eBook

Securing Operational Technology in Highly Regulated Industries

SteelCloud

As cyberthreats continue to plague government and industry, attention is turning to our nation's most highly regulated industries. Regulations in these industries cover many aspects, but increasing pressure is being placed on securing operational technology (OT). While information technology (IT) controls an organization's data, OT monitors and controls organization's operational equipment and assets.

IT and OT have been separate in the past living in two separate worlds. OT systems were intrinsically air-gapped to reduce vulnerabilities by moving data physically from one machine to another. But as technology advances, a convergence of the two is forming. And this puts OT (and its vulnerable legacy software) at greater risk, especially in highly regulated industries that depend on their OT to provide critical service.

The nuclear industry is the most highly regulated industry in the world. In addition, other regulated industries in the United States include healthcare, insurance, pharmaceutical, energy, telecommunications, and banking. These industries face a framework of rules and regulations at the federal, state, and sometimes even local level.

According to IBM, "Highly regulated industries are feeling pressure to transform, but they cannot afford to drop the ball on security, resiliency, and compliance."

According to IBM, Highly regulated industries are feeling pressure to transform, but they cannot afford to drop the ball on security, resiliency, and compliance.

With ever-present pressure to increase security, the time has come to treat OT with the same watchful eye as IT.

The convergence of IT and OT can strengthen your security posture.

IT and OT have been operating separately for decades and are often physically isolated. When these two independent systems are interlaced the combination of OT and IT provides a more secure infrastructure to benefit industries from manufacturing to energy. IT/OT integration can help solve everyday challenges, such as distributed asset management, an aging workforce and evolving customer expectations.

OT and IT network infrastructure have similar elements, like switches, routers, and wireless technology. Therefore, OT networks can benefit from the rigor and experience that IT has built over the years with standard network management and security controls to build a solid network foundation.

For example, OT often uses spreadsheets to manage compliance data, which is ineffective in highly regulated industries. Spreadsheets lack the capabilities to keep up with regulatory changes, putting companies at risk for non-compliance. They're not designed to handle high volumes of data. Integrating IT and OT can streamline processes and utilize the same approaches for securing and documenting compliance data.

Repeatable processes can help you respond quickly to evolving threats.

Almost every cybersecurity professional knows that a data breach is now a matter of "when" rather than "if." Nothing can be fully secured, and the more complex your stack is, the more likely malicious actors will find a way to get north of the wall. To establish a cyber-resilient security posture, you need to focus on having repeatable, proven processes to find the vulnerabilities and act before something terribly goes wrong, which it most likely will at some point.

Organizations in the defense industrial base and highly regulated industries often find it overwhelming to harden their systems against attack. In addition, many small and mid-sized businesses store, process, transmit, or collect Controlled Unclassified Information (CUI), and this complicates cybersecurity approaches because the processes for securing systems are highly mandated. As a result, automation is often used to meet government mandates, simplify processes, use well-proven tools, and ease the compliance burden.

Regulations impacting compliance and operational technology when IT and OT merge.

In September 2022, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) released a new cybersecurity advisory. It warns highly regulated industries—such as finance, insurance, transportation, manufacturing, and oil and gas—of increased threats to their operational technology (OT) and industrial control systems (ICS). It recommends tightening security around your OT and ICS.

The U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity spans IT and OT to promote the protection and resilience of critical infrastructure. However, their cybersecurity framework (CSF) neither suggests an implementation order nor provides detailed control recommendations.

Therefore, many organizations adopting the CSF also utilize the long-established Center for Internet Security (CIS) and Security Technical Information Guide (STIG). These controls and benchmarks help prioritize implementation, define more granular security controls, and address regulations impacting OT. STIG, and CIS controls are proven throughout the federal government and defense industrial base to secure even the most sensitive systems.

As Meritalk observes, while traditional ways of securing OT and ICS can't adequately address today's threats to those systems, the advisory states that "owners and operators who understand cyber actors' tactics, techniques, and procedures can use that knowledge when prioritizing hardening actions for OT and ICS." Because OT and ICS systems often incorporate vulnerable IT components and include external connections and remote access that increase their attack surfaces, that may be an excellent place to start looking for vulnerabilities.

CIS benchmarks can secure your IT, OT, and integrated systems.

Gartner states in their Market Guide for Operational Technology Security,

> **The OT security market is rapidly changing. The traditional niche OT security market emphasized products focused on legacy industrial systems and operations-only networks and firewalls. The market is shifting rapidly as new tools and services with an ever-increasing array of features become available. As OT continues to connect to IT systems, and newly designed CPS are deployed, OT management, governance, infrastructure, and security are evolving.**

As IT and OT continue to integrate and evolve, it makes sense to secure your OT the same way as your IT.

