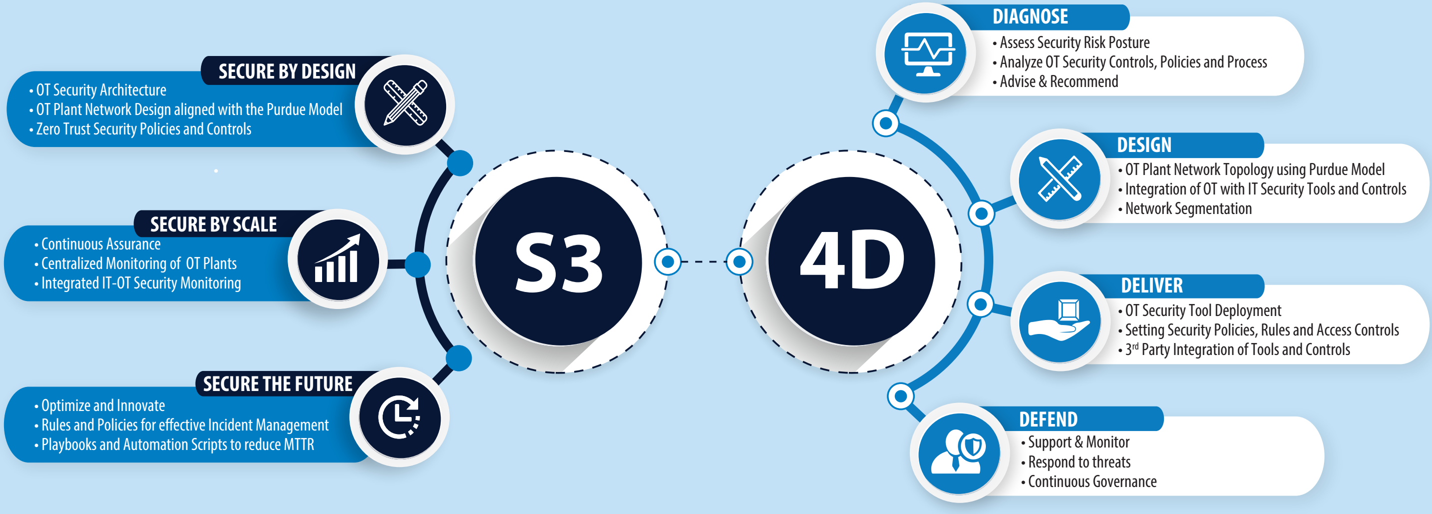
INFOSYS OPERATIONAL TECHNOLOGY (OT) SECURITY SERVICES

Infosys®
Navigate your next

Infosys Operational Technology (OT) Services built on the foundation of Infosys' **S34D principle** assures **digital trust** and **cyber resilience** at scale to its customers through **competence and delivery excellence.**



S3

SECURE BY DESIGN
- OT Security Architecture
- OT Plant Network Design aligned with the Purdue Model
- Zero Trust Security Policies and Controls

SECURE BY SCALE
- Continuous Assurance
- Centralized Monitoring of OT Plants
- Integrated IT-OT Security Monitoring

SECURE THE FUTURE
- Optimize and Innovate
- Rules and Policies for effective Incident Management
- Playbooks and Automation Scripts to reduce MTTR

4D

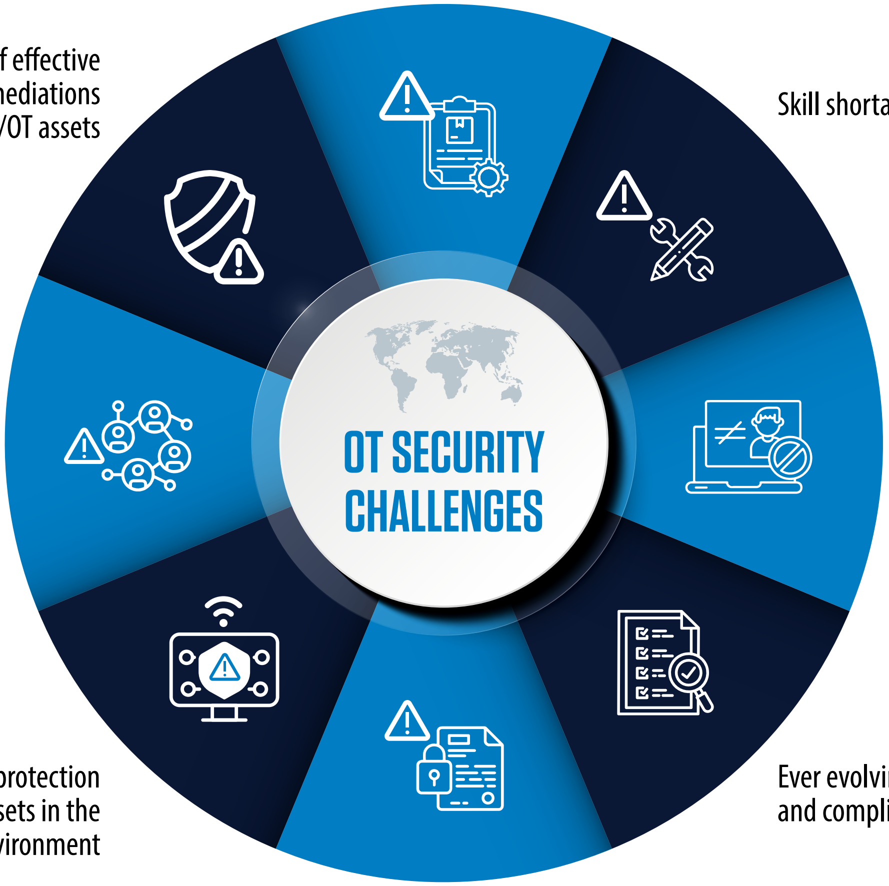
DIAGNOSE
- Assess Security Risk Posture
- Analyze OT Security Controls, Policies and Process
- Advise & Recommend

