

Developing a Comprehensive OT Cyber Security Strategy for Manufacturing Sites

Reynaldo Gonzalez

Principal Cybersecurity Architect

Cummins





About Me – Reynaldo Gonzalez

- Principal Cybersecurity Architect @ Cummins
 - Cisco Academy Instructor & Adjunct Professor @ Lonestar College
 - Background (18+ yrs): Networking, Web Development, Cable, Architecture, Security, Cybersecurity, Consulting
 - Member of CSNP, CS2AI, ISC2, InfraGard
 - B.S in Applied Networking & System Administration @ RIT
 - M.S in Cybersecurity: Cyber Operations @ Utica University
 - Teaching 12+ years: Networking, Cybersecurity, Ethical Hacking
 - Certifications: CISSP, CEH, CCNA/CCNP (R/S, Security, Design)
 - Lived in Europe – Supported customers in EMEA, USA, Central/South America
-



DISCLAIMER

Any views or opinions expressed in this presentation are solely my own and do not reflect, represent, or associate with my current and previous employers including professional organizations I participate in.

The information presented is for information and educational purposes.



Overview

OT State of Affairs

OT Security & Business Priorities

Stakeholder Engagement

OT Cybersecurity in Manufacturing

Involving Cybersecurity Architects for Guidance

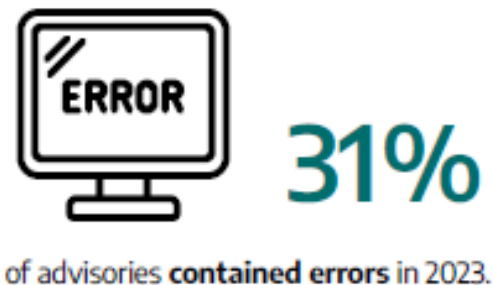
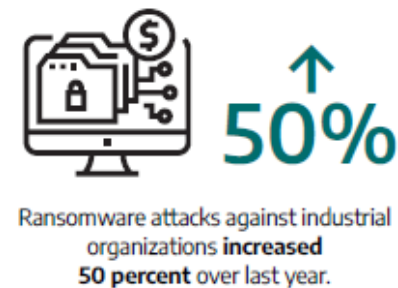
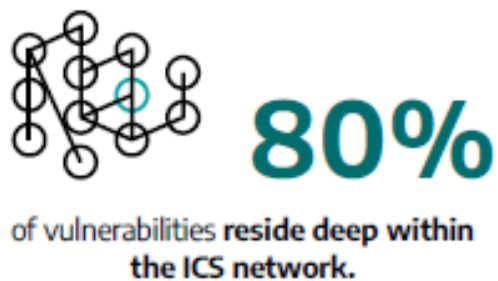
Technology Requirements and Implementation

Leveraging Current Tech vs Investing in Solutions

OT Security Strategy Plan

Key Takeaways





OT State of Affairs – Critical Infrastructures

- Nation State Actors
- Organized Crime
- Ransomware Gangs
- Cyber Warfare

Threat Group Highlights – 2023



Threat Actors Landscape = Critical Infrastructures including Manufacturing

Alignment with Business Priorities

Mapping out controls and policies

- Identify gaps and areas of improvement

OT security supports strategic goals

- Align security measures with business objectives

Adoption of frameworks and standards

- NIST CSF
- ISA/IEC 62443
- CMMC





Stakeholder Engagement and Risk Assessments

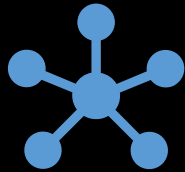
- Stakeholder Engagement
 - Operational teams
 - IT personnel
 - Network teams
 - Management
 - Security experts
- Risk assessments to prioritize security needs
 - Identify functional areas and risk tolerance levels
- Build trust and relationships across all levels
 - Culture of collaboration and communication
 - Importance of OT security in their roles



Importance of OT Cyber Security in Manufacturing

- Protects operational systems and processes
 - Practices
 - Strategies
 - Technologies
- Significance to Manufacturing
 - Protecting Critical Infrastructures
 - Mitigating Operational Risks
 - Preserving Product Integrity
 - Supply Chain Protection
 - Compliance with Regulations & Standards
 - Facilitating Innovation and Industry 4.0

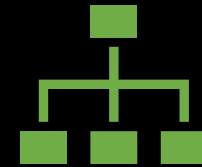
Architecture and Design Principles – Start Early



