Le Bon Bon Croissant

PENETRATION TEST DEBRIEF

TEAM INTRODUCTION

AGENDA

OVERVIEW OF ENGAGEMENT

DISCUSSION OF METRICS

STATISTICS

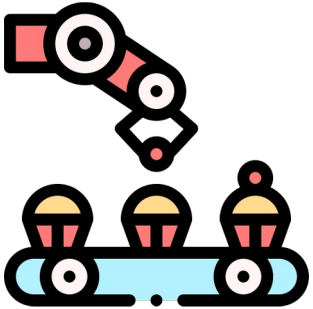
COMPLIANCE

KEY FINDINGS

SUGGESTIONS

OVERVIEW OF ENGAGEMENT

Risk Assessment



Process Control Infrastructure

Mitigate and Respond

DISCUSSION OF METRICS

TECHNICAL METRICS

+

HUMAN ANALYTICS

=

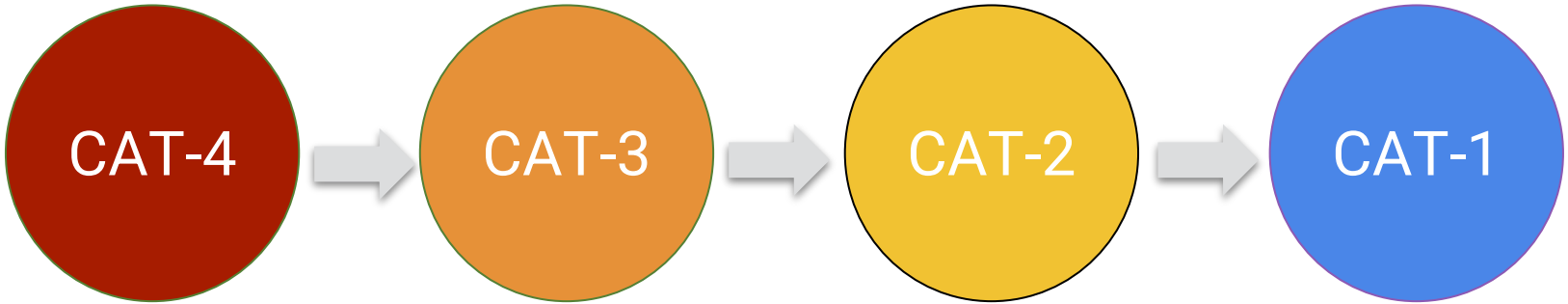
HOLISTIC ANALYSIS

DISCUSSION OF METRICS

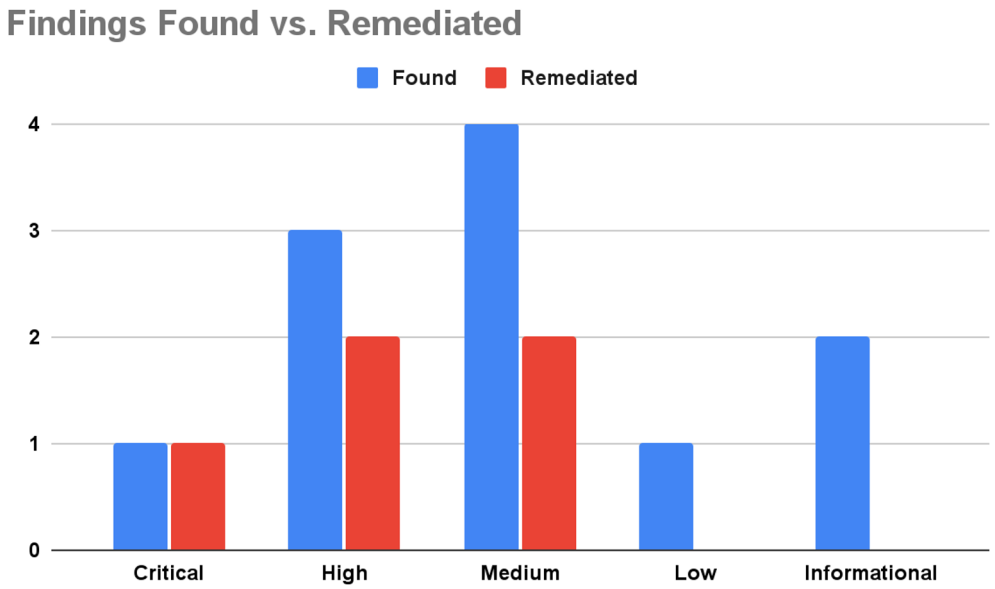
CVSS 3.1 SCORING		
SEVERITY	BASE SCORE RATING	ASSOCIATED COLOR
Info	0	
Low	0.1-3.9	
Medium	4-6.9	
High	7-8.9	
Critical	9.0-10.0	

