THALES
Building a future we can all trust

G-Cloud 15
OT Security Assessment

Doc Ref No: ThalesGC1505

INTRODUCTION

Thales' OTSA service provides the foundational insight required to make informed, defensible, cyber investment decisions that protect safety critical-systems, operational continuity and essential services

As Operational Technology (OT) & Informational Technology (IT) environments continue to converge across the UK, organisations are under increasing pressures to manage their cyber-physical risk posture.

Thales' Operational Technology Security Assessment (OTSA) is a consultant-led review of cyber-physical operations that builds a clear and evidence-based picture of OT assets, network communications, and operational and security risks, and benchmarks operations against frameworks such as IEC 62443 and NCSC CAF. Designed for cyber-physical environments including operators of essential services, Critical National Infrastructure sectors, manufacturing or regulated industrial sectors.

USE CASE

OTSA is typically used in the following scenarios:

- Establishing a baseline OT cyber security posture across a site, system or estate
- Preparing for regulatory assessment, audit or assurance activity
- Supporting NCSC CAF, IEC 62443 or sector-specific compliance obligations
- Understanding OT assets, data communications and network architecture
- Informing investment decisions
- Assessing cyber risk in safety-critical or high-availability environments
- Supporting mergers, acquisitions or operational change programmes
- Creating evidence to support security solution integrations or Secure by Design

SERVICE DESCRIPTION

Features

- Evidence-based maturity scoring and gap analysis aligned to IEC 62443 or NCSC CAF
- Passive OT asset discovery and inventory creation
- OT network architecture and segmentation assessment
- Key risks, vulnerabilities, prioritised findings and recommendations
- Review of OT-relevant governance, policies and standards
- Strategic roadmap aligned to operational, safety and regulatory needs
- Consultant-led delivery by Thales OT cyber specialists
- Non-intrusive assessment approach suitable for live operational environments

Benefits

- Establishes a clear baseline of the OT environment and risk posture
- Identifies where cyber risk matters most in relation to safety, availability and continuity
- Enables proportionate, risk-based cyber investment decisions
- Supports regulatory, audit and assurance activities with evidence-based outputs
- Reduces uncertainty caused by incomplete OT asset visibility
- Aligns cyber security activity with operational and engineering realities
- Improves collaboration between cyber, engineering, safety and operations teams
- Minimises operational disruption through passive assessment methods
- Creates a defensible foundation for future design, integration and assurance activities

DETAILED SERVICE OVERVIEW

Operational Technology environments underpin essential public services and safety-critical operations. Understanding cyber risk in these environments requires specialist OT expertise and an approach that recognises operational constraints, safety requirements and regulatory obligations.

Thales' OTSA delivers insights that provides predictive and business value beyond what traditional architecture-based risk and compliance assessments typically offer. Through this service, we document normal system and network behaviour within the scope environment, capturing operational context such as asset exposure, control activity, access by users, process states etc.

This establishes a baseline that can be used to detect anomalies, inform future risk assessment, and prioritise mitigation efforts.

OTSA enables buyers to proceed with confidence, knowing that subsequent security, design or integration activity is informed by a clear understanding of their operational context.

Scope

- OT maturity assessment against recognised frameworks (IEC62443 / NCSC CAF)
- OT asset discovery and inventory
- OT network and architecture assessment
- Key risks, vulnerability assessment
- Governance and policy review
- Strategic roadmap for cyber investment

Outcomes

- Baseline view of the OT environment and security posture
- Clear understanding of cyber risk in operational context
- Prioritised and actionable recommendations
- Evidence to support regulatory, audit and assurance discussions

Delivery Approach

- Consultant-led engagement delivered on-site
- Passive, non-intrusive assessment techniques by default
- Structured engagement covering preparation, assessment, analysis and reporting
- Stakeholder engagement across cyber, engineering, safety and operations teams

The OTSA typically follows a four-stage approach

- **Phase 1 – Engagement & Collaboration**

  In this phase we work with our customers to position the project for success. The aim of this phase is to understand and agree project objectives, customer engagement model, expectations, and risks.

- **Phase 2 – Preparation & Planning**

  The preparation phase ensures that our engagement is productive and effective to ensure the quality of the engagement. Thales will work with the nominated point(s) of contact and undertake an information gathering process to understand the customers' requirements. A Method Statement and Risk Assessment Method Statements (RAMS) form will be shared with the site points-of-contact so that both the customer and Thales have an agreement on the engagement expectations and timetables.

- **Phase 3 – Assess & Gather Evidence**

  OT Consultants will arrive at site to conduct an information gathering exercise. Figure 1 represents the activities that typically occur over the course of three days, though the order of individual activities may be varied by Thales on discussion with site personnel for reasons of efficiency and accommodation of onsite operations.