DESIGN
- OT Plant Network Topology using Purdue Model
- Integration of OT with IT Security Tools and Controls
- Network Segmentation

DELIVER
- OT Security Tool Deployment
- Setting Security Policies, Rules and Access Controls
- 3rd Party Integration of Tools and Controls

DEFEND
- Support & Monitor
- Respond to threats
- Continuous Governance

OT Security Challenges in Global OT/ICS Industries



OT SECURITY CHALLENGES

Lack of asset visibility, inventory, and CMDB

Skill shortage

Unauthorized/ unmonitored remote access

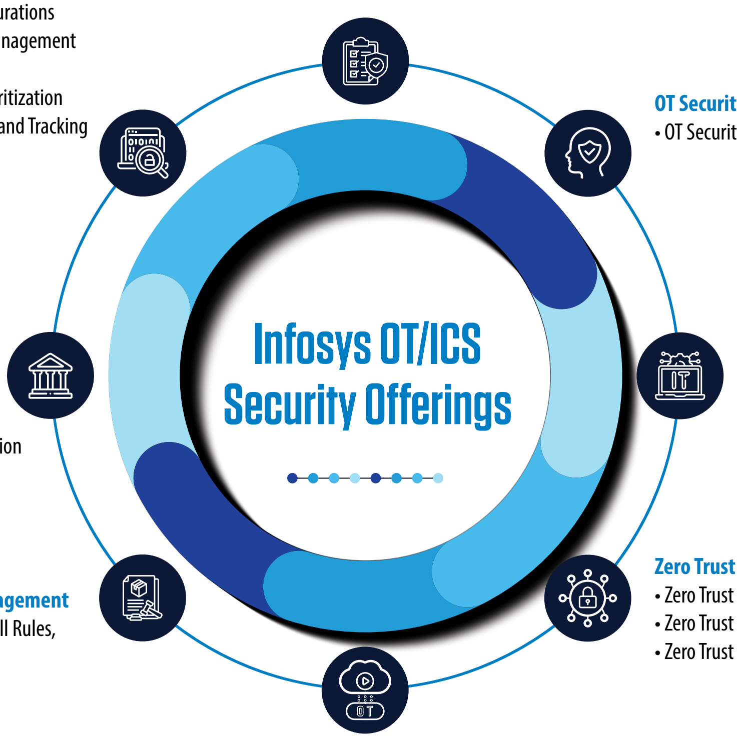
Ever evolving regulatory and compliance requirements

Insufficient security controls and policies implemented for OT environment

Lack of endpoint protection for legacy assets in the OT environment

Lack of network segmentation

Lack of effective vulnerability remediations for IT/OT assets



OT Security Assessment & Advisory

- OT Security Risk Assessments
- OT Security Recommendations, Advisory, Strategy & Roadmap

Vulnerability Management

- Asset Baseline Configurations
- IT-OT Vulnerability Management
- False Positive Analysis
- Risk Analysis and Prioritization
- Remediation Planing and Tracking

OT Security Training

- OT Security Awareness and Training for Plant Engineers

OT-IT Security Operations & Governance

- 24*7 Security Monitoring and Triaging
- Continuous Incident/Alert Management, Malware Analysis
- Continuous Security Assessment and Remediation

Integrated IT and OT SOC (MSS)

- IT - OT SOC Monitoring
- Incident Lifecycle Management
- 24*7 Security Monitoring

Compliance and Regulatory Management

- Review of Network Topology, Firewall Rules, NAC and Security Controls
- Security Posture Improvement

Zero Trust aligned OT Security Services

- Zero Trust Maturity
- Zero Trust Security Controls and Solution Implementation
- Zero Trust Aligned Design, Architecture and Services

OT Platform Design, Build and Management

- Plant Network Topology Design
- OT Security Platform Implementation
- Tuning, Alerting and Platform Optimization
- Integration with third party solutions like NGFW, SIEM, AV, EDR, ITSM tools

OT Security Partner Solutions for Next Gen Innovative Solutions

Asset Discovery

Discovery of IT-OT assets in an OT/ICS plant network with details of asset information for both connected and air-gapped plants.

CLAROTY
Microsoft
NOZOMI NETWORKS

Vulnerability and Risk Management

Identification of vulnerabilities linked to IT-OT assets with details such as CVE, risk rating and risk based prioritization for remediation.

