SecDes

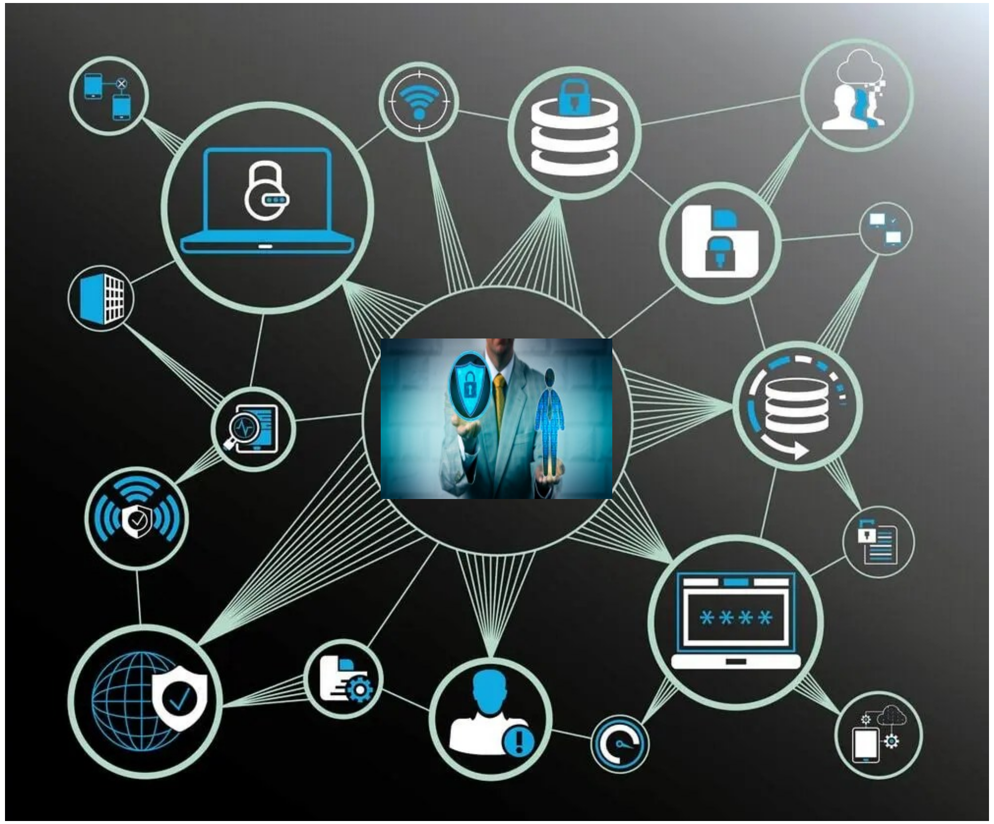
Software supply chain security, NIS2 and SBOM

TATIANA GALIBUS

CYBERSECURITY AMBASSADOR

innovation
forward

Takeaways



1. Start from the inventory and right questions.
2. Apply mitigations on 3 levels
   - Have clear list of requirements, procedures and policies (buyer`s guide)
   - Technical measures: SBOM+DevSecOps+physical measures
   - 3S of software supply chain

3. Comply with NIS 2 Directive – 18 October 2024

4. Digital services have to register in December 2024

innovation
forward

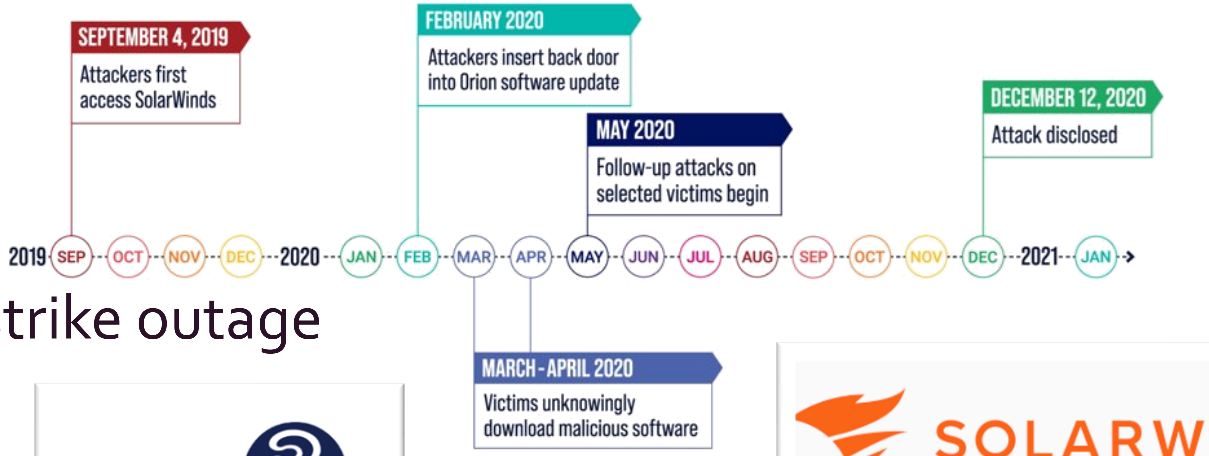
Supply chain security

Part of supply chain management that focuses on the risk management of external suppliers, vendors, logistics and transportation.

Identify, analyze and mitigate the risks inherent in working with other organizations as part of a supply chain.

Physical security and cybersecurity.

