OT Asset Discovery and Audit

MARKET CHALLENGES AND OPPORTUNITIES

Operational Technology (OT) and the Industrial Control Systems (ICS) that, literally, help to keep the power on and the food on our table, are becoming increasingly prone to cyber attack. As enterprises continue to seek greater operational efficiencies and effectiveness, they are introducing internet connections to elements of their existing OT networks. This delivers centralised visibility and control, increases breadth and use of real-time data and remote repairs performed by software updates to on-site systems.

Interconnectivity makes for an extremely vulnerable world, especially with respect to OT. As a result, industrial organisations are increasingly turning their attention and resources to securing this domain. Today’s cyber threats come from multiple sources:
- IT hackers
- Employees enabling unauthorised access. This latter source can either be intentional, through sabotage, or unintentional, through phishing or other social engineering
- Well-coordinated and well-funded groups, determined to cause harm to people or property. This may be for financial, criminal or political/economic reasons.

Examples of such attacks have the potential to pose serious danger to an entire community. In 2016, for example, an attack on a water treatment plant in the Asia-Pacific region enabled the infiltrators to access, not only the records of around 2.5 million consumers but, also, the system controlling the chemicals used to treat the water. Fortunately the attack was discovered and thwarted before any damage could be done.

The developers of the tools and techniques, used to attack industrial systems, are becoming increasingly sophisticated. These tools are also widely available and are easily modified, recorded and targeted towards an increasing number of industrial automation systems.

Because much OT equipment dates from the 1980s and 1990s, it was developed at a time when there was little notion that it would, one day, become central to a much-connected society. Therefore it came with no built-in modern-day digital security.

Without careful planning and effective monitoring, exposing thousands of physically distributed OT facilities to Information Technology (IT) networks is creating serious security challenges for most enterprises.

In recognition of this, there is an increasingly formal regulatory structure being introduced as well as legislation for reporting breaches and a highly vocal press and public ready to react when things go wrong.

With these added complexities, we recognise your priorities are safety, reliability and output.

THALES OFFER/PROPOSAL

Thales OT Asset Discovery uses highly skilled Cyber Security operatives with specialist domain knowledge of OT environments, spanning Nuclear Energy to Consumer Goods to Pharmaceutical environments. We will use industry-leading technologies, whilst remaining entirely vendor-neutral, to understand your environments, conduct logical and physical site surveys, providing an in-depth audit of the entire OT environment and networks. With advanced tools and methods at our disposal we highlight strengths and weaknesses and propose measures to increase and maintain your security posture.

Thales has developed a four-stage process from OT Asset Discovery through to fully managed OT SOC offerings to help contextualise, protect and develop your OT Estate. This can lead to compliance with IEC-62264 and 62443 compliance and legal requirements such as The NIS Directive (see EU 2016/1148).

OUR CREDENTIALS

Thales has long operated in the OT and Industrial arena. We are ourselves a manufacturer. Recent projects cover the following areas:
- OT Asset Discovery for Unilever globally
- Dubai Metro Cybersecurity Architecture
- Yorkshire Water
- EDF

WHY THALES?

Trusted by the military, governments and providers of critical national infrastructure around the world, Thales has the people, processes and technology to reduce risk, improve security and protect your industrial assets. As you would expect from Thales, the precise service that we provide to each of our clients is tailored to specific needs and always held in strictest confidence. Our cyber security experts and will deliver to you:
- A comprehensive OT Asset Discovery process with network topologies and contextual recommendations report per factory.
- Access to an extended team of specialists with expertise in relevant fields
- The facts you need to make informed decisions
- A comprehensive, tailored and impartial solution
- A full suite of OT-targeted capabilities, from Asset Discovery to fully outsourced OT SOC.

Value Proposition

Thales’s OT Asset Discovery and Audit provides a global and consistent identification service for your Industrial Operating Technologies complimented with a range of services to secure, protect as well as empower digital transformation projects and ensure regulatory compliance.