THALES
Building a future we can all trust

G-Cloud 15

OT – XDR – DESIGN & INTEGRATE

Doc Ref No: ThalesGC1507

INTRODUCTION

The Engineering-led Design, Integration & Configuration of an OT Intrusion Detection & Vulnerability Management Solution for Safety-Critical Industrial Environments.

Thales supports CNI organisations in the design, integration and configuration of an OT Intrusion Detection System (IDS) and Vulnerability Management capability; collectively referred to as Extended Detection & Response (XDR), designed specifically for operational technology and safety-critical environments.

Thales will integrate the capability in line with the customer's operational context and configure detection logic, visibility, reporting and enterprise integration, so that the platform delivers meaningful, trusted insight. Delivering a capability that is operationally aligned, assurance-ready and sustainable, without placing additional burden on internal teams.

SERVICE DESCRIPTION

Features

- OT IDS architecture design for cyber-physical environments
- Passive intrusion detection aligned to industrial protocols
- Anomaly and threat detection in OT networks
- Vulnerability exposure management integrated with asset context
- Configuration change tracking and reporting
- Automated report generation for operational and assurance use
- Centralised dashboards for mixed technical audiences
- Integration with enterprise monitoring and reporting platforms
- OT-safe deployment and validation

Benefits

- Improves visibility of OT assets, communications and operational behaviour
- Enables detection of anomalous or malicious activity without impacting live operations
- Provides contextual understanding of OT cyber risk, not only alerts
- Supports prioritisation of vulnerabilities based on operational impact
- Improves oversight of change management and configuration drift
- Reduces manual effort through repeatable, automated KPI reporting
- Supports audit, assurance and regulatory activities
- Supports enterprise-wide visibility of both OT/IT cyber risk (IT not in scope)

Use Cases

- Deploying capability in safety-critical environments
- Detecting anomalous behaviour or cyber intrusion in OT networks
- Understanding and prioritising OT vulnerabilities in operational context
- Monitoring configuration drift and unauthorised changes
- Supporting audit, assurance and regulatory reporting
- Enabling unified IT and OT cyber risk oversight

DETAILED SERVICE OVERVIEW

Operational Technology environments underpin essential public services and safety-critical operations. Integrating any new technology in such environments comes with risk and requires care, specialist expertise and an approach that recognises operational constraints, safety requirements and regulatory obligations. Poorly designed or incorrectly integrated security solutions can disrupt operations, undermine safety or fail to deliver meaningful value.

Thales' XDR service supports industrial operators with the design and integration of an OT security capability, without compromising safety, availability or operational continuity.

We bring deep experience in safety-critical and regulated OT environments - combining OT engineering discipline with cyber security expertise. We take responsibility for the solution architecture, integration, configuration, validation and handover, while removing the burden of complex design and integration from internal teams. Delivering a secure OT IDS and Vulnerability

Management capability that is enabled, validated and ready for use; with operational activity remaining under the control of the customer. This ensures OT security solutions are fit for purpose, trusted by operations teams and sustainable over time.

This service line exists to ensure that OT security solutions are:

- Designed for the operational environment they will operate in
- Integrated safely into live OT systems
- Configured so capabilities are usable, understandable and aligned to operational and assurance needs

Outcomes

- OT IDS and vulnerability management capability designed, integrated and configured to customer requirements
- Automated reporting and enterprise integration enabled
- A usable, trusted detection capability aligned to operational reality

Delivery Approach

Thales applies OT engineering discipline and cyber security expertise to ensure the capability is safely integrated and configured for the customer's environment.
Thales will:

- Design the OT IDS and vulnerability management architecture based on the customer's OT environment, network topology and risk priorities
- Define sensor placement, monitoring points and data flows to maximise detection value while minimising operational risk
- Integrate IDS capability using passive, non-intrusive techniques suitable for live OT systems
- Configure industrial protocol awareness and behavioural baselines aligned to normal operational behaviour
- Configure anomaly and intrusion detection aligned to OT operational context, reducing noise and false positives
- Configure vulnerability management to reflect asset criticality, operational constraints, and change control requirements
- Integrate IDS and vulnerability outputs with enterprise tooling such as SIEM, log management, or reporting platforms where required
- Design and configure automated reporting templates for operational, management, and assurance audiences
- Configure configuration-change visibility and reporting to support governance, audit, and investigation
- Validate detection outputs and reports with OT engineers and operations teams
- Provide structured handover and enablement

Thales enables detection and reporting capability but does not provide ongoing monitoring, alert triage or managed detection services.

THALES OT PRODUCT SUITE

A Resilience-Orientated Approach to the Through-Life Management of OT Security in Safety-Critical Industrial Environments.

The Thales UK OT Product Suite is a set of products or services that allow flexibility and adaptability to a customer's needs in moving them along their OT journey towards cyber resilience.

