CUTAWAY SECURITY

INFOSEC CONSULTANTS

ICS / OT Security Challenges, Assessments, and Takeaways

Don C. Weber - @cutaway

Principal Consultant, Founder

Cutaway Security, LLC / Don C. Weber

- ICS Security Program Maturity
- ICS Security Assessments
- Penetration Testing
- Security Research

Agenda

- Challenges Experienced
- OT Security Assessments
- Assessment Observations
- Questions and Answers

Industrial Security Challenges

Industrial Challenges: Differences

- Infosec is difficult because of the differences between Information Technology (corporate) and Operational Technology (process).
  - IT and Information Security teams need education in process requirements.
  - OT needs education in IT administration, networking, and security tactics and techniques.

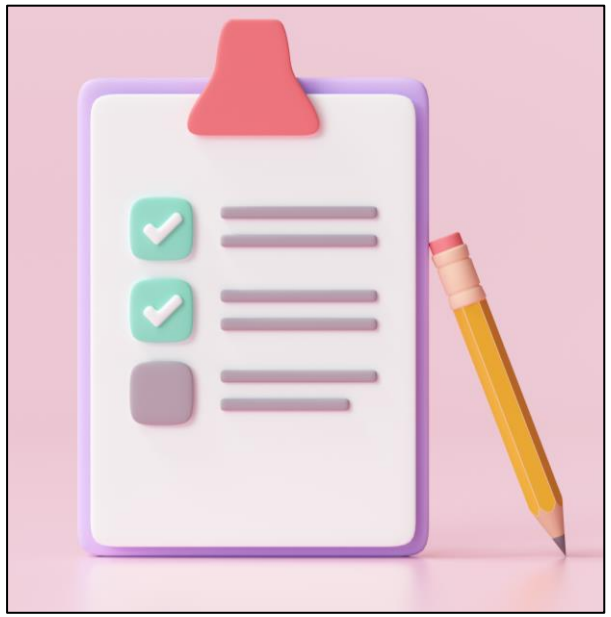
- BOTH teams need to collaborate and communicate. Stop operating in silos and vacuums.
  - OT teams need to STOP gatekeeping.
  - Infosec needs to STOP forcing IT remediation solutions to OT.

Industrial Challenges: Lifecycles

- Projects run for three to five years for design, procurement, deployment, testing, and initiation.
- Security requirements slowly working into design considerations
  - Implementing secure design and management differs from business unit to business unit.
- Lab environments for FAT, SAT, and security testing.
  - Many US utilities are pushing vendors and their teams to implement labs at the utility rather than the vendor factory.
- Implementers following Top 20 Secure PLC Coding Practices?
  - https://plc-security.com/

Image Source: https://www.cesi.it/app/uploads/2019/12/measuring-relays.jpg

Industrial Challenges: Vendors



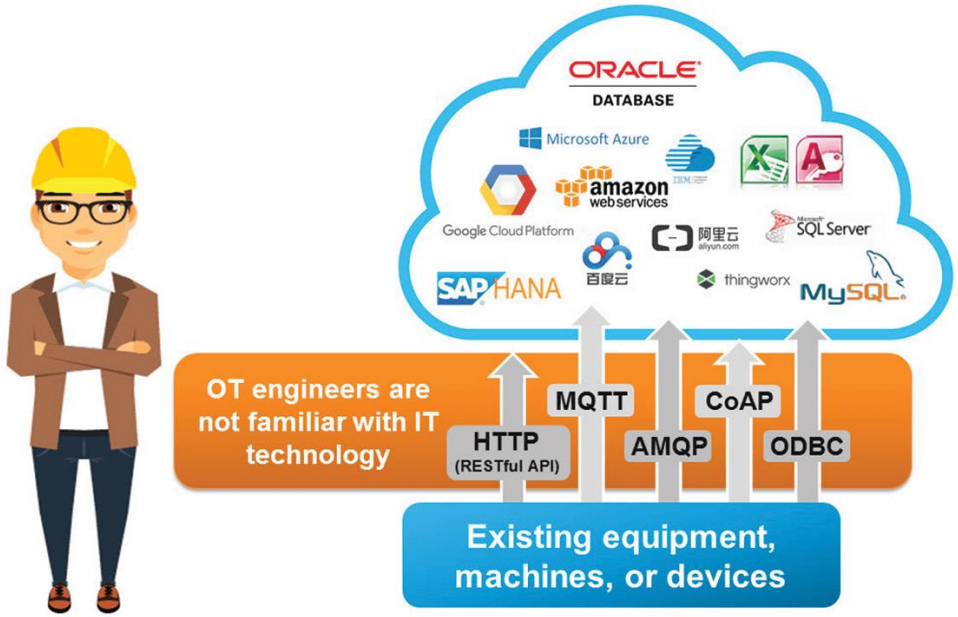
- Vendor specific solutions are may be built on top of thirty-year-old solutions.
- Vendor / Integrator implementation teams vary on their level of security expertise.
  - Some consider changing the default password to be ‘implementing security’ when left to their own determination of ‘securing’ the process.
- Hardening guides focus on general installation steps and recommendations.
  - Requires your team to set configuration requirements.
  - But, which teams are developing these requirements?
- OT teams often trust the vendors / integrators to ‘know’ what needs to be secured.
  - Threat modeling is done by non-security teams or penetration testers.