CLAROTY
Microsoft
NOZOMI NETWORKS

Network Protection

Ability to create network micro-segmentation, zoning and conduit for the OT-IT assets and implement security controls, firewall rules and policies. Ability to integrate with IT-security tools and controls.

FORTINET
CISCO
paloalto NETWORKS

Anomaly Detection & Security Monitoring

Real time threat detection and alert for any behavioral and operational changes, policy violations in the OT environment with the detailed root cause analysis.
Ability to perform centralized security monitoring from the platform console or integrated third part SIEM/SOC platform.

CLAROTY
Microsoft
CISCO
paloalto NETWORKS
FORTINET

Endpoint Protection

Endpoint protection to IT assets including legacy assets in the OT environment. Able to detect any vulnerabilities and reduce the attack surface from malware and cyber threats.

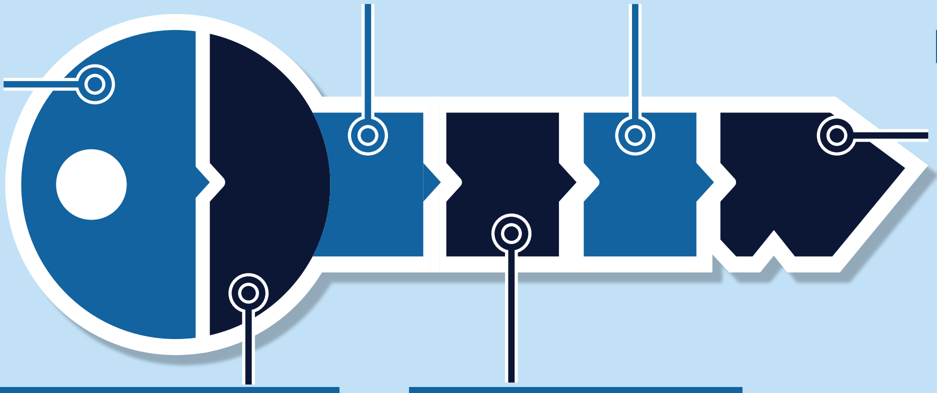
TREND MICRO
Symantec. by Broadcom
McAfee

Secure Remote Access

Ability to provide secure remote access to the OEMs/vendors for patching/upgrading of OT assets with session monitoring, authentication with multi-factor authentication and user access control.

FORTINET
CLAROTY
CISCO

Key Differentiators



Strong assessment framework with tool-based approach

Our security assessment framework is aligned with the NIST and ISA 62443 standard meeting NIS2, NERC-CIP and other regulatory compliance. We offer tool-based approach for security risk assessment of the sites resulting in deep visibility and elevated security posture.

Infosys Cyber Defense Center for IT-OT SOC Monitoring

Infosys' state-of-the-art Global Cyber Defense Centers spread across Americas, Europe, and India help in round the clock monitoring of both IT and OT environments.

Competency

We have a pool of 100+ experienced OT cyber professionals capable of managing multiple OT programs. Our academic collaboration with leading institutes such as Purdue University, and access to partner e-learning platforms, hands-on lab help us upskill our talent on continuous basis thus building competency at scale.

Automation for quick response

We have developed automation, workflows, SOPs for quick incident/alert management in OT environment. We bring 1000+ automation use cases developed for IT SOC which can be leveraged for OT system as applicable. We also work with clients for any use case creation as required to manage their OT system.

Experience in OT platform design and management

Extensive experience in providing end-to-end OT security including design of OT plant network using the Purdue model, product implementation, integration with third party IT tools and controls and management of the OT platform.

Partnership with leading OT Security vendors

Alliance with leading OT security vendors such as Claroty, Microsoft, ForeScout, Palo Alto Networks, Fortinet, Cisco, Armis, Nozomi etc. bringing together execution experience in various industries and verticals across geographies.

Success Stories

An American consumer packaged goods company

Infosys assessed and analyzed client's OT security platform, recommended and remediated the identified cybersecurity gaps. Infosys also deployed OT security components (sensors and servers) and provided end-to-end managed OT security services for more than 30+ plants.

One of the world's largest mining company based out of Australia

Infosys assisted the client in discovering the IT-OT assets for their 50 plants. Identified the vulnerabilities associated in the assets and did the risk analyses for the remediation of the critical assets. Managing the security incident and alert of the OT plant network from the customer SIEM platform.

One of the leading beverage manufacturer in the world

Infosys helped the client in designing the OT plant network for various plants with Claroty and Microsoft Defender for IoT solution. Infosys is managing their IT and OT security monitoring with Infosys Cyber Next platform which provides integrated IT-OT SOC from the same platform.

A UK based leading producer and supplier of specialty metal products and alloys

Infosys assessed and analyzed the client's OT/ICS environment, and prepared the report which helped the client in identifying the best fit OT security solution for asset discovery, vulnerability assessment, and anomaly detection on the plant network.

To know more about CyberSecurity, scan the QR code

For more information, contact askus@infosys.com

Infosys®
Navigate your next