tenable.ot™

USE CASE

# SECURING TRANSPORTATION INFRASTRUCTURE

## TOP TRENDS

- Increased use of automation to seamlessly connect logistics, scheduling, route and volume planning
- Heavy adoption of IoT technology to support GPS tracking of vessels, containers, vehicles and goods
- Adoption of "elastic" logistics and just-in-time manufacturing
- More frictionless travel without compromising security for improved customer satisfaction

## KEY CHALLENGES

- Interconnection of IT/OT relies on orchestration of complex systems that may contain cyber vulnerabilities, which you cannot take down to patch at a moment's notice
- Transportation systems are highly connected and interdependent and can experience security threats introduced by trusted entities
- Assets are in motion and highly distributed. As a result, they are more easily susceptible to cyber exposure and attack

## BACKGROUND

Transportation contains of a wide variety of subcategories, including transportation of people in cars, via rail, air and maritime; the shipping of goods by land, sea and air; and other shipping methods such as roadways, pipelines and other conveyances. OT technology plays a major role in ensuring the reliability of these complex systems and economies heavily rely on them to support society as we know it. Even a momentary interruption or failure that a security incident causes can have dire and cascading negative consequences.

Modern transportation infrastructures are increasingly more complex as different systems must interact with each other to coordinate activities and operations. Your infrastructure must be intelligent to support real-time tracking and coordination of many diverse assets. To support real-time operations, along with the multitude of changes that can happen at a moment's notice, your systems must interconnect with each other and the internet. As a result, visibility, security and control of your OT infrastructure are essential to ensuring reliable and efficient operations.

OT examples in transportation:

- At airports, OT operations are involved in screening baggage, coordinating refueling requirements, arranging maintenance and aircraft servicing, re-provisioning planes, etc.
- In maritime shipping, OT operations are involved in scheduling shipping schedules, loading ships and real-time tracking of vessels and individual containers.
- In roadways and railways, OT systems can manage traffic signaling, conditions, routing, maintenance and much more.

Your interconnected network, while creating great efficiencies, also yields a much wider attack surface with the capacity to easily proliferate from one area of your OT infrastructure to the next. Therefore, industrial cyber threats are now core risks to the availability, safety and reliability of transportation OT infrastructures.

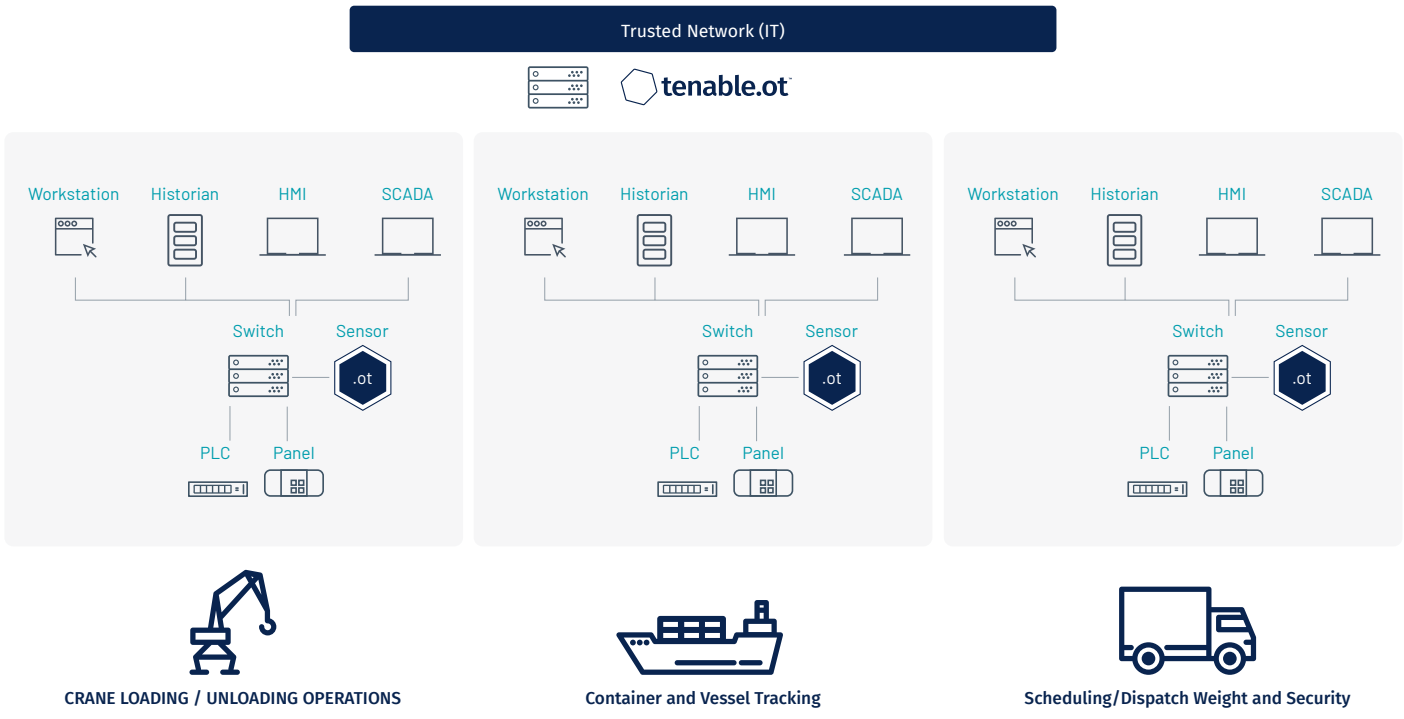
# ANATOMY OF A CYBER ATTACK IN TRANSPORTATION

1. Initiate infiltration to a transportation network.
2. Establish a beachhead in one of the assets in the network.
3. Initiate reconnaissance activity to map out targets, vulnerable devices and weak points.
4. Propagate to other assets to reach areas of interest.
5. Launch the attack, thus crippling normal flow of people, products and commodities, with reverberating effects to other industries dependent on transportation infrastructure.