Industrial Challenges: Brown / Green Fields

- Brown Fields
  - Working, therefore, modification are not trusted and unwelcome.
  - Updates require significant effort (and cost) to redo wiring diagrams, implement, test, and recertify.
  - Rely heavily on physical security but also do not address dilapidated infrastructure issues and leave external cabinets unlocked.
- Green Fields
  - Installed by OT teams that do not accept help from non-OT IT teams and deploy insecure solutions.
  - New physical security measures cause false sense of security and teams leave external cabinets unlocked.

Image Source: https://www.witf.io/wp-content/uploads/2014/08/Dehydration4-e1537479816963.jpg

Industrial Challenges: The Cloud



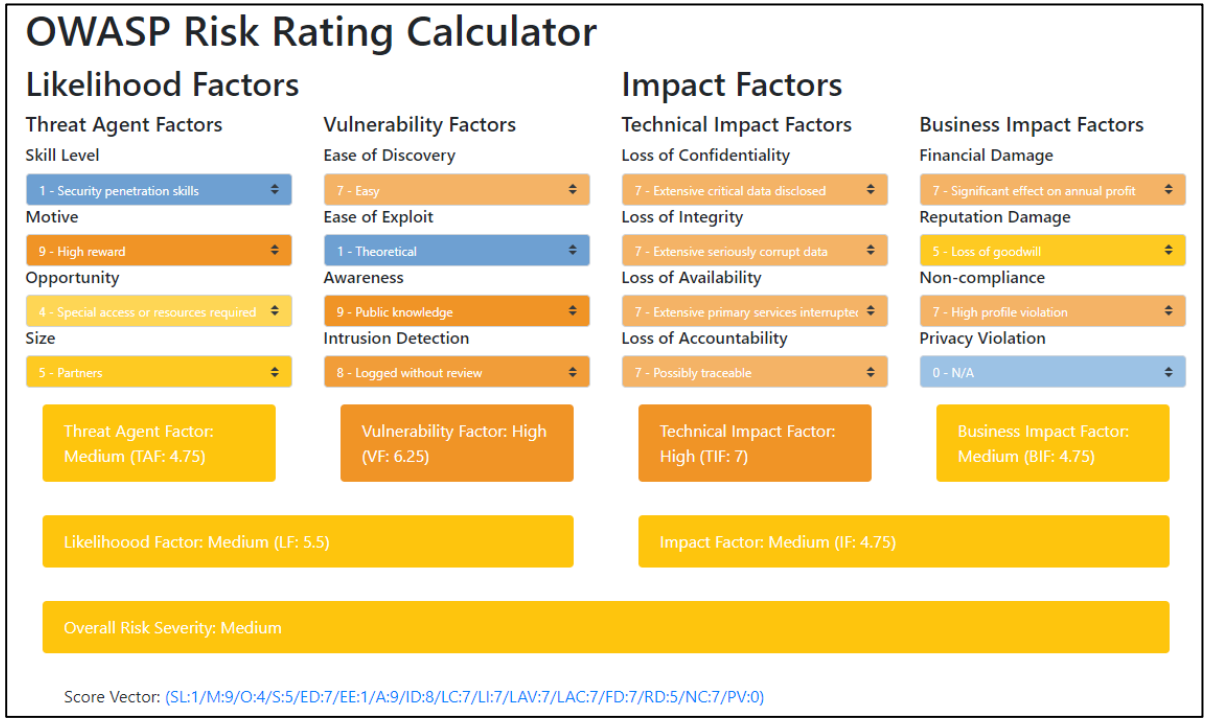
- OT Teams do not have questionnaires to evaluate cloud deployments, third-party administration, data flow, and vulnerability management.
- Vendors may or may not have conducted third-party web application and API testing.
  - How are they managing administrative roles / responsibilities and access monitoring?
- OT teams are NOT cloud experts.

