OT Security

What is it?

Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in an enterprise, according to Gartner. OT is common in Industrial Control Systems (ICS) such as SCADA Systems, DCS, HMIs, PLCs/RTUS etc. and in the world of critical infrastructure, OT may be used to control power stations or public transportation. As this technology advances and converges with networked technology, the need for OT security grows exponentially.

Who is it directed at?

We are seeing more industrial systems brought online to deliver big data and smart analytics as well as adopt new capabilities and efficiencies through technological integrations and adaptation to the Industry 4.0 era. IT-OT convergence gives organizations a single pane of glass of industrial systems together with process management solutions that ensure accurate information is delivered to people, machines, switches, sensors and field devices at the right time and in the best format. When IT and OT systems work in harmony together, new efficiencies are discovered, systems can be remotely monitored and managed and organizations can realize the same security benefits that are used on administrative IT systems.

Why is it important?

As industrial systems become more connected, they also become more exposed to vulnerabilities. The high cost of industrial equipment and the devastation to communities and economies that an attack could generate are key factors for organizations looking to protect their industrial networks. Add legacy equipment, safety regulations that may prohibit any modifications being made to equipment and compliance regulations that require sensitive data to be made available to third parties, and things become a little challenging. It is possible to secure industrial networks without disrupting operations or risking non-compliance. By using solutions that allow complete visibility of network control traffic and establishing the right security policies, you can put an effective OT threat model in place that will protect processes, people and profit and significantly reduce security vulnerabilities and incidents.

Where is it taking place?

Operational Technology is widely used in refineries, power plants, power transmission/distribution, Manufacturing, food & beverage etc. and as such has become a common, crucial element of critical infrastructure systems. Depending on the country there are increasing legal obligations for Critical Infrastructure operators with regards to the implementation of OT systems. It is also utilized in many sectors and environments, such as oil and gas, power and utilities, waste management, transportation. Scientific experimentation, critical manufacturing etc.

When is it going to make an impact?

From the very beginning security of Operational Technology has relied almost entirely on the standalone nature of OT installations. Recently OT systems have become linked to IT systems with the corporate goal of widening an organization's ability to monitor and adjust its OT systems, which has introduced massive challenges in securing them. Approaches known from regular IT are usually replaced or redesigned to align with the OT environment. OT has different priorities and a different infrastructure to protect when compared with IT; typically IT systems are designed around 'Confidentiality, Integrity, Availability' (i.e. keep information safe and correct before allowing a user to access it) whereas OT systems require 'Availability, Integrity, Confidentiality' to operate effectively (i.e. present the user with information wherever possible and worry about correctness or confidentiality after). In the fast changing industrial environment OT security has already made a major business impact and is expected to grow exponentially the coming years as the IT/OT convergences advances.

How will it affect your business?

With industrial systems becoming more connected, they are also being exposed to more vulnerabilities. The transition from closed to open systems and cloud applications also known as the IT-OT convergence, generates new security risks that need to be addressed. Key factors for organizations looking to protect their industrial networks are the high cost of industrial equipment and the devastation to communities and economies that an attack could generate. A strong negative impact of breaches or incidents that occur could even mean casualties in a worst-case scenario. Harmonizing the way IT and OT systems work together, increases efficiency and availability. Industrial systems can be remotely monitored and managed. The security benefits for organizations are the same as those used on administrative IT systems.