A best practice in most organizations is to create baseline technical security configurations. However, configuring systems is one thing. Maintaining those security configurations over time is a whole different beast. CIS controls offer companies a clear pathway toward maturing their cybersecurity programs and technical guidance for establishing and maintaining secure configurations. As cyber threats reach out to plague regulated industries and critical infrastructure, CIS can provide a solid security baseline and, with continued vigilance, maintain that baseline indefinitely.

Secure system connectivity in an increasingly integrated world.

OT and ICS assets operating, controlling, and monitoring day-to-day critical infrastructure are becoming more of a target for malicious cyber actors because they often incorporate vulnerable IT components and include external connections and remote access that increase their attack surfaces. The systems are critical in functioning physical processes, such as power generation and transmission or manufacturing production. These OT systems are built to last ten to twenty years, instead of the five-year lifecycles of traditional IT equipment.

Security becomes a more significant issue as OT and IT systems connect. Systems formerly air-gapped from enterprise IT and its access to the internet and communication applications, such as email and cloud interfaces, are accessing the enterprise infrastructure to take advantage of the opportunity to scale and the power of big data analytics. But this added benefit comes with risks from IT networks: ransomware, hacking for espionage, and potential disruption of physical processes to cause physical damage.

Cautionary tales about ransomware, hacking and IT and OT integration risks.

The boon of ransomware has been escalating, causing willful damage to companies and to entire communities. But unfortunately, pulling the curtains and locking the doors no longer secures you. Savvy adversaries are developing new methods of cyberattack to infiltrate entire networks and impact critical infrastructure across healthcare, financial, retail, manufacturing, oil, and gas—the industries on which our very lives depend.

In the latest round of cyberattacks, Binance, the world's largest cryptocurrency exchange, was hacked, and around $100 million of Binance Coin was stolen. Can your organization afford to lose even a fraction of that? And what are you doing to prepare for the next, more sophisticated round of cyberattacks?

Or take the case of the Colonial Pipeline, the largest fuel pipeline in the U.S. In April 2021, the pipeline was attacked by hackers. As a result, the company temporarily shut down its entire network—representing 45% of the fuel used along the east coast of the US.

Something as basic as an unprotected password led to severe fuel shortages and gas price spikes. The hackers got $4.4 million in ransom for their efforts, and it took two weeks and over $1 million for the pipeline to resume operations. A comprehensive audit trail of events carried out during the session and tamper-proof session recordings could have stepped up the inspection process.

Insecure endpoints enable ransomware to take hold. Therefore, all endpoints and devices must be assessed before accessing networks, VPNs, applications, and content. And this assessment of endpoint health and security capabilities must be continuous — not just at the point of login.

Finally, we have an example to illustrate how OT and IT convergence can increase risks. In 2021, a water treatment plant was breached in the tiny municipality of Oldsmar, FL—a town of 15,000. In this incident, the attacker attempted to change the alkaline levels in the water to a level that would severely damage human tissue. While that may be a shocking example of OT/IT convergence risks, every at-risk industry, from finance to energy, has the potential to create incidents this bad and worse.

As mentioned before, air-gapping machines should be considered a viable solution for sensitive data that doesn't need to be accessed over a network. But it is within the realm of possibility that your air-gapped machine is one USB drive from being compromised.

Cyber resilience can keep bad actors at bay.

Most cybersecurity professionals will tell you that a data breach is more a matter of "when" than "if." Nothing can be fully secured, and the more complex your stack is, the more likely malicious actors will find a way to hijack your system. Focus on having repeatable, proven processes that show you know how to respond when something goes wrong, which it most likely will at some point.

Cyber resiliency is vital. Cyber resilience is about showing that you can protect data and quickly respond when something goes wrong. The U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity spans IT and OT to promote the protection and resilience of critical infrastructure. NIST 800-70 offers best practices for using security configuration checklists like the CIS controls that are mandated to secure the infrastructure of critical industries.

Security challenges are only expanding throughout the nation as threats, vulnerabilities, and risk continue to shift; budgets and investments remain limited; and technology, economic and social change remains the norm. Implementing CIS benchmarks and establishing a practice of continuous network monitoring can go a long way to avoiding the horror stories others have experienced at the hands of cybercriminals.

SIEM solutions can monitor a network continuously, capture any information about possible threats and malware, and report them to the administrators for preventive actions. With meaningful insights like that, Colonial Pipeline could have mitigated damage to their network. This is a tactic all modern organizations with critical services—from finance to healthcare to energy—should implement to protect their customers and their infrastructure.

