eBook

SECURING the Software Supply Chain

SteelCloud

In 2020, hackers found their way into the back door of an IT performance monitoring solution called Orion, made by SolarWinds. And through this breach, the 30,000 organizations that used the Orion solution became vulnerable. More than 18,000 customers ultimately installed the malware, impacting private industry as well as government agencies such as the Department of Homeland Security, Department of Commerce and Department of State.

We may never know the who, why, and full impact of the SolarWinds attack. But we do know that it raised awareness of supply chain security and prompted new requirements in the government supply chain via Executive Order (EO) 14028.

PART 1: Compliance Requirements In The Supply Chain

If you want to be or stay part of the federal software supply chain, the rules of engagement have changed drastically over the past few years. Executive Order 14028 lists multiple requirements for developers of "critical software", including maintaining a software bill of materials (SBOM) and attesting to secure development practices. It also establishes a timeline for requirements and recommendations in regard to employing data encryption, auditing internal and external risks, using automation tools to identify and remediate vulnerabilities, and many other steps to take.

Determining the criticality of critical software.

As of now, the government is most concerned about securing "critical software". "Critical software" is not defined as essential software, enterprise software or any other moniker that sounds "critical". Rather it is the software that is most critical to secure—software that has a trusted, interactive relationship with other software in the system. This includes software that:

- ✓Is designed to run with elevated privilege or manage privileges
- ✓Has direct or privileged access to networking or computing resources
- ✓Is designed to control access to data or operational technology
- ✓Performs a function critical to trust
- ✓Operates outside of normal trust boundaries with privileged access

So, really, an essential question to answer is if you develop or handle critical software. If you do, you are subject to NIST 800-53 and SBOM mandates. If not, you should be tightening your risk management practices nonetheless to show customers and potential hackers that you're committed to following cybersecurity best practices.

If you handle CUI, you must comply.

Another marker for those who must comply is if you handle CUI. Controlled Unclassified Information (CUI) is government created or owned unclassified information that they routinely share in the course of business. That data needs to be safeguarded according to laws and policies. This includes health records, tax holder data and other data necessary to protect citizens' and the government's interests.

Many government contractors—even those who operate in an unclassified way with government agencies—handle or maintain some of this information in their systems. Those contractors need to comply with NIST SP 800-171. NIST 800-171 lists a series of 110 procedures and controls that must be implemented if you house, process or transmit CUI.

The sooner you implement NIST 800-171, the better for business. Implementation can be simple or complex, depending on the complexity of your operating environment and systems.

Additional requirements for the software development process.

EO 14028 also makes it necessary for developers to produce and maintain a Software Bill of Materials (SBOM). The SBOM is an inventory of all the software components used, including open-source software. This helps evaluate known vulnerabilities and risks in a product so it can be properly secured in the system.

In addition to the SBOM, developers need to attest to using secure development practices on software created or updated after September 2022 using the Secure Software Development Common Attestation Form. Practices include developing in a secure environment, maintaining trusted source code supply chains, maintaining provenance of third-party code, and employing automated tools to check for vulnerabilities.

Protecting government data with CMMC.

While CMMC is meant to protect government data and not a direct mandate for the entirety of the software supply chain, Cybersecurity Maturity Model Certification (CMMC) is another initiative that will help strengthen overall security within the supply chain.

Those who handle CUI also need CMMC. This step requires NIST 800-171 compliance and also requires self or third-party certification. This can take up to 2 years, depending on the level of CMMC certification to be met. Each level has progressively greater requirements:

Level 1: This is for organizations that only deal with Federal Contract Information (FCI). The requirement covers 17 practices, and you can self-assess your results.

Level 2: This level is for contractors handling CUI, which will be the bulk of government contractors. The requirement covers the 110 practices from 800-171 and tri-annual third-party assessments.

Level 3: This level is for contractors working with CUI on our nation's most sensitive contracts, such as developing advanced weapons and vehicles. The requirement here includes 800-171 controls, plus others and requires tri-annual, government-led assessments.

There is a deadline for CMMC certification. It is expected to start showing up in RFPs near the end of 2024. The government's goal is to have it implemented across the defense industrial base by October 2025. The sooner one complies, however, the better. As SteelCloud COO Brian Hajost says, "Compliance puts a halo around your proposal" and moves it to the top of the stack.

Automation is a necessary part of your requirements.

As mentioned above, the EO also calls out the need to use automation solutions in the development process, as well as in the organizational operating environment. The process of identifying and fixing vulnerabilities can take weeks or months to complete. And you want to maintain that secure baseline through updates, new installations, and new processes. This requires constant vigilance so your secure environment doesn't drift into vulnerable territory. An initial secure baseline can take weeks or months to achieve using manual processes. It only takes about an hour using automation.

Many will want to exceed requirements and adhere to Security Technical Implementation Guide (STIG) or Center for Internet Security (CIS) standards. Both incorporate 800-171 controls, but go way beyond to create iron-clad security across every endpoint in your system. As a result, automation tools made for STIG and CIS compliance can also help with 800-171 and CMMC. And as long as we are talking about the difference of just minutes to achieve compliance through any of those means, becoming STIG or CIS compliant will put an even bigger halo around your organization for little added effort once policies are established.

PART 2: Conducting A Risk Assessment

The first step toward securing your supply chain includes looking at your own practices and the practices of those you do business with, then assessing your risk in relation to established best practices. It sounds simple enough, but the road toward identifying potential threats and vulnerabilities in the supply chain is greater than what meets the eye. This process should consider the entire supply chain, including all suppliers, vendors and partners. And it should also consider all potential sources of risk, including natural disasters, cyber threats, geopolitical factors, and other disruptions.

Getting started with a supply chain risk assessment.

The first step involves situational awareness and getting the lay of the land in terms of risk and mitigation efforts up and down the supply chain. Here are some preliminary questions to ask:

- ✓How many vendors (from developers to janitorial services to third-party suppliers) are we associated with? This gives you an idea of potential sources of risk.
- ✓How strong are their physical security and cybersecurity practices? The strength of their practices will impact the strength of your own.
- ✓Do your own cybersecurity practices measure up? See if there are best practices you are missing and what can you learn from the choices others have made.
- ✓Have we or our vendors ever experienced a major breach? Has it been fully remedied? Do we know what caused the breach? Without strong policy and documentation, it can be hard to learn from mistakes.

Standards and practices the supply chain should adhere to.

After identifying potential threats and vulnerabilities, the next step is establishing a risk management framework that outlines the policies, procedures and controls required to mitigate these risks. Secure configuration management is essential to mitigating risk, and the government has many tools and guides to choose from in that regard. NIST 800-53, version 5 is one of these guides. It outlines mandated security and privacy controls organizations within the supply chain must adhere to.

In addition to coming into alignment with NIST 800-53, members of the supply chain also need to create and maintain a software bill of materials (SBOM), as required by EO 14028. This Executive Order outlines how government suppliers should inventory and keep the lineage of all the software components they use, including open source software. This helps evaluate the risk in a product and secure it in the system.

Supply chain security is a group effort.

On one hand, securing the software supply chain requires you to do your part as a supplier. But on the other, it requires you to work with everyone up and down the chain to present a united and secure front. This is a participation sport that needs to be continually and actively tended to.

Once you have completed an internal and external assessment of your risks, it's time to harden baselines, secure endpoints and lock down your enterprise. If there is no way to breach your system, there is no way to go through you to attack your customers. The government offers a good deal of guidance regarding these requirements.

PART 3: Creating Another Layer Of Security With Zero Trust

As previously mentioned, EO 14028 makes many recommendations specifically for the software supply chain, including making a risk assessment, securing your systems, and complying with mandates. Once you've aligned with the government's highly secure standards for supply chain security, the EO recommends an added layer of security: Zero Trust.

One permission too many is all it takes to create a vulnerability.

You can trust your employees with many things. But sooner or later, even the best employee will make a mistake. And some bad actor somewhere is going to take that mistake and run with it. With hackers becoming increasingly sophisticated, human error is a risk you can no longer afford to take. Zero Trust is a good answer.

Zero Trust moves network security from the perimeter to—or closer to—the individual data repository or application. Equally important, Zero Trust increases the breadth and depth of continual verification and evaluation versus the traditional single verification at the network perimeter. It requires both the validation of the user's identity and their system configuration before granting access to an application area. In theory and in practice, it assumes that no actor, service, or system can be trusted. With a September 2024 Zero Trust deadline looming for government agencies, software suppliers who align with the mandate now will show government agencies they're serious about cybersecurity and maintaining good cyber hygiene.

Once you've established your Zero Trust architecture, it's critical to communicate why this is important throughout the organization and create a culture of Zero Trust. You are asking people to adopt a more secure, but less convenient way of working. If they understand the weight of what you are all trying to accomplish as a team, you'll be more successful.

Trust no one. No one.

One of the tips for creating a Zero Trust network is to account for all users. This involves determining the level of access needed on a person-by-person basis. Job roles and responsibilities are a good way to do this. Performing individualized risk assessments can also help. Limiting use of permissions, such as allowing some user to only view and not edit or download files is a way to hone security even more. Of course, this is not just about internal users, but throughout your supply chain. Every vendor, client and user on your system needs to be considered.

PART 4: What To Do In Case Of A Breach

Let's say you've established government-level cybersecurity in your organization. You've assessed your risks. You've aligned with stringent compliance standards such as STIG, CIS or CMMC. Your systems are continually updated with security measures. And, you have started implementing Zero Trust. You may be a vendor in the supply chain, and your own security is as tight as the guys who protect the most sensitive data in the world.

Guess what? You can still be breached. People in your supply chain can be breached, or your customer can be breached. It may be less likely to impact people with world-class security, but there is always a risk. And if it happens, things will move so rapidly and the pressure will be so great you won't be able to think straight. So you will need an incident response plan in place to help steer you through the crisis.

Create a plan.

An incident response plan is a roadmap of the questions to ask, the steps to follow and the actions to take to contain damage and quickly recover from a breach. NIST has developed a comprehensive framework to follow to guide you on your way. Incident response can be broken down into four steps.

The first step is preparation. You have already done much of that or are planning to do it as part of your federal supply chain expectations. Preparation includes securing your systems, creating a baseline of activity and monitoring that baseline for changes. It also includes having an overall plan in place in case of a breach, including:

- ✓Which types of events should be investigated?
- ✓What is our response plan for each of those scenarios?
- ✓How do we respond if a breach happens to someone else in the supply chain?

Determine incident severity.

Once a breach has occurred, you need to get to the bottom of it. Collect data from your systems, security tools and people, then analyze it to find the breach and determine its impact. In a supply chain attack, you'll need to look at third-party tools and the remote access granted to suppliers as well.

You'll also want to ask questions like:

- ✓Was the breach caught immediately or has it gone undetected for some time?
- ✓Was the breach solely internal, or has it extended outside the organization? Alternately, was it solely external and what are the risks of it extending to your system?
- ✓Are there signs that this could repeat in the future or grow beyond where it is now?

Develop your response.

Now you have a clear idea of what has happened, it's time to stop the bleeding. This phase includes incident containment, threat eradication and system recovery. Here are some questions to ponder:

- ✓Who is the attacker and what is their IP? Determining this will allow you to block them from further harm.
- ✓How can we secure the breach? Do we need to keep critical services live while we eradicate the issue?
- ✓What do we need to share with customers and affected teams? And when? How will this information be disseminated? Who will be the communication point person?

Don't skip the postmortem.

Once the incident is contained and everything is recovered, it's critical to examine what happened and find the lessons learned. Key questions to ask and document at this time include:

- ✓What information could we have benefitted from knowing sooner?
- ✓What could we do differently next time in the same situation?
- ✓Did we look for and find indicators of similar incidents to watch for in the future?
- ✓What additional tools or resources are needed to prevent breaches and mitigate damage in the future?

PART 5: The Easy Choice

EO 14028 repeatedly mentions using automation to create efficiencies. In fact, it's one of the government's requirements. They know they are asking a lot of people to adhere to mandates, create secure baselines and build a Zero Trust program on top of that secure foundation. Today's threats, combined with a shortage of workers and the increasing capabilities of hackers and AI, are making automation an absolutely necessary part of the process.
How automation can help.

There are many key aspects of automation that make it perfect for securing the supply chain. The claims below are for ConfigOS, SteelCloud's patented compliance automation solution. ConfigOS is the #1 choice for compliance automation in the DoD, so using it will align with your customers' security processes and give you a proven solution to count on. Here is how automation helps:

Save effort.

Creating and maintaining a secure baseline is a monster of a job, usually requiring overtime and sleepless nights. Automation has been shown to remove up to 90% of that effort.

Save time.

It can take weeks or months of continual manual effort to create a secure baseline. With requirements being updated quarterly, it's a marathon that never ends. But automation reduces that work to a sprint, creating a secure baseline in less than an hour.

Save money.

Experts in compliance automation don't come cheap. They also don't come easy. If you're going to approach compliance manually, you'll need to hire a team of highly competent experts who are in short supply. Automation makes it easy for people at any level of competency to do the work and it helps you save 70% of the costs of compliance.

Be more accurate.

People make mistakes. Overworked people make even more mistakes. Automation eliminates the human error that comes from tedious hours of manual updating and monitoring. Better yet, automation doesn't even need a bathroom break to be happy at its job.

Create a healthy work environment.

This element of cybersecurity isn't spoken of often, but it is a critical consideration. Mental health issues abound in the industry due to long hours, constant stress and, yes, worrying about breaches. Automation relieves a lot of the stress of a job in cybersecurity.

Automation and EO 14028.

SteelCloud's ConfigOS is built specifically for the challenges posed by EO 14028 and CMMC. ConfigOS automates the process of establishing baseline security—the biggest part of the job when it comes to compliance—and helps you reestablish security during and after an attack. The data collected by the solution simplifies SBOM and other reporting requirements. The secure baseline you create helps implement Zero Trust faster and automate certificate issuance, renewal, and revocation. And you can tailor the solution to specific requirements, best practices and lessons learned.

The thing to know more than anything, though, is that while you're looking at a huge initiative that could take months of focused, all-hands manual effort on your part, automation is ready to do the job in an afternoon. Automation never sleeps. It never wonders what to do. And it never makes mistakes. To see a demonstration or ask one of our experts for advice on CMMC, Zero Trust, software supply chain compliance or to otherwise put a halo on the good work you do, contact SteelCloud today.

About SteelCloud

SteelCloud's patented ConfigOS software is the industry leader for automating STIG, CIS and CMMC compliance, detecting vulnerabilities, and remediating issues. With ConfigOS, weeks of manual work is completed in about an hour. Better yet, maintaining secure baselines is effortless, providing a strong foundation for Zero Trust and other emerging cybersecurity initiatives in the government and DIB. SteelCloud makes hard things—and hardening things—simple. For more information call (703) 674-5500, email info@steelcloud.com or visit www.steelcloud.com.

SteelCloud

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