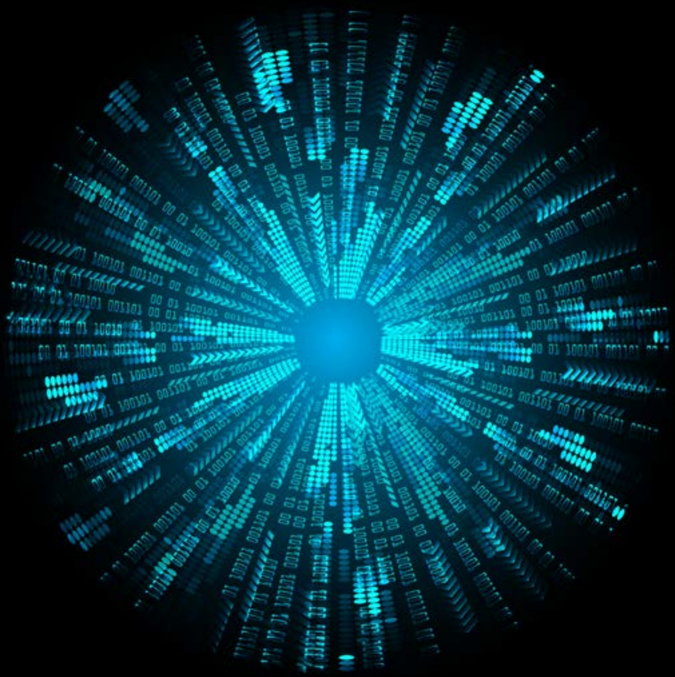
Deloitte.



Powering growth through smart cyber

You build. We secure.

Risk Advisory

Contents

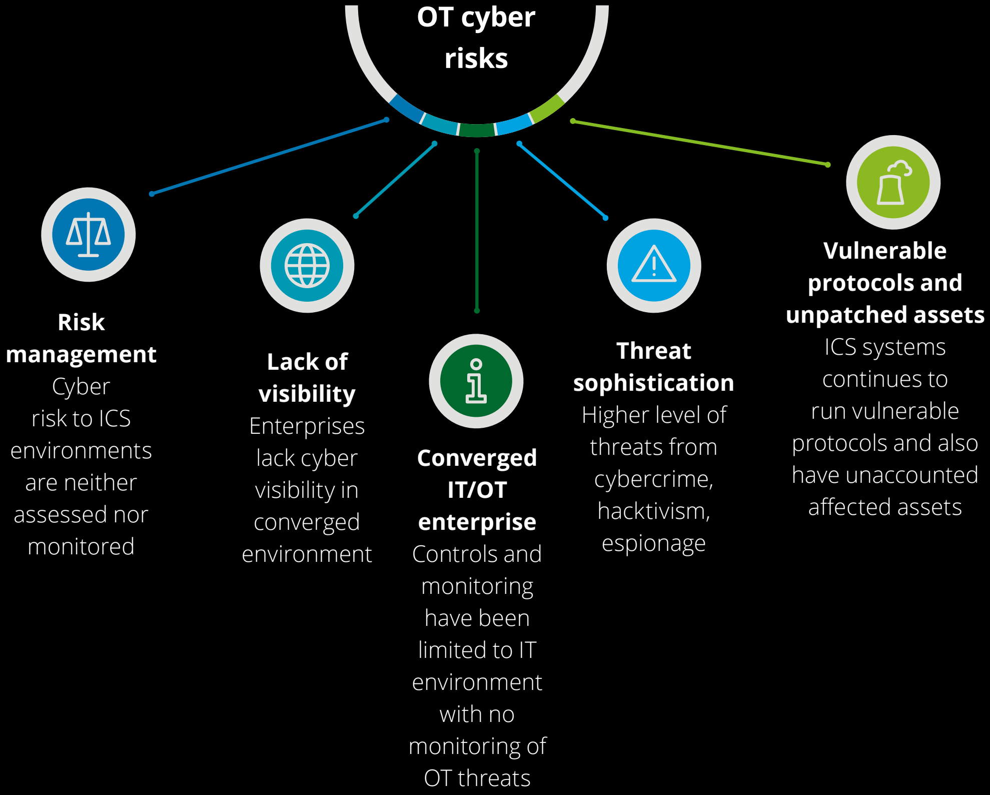
Securing Industry 4.0: Cyber threat management for Operational Technology (OT)

Evolution of Industry 4.0 and connected machinery enables the enterprises to transform the production with increased threat to converged digital infrastructure. Gaining cyber visibility remains a crucial need to effectively mitigate security threats to this hyper converged information technology (IT) and OT infrastructure.

Deloitte's cyber threat management for OT uses a combination of innovative cybersecurity solutions and services to manage cyber risks in Industrial Control Systems environments.

An advanced cyber risk offering provides a more integrated view of an organisation's threat landscape across IT and OT environment in order to gain visibility and deliver better threat management and security operations capabilities. The integrated end-to-end offering leverages Industry leading technology platforms, Deloitte Cyber Intelligence Center (CIC), and our dedicated Industrial Control System (ICS) threat intelligence team. These form a powerful ecosystem that is built to provide strong industrial cyber identification, monitoring, and defense.

Operational Technology cyber threat management challenges



OT cyber risks

Risk management
Cyber risk to ICS environments are neither assessed nor monitored

Lack of visibility
Enterprises lack cyber visibility in converged environment

Converged IT/OT enterprise
Controls and monitoring have been limited to IT environment with no monitoring of OT threats

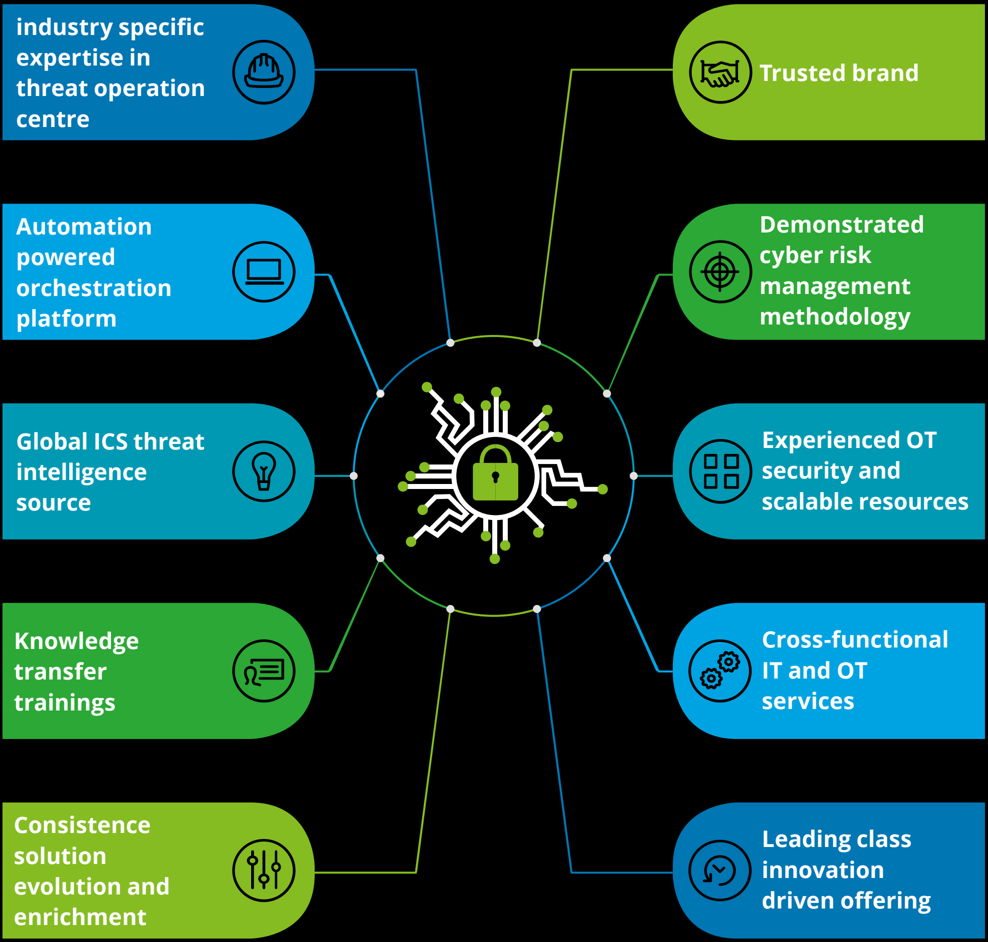
Threat sophistication
Higher level of threats from cybercrime, hacktivism, espionage

Vulnerable protocols and unpatched assets
ICS systems continues to run vulnerable protocols and also have unaccounted affected assets

Common vulnerable components

Device software	Firmware	Removable media	Physical access	Database and/or storage	Applications
Remote support/ maintenance	Device hardware	Network access/firewall	Operating system	Ports/interface	

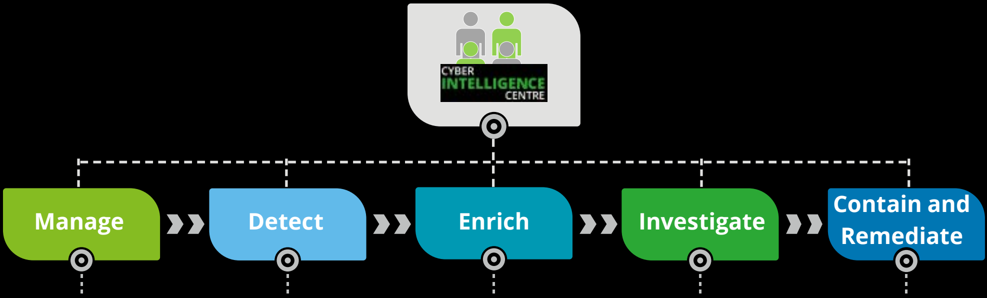
Deloitte ICS/Supervisory Control and Data Acquisition (SCADA) cyber threat management capabilities: Differentiated through proven 24x7 operations, deep ICS/SCADA threat research, and intelligence powered by CIC


industry specific expertise in threat operation centre
Trusted brand
Automation powered orchestration platform
Demonstrated cyber risk management methodology
Global ICS threat intelligence source
Experienced OT security and scalable resources
Knowledge transfer trainings
Cross-functional IT and OT services
Consistence solution evolution and enrichment
Leading class innovation driven offering

Deloitte offering for ICS/SCADA cyber threat management enables design, development, and implementation of systems to identify, monitor, record, and analyse security events and incidents of connected products across the ecosystem (IT and ICS/CS or OT), in real-time.

Our Approach to Cyber Threat Monitoring:

End-to-end accountability from detection to containment



Manage ›› Detect ›› Enrich ›› Investigate ›› Contain and Remediate

Integrated platform management and service management
Platform management of Security Information and Event Management (SIEM), vulnerability management, and threat intelligence integrated with OT monitoring solution.

Integrated service portal, Service Delivery Lead (SDL), and Technical Delivery Lead (TDL).

Proactive hunting
Proactive hunting for advanced threats that evade detection by conventional security controls.

Cyber monitoring
24x7 monitoring and response to security events across IT and OT.

Threat intelligence
Correlation with monitoring and IOC-driven inputs to threat hunting.

Vulnerability management
Enrich and correlate threat visibility with insights on open vulnerabilities.

End-to-end threat analysis, validation, containment, forensics, and incident response
CIC threat analysts will take end-to-end responsibility from initial detection of alerts to analysis, validation, and containment on the endpoint.

Deloitte enables the incident response process and provides onsite incident response support as required.

Services Description

Deloitte's OT cyber threat management services helps organisations to respond rapidly to threats, gain greater threat visibility, and use the resources in the areas of greatest impact in managing business risk. The core capabilities include network and endpoint behaviour monitoring, log management, risk analytics, workflow integration, incident response orchestration, and advanced cyber hunting.

Deloitte uses a **technology platform, which helps in managing asset inventory and ICS assessments** in order to passively identify and map networked assets in customers' ICS and surrounding networks.

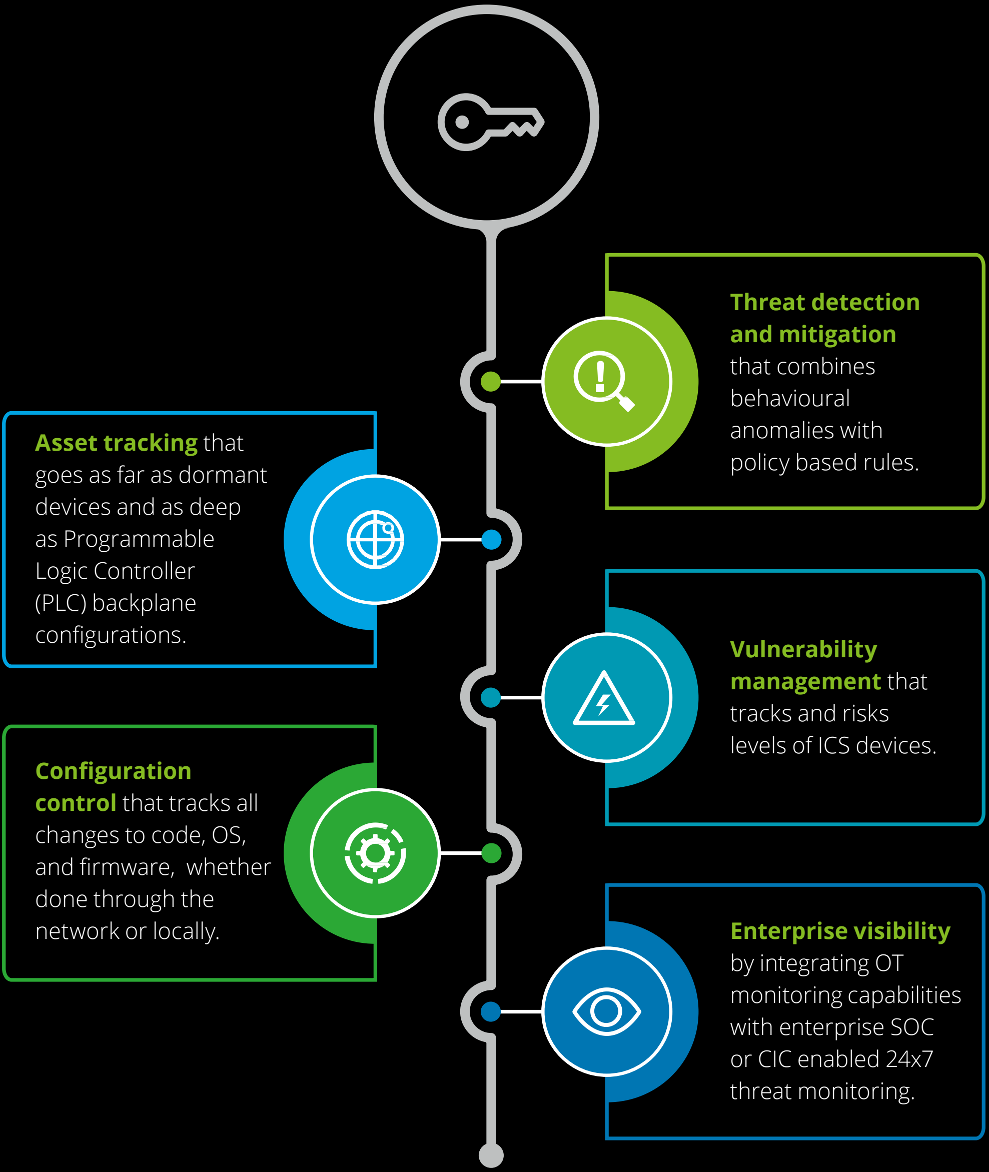
Deloitte assists with deploying the **Industrial control System platform for continuous monitoring** in the environment. Thus, it enables enhanced asset identification, threat detection, and efficiency through automation.

Deloitte Secure Operations Center (SOC) as a managed service helps with surges, requirements, and unmanned hours. The Deloitte SOC is also powered by the ICS specialised technology platform for OT environments.

Deloitte leverages the technology partner's Threat Operation Center for extended ICS knowledge, training, and intelligence to better support customers' risk evaluations and manage service needs.

The Deloitte CIC offers on-demand access to industry-specific, ICS-focused specialists and intelligence. It also offers formalised and scoped engagements or ad-hoc, remote-access advice, and support.

Key solution and benefits



Threat detection and mitigation that combines behavioural anomalies with policy based rules.

Asset tracking that goes as far as dormant devices and as deep as Programmable Logic Controller (PLC) backplane configurations.

Vulnerability management that tracks and risks levels of ICS devices.

Configuration control that tracks all changes to code, OS, and firmware, whether done through the network or locally.

Enterprise visibility by integrating OT monitoring capabilities with enterprise SOC or CIC enabled 24x7 threat monitoring.

Contacts

Rohit Mahajan
President–Risk Advisory
rmahajan@deloitte.com

Shree Parthasarathy
Partner
sparthasarathy@deloitte.com

Gaurav Shukla
Partner
shuklagaurav@deloitte.com

Anand Tiwari
Partner
anandtiwari@deloitte.com

Gautam Kapoor
Partner
gkapoor@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.