tenable OT Security

USE CASE

SECURING OIL & GAS OPERATIONS

TOP TRENDS

- Sustained low oil prices are driving the adoption of digitization across the oil and gas industry, ramping up the stakes for cybersecurity.
- Expansion into new geographical regions and environments - such as ultra deep-water drilling, fracking and tar sands.
- Major global oil reserves are situated in conflict zones and transporting these reserves can be a challenging security task.
- Increased reliance on the third-party value chain to provide specialist equipment and expertise for different parts of the oil and gas supply chain. This includes extending from wellheads to pipelines through to the supply of natural gas to an electric power generation facility or gas utility; as well as to the supply of oil to a refinery through a gasoline station.
- Achieving fully integrated systems and a culture directed at gaining greater lifetime effectiveness, value, safety, availability, profitability and return from production and manufacturing assets.

BACKGROUND

The oil and gas industry heavily depends on automation for a variety of different operations. New automation technologies assist in developing new sources of energy such as deep-water drilling, tar sands and fracking, new fuel sources have been made available for the very first time. Concurrently, collaboration across the third-party value chain have yielded specialist properties and equipment resulting in efficiencies that were previously thought impossible. The symphony of operations required to find, extract, refine, mix, collaborate and ultimately deliver oil and gas all rely on the OT (Operations Technology) infrastructure.

Demand for oil and gas is projected to only increase over time. Though COVID caused a dip in Oil and Gas demand BP's Energy Outlook predicts that demand will rebound to pre-pandemic levels in 2022. The flawless delivery of oil and gas requires the highest engineering and safety standards. This relies not only on automation but also on maintaining the security of the OT environment. It's both a tall order and a major goal for the industry to attain.

In a recent SANS OT/ICS study, 48% of survey participants did not know whether they'd had an incident, indicating a clear need to improve our detection and response capabilities as a community. This sentiment was confirmed in a recent DHS report where an audit identified nearly 900 security vulnerabilities within U.S. energy companies, a figure that was higher than any other industry[1]. To maintain the flawless and uninterrupted flow of oil and gas, it is imperative for the industry to gain the visibility, security and control of its OT infrastructure.

[1] ATT Business - What's fueling cybersecurity concerns in the oil and gas industry?

KEY STANDARDS

API Standard 1164
Content unique to pipelines not covered by NIST CSF and IEC 62443.

NIST cybersecurity framework for improving critical infrastructure cybersecurity (NIST CSF)
Pre-eminent framework adopted by companies in all industry sectors; Natural gas and oil companies increasingly orient enterprise-wide programs around NIST CSF.

Department of energy cybersecurity capability maturity model
Voluntary initiative using industry-accepted best practices to measure the maturity of an organization's cybersecurity capabilities and strengthen operations.

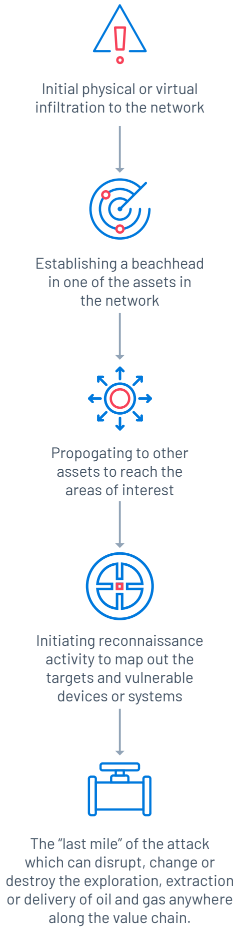
International electrotechnical commission's IEC 62443
Family of standards for industrial control systems (ICS) security; widely-adopted by production segment of natural gas and oil industry; applicable to any type of natural gas and oil ICS.

International organization for standardization ISO 27000
Leading standard in the family providing requirements for an information security management system (ISMS).

KEY CHALLENGES

- Major global oil reserves are situated in conflict zones and transporting these reserves can be a challenging security task.
- Lack of visibility into complex operations to control costs and the security of employees, facilities and assets.
- Gap in collaboration with remote and third-party facilities necessary to improve transport and logistics.
- Insufficient security for remote work during operations and maintenance.
- Little to no situational awareness or real-time insights into asset management and execution.
- Ineffective means to ensure cyber security awareness and training among employees.
- Use of standard IT products with known vulnerabilities in the production environment.

