SOLUTION BRIEF

ReversingLabs

NIST, ISO, FFIEC, and HITRUST: Guide to following C-SCRM best practices

80%

of organizations discovered vulnerabilities or attacks in their software supply chain[1]

70%

of companies lack polices for securing open source[2]

NIST, ISO, FFIEC, HITRUST

have new software supply chain security guidelines

The Rise of Supply Chain Attacks and The Impact on Risk and Compliance

According to Sonatype, in 2022 software supply chain attacks increased by 633% with 80% of organizations discovering vulnerabilities or attacks throughout their supply chain[1]. However, Dynatrace's recent survey indicates that 70% of companies lack the proper policies to securely operate and monitor open source and third party tools[2].

Software supply chain attacks are becoming increasingly common while organizations lack proper security measures to protect themselves from this threat. To support enterprises against this growing threat, NIST, ISO, HITRUST, and FFIEC have all released key practices and requirements for software supply chain security.

Software supply chain attackers occur when malicious actors modify code to insert active threats in open source or third party software components. When users update or integrate these components, active threats enter their environment. Because of this, each mandate outlines how to avoid downloading or updating components containing malicious code.

New Compliance Mandates for the Software Supply Chain

Security teams must identify malware and tampering, audit their attack surface, validate the integrity of all components, enforce custom policies, and receive contextual alerts to achieve supply chain compliance. As a result, these teams can prevent active threats from being deployed, understand their risk, enforce consistent and effective security standards, and quickly react to issues.

Sources:

[1] "State of Software Supply Chain Report"
https://www.sonatype.com/press-releases/2022-software-supply-chain-report

[2] "Why Software Supply Chain Attacks are Increasing"
https://www.dynatrace.com/news/blog/why-software-supply-chain-attacks-are-increasing/

These practices are listed in NIST's, ISO's, HITRUST's, and FFIEC's supply chain security guidelines and in the table below.

	NIST	FFIEC	HITRUST	ISO
Software Bill of Materials	Yes	Yes		Yes
Tampering Detection	Yes	Yes	Yes	Yes
Malware Detection	Yes	Yes	Yes	Yes
Third Party Risk Management	Yes		Yes	Yes
Contextual Alerting	Yes			
Custom Policy Enforcement	Yes	Yes	Yes	

These key practices ensure that enterprises can consistently identify their risks, active threats leading to supply chain attacks, and can react quickly to severe issues, helping them efficiently and effectively secure their components' code and protect against software supply chain attacks.

With attack vectors and compliance mandates constantly evolving, enterprises struggle to adapt their best practices and tools to address new problems and requirements. Ultimately, the legacy solutions enterprises have relied on to help address the compliance changes over the last decade are unable to scale with new rules and mandates, leaving critical gaps in the environment.

Coverage Gaps Make Compliance Challenging

Enterprises have coverage gaps as they commonly lack the proper tools to effectively understand their risks, audit their environment, and identify active threats across their software supply chain.

They typically use SAST, DAST, and SCA tools which locate vulnerabilities by evaluating source code, behaviors, and open source components, however, they fail to identify active threats embedded into their development environment. This would allow them to remove major threats before they're distributed to their users. Additionally, they only protect open source components, have limited policy customization, and may generate alerts with little to no context, providing partial coverage and inefficient security operations.

Legacy tools' limitations lead to unidentified threats, inconsistent security practices and policy enforcement, and excessive noise, causing greater risk for software supply chain attacks.

ReversingLabs Addresses Critical Coverage Gaps

The ReversingLabs Software Supply Chain Security Platform (SSCS) provides well-rounded coverage of 3rd party software and open source components. This platform enables enterprises to identify active threats, validate the integrity of product updates, and enforce custom policies to manage risks across the software supply chain.

Cybersecurity supply chain risk management (C-SCRM) is a methodology that outlines preventative security measures for supply chain attacks. SSCS provides the tools necessary for organizations of all sizes to enforce NIST C-SCRM compliance, moving beyond the capabilities of the legacy SCA, SAST, and DAST tool sets.

5 key practices for developing a C-SCRM program - inspired by NIST	**Why it's important**	**How ReversingLabs SSCS Helps**	**Where SAST, DAST, and SCA Tools Fail**
1. Know and manage critical components and suppliers	Observing all vendors and open source components	Generate an SBOM for open source and software components	SBOM does not list 3rd party software vendors
2. Establish consistent security requirements everywhere	Determine whether 3rd party software uphold your security standards	Create custom policies to assess compliance with best practices	Has built in policies with limited customization and scanning
3. Confirm the integrity of every software or tooling update	Recognize if tampering is embedded in your components	Validate software components by analyzing changes and who made them	Detects common vulnerability exploits (CVEs) but not active threats like tampering
4. Understand suspicious behaviors, what they mean, and how to react	Identify the presence, severity, and implications of active threats	Identify baseline behaviors, scan for anomalies, and find suspicious behaviors	Does not detect suspicious behaviors and codebase changes
5. Remediate the right threats efficiently by developing actionable insights and alerts	Generate alerts which allow security teams to understand issues and react in a targeted manner	Rank issues by time to resolve and severity and receive recommended steps for remediation	Provides many false positive and negative alerts with little to no context or steps for remediation

Our Software Supply Chain Security Platform (SSCS) enables teams to consistently scan and identify active threats which lead to supply chain attacks, respond to severe issues, understand their risk profile, and achieve NIST, HITRUST, FFIEC, and ISO compliance by providing greater coverage and security than SAST, DAST, and SCA tools.

ReversingLabs SSCS Features

The ReversingLabs SSCS Platform secures open source and 3rd party software components and protects organizations from persistent and major threats and risks. With a holistic approach to supply chain security, our platform enables enterprises to achieve compliance and prevent attacks.

Compliance

Achieve NIST C-SCRM, ISO and FFIEC supply chain, and HITRUST 3rd party risk management compliance.

Comprehensive Security Coverage

Monitor and secure open source and 3rd party software components to identify malicious updates and packages.

Active Threat Detection

Identify and eliminate malware and tampering before deployment.

Contextual Alerting

Ranks alerts by severity and time to resolve to help teams efficiently respond to the right threats and vulnerabilities.

Risk Auditing

Collect a software bill of materials (SBOM) and historical record to identify all 3rd party software and open source components that existed in your environment to visualize your attack surface.

Suspicious Behavior Identification

Understand baseline behaviors and identify suspicious actions and anomalies.

Policy Customization

Create custom policies to locate and prioritize threats and risks specific to your environment and enforce consistent security standards.

Get Started!

REQUEST A DEMO

www.reversinglabs.com

About ReversingLabs

ReversingLabs, the leader in software supply chain security, offers the only holistic software supply chain solution that secures 3rd party software and open source components and identifies active threats. ReversingLabs provides protection against malware and tampering in pre and active production. For more information or to schedule a demo, contact us today.

REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com