RISK MATRIX		THREAT IMPACT			
		LOW	MEDIUM	HIGH	CRITICAL
LIKELIHOOD	RARE	Low	Low	Medium	Medium
	UNLIKELY	Low	Medium	High	High
	LIKELY	Low	Medium	High	Critical
	VERY LIKELY	Low	Medium	Critical	Critical

PRIORITIZATION METRICS

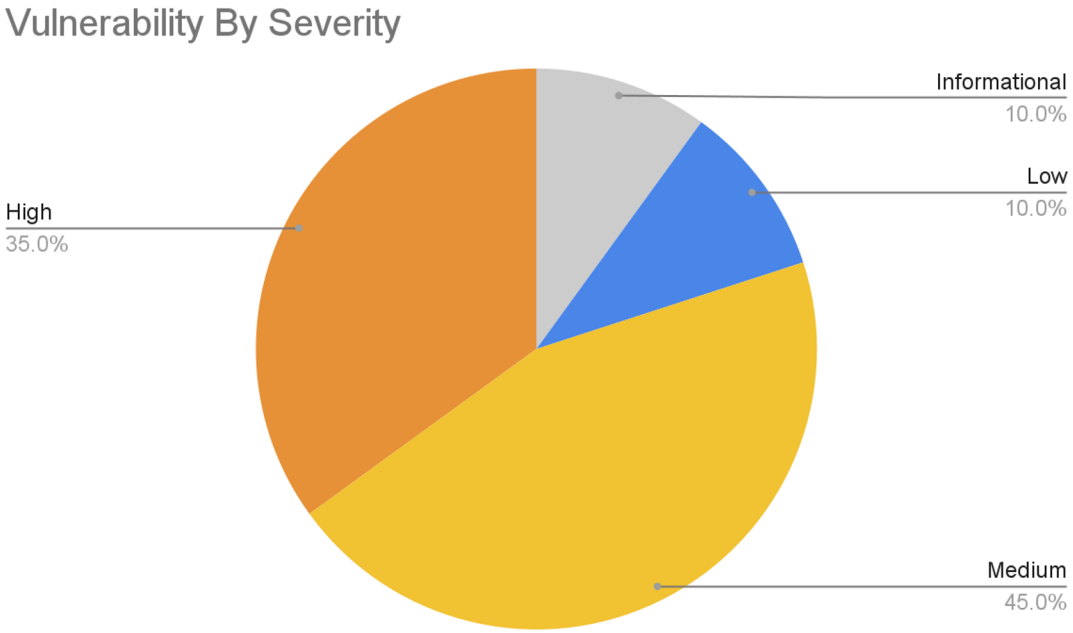


STATISTICS



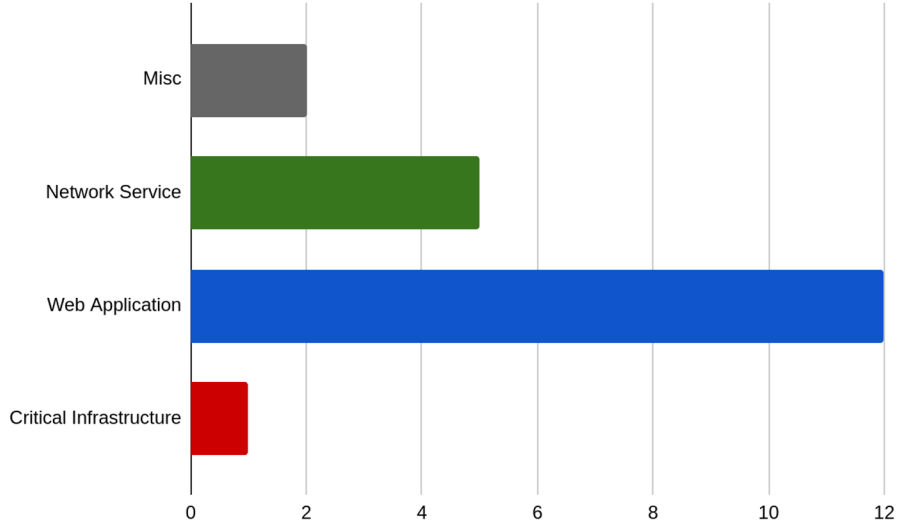
Findings Remediated

STATISTICS



Total Findings during Test-2

STATISTICS



Findings by Services

PCI-DSS COMPLIANCE

Req	Domain	Violations
R1	Build and Maintain a Secure Network	3
R2	Protect Cardholder Data	2
R4	Implement Strong Access Control Measure	3

GDPR COMPLIANCE

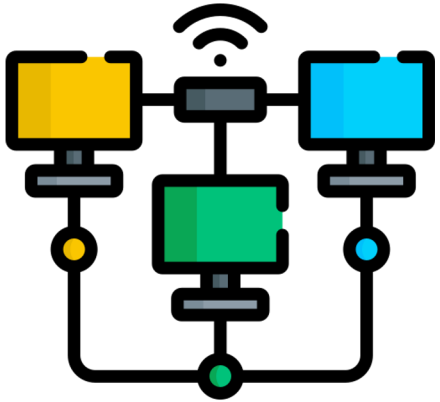
Req	Domain	Violations
Article 32(1.b), Article 32 (1.a), Recital 83	Security of Processing	6

