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.

OT Security Challenges in Global OT/ICS Industries

- 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 effective vulnerability remediations for IT/OT assets
- Lack of network segmentation
- Ever evolving regulatory and compliance requirements
- Insufficient security controls and policies implemented for OT environment
- Unauthorized/ unmonitored remote access
Infosys OT/ICS Security Offerings

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

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

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

OT Security Training
- OT Security Awareness and Training for Plant Engineers

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

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 party SIEM/SOC platform.

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.

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.

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

Anomaly Detection & Security Monitoring
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.

Endpoint Protection
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.

Anomaly Detection & Security Monitoring
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.

External Document © 2023 Infosys Limited
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 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.

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.

Infosys helped the client in designing the OT plant network for various plants with Clarity 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.

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.

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.

Experience in IT platform design and management

Infosys has 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.

Automation for quick response

We have developed automation, workflows, 500s 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.

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’ 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.

Infosys Cyber Defense Center for IT-OT SOC Monitoring

Experience in IT 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.

Automation for quick response

We have developed automation, workflows, 500s 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.

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 Clarity 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