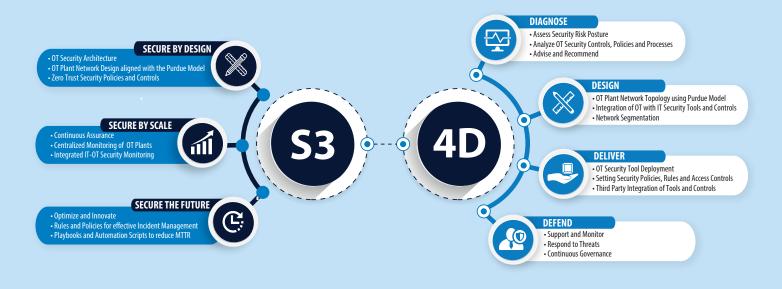
INFOSYS
OPERATIONAL
TECHNOLOGY (OT)
SECURITY SERVICES





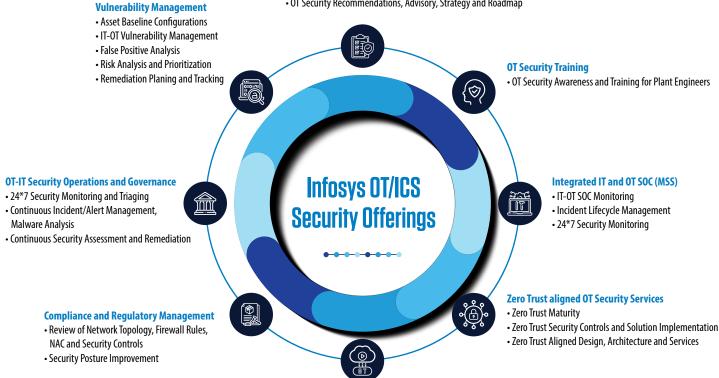
Infosys Operational Technology (OT) Security Services, built on the foundation of our S34D principle assures digital trust and cyber resilience at scale to our customers through competence and delivery excellence.



# **Infosys OT/ICS Security Offerings**



• OT Security Recommendations, Advisory, Strategy and Roadmap



# **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

# **Advanced Security Solutions for OT Assets**

# Asset **Discovery**

Discovery of IT-OT assets in the 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**

Create network microsegmentation, zoning and conduit for the OT-IT assets, and implement security controls, firewall rules and policies. Ability to integrate next generation firewall and **Network Access Control List** (NACL) with **IT-Security tools** and controls.

## **Anomaly Detection and** Security **Monitoring**

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

### **Endpoint Protection**

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

### **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.

# **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.

# **Building Cybersecurity Expertise**

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, access to partner e-learning platforms, and hands-on lab help us upskill our talent on continuous basis, thus building competency at scale.

# $(\bigcirc)$

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 bringing together execution experience in various industries across geographies.

# 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.

# **Success Stories**



**An American consumer** packaged goods company

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



One of the leading beverage manufacturer based out of US

Infosys helped the client in designing the OT plant network for their various plants. We also monitored their IT and OT environments through our 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.



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. We further helped in identifying vulnerabilities associated with the assets and performed risk analysis to remediate critical assets. We also managed the security incident and alert of the OT plant network from the customer SIEM platform.

# **Client Testimonial**



Infosys conducted an OT security assessment for all our plants, which provided us with great value. The report from the delivery team was thorough and tangible and gave us a great overview of our external attack surface. The Infosys team also provided us with clear and actionable recommendations for the short term and long term for reducing our risk surface and building a strong cyber security incident response mechanism. It has been a pleasure working with Infosys as they brought in their expertise and helped us in improving our OT cyber security posture and strengthening our defense against cyberthreats.



**BEATRIZ GARCÍA-COS MUNTAÑOLA** - Chief Finance Officer & IT, Ferroglobe



To know more about CyberSecurity, scan the QR code

For more information, contact askus@infosys.com



© 2024 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.

Stay Connected



