Cymulate

Securing Software Supply Chain with Continuous Security Validation

Cymulate

Table of Contents

01 Abstract

Supply chain attacks have become so prevalent that large organizations now have a dedicated budget entry for Third-Party Risk Management (TPRM) and even reached governments' awareness, leading to their inclusion in Executive orders and Standards. Published in May 2021, EO 14028 already includes an entire section on supply chain attacks prevention that led NIST to create a dedicated Software Supply Chain Security Guidance in early 2022. In June 2022, MITRE unveiled its System of Trust (SoT) Framework prototype, a comprehensive supply chain integrity evaluation framework.

This rising concern about the risks posed by software supply chains stems from the nature of the attacks, particularly their long-term effect and long-tail reach. Finding solutions that curb the risks supply chain attacks pose without slowing down the growth resulting from the ever-growing interconnection of all players in the digital realm is a conundrum the best experts are trying to solve, but, to date, no regulatory solution is in sight, and best practices are only addressing some of the issues that make software supply chain attacks such a complex risk to manage.

As legislative and advisory boards scramble to conceptualize standards and best practices for Third-Party Risk Management (TRPM), organizations can already take measures to reduce risk emanating from third parties.

In this paper, after a brief reminder of what a software supply chain is, we will briefly revisit the main reasons software supply chain attacks are gaining in popularity among cyber-attackers before delving into various aspects of what makes supply chain attacks so dangerous.

We will then broach the various regulatory and technological initiatives aiming at minimizing software supply chain attack risks and what can be done already today.

02 What is a Software Supply Chain?

The overwhelming majority of software applications are a conglomeration of hundreds or thousands of open-source software components held together by a little bit of code. In other words, developers grab significant chunks of functionality from open-source components and then implement a specific application by writing code that uses those components.

While creating applications this way is fast and much easier than building everything from the ground up, it does raise some important questions related to risk. Which components are used? Do they work correctly? Do they have security vulnerabilities? How were they tested? Are the component licenses compatible with your application license? If you find a problem in a component, are the component maintainers likely to fix it?

A software supply chain consists of everything that goes into software until the point users touch it. For example:

01 Third-party code such as open-source components often makes up the bulk of an application and must be managed appropriately.

02 First-party code is the code the vendor's developers write. Their developers are human, which means they will make mistakes that can result in quality and security problems.

Understanding the provenance of components is equally important. Where do they come from?

Developers often use a default repository, but they might not consider the security ramifications of those components.

Any container images or operating system images used to deploy applications are also part of the supply chain. These typically also contain many open-source components.

The provenance of container images is likewise essential. Did they just pull that image out of a public repository? Who built it? How did they build it? What is in it?

Configurations are another vital part of the supply chain. For example, the configuration of a container using infrastructure-as-code can have functional and security consequences. Likewise, the configuration of the open-source components you are using can be critically important.

Any APIs and protocols used or exposed are also part of the supply chain.

To complicate matters even further, all companies today have a minimum of two levels (tiers) of suppliers:

01 **Tier One:** directly contracted suppliers

02 **Tier Two:** suppliers to the Tier One suppliers

Even accurately assessing risk exposure to Tier One suppliers during the initial assessment and contracting process is insufficient to ensure watertight protection against supply chain attacks. Without running in-depth assessments of Tier Two suppliers, the risk of a cyber-attack can increase dramatically after the first few months of a contract term and can continue to increase over the life of the contract.

To make matters even worse, Tier Two suppliers can add Tier three, four, and more supplier layers, compounding the issue and rendering a comprehensive assessment virtually unattainable.

03 | Why Are Software Supply Chain Attacks So Attractive to Cyber Attackers?

In brief, there are two main reasons cyber attackers love hitching a ride on the software supply chain. They benefit from the vendor's software access privileges, and a single breach opens many doors.
Cybercriminals' supply chain attacks can yield a high return on investment. Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a threefold increase from 2021. In fact, with the global software supply chain becoming increasingly interconnected, Gartner has identified digital supply chain risk as one of its top seven security and risk management trends for 2022 and qualified it as a high momentum threat.

If the Main Lobby is Guarded, Use the Service Door

Betanews reported that cybercriminals can penetrate 93% of company networks, yet that does not necessarily mean that they can get passed the main lobby, so to speak. The difference between gaining an initial foothold and getting access to the crown jewels is basically the difference between a minor incident and a catastrophic breach.
Cymulate 2021 Ransomware survey results clearly indicate that SOC teams are learning fast how to make sure that a surface breach does not lead to a catastrophe.
In other words, as the adoption of best practices and the integration and configuration optimization of tools such as email and web gateways, WAF, EDR, etc. grows, the effectiveness of a surface breach diminishes.
This is why cyber-attackers are now focusing on supply chain attacks. Organizations need to grant access permission to SaaS and other software for their services to function properly. Hitching a ride on those suppliers' credentials gives attackers a significant advantage.

The "Hack One, Reach Many" Bonanza

Anyone who remembers SolarWinds does not need a reminder of the destructive potential of a single breach into a software supplier environment. Breaching a single such organization grants access to hundreds, thousands, or even millions of other organizations. Kaseya attack, for example, resulted in 1500 businesses being held for ransom at once. That makes suppliers a bullseye for hackers looking to exploit this incredibly efficient and potentially lucrative shortcut opportunity for hackers.

04 Why Are Software Supply Chain Attacks So Egregious?

Supply chain attacks have widespread and long-lasting consequences.
Over a year after the SolarWinds debacle, the full extent of that cyber-attack ramification is still impossible to evaluate. Even without getting into the long tail costs known victims are still uncovering, no one knows how many backdoors SolarWinds might have opened.
The odds are these yet-undiscovered backdoors allow the attackers' persistent presence on a myriad of networks.
Similarly, the long tail effect of non-malicious components such as Log4j can have a long-term domino effect if third-party software contains an unpatched Log4j library.
Despite the rapid and slightly chaotic publication of a series of patches at the end of 2021, over six months later, cyber attackers continue to scan targeted organizations for unpatched Log4j, and log4j is now included in malicious vulnerability scanning toolkits used by cyber-attackers.
Should they uncover an unpatched log4j library in software distributed to supplier customers, the consequences could be wide-ranging.

In its most recently published guideline program, Continuous Threat Exposure Management (CTEM), Gartner also recommends mapping the external attack surface and the risks associated with SaaS and software supply-chain.

	Risk category	Main Threat vectors
01	Information shared with vendors or held on behalf of your clients (as a vendor)	Targeting contractors doing work on behalf of someone else, for example, to exfiltrate protected data
02	Infrastructure or services shared with others in a combined supply chain	Targeting cloud service and managed services providers to reach multiple victims via a single entry-point
03	Purchased software, firmware, hardware, cyber-physical systems, or digital services (Risk to your own environments)	• Hijacking Updates • Undermining Code Signing • Open-Source Compromise • App Store Attacks • Code injection • Tampering
04	Sold software, firmware, hardware, cyber-physical systems, or digital services (Risk to your customers' environments)	

VirusTotal's June 2022 "Deception at Scale- How Malware Abuses Trust" report digs deeper into the techniques used in supply chain attacks, drawing a worrying picture of their efficacy and ubiquitousness. The most prevalent techniques are:

- Stealthily compromising and then using legitimate domains to distribute malware
- Stealing and then using valid signatures
- Visually mimicking legitimate applications
- Leveraging social engineering to infect legitimate app installers

05 | Understanding the Main categories of Software Supply Chain Security Risks

In its July 2001 "ICT Supply Chain Risk Management Is Mission-Critical, but Best Practices Are Just Emerging" analysis, updated in April 2022, Gartner defines four risk categories, each with an associated threat vector, as summarized in the table below.
Practically, these can be grouped into three main risk factors:

01 **Vulnerable Packages Usage:** There are two attack vectors that leverage open-source packages.

a. Exploiting unpatched vulnerabilities: Exploiting existing vulnerabilities discovered in OS packages and leveraging them to execute the attack. (i.e., Log4j).

b. Package poisoning: taking control of a popular package/public repository and stealthily injecting malicious code in the open-source packages, luring the developers or pipeline tools to add it as part of the application build process. (i.e., us-parser-js)

01 **Compromised CI/CD Pipeline:** Attackers can take advantage of privileged access, misconfigurations, and vulnerabilities in the CI/CD pipeline infrastructure and get access to the development processes and launch their attacks. A compromised tool can expose an application's source code, enable attackers to manipulate the code during the build process, and add vulnerabilities to the application (i.e., SolarWinds).

01 **Code/Artifact Integrity:** uploading harmful code to source code repositories directly impacts the artifact quality and security posture. Common issues found in most customer environments were sensitive data in code (secrets), code quality and security issues, infrastructure as code issues, container image vulnerabilities, and misconfigurations.

06 | Recent Software Supply Chain Related Regulations and Standards

As cyber-attackers weaponization of the software supply chain increases, both regulators and standards issuers are paying attention. Listed below are the main initiative currently being implemented. While valid efforts to try and tackle this growing issue, none of these initiatives currently offers a practical way to provide an effective defense against supply chain attacks. Yet, as they are likely to impact compliance rules, it is always a good idea to keep an eye on the concepts governing bodies and standards advisory boards are trying to push forward as those are likely to be incorporated into compliance requirements in the near future.

A

From NIST

As a result of its obligations delineated in EO 14028, in May 2022, NIST published its Special Publication NIST SP 800-161r1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations that introduces the concept of C-SCRM, short for Cybersecurity Supply Chain Risk Management.

The aspects it addresses are those defined in EO 14028 and listed above.

B

From MITRE

In June 2022, MITRE unveiled its prototype Supply Chain Security System of Trust (SoT) Framework to tackle the third-party threat management issue. In the absence of statistics on which to base probabilities, the crux of MITRE recommended efforts in facilitating the risk evaluation for the software supply chain revolves around a combination of extensive due diligence and obtaining a Software Bill of Materials (SBOM):

- **Extensive Due Diligence:**
  MITRE SoT delineates14 top-level decisional risk areas associated with trust that agencies and enterprises must evaluate and make choices about during the entire life cycle of their acquisition activities.
  These 14 risk areas are subdivided into around 200 risk sub-areas evaluated with the help of about 2200 questions that aim to provide a scalable, repeatable, evidence-based, and customizable supply chain risk assessment process.
  The lion part of these questions is related to non-digital related due diligence questions related to the supplier's reliability from multiple angles, ranging from financial stability to organizational stature, external influence, and maliciousness, and including organizational security. All these aspects remain relevant when evaluating a software supplier.
- **SBOMs:**
  defined in EO 14208 section 4 as "a formal record containing the details and supply chain relationships of various components used in building software," SBOMs reflect the reality that software developers and vendors often create products by assembling existing open source and commercial software components, which justifies the requirement of a list of components similar to a list of ingredients on food packaging.
- As the generic idea behind SBOMs is to ensure that the IT and SOC teams have full visibility into the components. As the SBOM format is not yet standardized, a section about the elements, advantages, and limitations of SBOMs is expanded upon below.

C

From the White House

The growing criticality of securing software supply chains is also glaringly apparent in the attention it directly received from the White House.
Promulgated in February 2021, EO 14017 on "America's Supply Chains" that, though focused mainly on physical supply chains, includes a request for a report on supply chains for critical sectors and subsectors of the information and communications technology (ICT) industrial, including the industrial base for the development of ICT software, data, and associated services.
Executive Order 14028 on Improving the Nation's Cybersecurity, promulgated in May 2021, includes an entire section devoted exclusively to "Enhancing Software Supply Chain Security", the bulk of which requires NIST to devise and publish guidelines (See Annex 1).

As we can see, legislative and advisory boards' recommendations are still at an early stage. Though it augurs well that the problem is identified and in the process of being tackled, it provides limited help today.
As we can see, the process of securing software supply chains is still a work in progress at the highest level, and, though it is evolving fast, it is far from being crystallized. This means that individual organizations need to fully understand the nature of the risk posed by software supply chains and prioritize their integration of best practices in line with this rising threat to their integrity.

07 | Understanding CISA's SBOMs

As the legislation regarding SBOM is still a work-in-progress, and the integration of SBOMs into a cyber-defense array is an emerging field, it helps to understand in-depth what SBOM should include, how they can help and what their limitations are.

A

SBOM Elements

As its name indicates, a Software Bills of Materials is a list of all the software components.

Minimum Required

The NTIA (National Telecommunications and Information Administration) defines the SBOM minimum constitutive elements as:

- Data Fields: Documenting baseline information about each component that should be tracked
- Automation Support: Allowing for scaling across the software ecosystem through automatic generation and machine readability
- Practices and Processes: Defining the operations of SBOM requests, generation, and use

Those are reflected in NIST recommendations.

B

SBOM Benefits

SBOMs help organizations determine if they are susceptible to security vulnerabilities previously identified in software components, whether those components are internally developed, commercially procured, or open-source software libraries.
SBOMs generate and verify information about code provenance and relationships between components, which helps software engineering teams detect malicious attacks during development and deployment.

Log4j is the most famous recent example of the importance of an SBOM for all third-party software and applications used by an organization. Without such documentation, developers are unable to identify applications using the infected library and map vulnerable dependencies. When such zero-day high-risk vulnerabilities are uncovered, a fast response time is crucial to mitigate the potential damage, and an SBOM optimizes and accelerates security teams' work.
SBOMs also increase efficiency by connecting open source and third-party software. While every organization uses the same components, each organization scans for vulnerabilities and analyzes compliance risks separately. SBOMs' common infrastructure and data exchange format could save companies time by creating greater collaboration between organizations.

C

SBOM Limitations

As pointed out by Robert Martin during CAPEC Summit, despite their undeniable value, SBOMs lack some critical elements. It neither detects potential breaches at the supply chain level nor includes immediate disclosure of such a breach when detected by the supplier. SBOMs would help for emerging critical vulnerabilities such as Log4j, as the end-users could immediately see that the supplied software is at risk of being impacted by a newly publicized vulnerability and could therefore patch in time.

Yet, for a SolarWinds type of attack, the SBOM would be of little to no use, as the stealth techniques used by the attacker would not show up on that list. Nor would it be of much use to protect against supply chain vulnerabilities such as Follina, for which a patch is still missing two weeks after the vulnerability publication.

This would require obligating suppliers to integrate continuous security validation and provide their live security posture score to their users. At this stage, such capabilities are not on the horizon, but, in time, they might be considered for inclusion in the organizational security part of MITRE SoT.

In the age of agile development, SBOMs cannot anymore remain static documents. Every new deployment or update should be accompanied by a new SBOM.
This means that the effectiveness of SBOMs is directly proportional to the effective integration of SBOM generation and management tools that integrate SBOM functionality into software development at the vendor end and integrate with vulnerability management solutions at the user end.

08 What Can You Do Today to Insulate Against Software Supply Chain Attacks?

Despite their current limitations, it is a good idea to start by following legislative and advisory boards' recommendations that center around:

A

SBOMs

Obtaining an exhaustive Software Bills of Materials from the supplier is undoubtedly a major improvement in gaining visibility into the third-party service.
Yet, to maximize the efficiency of incorporating SBOMs in third-party services evaluation and integration in the overall security posture evaluation, it is crucial to fully understand its benefits and, more importantly, its limitations, as expanded upon above.

B

Risk evaluation

running an in-depth due diligence process on prospective (and existing) suppliers.
In addition to classic non-technical due diligence verification such as the provider's company financial health, team composition, churn, and more, there are tests that can be run to evaluate their security posture.

- Running a recon test to check whether their external attack surface is porous. Cymulate EASM module can provide an instant evaluation.
- Requiring a free trial and running security validation assessment on your environment before and during the free trial to see if it introduces new security gaps.
- Ask vendors to run security validation assessments and provide a detailed report.

C

Risk reduction

Even with thorough risk evaluation, the fluid nature of agile development implies that new security gaps can appear in the third-party service after the initial assessment is completed. There are a few measures that can be implemented with all suppliers to preemptively reduce exposure and increase resiliency:

- Minimize the number of people involved in installing, configuring, and using the service.
- Include the third-party provider in response and remediation plans.
- Strictly limit access to sensitive data on a need-to-know basis.
- Immediately remove access to sensitive data to reflect evolving SLAs or contract termination.
- Require the third-party supplier to run continuous security validation in their own environment and provide frequent reports of the resulting security posture scores, and include a minimum security-score threshold in the SLA (Note: at time of writing, this is realistically achievable only for large contracts, but as continuous security validation processes become more widely adopted, it will gradually become easier.)

09 | How XSPM Platform Can Increase Software Supply Chain Risk Resilience

Cymulate's Extensive Security Posture Management platform can assist in both risk evaluation and risk reduction.

Third-Party Risk Management Stages

Software Supplier Risk Evaluation

Cymulate's External Attack Surface Managment (EASM) module can identify all the software supplier exposed assets and evaluate how resilient those exposed assets are to attacks attempting to use them to gain an initial foothold.
Though this gives only a partial evaluation of the overall security posture of the software supplier, finding out at that stage that a prospective software supplier is derelict in securing its external attack surface clearly indicates that security is not their top priority.
Assess the impact of running a free trial of the prospective software by running an assessment before and during the free trial to see if it opens new security gaps.
When evaluating multiple candidates for a service, this can be performed for each candidate at no extra cost, which facilitates including a security score in the comparative process between prospective suppliers.
Conditional to the prior agreement of the software supplier, Cymulate can run a combination of agent-based emulated attacks (BAS) and red teaming campaigns to assess their:

- Security controls resilience
- SIEM and SOAR efficacy
- Overall security posture

The software supplier infrastructure evaluation scope needs to be agreed upon and confirmed in writing and coordinated with Cymulate team to enable Cymulate to run assessments on their infrastructure.

Software Supplier Risk Reduction

Running Cymulate XSPM platform already provides built-in software supplier risk reduction as the off-the-shelf attack templates are designed to identify security gaps, whether native or imported.
In addition to continuously validating the security posture of your own organization, as the only continuous security validation platform to offer modular access to comprehensive Breach and Attack Simulation (BAS), Red Teaming Campaign Automation, and Advanced Purple Teaming Framework, Cymulate enables your SOC team to:

- **Create and Run Software Supplier Specific Security Validation & Optimization Scenarios**
  Cymulate is the only continuous security validation platform with the integrated ability to launch production-safe emulated attacks to assess resilience against specific attack tactics, techniques, and processes, assuming the attacker has already gained an initial foothold.
  Depending on the access rights granted to a software supplier, this unique ability makes it easy to assess the potential damage an attacker could potentially inflict by launchin an emulated attack array from the software supplier access point or points.
  This opens the door to an exact evaluation of the potential risks of an attacker hitching a ride on that software supplier's access privileges.

- **Use the zero-code purple teaming framework to design custom-made attack templates**
  Cymulate's Advanced Purple Teaming Framework provides an extensive collection of customizable advanced scenarios with a rich library of widgets to create customized scenarios mimicking attacks using privilege access granted to the software supplier to map potential attack routes and preemptively set up compensating security controls.
  Ideally, require the software supplier to integrate Cymulate XSPM in their own environment and share up-to-date security scores at regular intervals.

For more information about Cymulate:

- Download the XSPM Overview eBook
- Download the Continuous Threat Exposure Management eBook
- Book a free trial

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data.
Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931, 7546302, Israel | +972 3 9030732 | info@cymulate.com

10 Annex 1 – Extract of Executive Order 14028, Section 4

Executive Order 14028, Section 4 - "Enhancing Software Supply Chain Security", requires the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, to issue guidance identifying practices that enhance the security of the software supply chain. Such guidance shall include standards, procedures, or criteria regarding:

01 secure software development environments, including such actions as:

- **a.** using administratively separate build environments;
- **b.** auditing trust relationships;
- **c.** establishing multi-factor, risk-based authentication, and conditional access across the enterprise;
- **d.** documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;
- **e.** employing encryption for data; and
- **f.** monitoring operations and alerts and responding to attempted and actual cyber incidents.

01 generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection 1) above

02 employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

03 employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

04 providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsections 3) and 4) above, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

05 maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

06 providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

07 participating in a vulnerability disclosure program that includes a reporting and disclosure process;

08 attesting to conformity with secure software development practices; and

09 ensuring and attesting, to the extent practicable, to the integrity and provenance of open-source software used within any portion of a product.

11 Annex 2 – Sources

- Anchore -2022 - 2022 Security Trends: Software Supply Chain Survey - https://anchore.com/blog/2022-security-trends-software-supply-chain-survey/
- CAPEC (Common Attack Pattern Enumeration and Classification) - 2022 - CAPEC User Summit Transcript - "Supply Chain Attacks—MITRE's System of Trust™ and CAPEC" - Robert A. Martin, The MITRE Corporation - https://capec.mitre.org/documents/summit-2022/capec-summit-2022-session-5.html
- Betanews- 2022 - 82 percent of CIOs believe their software supply chains are vulnerable - https://betanews.com/2022/05/31/82-percent-of-cios-believe-their-software-supply-chains-are-vulnerable/
- Betanews – 2022 - Cybercriminals can penetrate 93 percent of company networks - https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/
- CISO Online – 2022 - Software supply chain attacks hit three out of five companies in 2021 - https://www.csoonline.com/article/3650034/software-supply-chain-attacks-hit-three-out-of-five-companies-in-2021.html
- Cymulate – 2022 - The Quickest Way to Comply with NIST Revision 5 - https://cymulate.com/blog/comply-nist-revision-5/
- DarkReading – 2022 – MITRE Creates Framework for Supply Chain Security - https://www.darkreading.com/application-security/mitre-creates-framework-for-supply-chain-security
- Forbes – 2022 - The State of Security 2022: To Address Supply Chain Risks, Build An SBOM - https://www.forbes.com/sites/splunk/2022/04/12/the-state-of-security-2022-to-address-supply-chain-risks-build-an-sbom/?sh=69bca6b155e6
- Gartner – 2022 revision – ICT Supply Chain Risk Management Is Mission-Critical, but Best Practices Are Just Emerging - https://www.gartner.com/en/documents/4003317
- Gartner - 2022 - Implement a Continuous Threat Exposure Management (CTEM) Program - https://www.gartner.com/doc/4016760?ref=AnalystProfile&srcId=1-4554397745
- Homeland Security Today – 2022 -SUBJECT MATTER AREA CYBERSECURITY FEDERAL GOVERNMENT - State of Cyber and IT: Industry Partners Critical in Achieving Better Supply Chain Cybersecurity, Says DHS CIO2 - https://www.hstoday.us/federal-pages/dhs/state-of-cyber-and-it-industry-partners-critical-in-achieving-better-supply-chain-cybersecurity-says-dhs-cio/
- IT Supply chain – 2022 – Six Month Later – Has the Log4j threat disappeared? Data says no - https://itsupplychain.com/six-months-later-has-the-log4j-threat-disappeared-data-says-no/
- Infosecurity– 2022 – Only more secure coding can protect the software supply chain - https://www.infosecurity-magazine.com/opinions/secure-coding-software-supply-chain/
- MITRE -2022 - MITRE'S NEW "SYSTEM OF TRUST" PROTECTS VULNERABLE SUPPLY CHAINS - https://www.mitre.org/news/press-releases/mitre-new-system-of-trust-protects-vulnerable-supply-chains
- NIST – 2002 - - NIST Special Publication NIST SP 800-161r1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
- NIST – 2022 - NIST Updates Cybersecurity Guidance for Supply Chain Risk Management - https://www.nist.gov/news-events/news/2022/05/nist-updates-cybersecurity-guidance-supply-chain-risk-management
- NIST – 2022 - Software Supply Chain Security Guidance: Attesting to Conformity with Secure Software Development Practices - https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/software-supply-chain-security-guidance-1
- NIST – 2021 - Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order - https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
- PwC – 2022 - 2022 Global Digital Trust Insights Survey - https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html
- SEC - 2022 - Statement on Proposal for Mandatory Cybersecurity Disclosures - https://www.sec.gov/news/statement/gensler-cybersecurity-20220309
- SEC - 2022 – Fact Sheet: Public Company Cybersecurity; Proposed Rules - https://www.sec.gov/files/33-11038-fact-sheet.pdf

01 | Annex 2 – Sources

- Security Boulevard – 2022 - MITRE's System of Trust: A proposed standard for software supply chain security - https://securityboulevard.com/2022/06/mitres-system-of-trust-a-proposed-standard-for-software-supply-chain-security/
- Security Magazine – 2022 - A focus on risk in software supply chain security - https://www.securitymagazine.com/articles/97795-a-focus-on-risk-in-software-supply-chain-security
- Security Week – 2022 - Cyber Insights 2022: Supply Chain - https://www.securityweek.com/cyber-insights-2022-supply-chain
- Splunk – 2022 – The State of Security 2022 - https://www.splunk.com/en_us/form/state-of-security.html#
- TechTarget – 2022 - The benefits and challenges of SBOMs - https://www.techtarget.com/searchsecurity/post/The-benefits-and-challenges-of-SBOMs
- Venafi – 2022 - CIO Study: Certificate-Related Outages Continue to Plague Organizations - https://www.venafi.com/resource/CIO-Study-Certificate-Related-Outages-Continue-to-Plague-Organizations#
- US GAO - 2022 - Business Systems: DOD Needs to Improve Performance Reporting and Cybersecurity and Supply Chain Planning - https://www.gao.gov/products/gao-22-105330
- VirusTotal – 2022 - Deception at Scale- How Malware Abuses Trust - https://blog.virustotal.com/2022/08/deception-at-scale.html
- White House – 2021 – EO 14017 – Executive Order on America's Supply chain - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
- White House – 2021 – EO 14028 Executive Order on Improving the Nation's Cybersecurity - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/