SRC CYBER SOLUTIONS LLP

A Compelling Case For Digital Supply Chain Security

SRC CYBER
SOLUTIONS LLP
CYBER RISK SOLUTIONS

srccybrsolutions.com

Achieving mastery over an enterprise's digital supply chain is a critically important goal. Before jumping int discussion on how such a journey may be embarked upon, it is worth agreeing on some basic terminology and scope. The digital supply chain has its origins from around the 2000's, in the relatively modern sense. It's been over 20 years now since we as security professionals have been including SDKs in the software code that our development teams have been writing. In fact, looking at the ACM paper from the year 2000 [1] one can easily venture a guess that SDKs existed even pre the Dot Com Boom in 1999/2000.

The digital supply chain consists of 4 pillars - APIs, Code Libraries, Operating System Libraries and Standalone software and services. We will discuss each one in detail and then link back to how one may go about building a successful program for achieving security for the digital supply chain.

APIs - APIs stand or application programmable interfaces. APIs are used for connecting control and data transfer from one resource to another. APIs are now a primary source of data transfer between pieces of software. APIs are heavily used by enterprise organizations to transfer customer data to various third party services.

Code Libraries - Code libraries are pre-packed pieces of code that expose certain easy to understand, and use, interfaces that developers can plug and ply to achieve functionality within a short period of time. Typical examples would be developers no longer have to write their own cryptographic algorithms, instead use code libraries that provide an easy way to achieve the functionality without writing code from scratch.

Operating System Libraries - Operating system libraries are functionality that is exposed by the operating system like Windows and Linux which allows the computer code crafted by developers to perform specific functions that are optimized for by the operating system. A typical example of an Operating System library would be a random number generator. Instead of the developer performing random number generation in code, they can tap into the operating system which would generate a random number with a combination of hardware and software, very efficiently.

Standalone Software and Services - The services typically fall in the bucket of kiosk based terminals which do not interact with product code. Another class of services that falls in this classification is SaaS services being employed directly through the browser of an employee, having no hooks whatsoever in the company's code base.

The path to success for a watertight digital supply chain security program is neither short, or easy. However, it is achievable and attainable with a reasonable level of effort. However, this requires focus and a minimum level of technical sophistication from an enterprise's security, ops teams as well as sufficient support from the C suite.

The risks of not doing anything, and giving in to inertia are significant. We have all seen breaches beginning with the Target breach to Solarwinds, Kaseya, Log4j and more over the years. Time and time again companies have paid the price for not having visibility, control and processes to manage their software supply chains. The revenue generating engines for each enterprise depend on competent software to keep powering the engine. Not understanding the inner workings, and simply buying cyber insurance is not a viable strategy.

Most organizations must focus on a couple of areas to understand their security posture and protect against software supply chain attacks - a) keep an inventory of the various libraries and the corresponding applications where they are used (clean and up to date CMDB for the codebase) b) include all 3rd party integrations in the overall enterprise's continuous monitoring program. In fact most healthcare organizations are aware of HiTrust guidelines and do try to align their security and audit programs with these recommendations. HiTrust clearly defines the need for constant monitoring. When dealing with similar guidelines for ISMS and QMS healthcare companies need to understand the risk exposure they have as a result of using these 3rd party building blocks in their codebase.

Managing risk for these 3rd party components is a very important part of the security and compliance processes in any enterprise. The challenges here though make it very difficult to make sure that the security and compliance teams can provide (1) sufficient coverage (2) sufficient reliability and (3) accuracy. The challenges stem from the fact that many development teams use 3rd party software in isolation from the security and compliance organizations. This is not for the lack of trying though. It is primarily the result of how organizational silos are built. The incentives for development teams are usually lined up with the need to ship better products, faster, with less bugs and more functionality. The chasm which exists between development and security and compliance is one of the primary reasons why we see that security and compliance organizations always find out later about which vendors and services are actually posing a risk to the business's revenue stream.

The benefits for any enterprise that takes a second look at making sure they have everything buttoned down is tremendous - the ability to have your cake and eat it too. It makes perfect sense to let development teams maintain their level of freedom yet at the same time provide the security and compliance teams. The risk reduction and peace of mind for security, compliance and legal teams is massive. To be able to understand whether the building blocks on which your revenue generation engine is based off, is a potential liability or an asset, is critical to the long term success of the company.

Compliance teams can respond faster to customer inquiries for security posture. The security team can have a tighter handle and make sure the attack surface is kept under tight check while the legal team can lower the liability from a data leak perspective and manage the process better by having vendors map to the various minimum criteria required for safely conducting business.

Who Will Benefit

01

Sales and Revenue Generation Teams

Riscosity helps increase the bottom-line for companies. Lowering deal close times as well as allowing customers to do more with less – maintaining small governance, risk and compliance teams yet being able to respond faster and more completely to potential due diligence questions from buyers propels sales momentum.

02

C Level Execs and Company Boards

Riscosity provides effective and clear reporting that enables executives to understand the risk posture for the company and take appropriate recommended actions in line with fiduciary responsibilities.

03

CIO's Organization, Governance, Legal and Compliance Teams

Riscosity correlates the vendors and data being exchanged with various compliance standards. This helps CIOs present an accurate picture of the organization to the board. GRC teams can cut down compliance effort by 40% using auto cataloging of vendors and compliance mapping. General Counsels can get much more accurate information in real time, and hence can evaluate liability to the company appropriately.

Value for Multiple Groups

04

CISO and Security Teams

Riscosity accelerates security reviews and helps maintain control over the security posture of the organization. Gain total, and reliable (with low false positives) coverage when analyzing and cataloging all 3rd party interactions. Automated services, with intelligent policies cut down effort needed for security teams to act quickly and generate, audit reports .

05

Development and Ops Teams

Riscosity helps Development teams identify opportunities to improve 3rd party integration points in the native codebase. With automated failover switching (to secondary services) if the primary 3rd party service provider fails, ops teams can rest easy knowing that they will not have to perform middle of the night, manual configuration changes in production environments.

Financial Industry Risk Management Use Cases

FFIEC - FIL Aug 11 2021 [1]	Understand Risks Inventory of Systems MFA, Rate Limiting
23 NYCRR 500 [2,3]	Manage Risk MFA, Rate Limiting
PCI DSS 2016v1.1 3rd Party Security Assurance [4]	Risk Assessment for 3rd Party, Nested providers - sec 3.3, 3.4 Monitor 3rd Party - sec 6.1 Network Diagrams

Specifically for APIs and 3rd Party Security

Quick Impact	Comply with Best Practices for Banking and Card Processing Industry
Free Up Cycles	Save significant manual effort on cataloging, tracking sensitive data flows
Real Time Reports	Get real time alerts if any changes occur in posture, one click report download

[1] https://www.fdic.gov/news/financial-institution-letters/2021/fil21055.html
[2] https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf
[3] https://www.okta.com/resources/whitepaper/need-to-know-nydfs/
[4] https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf