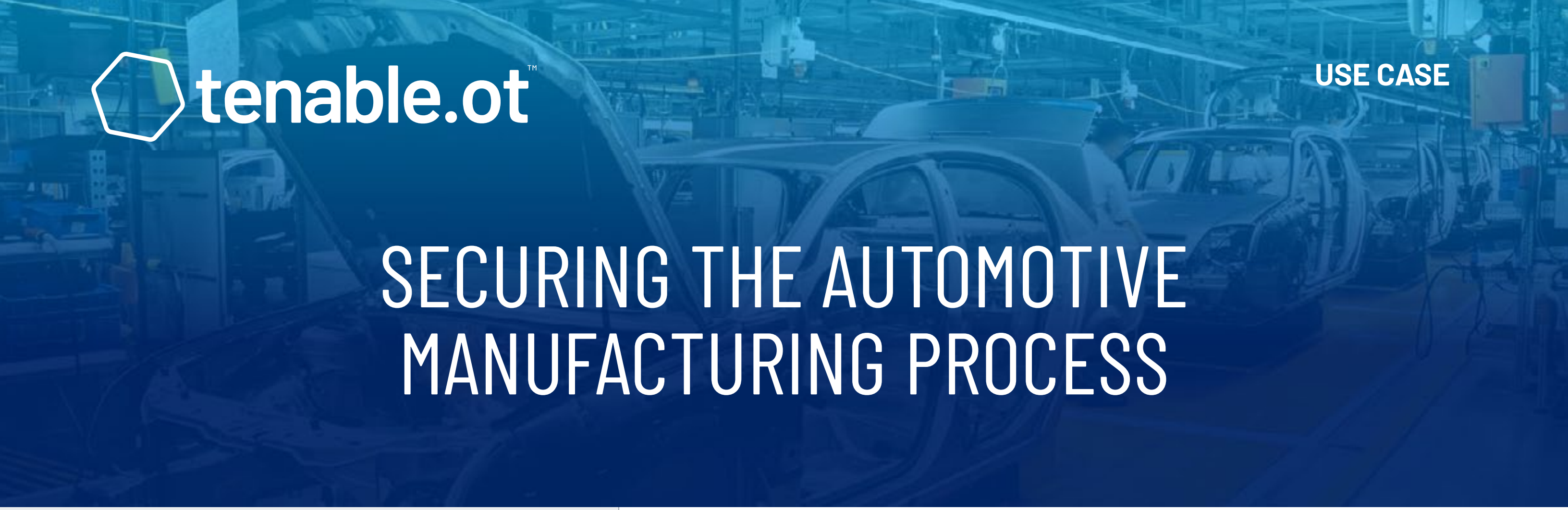


tenable.ot™

USE CASE

SECURING THE AUTOMOTIVE MANUFACTURING PROCESS

TOP TRENDS

- Auto manufacturing is a top target accounting for 30% of all industrial cyber-attacks[1].
- Cars contain more technology than ever before with 50 microprocessors in the average vehicle[2].
- Connected cars are rapidly being adopted with a TAM of $59.70 billion in 2021 and it is estimated to grow up to $255 billion by 2026[3].
- In order to comply with performance and emission standards, vehicles are engineered to closer tolerances than ever before.
- Most car components and parts are being made using digital technology.
- Sourcing all the components and ensuring compliance with manufacturing specs requires precision with the supply chain as well as the transportation and logistics in getting them on site exactly when they are needed.

BACKGROUND

The automotive manufacturing industry heavily depends on automation and operational technology (OT) to ensure high efficiency and minimal down time. It also strives to meet the highest engineering and safety standards. While that balance creates a challenge, when you add in cybersecurity threats that can shut down productivity and potentially endanger lives, it's downright daunting.

Some of the largest global automakers with tens or hundreds of manufacturing facilities across the US, Europe, Asia and Africa rely on a secure supply chain and equally secure manufacturing and fabrication process to produce thousands of cars daily. In fact, automobiles are manufactured with more technology than ever before and are built to exacting standards. Once these cars are on-the-road, even the slightest deviation in the manufacturing process can cause catastrophic failures and massive recalls.

Production slow-down or shut-down due to an unauthorized intrusion or security incident can produce massive losses before the cars roll off the assembly line. Cost estimates for auto production downtime can be as high as $22,000 per minute[4]. Unplanned downtime levels were highest in the automotive sector, where plants lost 29 production hours a month, on average, at the cost of $1.3 million per hour. Given these facts, security in the supply chain, auto manufacturing and subsequent auto use by the consumer is paramount. That's why securing industrial operations is essential.

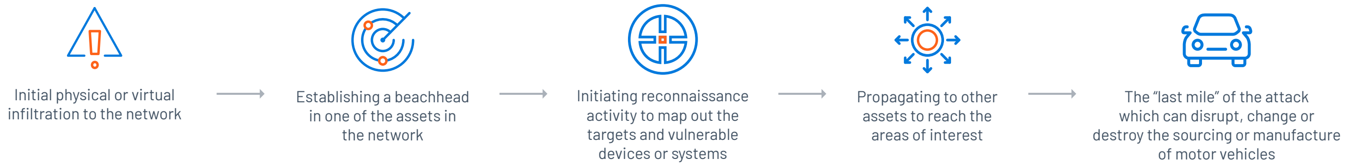
[1] EY Consulting - Operational Technology Cybersecurity

[2] HowStuffWorks.com - How Car Computers Work

[3] marketdataforecast.com

[4] Business Insider - What 1 Minute of Unplanned Downtime Costs Major Industries

ANATOMY OF A CYBER ATTACK IN AUTOMOTIVE



Initial physical or virtual infiltration to the network →

Establishing a beachhead in one of the assets in the network →

Initiating reconnaissance activity to map out the targets and vulnerable devices or systems →

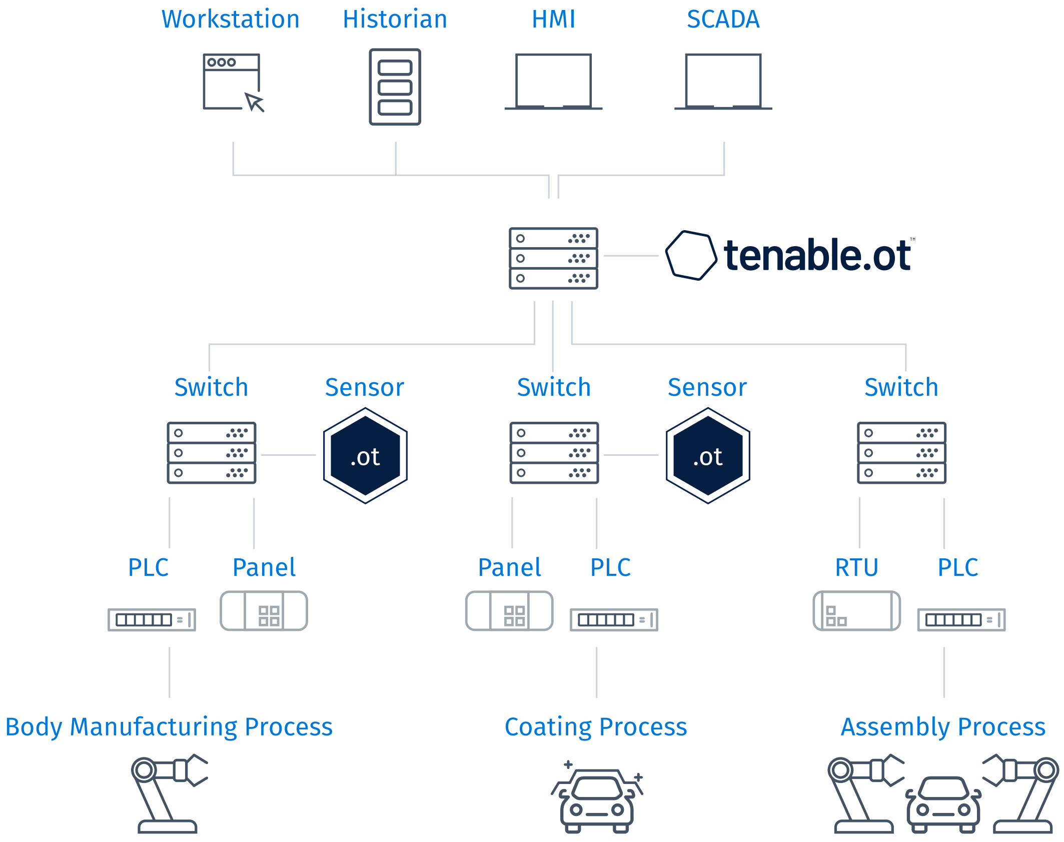
Propagating to other assets to reach the areas of interest →

The "last mile" of the attack which can disrupt, change or destroy the sourcing or manufacture of motor vehicles

KEY CHALLENGES

- Auto manufacturing requires constant uptime. One minute of downtime equates to $22,000 in losses.
- With an average of 50 microprocessors in a typical vehicle and up by 200% from only five years ago, auto manufacturers must ensure that they are hardened against potential attacks.
- Connected cars are always connected and thus are always vulnerable to attacks both during the manufacturing process and while in use by the end customer.
- Due to the enacting tolerance thresholds in which cars are manufactured, even a small deviation from specs can lead to catastrophic failures.
- Many vehicle components such as airbags are digitally manufactured by an outside third party and require the same level of security in that process as in the manufacture of the actual automobile.
- Auto manufacturing demands the full correlation and of the supply chain thus requiring the secure sourcing, manufacturing and delivery of components from a transportation and logistics perspective.

STANDARD AUTOMOTIVE INDUSTRIAL CYBERSECURITY DEPLOYMENT



COMMON VULNERABILITIES

- Auto manufacturing requires sourced sub-components from different manufacturers; this extends their vulnerability beyond their own plant to the plants of every one of their supply chain partners.
- Assembly facilities are turned over every year to accommodate the manufacture of the new model year, exposing them to new security threats in the manufacturing process.
- This increasing reliance of computers and microprocessors in cars that support the new technology in the car increases the attack surface and vector potential in each vehicle.