CROSS COLLABORATION FOR
DEFENSE IN-DEPTH ARCHITECTURE



INCORPORATE SECURITY BY
DESIGN PRINCIPLES



RIGHT LEVEL OF GOVERNANCE:
GUIDELINES, PROCESSES

Strategy & Implementation Planning



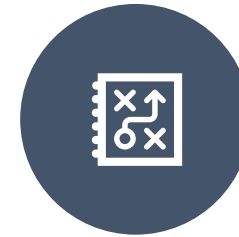
ASSESS
TECHNOLOGY
REQUIREMENTS



BUSINESS USE
CASES



SECURITY REVIEW
PROCESS



TRAINING IT/OT



DETAILED
IMPLEMENTATION
PLAN

Security Technology Evaluation



Evaluate the effectiveness of current solutions



Explore innovative solutions



Balance cost of new investments versus improved security postures



Security Tooling Strategy for Manufacturing



Endpoint Protection



Secure OT/IoT Remote Access



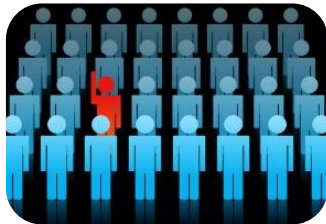
Asset Management



Vulnerability Management



Data Security



Identity Threat Protections



Segmentation



Response & Monitoring



Security Visibility

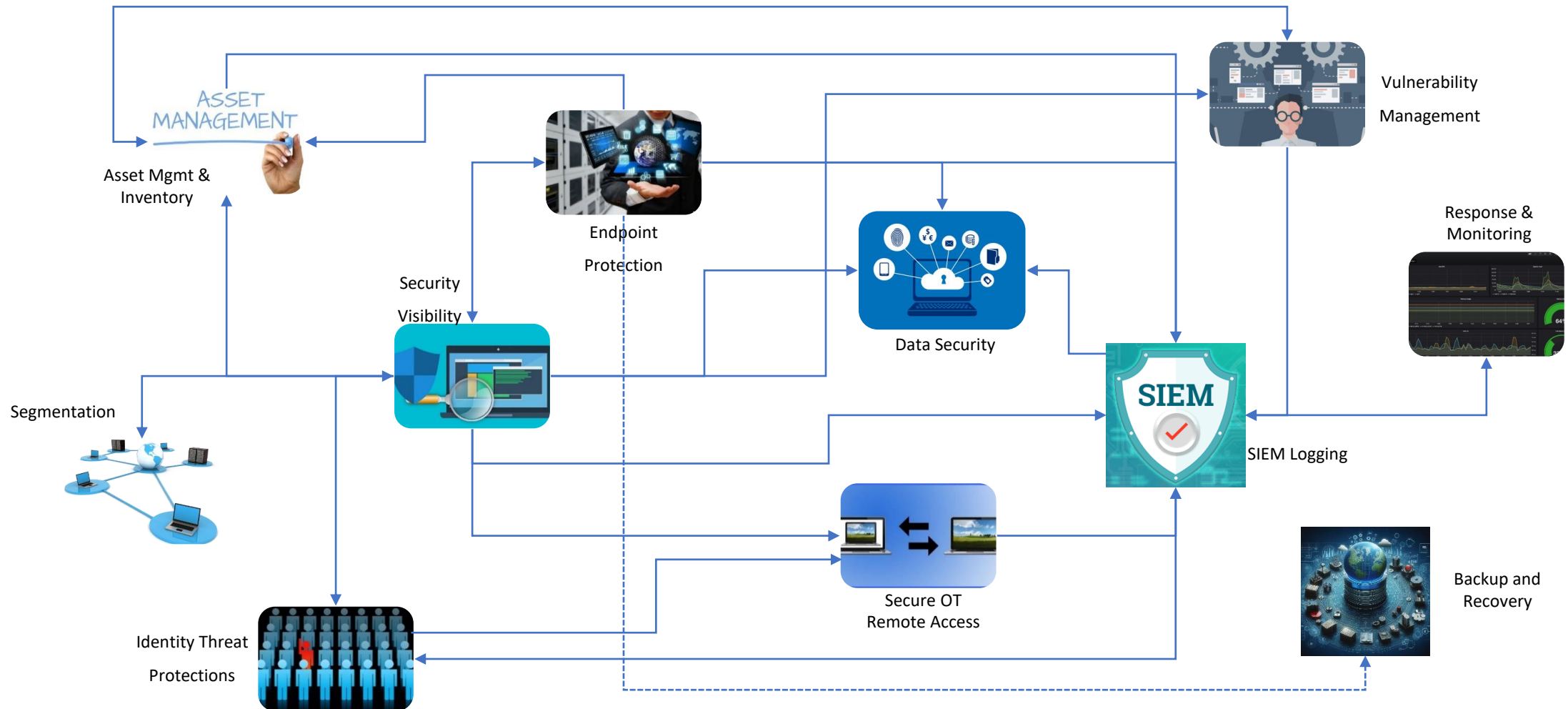


Backup & Recovery

Process: Cybersecurity Architecture Security Design Review: Security Controls, Requirements, Guidance, Reference Architectures

Why Security Technology Evaluations Matter?

