tenable + Indegy

Mind the Gap:
A Roadmap to IT/OT Alignment

Introduction

Modern day industrial operations often span complex IT (information technology) and OT (operational technology) infrastructures. In a very standard environment, thousands of devices exist and are increasingly being connected via the Industrial Internet of Things (IIoT). This creates new challenges in securing industrial environments specifically by making cyber- security threats even more difficult to detect, investigate and remediate.

What has made this an even more challenging endeavor is that IT and OT have typically inhabited different parts of the organization; and with good reason. Up until only recently the IT infrastructure played front and center in terms of ensuring complete visibility, security and compliance mostly because this was where organizations were being attacked. For the better part of two decades these were the things that kept the CISO up at night; but the reality has changed. With our increasingly interconnected world, OT has quickly caught up as a lightning rod for new attacks and increased security concern.

Ground Zero

The focal point for attacks on industrial operations and critical infrastructure has centered on Industrial Controllers. Depending on the type of industry, this may be referred to as PLCs, RTUs or DCSs. What really matters is that these controllers are extremely reliable and literally control everything from cooling stations to turbines, electrical grids, oil and gas and much more. Industrial Control Systems (ICS) literally keep the lights on. Because of their reliability, many of these devices have been in place for years. They are the workhorses of today's modern society and therein is why they are ground zero for attacks.

When industrial controllers were first deployed, they were not connected and interconnected. Today's advances in technology have put these devices online and thus they have become the target of the hacker. Furthermore, controllers were not built to address the security threats or the quite innocent human errors we now experience. Outsiders, insiders, and outsiders masquerading as insiders are all possible actors that launch sophisticated attacks to take over machines for nefarious purposes. More recently hackers are no longer rogue individuals but are often a carefully curated and systematic program by well-funded and highly motivated organizations and countries. A carefully executed attack can accomplish as much if not more than modern day warfare.

Few argue that the attack surface has changed to encompass both IT and OT. Because these two different worlds are now connected, an attack that starts on an IT environment can quickly move to an OT environment and vice versa. Lateral movement is almost the preferred attack methodology amongst hackers because of the relative ease of finding a weak link in the system, leveraging it as the point of entry, and then quickly owning the entire network.

Convergence of IT and OT

Few organizations currently manage IT (and OT) with the same staff and tools. After all, these networks evolved with a different set of priorities and they operate in inherently different environments. Nevertheless, in order to address this new complex threat and to protect this broader attack surface, many industrial organizations have begun to converge their IT and OT groups. The 'convergence initiative' is anything but simple. The growing pains associated with bringing together these two substantially different worlds can prove to be a challenge.

The IT/OT convergence trend is not only driving integration of IT tools with OT solutions, it also requires alignment of the strategic goals, collaboration and training; and this is only the beginning of the challenge.

One of the biggest differences between an IT and OT environments is their pedigree and approach. Both environments are managed by professionals with different backgrounds and with different mindsets. IT environments are very dynamic and for good reason. IT staff are typically concerned about data confidentiality, integrity, and availability. Because for so long IT played the front line in identifying, mitigating and reporting on attacks, the fluidity of thebenvironment had to constantly evolve. As a result, IT professionals worth their salt have to keep up on the latest IT trends and threats.

In contrast, OT staff work in an operational environment where stability, safety and reliability are top priorities. Their jobs involve maintaining the stability of complex and sensitive environments such as oil refineries, chemical plants and water utilities that are populated with legacy systems which were implemented and haven't changed for decades. Their motto is: "if it works, don't touch it". In fact, OT engineers recoil at the thought of IT personnel being involved in the safety of their plants or tinkering with industrial control systems (ICS). IT personnel have typically not been exposed to this operating paradigm, and few of them have ever set foot on a plant floor.

Different Worlds, Different Technologies

In general, IT people are used to working with the latest and greatest hardware and software, including the best security available out there to protect their networks. They tend to spend time patching, upgrading and replacing systems.

Meanwhile, OT staff are used to working with legacy technologies, many of which pre-date the internet era. These often use proprietary network protocols, and lack basic security controls like authentication or encryption. They also don't have event logs or audit trails. As a result, incident detection and response in an OT environment is very different than in an IT environment.

Whatever technology is deployed and regardless of the mindset that the individual has been used to, both the IT and OT environments must now come together to address the security threats on both sides of the network. Further, they must collaborate to stop lateral creep of an attack that may have started in one environment and successfully spreads to the other.

