analysabl
EXAMINE | INTERPRET | TRANSFORM

OT Security

OT Security Audit

- Asset discovery & network analysis.
- Identify and analyses the security risks and threats exposure for the OT/ IT/ ICS systems.
- Review OT machine status w.r.t upgrades, AV, OS patching etc.
- Network segmentation + network security study and analysis (switch settings/ ACLS, firewall rules) etc.
- Wireless setup security review, security logs review.
- Configuration review of all the OT systems.
- Review and recommend architecture and detailed BOQ (generic) for future IDS/ IPS / OT SOC.
- Build roadmap for OT/IT convergence.
- Review existing OT security processes and procedures and support in preparation/fine tuning.
- Third party and vendor remote access review.
- Backup and storage review, identity and access management review.
- Removable media usage review, data security review.

Cyber Physical systems and Operational Systems Health

Deceptions & Honey Pots

Identity and Access Management

IIOT Device Security

Secure Remote Access & Zero Trust

IT/OT End Point Security & Patch Management

Network Discovery Monitoring and Threat Detection

Perimeter Security and Network Segmentation

Product and Supply Chain Security

Social Engineering and Phishing Security

analysabl
EXAMINE | INTERPRET | TRANSFORM

Methodology

- Architecture Assessment: Gather information interviewing IT & OT stakeholders.
- Operations Risk Assessment: Physical Assessment at the plant.
- OT Visibility and Anomalies Detection: Deploy tools to understand the OT Protocols, OT Assets, and Anomalies.
- IT-OT Cyber Risk Assessment: OT Threat Modelling based on the MITRE Attack Framework, ISA99 Architecture, CIS and IEC 62443:3.

OT Security Audit – Packages

	Standard	Advanced	Premium	Custom
Number of Assets	< 25	26 to 50	51 to 100	Any
Duration	6 Days (3 Days Onsite)	10 Days (5 Days Onsite)	15 Days (7 Days Onsite)	Scope Based
Asset Investigation	✓	✓	✓	✓
PCAP Analysis	✓	✓	✓	✓
OT Security Audit Report	✓	✓	✓	✓
Threat Modelling workshop	✗	✓	✓	✓
Port Scans and VA	✗	✗	✓	✓
Data Security Assessment	✗	✗	✓	✓
OT Security Roadmap	✗	✗	✗	✓
Security Process Review	✗	✗	✗	✓
Incident Response Planning	✗	✗	✗	✓

Note: For pricing contact us.