Recent Events

- **June 2020:** Honda had to stop production in a number of its plants due to a ransomware attack that targeted its networks in Europe and Japan[5].
- **July 2019:** Subaru announced a recall on their Outback and Legacy line due to poor or missing spot welds which compromised the body frame strength on the effected vehicles[6].
- **June 2018:** Tesla employee takes vengeance by changing manufacturing source code and exfiltrating sensitive data to outsiders[7].

[5] https://www.sme.org/technologies/articles/2021/august/automotive-cybersecurity-vital-for-vehicles-and-factories/

[6] Cars.com - 2019 Subaru Legacy, Outback: Recall Alert, July 12, 2019

[7] CNBC - Elon Musk emails employees about 'extensive and damaging sabotage' by employee, July 19, 2018

SEE MORE, SECURE MORE

While auto assembly lines were once isolated, today they are connected to IT and anywhere access. This has created an environment that can impact the integrity of the entire manufacturing process. The elimination of "air-gapping" enables bad actors to penetrate parts manufacturing or the assembly environment from either the IT or the OT side. To identify a variety of suspicious behaviors it is essential to leverage several detection engines.

1. Device mapping and traffic visualization will identify and alert on risky communications and behaviors that may pose a security concern.
2. Anomaly detection to pinpoint traffic patterns that are outside of the regular network operation.
3. Signature based detection to identify known threats which are used by attackers for known attacks.

Commonly Used Protocols

- Modbus
- Ethernet/IP
- ControlNet
- DeviceNet
- DF-1
- Sinec H1
- CIP
- AS-i
- FINS

CLOSE VULNERABILITIES FASTER

Due to the cost of downtime in auto-manufacturing and the need to adhere to a strict production schedule, it's difficult to stop operations to perform routine maintenance or even apply patches when a vulnerability is discovered. Furthermore, in distributed manufacturing facilities, it is difficult to maintain an up-to-date inventory capable of zeroing in on specific devices to perform the servicing needed to keep operations running smoothly and securely. The result is that vulnerability windows can remain open indefinitely and be susceptible to both known and unknown threats. To ensure the security of the OT network, organizations must employ a system that can perform regular inventory checks that provide situational awareness into each and every asset in the converged infrastructure. Doing so will pinpoint the devices that require maintenance, and allow for specific operations procedures until the plant can be idled to perform the required maintenance.

SECURE THE DISTRIBUTED ECOSYSTEM

Auto manufacturing requires a vast supply chain that may be comprised of hundreds of third-party component suppliers and even multiple departments within the actual manufacturing facility. This necessitates synchronized operations among all of them as well as access to credentials by a wide, heterogeneous audience. Individuals may include authorized employees, partners, agents and subcontractors.

Access requirements may extend beyond the actual auto assembly plant to offsite and remote facilities across the globe. These remote locations must also retain the same level of security as the main campus. Consequently, it is essential to maintain access and configuration control that spans from the main facility to all locations. To accomplish this, the OT security solution must periodically query individual devices at all locations and identify if any changes have been performed. It is important to query servers, workstations, networking equipment, gateways, and any other devices that are critical to the regular network operation. Deep knowledge, including visibility to all types of devices, patch levels, firmware versions and backplane information is essential. It is also critical to account for dormant devices that are not communicating regularly over the network. This should be uniformly applied to all location whether at headquarters, regional or remote locations since an attack can strike at any part of the facility and quickly propagate to all facilities.

MAINTAIN THE PAPERTRAIL

To help comply with IATF and ISO standards, it is necessary to proactively maintain a proper paper trail capable of demonstrating compliance with regulatory standards. To achieve both proper security and compliance standards, you need deep awareness of the state and characteristics of every device. You also need accurate matching between the specific condition of the devices and the available knowledge base on vulnerabilities to eliminate false positives.

Because of the constantly changing threat conditions, this information should be updated regularly and kept in sync with newly discovered vulnerabilities. If a deviation is detected, it must be captured in real-time, as well as historically. Furthermore, if changes are made, a full paper trail is essential. This should include the user that logged in, the processes that were running, the code downloads initiated, as well as whatever was changed in the environment — and much more. Capturing and maintaining this detailed information can help speed incident response and demonstrate proactive compliance both internally and to the required compliance organizations.

SUMMARY

Industrial cybersecurity is paramount to eliminate many of the core risks associated with the new trends and challenges that are present in the automobile manufacturing industry. To mitigate the OT risks, it is essential to gain full visibility, security and control into all the operational assets that control the myriad of sourcing, fabrication, assembly processes that are central to the manufacturing process.

Tenable uses an advanced multi-detection engine that employs both passive detection and patented active querying to detect any threat to your network. This ensures that you can gain the full visibility, security and control across the manufacturing process across your entire converged environment. Automatically having an up-to-date and granular inventory list will help you prioritize and close vulnerabilities while also enabling you to maintain capacity planning and maintenance schedules. In addition to maintaining a full paper trail of all the changes in the network, the sitewide audit information can assist with proactively demonstrating compliance to regulatory bodies. This will empower your engineering and security teams to keep your organization running at peak efficiency without exposing the manufacturing process to unacceptable 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.