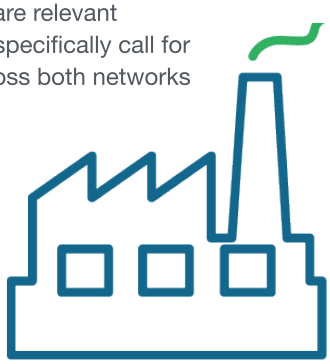
Best Security Practices

While there are significant differences between the worlds of IT and OT, one thing that can be agreed on are the key elements in establishing a robust security posture when it comes to industrial security. They include:

- Threat detection & mitigation that combine behavioral anomalies with policy-based rules.
- Asset tracking that includes dormant devices and goes as deep as PLC backplane configurations.
- Vulnerability management that tracks and scores patch & risk levels of ICS devices.
- Configuration control that tracks all changes to code, OS & firmware regardless whether done through the network or locally.
- Enterprise visibility to ensure that all data collected integrates to a single pane of glass.

Regulations Require IT

When one hears about a potential security incident, few dismiss it as a once in a lifetime event. The truth is that security threats are almost constant and successful attacks are occurring regularly. Thus, another impetus that is driving the IT/OT convergence trend is regulatory compliance. For example, North American Electricity Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) require IT and operations staff in critical infrastructure to collaborate and manage risks cooperatively and share relevant documentation to ensure security and reliability. In fact, regulations specifically call for an environment in which there is the ability to conduct forensics across both networks in order to identify, thwart and report on incidents that can disable significant industrial deployments and critical infrastructure.



This is just the tip of the iceberg in regulatory compliance. Virtually every vertical has an alphabet soup of regulatory compliance requirements associated with it. Bringing together IT and OT hastens compliance with regulatory statutes, and the ability to proactively report on and demonstrate compliance makes any potential audit significantly easier.

Your Business Demands It

To this point, we have discussed the need for IT and OT convergence because the new threat paradigm demands it and compliance standards require it. The third and most important leg in this stool is the business element. Organizations that fail either of these two areas are often put in the hot seat to respond to a shareholder and customer base inquiry that will demand answers.

In recent incidents CSOs, CROs and their staff can be called in front of the board to answer hard questions. In some cases, they have been personally held liable for significant lapses in coverage, protection and diligence.

In virtually every case however, shaken customer confidence directly translates to the bottom-line and manifests both in the form of shareholder value or in revenue. This largely could have been avoided by de-siloing the IT/OT environment and applying a robust security solution across these intercoupled environments.

C-Level Support Can Make It Happen

The successful deployment of industrial cybersecurity initiative must leverage resources from both IT and OT. To bring IT and OT staff together and unify security thinking and practices, organizations need to create a culture of collaboration between both camps for the common good of the business.

And despite the challenges of bridging this divide, a number of organizations have achieved deep collaboration between these distinct but increasingly intertwined worlds. The key to success is getting C-level support.

Some organizations begin by creating a C-Level role to facilitate the convergence. For example, it's quite common to find a Chief Digital Transformation Officer whose role is to bridge the gap between IT and OT, merge the culture divide, and establish incident response processes that span both groups.

Business-level oversight and C suite leadership helps ensure that the two sides will collaborate effectively with each other. To make this happen, more and more organizations are taking senior, experienced engineers from OT business units, and assigning them to support incident response within the Security Operations Center (SOC). This creates an environment where people, processes and technologies straddle and unify both sides of the IT/OT fence.

The Benefits to Be Reaped

They say that nothing rewarding in life comes easy. This has never rung truer than creating alignment between the world of IT and OT. Doing so, however can reap significant benefits including:

- Improved security automation, sensing and visibility
- Increased control over distributed operations
- Better compliance with regulatory requirements and tracking
- Higher responsiveness when incidents occur and improved organizational performance
- Better decision making based on more detailed information
- Proactive maintenance and reduced response times to unforeseen disruptions
- Improved flow of information to stakeholders

Many pundits and experts in the field say that it is not an issue of “IF” but rather a matter of “WHEN” a security incident occurs. Bringing the IT and OT worlds into the same orbit will help ensure that when an incident occurs, that the organization can weather the storm and in fact thrive amid the chaos.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 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 25 percent of the Global 2000 and large government agencies.

Learn more at tenable.com.