Figure 1 shows the OT journey to value as an organisation progresses from cyber awareness to cyber resilience maturity: with each column building upon the last.

This service forms part of the Thales UK, OT Product Suite situated within the 'DESIGN & INTEGRATE – ENACT' category (outlined in red - Figure 1). This category provides the solutions and capabilities required to safely design, integrate and sustain OT security solutions as part of a broader journey towards cyber resilience.

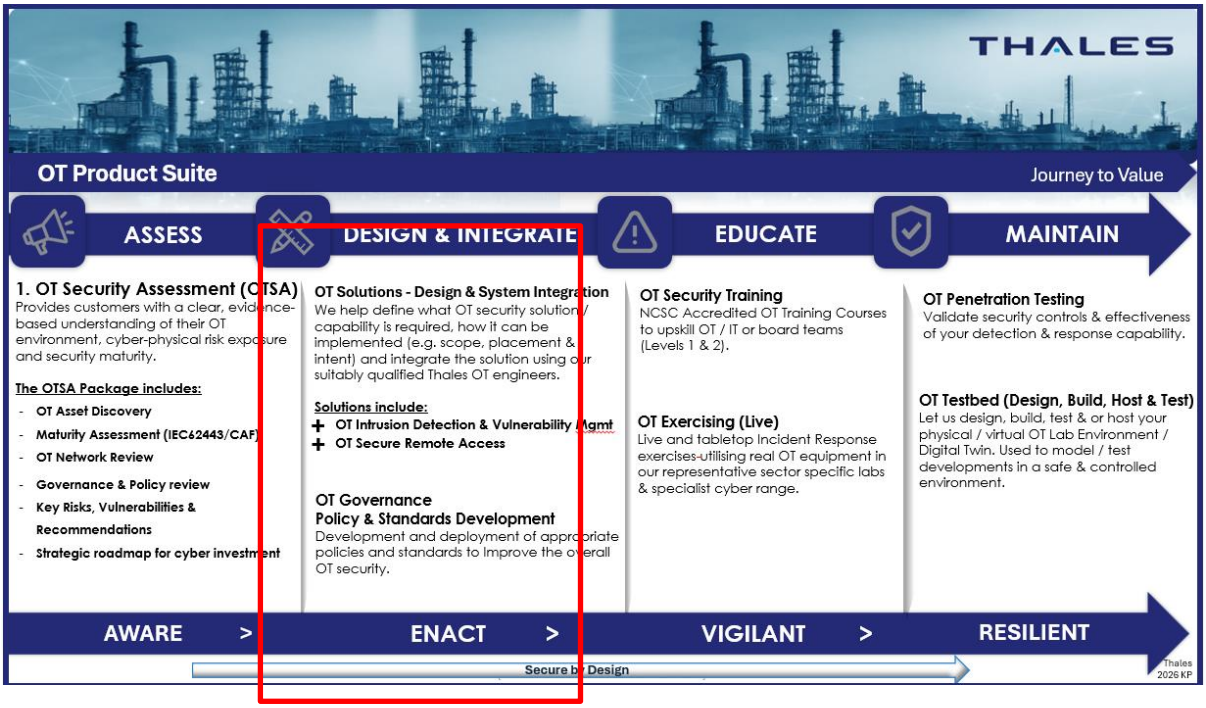

Figure 1 Thales UK OT Suite - Journey to Value with Cyber Resilience

OUR EXPERIENCE AND EXPERTISE

Thales is trusted and relied upon by its customers to ensure that their critical services & infrastructure remain operational, secure and effective; we are a company where security is at the core of all our products and services. Thales designs, builds, delivers and sustains mission-critical information systems and solutions all over the world for government agencies, industry and critical national infrastructure.

ABOUT THALES

Thales in the UK has been harnessing technology to benefit the nation for over a century. Across all walks of life, you will find us securing and protecting every moment. We develop world-leading capabilities to help our customers think smarter and act faster.

Thales collaborate with partners in both government and industry, providing cutting-edge technologies to the civil and defence markets.

Thales has a significant presence across the UK, with locations strategically positioned in England, Wales, Northern Ireland, and Scotland. This geographic reach enables us to effectively support the diverse needs of local communities while contributing to the economic prosperity of all four nations. Our key facilities, along with several customer-facing sites, extend from the South West of England to Glasgow, reinforcing our commitment to regional investment and development.

The most trusted organisations in the world rely on Thales for cybersecurity solutions that keep critical assets safe. With more than 6,000 cybersecurity experts worldwide, our portfolio protects applications, data and identities, including services that close compliance gaps, detect and monitor threats and strengthen defences.

For further information, please see https://www.thalesgroup.com/en/worldwide/united-kingdom