ANATOMY OF A CYBER ATTACK IN OIL AND GAS



Initial physical or virtual infiltration to the network

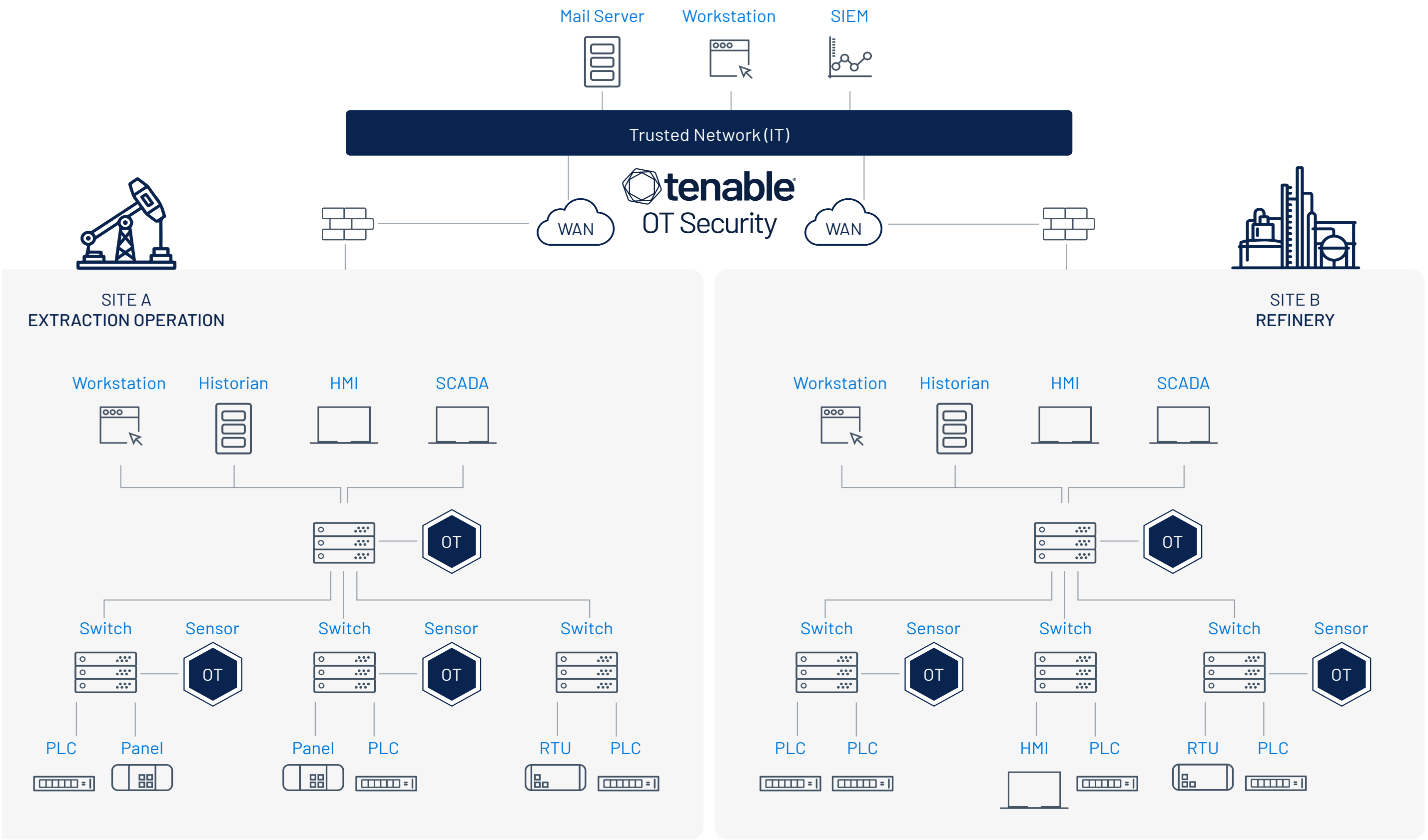
Establishing a beachhead in one of the assets in the network

Propogating to other assets to reach the areas of interest

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

The "last mile" of the attack which can disrupt, change or destroy the exploration, extraction or delivery of oil and gas anywhere along the value chain.

LOGICAL OIL & GAS DEPLOYMENT



COMMON THREATS

- Oil and gas production and refinement increasingly require cooperation of and reliance on third-party partners and specialists along the value chain consequently introducing a more heterogeneous audience into the OT infrastructure.
- Exploration and drill sites are often located in remote locations where deploying OT security is not always feasible. Transport along pipelines add to the security complexity by not only having to secure remote locations but also distributed locations.
- The convergence of IT and OT operations combined with the increased reliance on IoT technology to increase efficiency and decrease costs introduces additional threat vectors and attack surfaces.

Recent Events

- **May 2021** - The 5,500 Colonial Pipeline that runs up the east coast of the US and supplies 45% of the oil & gas to the east coast had to halt operations due to a cyber attack.
- **February 2021** - A cyber attack was launched against a natural gas facility concurrently encrypting both the IT and OT networks locking access to the HMI, data historians and polling servers. The pipeline was forced to shut down for two days.
- **December 2018** - Saipem, an Italian oil and gas industry contractor, fell victim to a cyber attack that hit servers based in the Middle East, India, Aberdeen and Italy.
- **April 2018** - A cyberattack on a shared data network forced four of the nation's natural-gas pipeline operators to temporarily shut down computer communications with their customers.

SEE MORE, SECURE MORE

While oil & gas' OT operations were once isolated, today they are connected to IT and anywhere access. The digitization creates an environment that can impact the integrity of the exploration, extraction, refining and delivery process. The elimination of "air-gapping" enables bad actors to penetrate parts of the operations 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. Traffic mapping and traffic visualization will identify and alert on communication attempts from external sources in addition to devices that should not be talking to one another.
2. Anomaly detection to pinpoint traffic patterns that are outside of the regular network operation.
3. Policy and signature based detection to identify known threats which are used by attackers.

Commonly Used Protocols

- Modbus
- OPC
- Ethernet/IP
- ControlNet
- DeviceNet
- CIP
- Fisher ROC/ROC+
- ABB TotalFlow
- ELAM (Lufkin)
- DNP3
- S7
- Melsec
- Honeywell DCS
- Omron Fins

CLOSE VULNERABILITIES FASTER

Due to the cost of downtime in the oil & gas industry 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 remote and distributed oil & gas environments, it is difficult to maintain an up-to-date inventory capable of zeroing in on specific devices and 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 detail including the devices model numbers, firmware version, vulnerabilities, patch levels and much more. Doing so will pinpoint and triage the devices with the most serious vulnerabilities to deal with first when plant can be idled to perform the required maintenance.

SECURE THE DISTRIBUTED ECOSYSTEM

The oil & gas industry increasingly relies on an extensive value chain of partners and specialists to increase the efficiency of operations while concurrently reducing costs. This requires synchronized operations across 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 refinery plant to offsite and remote drilling locations 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 control over configuration changes that spans from the main facility to all locations regardless of how remote or distributed they are. 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 PLCs, HMIs, controllers, engineering stations, PLCs, HMIs, controllers, networking equipment, gateways, and any other devices that are critical to the regular network operations. Deep knowledge, including visibility to all types of devices, patch levels, firmware versions and backplane information leveraging is essential. It is also critical to account for dormant devices that are not communicating regularly over the network.

MAINTAIN THE PAPERTRAIL

To comply with the standards noted earlier, it is important to proactively maintain a proper paper trail capable of demonstrating compliance with regulatory standards. To achieve both proper security and compliance standards, deep awareness of the state and characteristics of every device is required in order 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, highlight and prioritize newly discovered vulnerabilities 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 oil & gas industry. To mitigate the OT risks, it is essential to gain full visibility into all the operational assets that control the myriad of exploration, extraction, refinement and delivery processes collectively define the oil & gas industry.

Tenable OT Security uses an advanced multi-detection engine that employs both network and patented device based Tenable. ot technology to detect any threat to your infrastructure. This ensures that you can gain full visibility and security across these extensive and complex processes both on the main campus as well as at remote and distributed locations. Automatically having an up-to-date and granular inventory list will help you identify, prioritize and close vulnerabilities and enable 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. The combination of full visibility, security, and control will empower your engineering and security teams to keep your organization running at peak efficiency without exposing the oil and gas refinery process to unacceptable risk.

To learn more, visit: tenable.com. Contact Us: Please visit us at tenable.com/contact

tenable®