Best practices for securing OT and ICS

Industrial Control Systems (ICS) often operate software and hardware that directly control physical equipment or processes. Many of these systems not only have a high availability requirement, but are also the foundation of our critical infrastructure, our crown jewels. In industries such as utilities, transportation, finance, manufacturing and oil and gas, we're talking about equipment that can shut down lives and cause grave danger to humans and the environment. For this reason, third-party resources should be scrutinized to eliminate risk in the supply chain, which includes evaluation and confirmation of experience, skills, and knowledge before sharing access to critical systems.

In response to threats on critical infrastructure, the Director of DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), Puesh Kumar says, "We have a strategic opportunity like we've never had before. We can address both climate risks by deploying clean energy solutions and integrating cybersecurity into those systems from the ground up. This is good for U.S. energy security and U.S. national security."

Mitigating the risk right under your nose.

In the OT environment, countless off-the-shelf, web-based, and proprietary applications may already be running on a network, which can be daunting for system administrators. In addition, it's not uncommon for ICS environments to contain some custom-engineered, in-house built web-based software that is unique to the given system. These applications and services may only sometimes follow a disciplined engineering development, test, and maintenance process, leading to application vulnerabilities that an attacker can exploit.

Regulations impacting OT, such as CIS, include security protocols for software built by in-house OT teams, though minor modifications may apply. The same control even applies to COTS software sourced from vendors. The goal is to find vulnerabilities and shore them up. It may be the most significant thing you can do to secure ICS after it is built.

An ounce of prevention is worth a pound of cure—shifting left.

Perhaps the most effective approach you can take to secure ICS is by baking security in during the DevSecOps phase. The use of automation during the development stage shifts cyber assurance "left" along the development timeline, adding security while the technology is in the production phase instead of waiting until the final stages of development or adding a patch after the fact.

True to its name, DevSecOps emphasizes the need to incorporate security into every development phase. The obvious advantage of doing this is to identify potential vulnerabilities and work on resolving them sooner. But it also means that security becomes an organic part of the software development process—a conscious and continual effort.

Shifting left might temporarily disrupt your existing DevOps process workflow. Overcoming this might be challenging, but it's best practice to shift left in the long run if you adopt DevSecOps. By integrating and automating various compliance checks throughout development, organizations create an environment of continuous compliance built upon automated integrated processes and workflows that promote compliance as a requirement, such as CIS, STIGs and other mandates.

Reducing siloes and automating policy compliance.

A third best practice is to move away from siloed, static approaches that involve human error, like traditional Excel-based questionnaires, and begin using a standardized data set that can be shared.

Automation can help significantly with everything from risk management to shifting left to monitoring and standardizing data. SteelCloud's ConfigOS does it all in one product and ConfigOS DashView can monitor your hardening compliance and dramatically reduce the time spent monitoring regulations impacting OT, like with CIS benchmarks. Getting compliant is difficult but maintaining that compliance posture is even more difficult. ConfigOS DashView leverages Splunk's "Big Data" platforms to automate these processes and provide the organization with real-time awareness.

More best practices to avert disaster.

Other best practices for highly regulated industries include:

- ✓ Conducting regular, non-intrusive security assessments with the assistance of third parties to identify a greater diversity of vulnerabilities and attack vectors that can be used to breach security of ICS systems.
- ✓ Putting the proper systems in place to manage the identity lifecycle and risk of third-party workers with the same or greater diligence as their employees.
- ✓ Ensuring security tools do not automatically deploy software. These tools should report and identify where security updates are needed but allow the OT team to deploy updates when it is safe to do so.
- ✓ Leveraging CIS benchmarks and controls to uncover vulnerabilities and fix them so your system is secure and compliant. CIS benchmarks, for the most part, mirror the proven STIG controls the government uses to keep our nation's critical data safe from attack.
- ✓ Using automation solutions like ConfigOS and DashView to simplify and strengthen your security posture, comply with CIS mandates and uncover areas of vulnerability so you can shore them up.

A few words about how third parties can help.

While we recommend scrutinizing third-party resources with an eye on security before trusting them, vendors can also be your best resource in helping you merge your IT and OT systems or secure systems against cyberattacks. Your vendors can help you by:

- ✓ Outsourcing to bring in strategic skills and knowledge
- ✓ Reducing costs by doing the same work you'd hire new team members to do, but at a lower rate
- ✓ Simplifying and accelerating your risk assessment preparedness
- ✓ Putting industry standards in place to ease compliance
- ✓ Finding the gaps in your security so you can fill them
- ✓ Removing burdensome human effort through automation
- ✓ Delivering greater agility at a lower risk
- ✓ Establishing a Zero Trust stance and rapidly validating and verifying everything inside and outside your network

Automation is the best helper you'll get for securing your OT.

