Cybels OT Security Case Study
THE REQUIREMENT
A large global manufacturer wanted to obtain a snapshot of their operational technology (OT) cyber security posture at one of their factories. The facility manufactures electronic equipment and power supplies which are supplied to aerospace, defence and other industrial sectors. In order to inform them in creating an appropriate OT cyber security strategy and solution, they asked Thales to provide them with:
• A detailed inventory of their OT assets and their connectivity
• An understanding of their current vulnerabilities and threats
• Options and recommendations for next steps to improve the maturity of their OT cyber security posture

WHY THALES?
Thales is the European leader in cyber security and the worldwide leader in data protection. It is a trusted provider of cyber security services and solutions to the UK Ministry of Defence and the UK Government, and is accredited as a Certified Cyber Security Consultancy by the National Cyber Security Council (NCSC).

With inside knowledge coming from more than 40 years of designing and maintaining OT systems, Thales has a proven track record in successfully delivering OT Transformation Programmes for diverse clients, from Fast Moving Consumer Goods (FMCG) organisations with a global footprint through to smaller organisations with fewer sites. Its vendor agnostic approach ensures OT security assessments provide the best possible coverage, quality and deliverables and are independent of the IT or OT vendor installed. Thales assessments include interviews with staff, factory walk rounds and the use of passive, and soft inspection techniques, taking advantage of the principles of the internet to discover the external boundary whilst ensuring that ongoing customer operations are not disrupted.

USE CASE:
OT security assessment for large manufacturer to reduce the risk of a cyber-attack causing lost production and financial loss.

THE SOLUTION
Thales’ approach in this instance was typical of other assessments of OT Security it has carried out, and consisted of four stages designed to build a holistic picture of the business, where potential vulnerabilities existed, and with recommended mitigating actions and procedural improvements to OT Security.

Stage 1 – OT Asset and Data Flow Discovery
A passive network monitoring tool captured and reported OT assets, network flows and cyber security vulnerabilities in several network segments. This was augmented with information on network architectures/floor plans and other metrics collected from interviews and factory walk rounds. Meanwhile, stakeholder engagements enabled an assessment of the businesses approach to risk management/business critical operations. The final analysis included a review of the OT network architecture, an assessment of the configuration of factory end points, and an assessment of the configuration of the OT network segmentation/security controls.

World leading facilities include an extensive OT Lab and Cyber Range environment at the National Digital Exploitation Centre, located in Ebbw Vale, South Wales. Here, representative systems can be built to safely test any remediation and provide confidence that recommendations are compatible with the deployment in question, minimising the risk to ongoing operations.

USE CASE:
OT security assessment for large manufacturer to reduce the risk of a cyber-attack causing lost production and financial loss.
Stage 2 - Data Examination and Gap Analysis
This stage combined the assessment results from Stage 1, enabling Thales to identify where a gap in governance maturity could lead to technical vulnerabilities that could directly cause harm to the organisation. The data sources were also used to understand how the OT environment communicated with the corporate IT and external networks. In addition, vulnerabilities and/or risks associated with each OT asset were identified to determine the potential impact on the business should vulnerabilities or weaknesses be exploited.

Stage 3 - Mapping Logical and Physical Networks
Assets were arranged into logical and geographical topologies to map out a graphical representation of assets and data flows, with assets identified on the customer’s factory CAD/floor-plan for the latter. This provided the factory engineers with a geographical topology to enable them to quickly find each of the assets for asset tagging and remedial activities. Where possible, assets were identified with their host names, IP addresses, MAC address, roles, and with any notable traffic communications highlighted.

Stage 4 - OT Security Assessment
The OT Security Assessment is similar to a roadworthiness test for a vehicle. It summarised the vulnerabilities discovered during testing, and reported those that required immediate attention. The level of maturity of the OT cyber security processes in place were assessed, by comparing with industry best practice. The final report covered a list of prioritised risks to be addressed and recommended mitigating actions, highlighting quick wins. It also included a set of objectives and recommendations to drive an OT Security programme, incorporating a gap analysis against industry standards.

OUTCOMES
The assessment identified numerous vulnerabilities including, 47 unique issues, 40 security threats, 1 of which was a critical attack vulnerability, and 7 networking problems. This level of issues and vulnerabilities identified is not un-typical in Thales’ experience.

Examples of the vulnerabilities identified included:
- No network segregation between OT and IT equipment
- Single-points of failure with interlinked dependencies. An attacker able to compromise the OT perimeter could cause significant damage to factory operations
- A VLAN configuration giving unfettered access to the factory/IT networks meaning a compromise of any device within their IP address range would enable a jump to be made between IT and OT engineering machines
- A lack of comprehensive backup and configuration management meaning an infection by crypto-malware would be difficult to recover from quickly, impacting factory operations
- Staff credentials could easily be obtained

Many good security aspects were observed such as multiple layers of physical access control that would make it more difficult for an adversary to physically interact with OT assets unnoticed, and well informed IT/OT engineers who were technically very capable at building and restoring functionality. However, risks were not comprehensively identified, evaluated or managed, and there was no systemic ability to detect, respond or recover from a cyber-attack and no resiliency from an insider attack or accidental compromise. These and other factors meant that overall, the site OT cyber security maturity was assessed as being “partial” (Tier 1) within the NIST Cyber Security Framework maturity model.

The company is now implementing the report recommendations in order to raise its maturity to operate at the NIST Tier 2 – “Risk Informed” level and to the Tier 3 – “Repeatable” level for business critical functions. Immediate vulnerabilities have been remediated, and a plan is in place to address others, considerably reducing the risk of a cyber-attack on OT assets and the consequent significant financial impact that would result from lost production.