### Recent Events

- **2020 –** Attackers targeted Shahid Rajaee port terminal in Iran, which shut down all port operations and had major impacts on loading/unloading of ships. It also had further reverberations deep into the supply chain.
- **2018 –** Subaru issued a car replacement notice for the new Ascent model. The company had to replace vehicles rather than recall them because of a missed critical spot weld. Later analysis revealed the cause was due to "improper software programming for the welding robots."
- **2017 –** NotPetya malware caused an estimated $10 billion in damage, severely disrupting transportation firms such as Maersk and TNT. In some cases, terminals and distribution centers ceased operations because of inoperable computers.

# LOGICAL SAMPLE DEPLOYMENT: MARITIME SHIPPING



# VISIBILITY ACROSS SYSTEMS

In transportation environments, there are many systems that must work in perfect synchronization with each other for successful operations. For example, in an airport, a plane that just landed often has less than a 90-minute turnaround. To ensure a safe and on-time departure, teams and systems must work together to successfully assign a gate and execute unloading, re-provisioning, maintenance, fuel, flight routes, weather, aircraft weight, and physical security protocols and other critical operations.

The systems that make all of this happen rely on a converged IT/OT infrastructure. As such, complete 360-degree visibility across the entire infrastructure will ensure there are no security blind spots that can potentially disrupt or disable operations. Visibility must be at the network level to identify questionable or anomalous traffic, and at the device level to find infected devices that may or may not communicate on the network. Further, since attacks can form in one area and quickly proliferate to another, visibility should include both IT and OT devices.

# IDENTIFY THREATS FASTER

Unlike traditional IT networks or manufacturing plants that are usually in one large complex, transportation, by nature, is physically distributed across a large area and almost always in motion. For example, shipping companies operate megaships that can contain thousands of shipping containers. A large shipping company must account, in real-time, for its fleet, which may be operating around the globe, as well as each of the thousands of containers and contents in each ship. This requires a robust OT network.

Asset tracking will keep OT inventory updated and alerts can warn of unauthorized activities or unaccounted changes. Real-time alerting of all activities is particularly important, both while ships are underway or in port. As a result, your OT security solution must periodically query individual devices that maintain OT operations at all locations to ensure deep situational awareness and identify changes. Your OT solution should query all PLCs, HMIs, servers, workstations, networking equipment, gateways and other operational devices for shipping.

Tenable.ot leverages patented active-querying technologies and is also the first to specifically build active-querying engines for transportation environments. The technology employs active querying for both documented and undocumented protocols to achieve maximum situational awareness and provides coverage for all devices in a distributed OT environment.

# SECURE THE DISTRIBUTED ECOSYSTEM

To identify events at any stage of an attack, you need multiple detection engines. They should include:

**a)** Attack vectors that can proactively identify weak points before threat actors launch an attack. General traffic mapping and traffic visualization, identification of risky protocols, open ports, and vulnerabilities to eliminate risk factors across your infrastructure.

**b)** DPI engines for both documented and proprietary protocols to identify activities that break established rules and identify reconnaissance events. This typically relies on policies that can protect against known attacks.

**c)** Anomaly detection to identify zero day or targeted attacks that do not have a signature yet identified. This should be used to pinpoint traffic patterns and behaviors outside of regular daily operations.

**d)** Signature-based detection involves a database such as Suricata. It is open-source and valuable because the greater security community can add new signatures, thus benefitting the larger OT security community. Leveraged it to identify known threats attackers use to establish beachheads or propagate through your transportation infrastructure.

# MAINTAIN THE PAPERTRAIL

OT environments often contain a mix of older devices typically not found in IT environments. With various patch levels across each device type, it is difficult to maintain an up to-date patch management program. Because you cannot take down transportation environments for regular maintenance windows, you can operate with known vulnerabilities for an extended time period. Nevertheless, once you schedule a maintenance window, if you perform manual patching, there is potential for misses and mistakes, not to mention dedication of massive amounts of time and effort, which perhaps won't even address your most critical vulnerabilities first.

It's critical to maintain deep awareness of the state and characteristics of all of your devices. This includes accurate matching between specific device condition and the available vulnerability knowledge base that has associated exploits. Because of the dynamic nature of transportation environments, your OT solution should update this body of knowledge regularly and keep it in sync with newly discovered vulnerabilities. A Vulnerability Priority Rating (VPR), for example, can provide a triaged list of vulnerabilities you should deal with from most serious to least, based on a variety of factors such as CVSS score, asset criticality, position in your environment and much more. This delivers an automated, fully vetted, and prioritized list of vulnerabilities you should address to reduce the cyber exposure specific and relevant to your environment.

# SUMMARY

OT cybersecurity is now widely recognized as a core ingredient to ensuring a reliable, efficient and safe transportation environment. To mitigate that risk, you need full visibility, security and control into all of your operational assets.

Tenable.ot provides complete visibility across both IT and OT assets. Asset inventory identifies each and every asset in your environment along with deep situational analysis down to the firmware and backplane level. Threat hunting involves proactive attack vectors that identify weak points before threat actors launch an attack. A hybrid detection engine identifies both known and unknown threats when they happen. Vulnerability management prioritizes vulnerabilities with known exploits that are relevant to your specific environment. Configuration control identifies and provides snapshots of any changes made to your OT infrastructure for auditing and rollback purposes, if and when and necessary. Tenable.ot's flexible deployment options and integration with leading IT security vendors will ensure transportation infrastructures operate safely and with reduced risk.

# ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.