Evaluation Methods
- ★ Statistics
- ★ Compliance and Regulations
- ★ Key Findings and their Impact
- ★ Suggestions for Improvements

# Engagement Overview

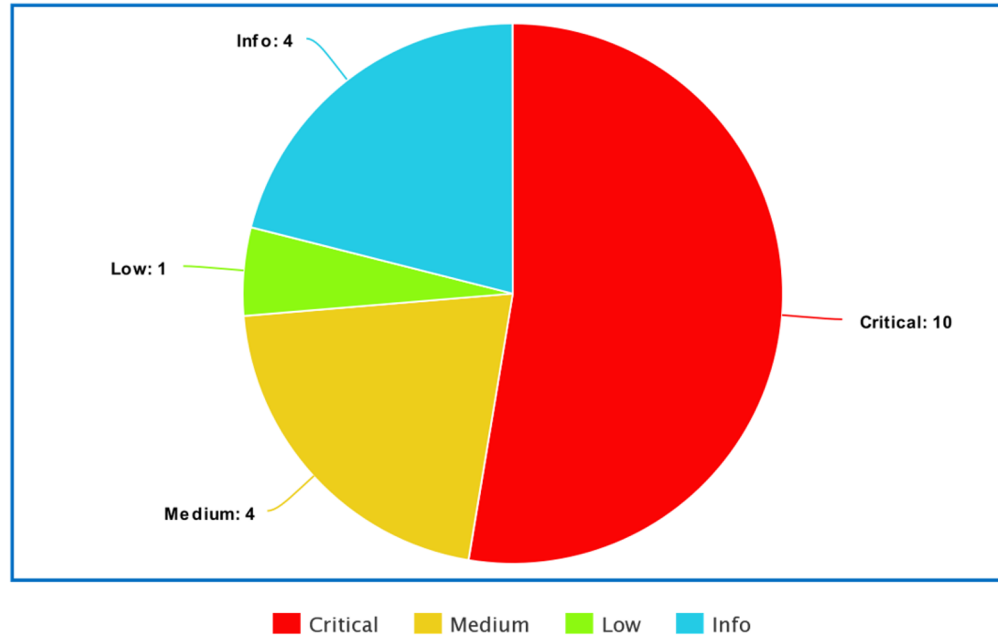
- ★ Second iteration
- ★ Primary goals
  - Integrity of business process and customer experience systems
  - Customer rewards program
  - E-commerce and payment processing applications
  - Industrial control systems
- ★ Scope
  - Paris warehouse subnet



# Evaluation Methods

- ★ Technical metrics for vulnerability rating - CVSS
  - Considers the impact on availability, integrity and confidentiality
  - Depends on the complexity of carrying out the attack
  - Assigns an empirical score, and an impact class
- ★ Business impact class
  - Low/Medium/High
  - Tailored to LBC's goals and needs

# Statistics



LE BONBON CROISSANT

CPTC 2021

# Compliance and Regulations

- ★ Payment Card Industry Digital Security Standard
- ★ Data protection regulations based on customer locations
  - General Data Protection Regulation (EU)
  - California Consumer Protection Act
  - Consumer Data Protection Act
  - and more
- ★ Several violations discovered by our team



# Key Findings

- ★ System misconfigurations
- ★ Inadequate password management
- ★ Improper access control settings
- ★ Deficient network segregation

# Impact

- ★ Customer data is vulnerable to leakage, unauthorized change
- ★ Access to business-critical Infrastructure
- ★ Compliance and regulation violations
- ★ Reputation and financial losses



# Suggestions for Improvements

- ★ Address the reported issues - prioritized by impact rating
- ★ Revisit security policies
- ★ Assess policy enforcement mechanisms
- ★ Revise network design

# Thank You for Your attention!

Time for  
questions!



Paris, France  
LE BONBON CROISSANT

CPTC 2021