KEY FINDINGS

Lack of Authentication

- 5 Findings
- **Critical** - Technical
- **CAT-4** - Prioritization
- PCI-DSS and GDPR

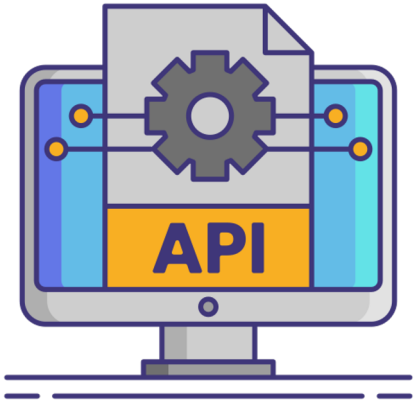
KEY FINDINGS



Lack of Segmentation

- 1 Finding
- **Critical** - Technical
- **CAT-4** - Prioritization
- PCI-DSS and GDPR

KEY FINDINGS



Poor Web Application Architecture

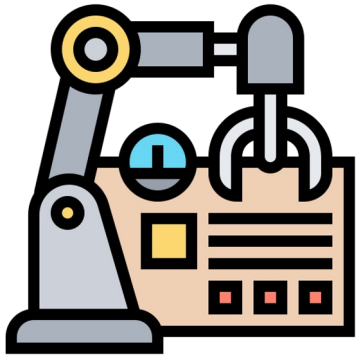
- 11 Findings
- **Medium** - Technical
- **CAT-2** - Prioritization
- PCI-DSS and GDPR

IMPACT

- Attackers can gain access to critical infrastructure
- Customer PII and payment information can get leaked
- Findings deviated from PCI-DSS and GDPR

SUGGESTIONS

Implement Authentication



ICS Segmentation

Secure Code Review

THANK YOU

Any Questions?