Image Source: https://iebmedia.com/technology/edge-cloud/deploying-operational-data-to-an-ot-it-cloud/

CutSec CloudSec-IACS: https://github.com/cutaway-security/CloudSec-IACS

Industrial Challenges: Rating / Discussing Risk

- MITRE ICS ATT&CK Impacts are different than corporate impacts.
- IT / Infosec Teams need to be experienced in talking about work-arounds and risk acceptance when it comes to new vulnerabilities.
- Risk is often tied to compliance. However, compliance DOES NOT equal security.
- One work-around or patch might require recertification of the whole line / process. $$$



CutSec IACS System Testing and Assessment Rating Methodology (IACS STAR): https://github.com/cutaway-security/IACS_STAR_Methodology

Image Source: https://www.owasp-risk-rating.com/

OT Security Assessment

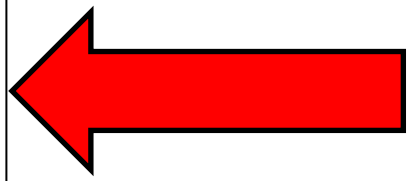
Types of Assessments

- Defining and communicating types of assessments reduces confusion
- Select assessment types based on the organization's goals
- Risk and cost vary by goals and experience
- Assessment results should improve process operational requirements

OT Risk	Assessment Type	Estimated Cost
	Vendor Review	$
	Security Research	$ $
☢	Security Assessment	$ $ $
	Threat Modeling	$ $
☢ ☢	Security Program Maturity	$ $ $
☢ ☢ ☢	Penetration Test	$ $ $
☢ ☢ ☢ ☢	Red Team	$ $ $ $

IT / OT Security Effort Prioritization

- Separate policies / standards for IT and OT environments
- Segmentation and Isolation
- Access Control / Authorization
- Attack Surface
- Logging and Monitoring
- Asset Inventory
- Incident Response and Recovery



Tactical ICS Security Starts Here

Risk Analysis Via Process Familiarization

- Architecture Review
- Site Walk Thru
  - Physical Security
  - Engineer / Operator Actions in Process
- Interviews
  - Managers
  - Engineers / Operators / Programmers
  - IT Team
  - IT Security
- Network Traffic Capture and Analysis
- Enforcement Boundary Testing
- Attack Surface Mapping
- Asset Management Review

