TRIDIUM

NS2024

APRIL 15 - 17 | ANAHEIM, CA

Disclaimer

- This session is provided for information purposes. The views, information, or opinions expressed during this presentation and/or its associated/referenced materials are solely those of the individuals and/or organizations involved and do not represent those of Tridium, its affiliates or its employees.
- With respect to this presentation and the information and materials presented, Tridium makes no warranties, express or implied, including the warranties of merchantability and fitness for a particular purpose, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately owned rights.
- Tridium is not responsible for and does not verify the accuracy or reliability of any of the information contained herein. Results referenced, if any, may vary and past performance is not indicative of, and Tridium does not guarantee, future results. This information does not constitute professional or other advice or services and is presented for informational purposes only.

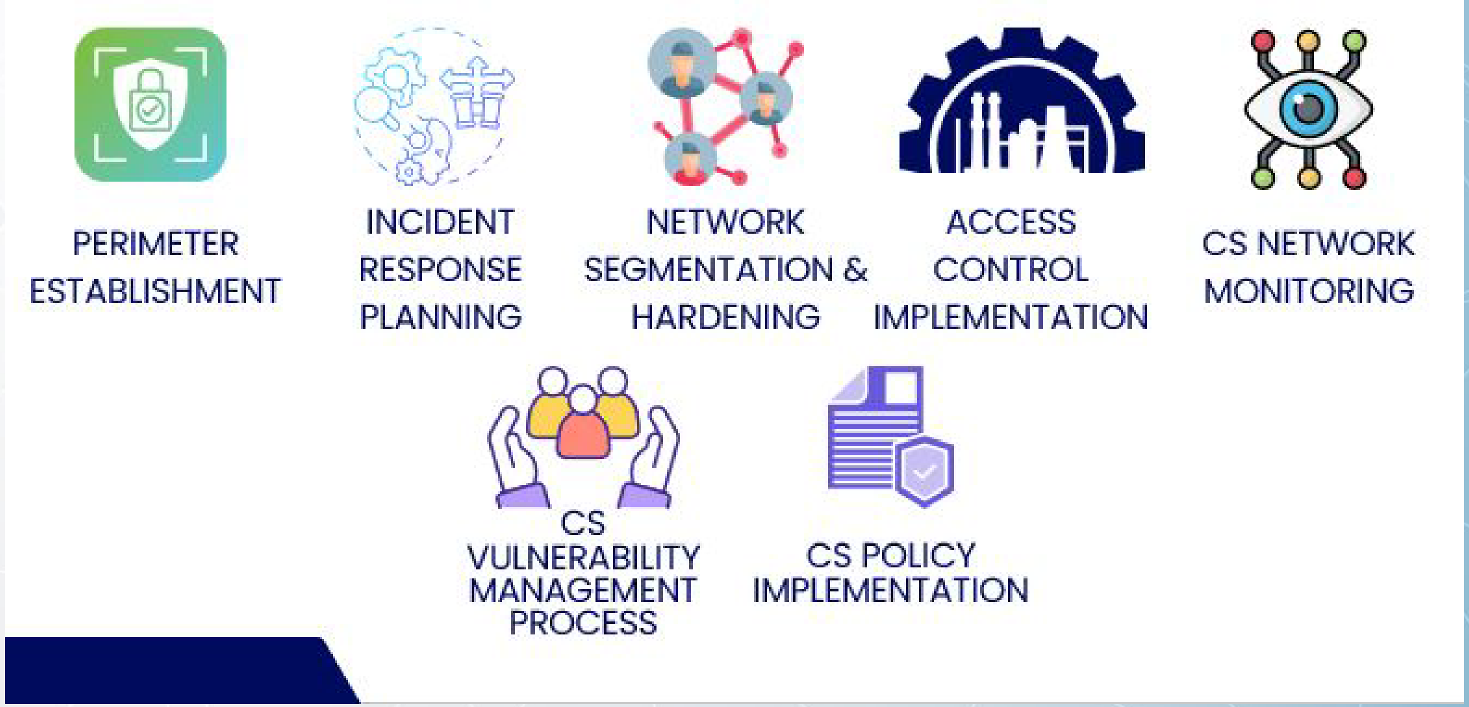
TRIDIUM

25 Years

NS2024

POWER OF PARTNERSHIP

7 Controls to Help Reduce Risk



PERIMETER ESTABLISHMENT

INCIDENT RESPONSE PLANNING

NETWORK SEGMENTATION & HARDENING

ACCESS CONTROL IMPLEMENTATION

CS NETWORK MONITORING

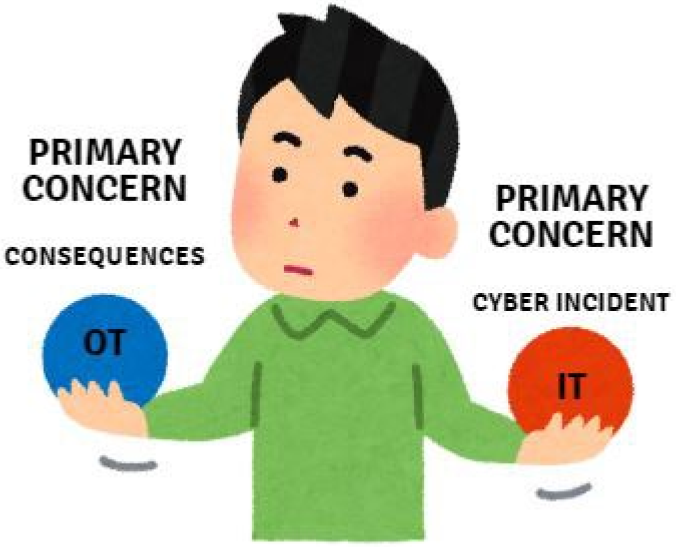
CS VULNERABILITY MANAGEMENT PROCESS

CS POLICY IMPLEMENTATION

NS2024

APRIL 15 - 17 | ANAHEIM, CA

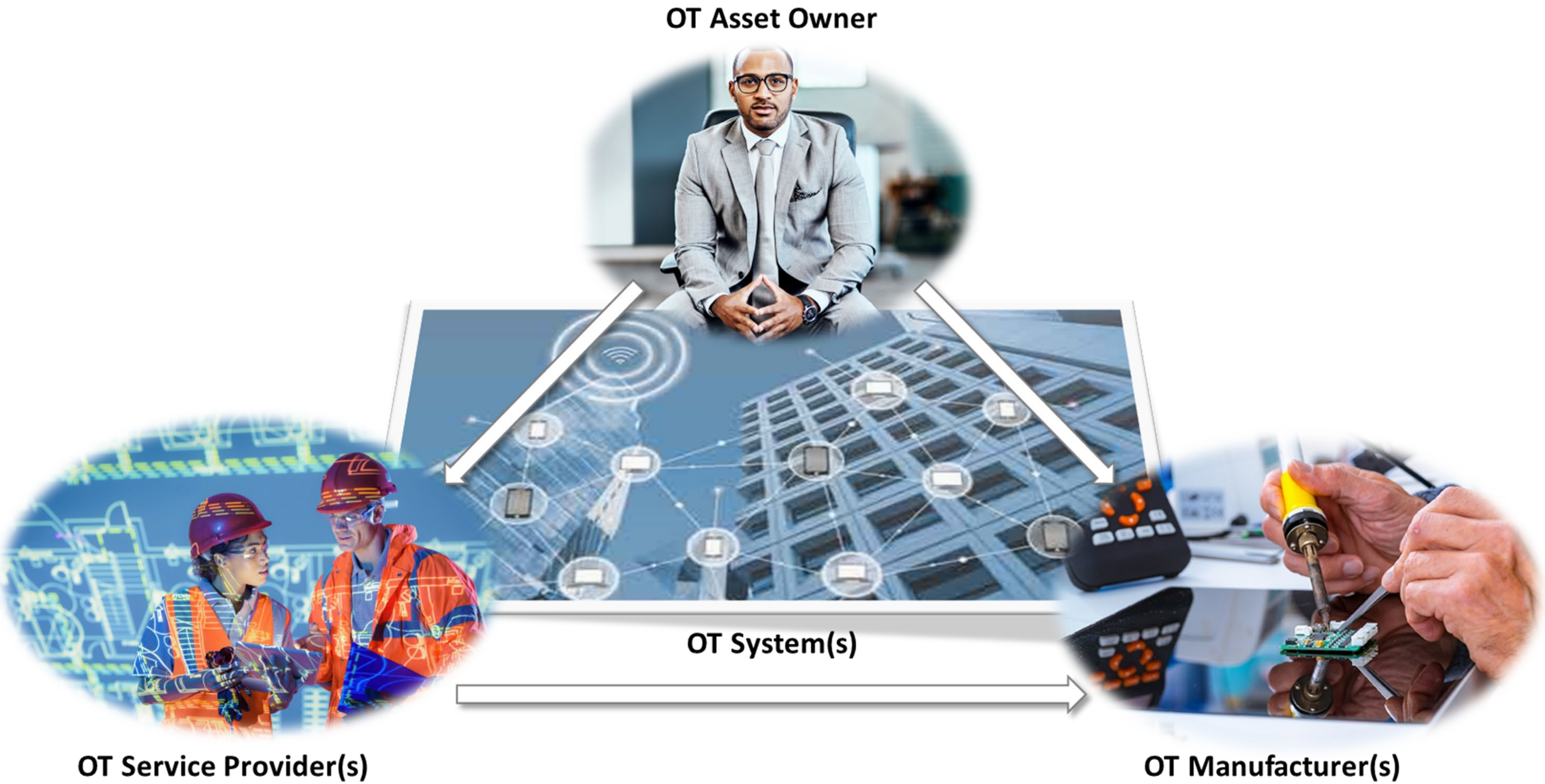
What is Unique About OT Risk Assessments?