Figure 1 On-site methodology

- **Phase 4 – Evaluate, Report, Deliver**

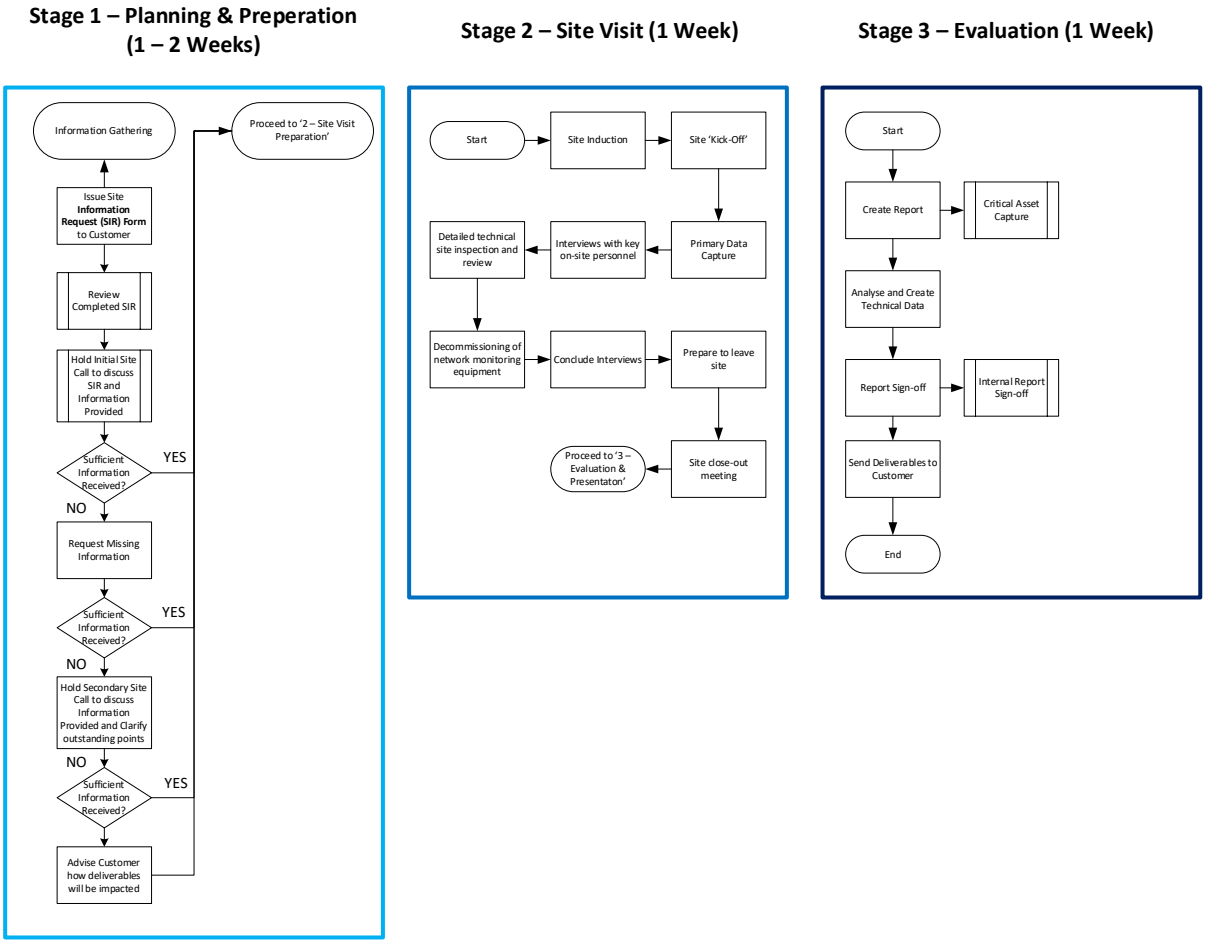
  The Thales consultants will evaluate and assess the data collected which will be used to inform the customer deliverables.

  As per our NCSC Certified Service, each deliverable will go through a peer-review and a formal approval process conducted by Head of discipline. Once complete the output will be delivered to the customer via our secure portal for review and sign off.

Typical Duration

The figure below shows the sequence of tasks involved in performing an OTSA, as well as the associated durations.

The onsite assessment itself is typically delivered over a three-day site visit.



Security & Assurance

- No intrusive or active scanning unless explicitly agreed
- Secure handling of customer data throughout the engagement
- Anonymised reporting where appropriate
- Outputs suitable for executive, technical and assurance audiences

Assumptions & Constraints

- Access to relevant OT stakeholders and documentation
- Network visibility via SPAN, RSPAN or TAPs provided by the customer
- Final scope and duration agreed prior to delivery

THALES OT PRODUCT SUITE

The Thales OT Product Suite is a resilience-orientated approach to the through-life management of security & resilience in safety-critical complex OT 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 2 shows the OT journey to value as an organisation progresses from cyber awareness to cyber resilience maturity: with each column building upon the last.

OTSA forms part of the Thales UK, OT Product Suite situated within the 'ASSESS - Establish Context' category (outlined in red - Figure 2). This category provides the foundational understanding required to safely design, integrate and sustain OT security capability as part of a broader journey towards cyber resilience.

Figure 2 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