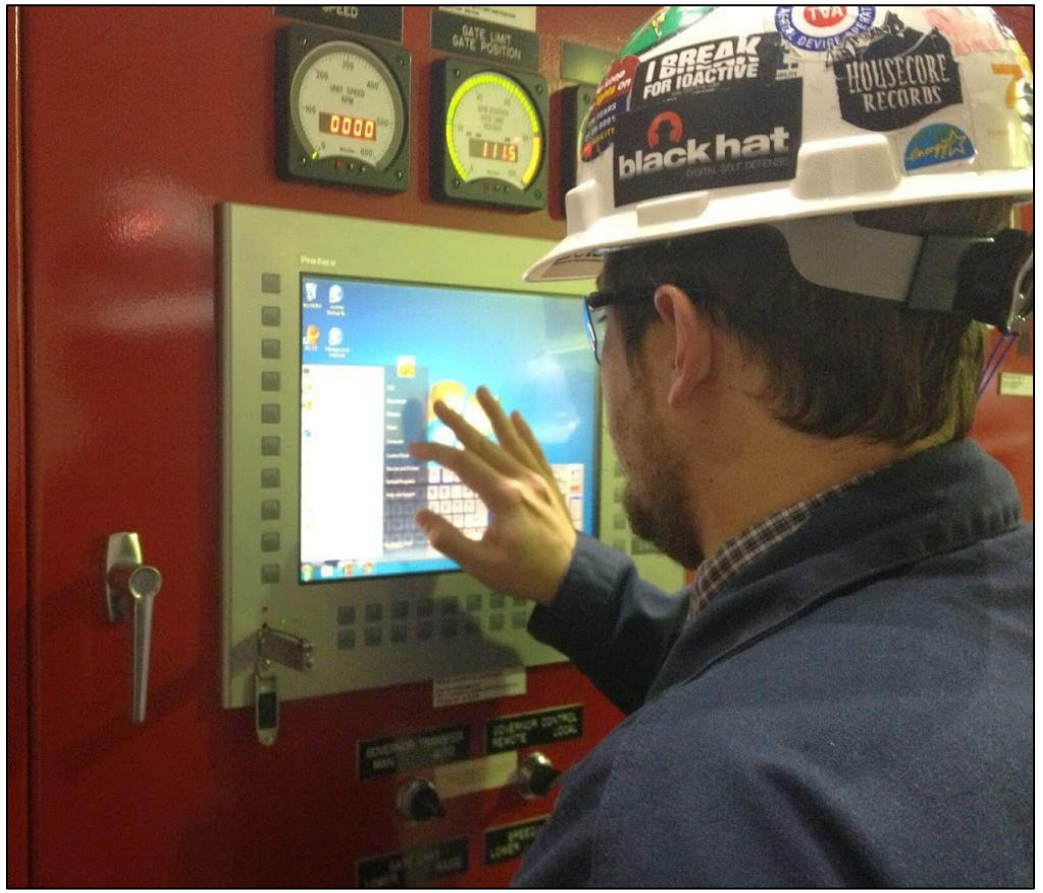


Image Source: https://www.controlthings.io/ - Accessing and Exploiting Control Systems

Assessment Observations

Assessment Takeaways (1)

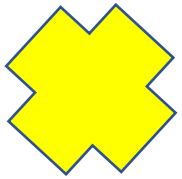
- **Vendors / Integrators expect security requirements from clients. Clients expect vendors / integrators to provide secure solutions.**
  - Result: Solutions are getting deployed without security or with ineffective controls and procedures.
  - Recommendation: Clients, this is YOUR issue – define security requirements and test to them. *Find ways to hold vendor / integrators accountable.*

- **Vendors / Integrators are not providing their OT teams with security configuration guidance.**
  - Result: Your team is, right now, deploying insecure client solutions that will be in place for years.
  - Recommendation: Develop and implement specific network, application, and device configurations to address basic security issues and centrally log events. Train your teams. Provide to your clients – *security shouldn't cost extra*.

Assessment Takeaways (2)

- **Lack of communications between OT and IT teams.**
  - Result: Exacerbates OT's isolation and self-reliance
  - Recommendations: IT / IT Sec teams need to get to know the process and OT team members. OT team members need to understand IT / IT Sec teams want to improve (not limit) the process. *OT team are not experts in Active Directory, databases, web servers but they are deploying them without IT / IT Sec assistance.*

- *** **There is NOT enough monitoring and incident response planning.** ***
  - Result: Spending loads of money for security, but still surprised when getting compromised and recovery times do not meet expectations.
  - Recommendations: Improve local logging on servers and workstations in Level 3. Centrally log and monitor these events. Review recovery efforts involving cyber incident response with full team - training.



Questions and Answers

CUTAWAY SECURITY

INFOSEC CONSULTANTS

Don C. Weber - @cutaway
info@cutawaysecurity.com
https://www.cutawaysecurity.com
https://www.linkedin.com/in/cutaway/