CIS benchmarks and DISA STIGs establish policy compliance baselines around system-level controls. Making policy compliance work for you and managing a system well gives you tremendous security value. It is more than just a set of good things to do, and a checklist to check them.

The bedrock principle of good security management is around good configuration management. SteelCloud's ConfigOS is proven to automate CIS and STIG processes for simplified security, rapid hardening and policy compliance.

As technology improves and cybercriminals perfect their techniques, deploying a holistic approach where OT, and IT are managed by a coordinated effort makes sense. By simply implementing SteelCloud's ConfigOS software, you can easily create—and maintain—that secure baseline you need to avoid your data getting into the wrong hands. ConfigOS automates the process of identifying vulnerabilities, mitigating control issues, and maintaining that security over time:

SCAN. Achieve secure policy requirements by scanning a single endpoint or your entire infrastructure (laptops, desktops, physical or cloud servers) with SteelCloud's patented scanning software. Each instance of ConfigOS can scan 5,000-15,000 endpoints per hour – supporting the requirements of small to even the largest infrastructures and reducing workdays to just an hour.

REMEDIATE. The time it takes to remediate hundreds of CIS controls on each endpoint is typically under 2 minutes, and ConfigOS executes multiple remediations simultaneously. Remediating security controls is accessible by using your customized policies. With its patented remediation engine, each instance of ConfigOS can remediate 3,000-5,000 endpoints per hour. Add more instances to meet your performance requirement.

REPORT. Reporting in an organized easy-to-understand format, ConfigOS simplifies compliance reporting. Customize and filter your results with our built-in tools. Complete STIG Viewer checklist integration is at your fingertips, including automatic entry of documentation details and waiver descriptions.

In addition, SteelCloud can help organizations meet various challenges — like managing unpredictable, complex, multi-domain operations; understanding and addressing different areas of risk where significant uncertainties are involved; conducting regular risk assessments and collaborating with partner organizations like information technology. Better yet, our ConfigOS software can automate the process of meeting CIS benchmarks and continuous monitoring and maintenance. Watch it in action and see how much it simplifies complex cybersecurity.

Success comes from a strong partnership between CIS and SteelCloud.

SteelCloud is a recognized leader in developing compliance automation software to help government and commercial enterprises worldwide automate policy and security remediation by reducing the complexity, effort, and expense of meeting industry security standards, such as the CIS Benchmarks. As a CIS SecureSuite partner, SteelCloud can integrate the security recommendations of the CIS Benchmarks directly into our solutions like ConfigOS. We are certified by CIS to accurately assist its customers in complying with CIS's globally recognized secure configuration guidelines.

In March 2022, SteelCloud licensed our ConfigOS technology to a major U.S. energy company to secure its operational technology (OT) assets. Currently implemented in hundreds of commercial and government organizations, ConfigOS helps harden endpoints against CIS security best practices. It is particularly beneficial to operational technology (OT) operators because its agent-less architecture removes the need to load software on assets.

According to CIS's configuration guidelines for system level controls, large highly regulated energy company used ConfigOS to harden thousands of process control and SCADA assets according to CIS's configuration guidelines for system-level controls. By using SteelCloud's CIS-certified solution, the company will be able to improve its security posture and protect its assets against common cyber threats using the CIS Benchmarks' consensus-based configuration recommendations in a fraction of the time it would take to do so manually.

With threats quickening and regulations looming, highly regulated industries simply can't afford to address security with anything other than urgency. SteelCloud will help you establish a secure baseline fast and maintain it indefinitely to protect your assets and reputation. Here are a few more resources to help you meet CIS Benchmarks:

WATCH: Making Policy Compliance Work for You—CIS Benchmarks

WATCH: ConfigOS CIS Benchmarks Demo

READ: CIS Benchmarks Datasheet and SteelCloud Partnership

About SteelCloud

SteelCloud develops STIG and CIS compliance software for government and commercial customers. Our products automate policy and security remediation by reducing the complexity, effort, and expense of meeting government security mandates. SteelCloud has delivered security policy-compliant solutions to enterprises worldwide, simplifying implementation and ongoing security and compliance support. SteelCloud products are easy to license through our GSA Schedule 70 contract. SteelCloud can be reached at (703) 674–5500 or info@steelcloud.com. Additional information is available at www.steelcloud.com.

SteelCloud

20110 Ashbrook Place, Suite 200 | Ashburn, VA 20147
1.703.674.5500 | info@steelcloud.com | **steelcloud.com**