Effectiveness of Integrations – *Data Enrichment*



OT Cybersecurity Strategy Plan for Increased Security Posture in Manufacturing



Takeaways: Proactive over Reactive



Collaboration is Key



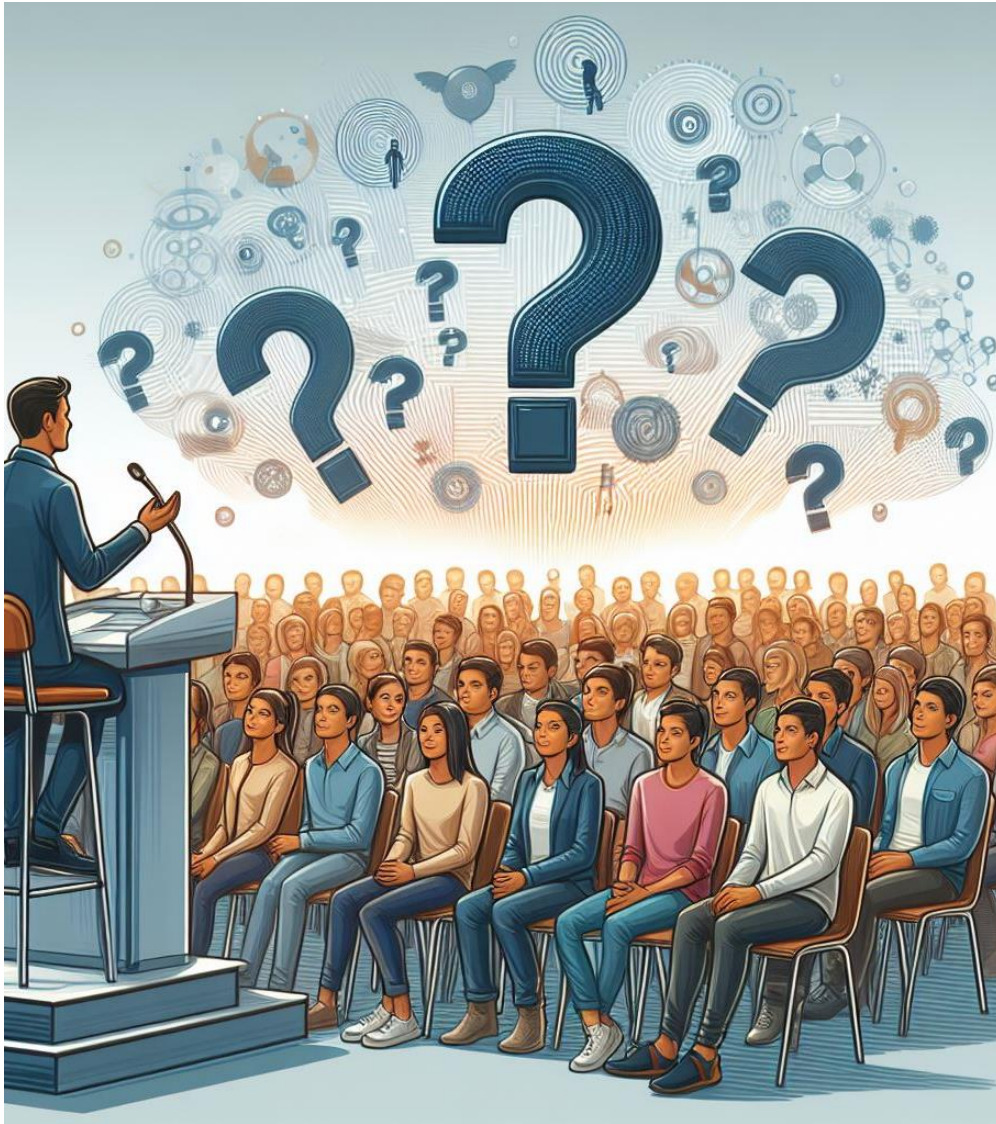
Security By Design Approach



Continuous Evaluation



Comprehensive Strategy



Happy to connect further...



Reynaldo Gonzalez

Principal Cybersecurity Architect & Leader
| HITEC | Speaker | Educator | CISSP | CE...



www.linkedin.com/in/reynaldoglz