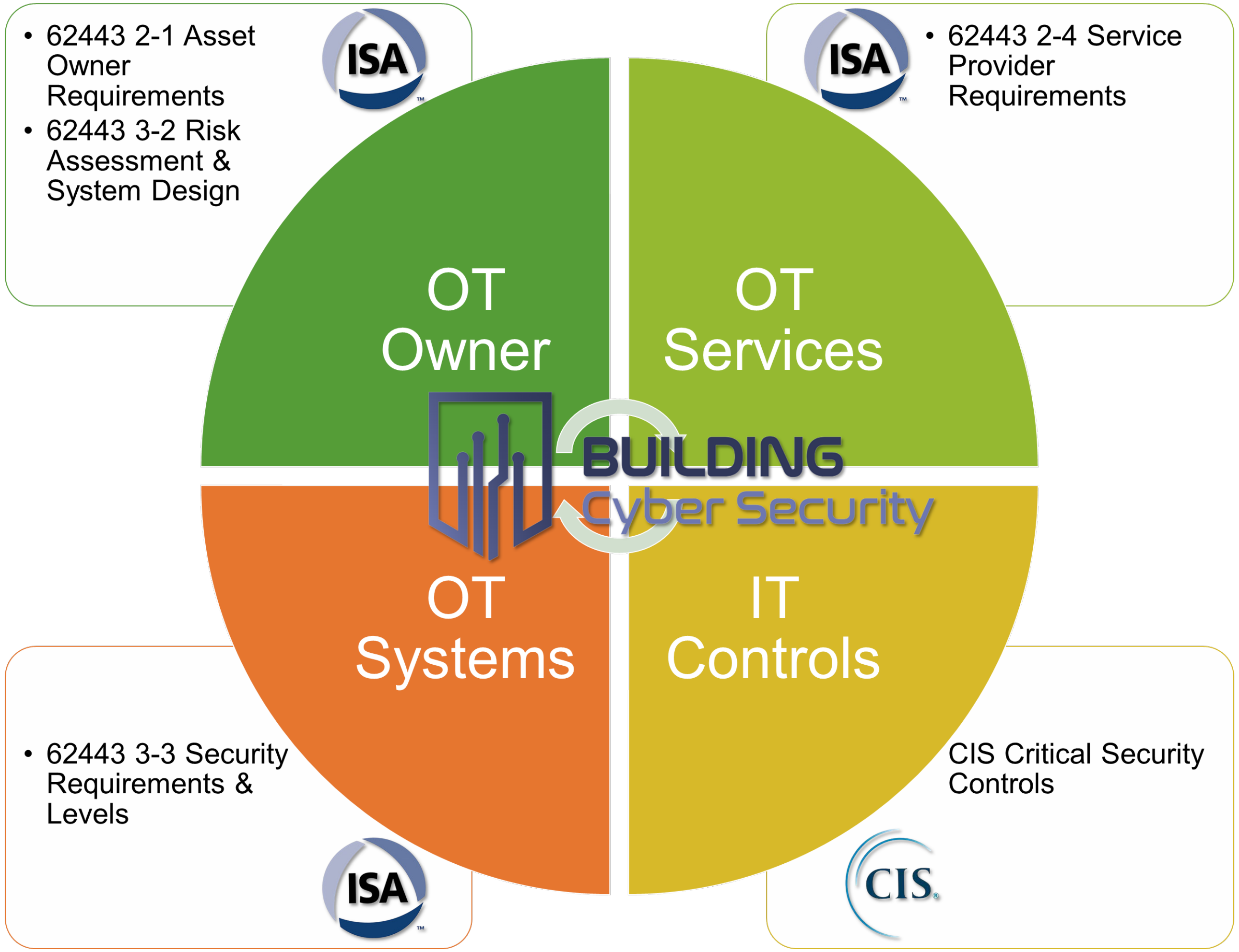
OT ADVANTAGE IS IN THE DESIGN

TRIDIUM

ISA / BCS 62443 – RESPONSIBILITY MATRIX



CONTROL SETS



- 62443 2-1 Asset Owner Requirements
- 62443 3-2 Risk Assessment & System Design

- 62443 2-4 Service Provider Requirements

- 62443 3-3 Security Requirements & Levels

CIS Critical Security Controls

NS2024

APRIL 15 - 17 | ANAHEIM, CA

TYPICAL OPSEC REQUIREMENT

Operations Security (OPSEC). Contractor must develop and implement processes and procedures to protect unclassified and sensitive aspects of the project from disclosure to unauthorized personnel (i.e., anyone operating outside the scope of the project). Information that must be protected falls into three categories: (1) administration / organization, (2) operations, and (3) facility design. The contractor must protect organizational data that includes unit mission, organizational structure, administrative & operational support relationships with higher headquarters and host nation organizations. The contractor must protect operations data that includes installation activities & operations, construction activities & operations, and installation & construction security procedures and protocols. The contractor must also protect facility design information reflecting sensitive capabilities and vulnerabilities. The critical information list highlights other unclassified and sensitive information that may require protection from disclosure to unauthorized personnel.

Contractors may be required to sign the non-disclosure agreements indicating that they will not reveal or discuss project or installation details with unauthorized personnel. Unless authorized by installation security officer, cameras, and communications devices (e.g., cell phones, laptops, thumb drives) are prohibited on installation.

FOCUS ON OT…

What details to watch, such as:

- Building floor plans … with occupant names, functions, etc.
- Occupancy schedules… or loads, sensors
- Current or future operations… equipment status, out of service, remodeled, bid specs
- Security procedures… who has access, who and when audits happen, analytics of the system, backups
- Prequalify your vendors, suppliers, subcontractors… before
- Who has a “need to know”… don’t share if they don’t need it.
- Silo your information… don’t let one person (external) know everything about your system

Cyber Regulations impact YOU & YOUR Customers

Governments around the globe are reacting with new cyber regulations….

- USA - CISA NIST Secure Software Development Framework Attestation form – (EO 14028) impacts selling or operating with the US Gov
- EU - NIS2 – Cyber for infrastructure in EU larger scope and IR requirements
- USA - Cybersecurity Maturity Model – Impacts sales to DoD

Coming

- Proposed Rule: Cyber Threat and Incident Reporting and Information Sharing - FAR (EO 14028)
- EU Cyber Resiliency Act – Implementing acts being developed now will impact all digital products sold and deployed in Europe (2027).

Integrators and installers and vendors must get out ahead of this otherwise more nimble will…

Going beyond Secure by design..

- Secure by design is a great start – but you/we aren't finished!
    - Secure by deployment
    - Secure by Operate
- Must do ALL 3 to have a secure product & to STAY secure.
- Integrators have a responsibility to ensure Secure deployments
    - Drive security requirements not just the recipient of them (or lack there of)
    - Build and grow training of all integrators and installers to ensure always secure in any installation.
- Leverage global standards to set the bar like ISA/IEC 62443-2-4 Security program requirements for service providers

TRIDIUM

25 Years

NS2024

POWER OF PARTNERSHIP