Threats


SEPTEMBER 4, 2019
Attackers first access SolarWinds
FEBRUARY 2020
Attackers insert back door into Orion software update
MAY 2020
Follow-up attacks on selected victims begin
DECEMBER 12, 2020
Attack disclosed
2019 SEP OCT NOV DEC 2020 JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC 2021 JAN
MARCH - APRIL 2020
Victims unknowingly download malicious software

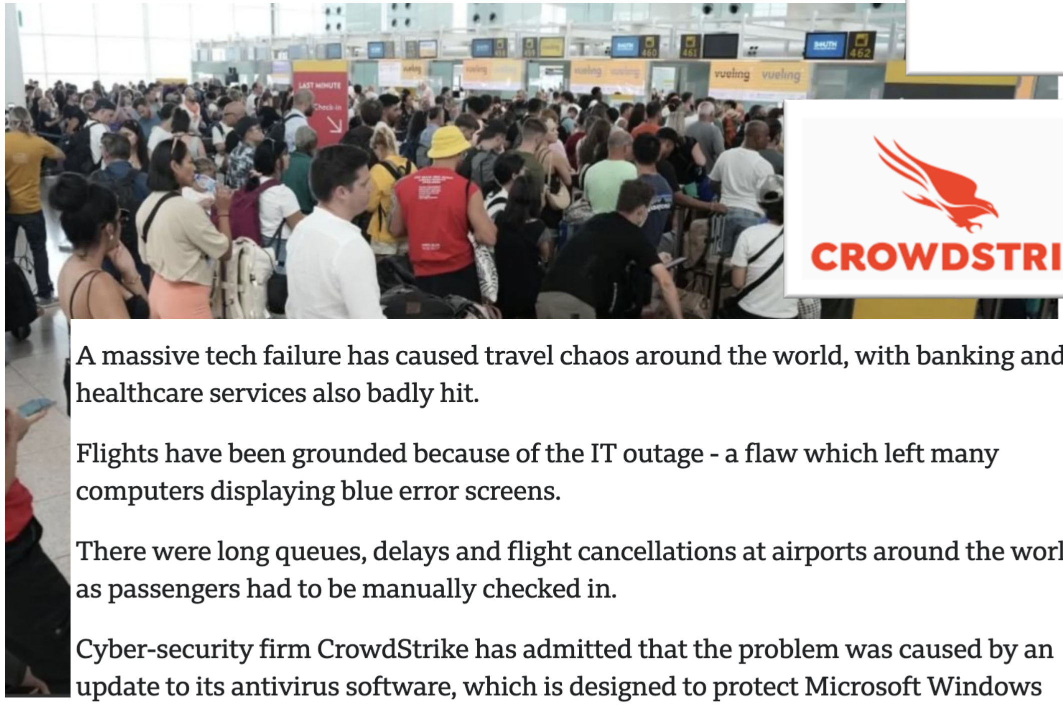
Solarwinds attack , Log4j, Crowdstrike outage

- Complexity, digitalization

LOG4J

SOLARWINDS

CROWDSTRIKE

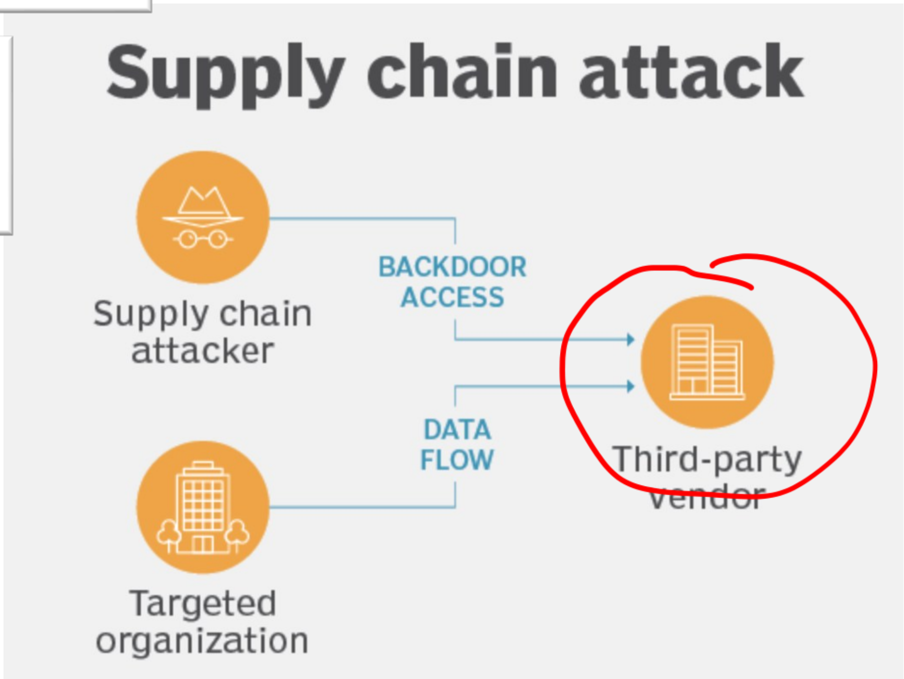


A massive tech failure has caused travel chaos around the world, with banking and healthcare services also badly hit.

Flights have been grounded because of the IT outage - a flaw which left many computers displaying blue error screens.

There were long queues, delays and flight cancellations at airports around the world, as passengers had to be manually checked in.

Cyber-security firm CrowdStrike has admitted that the problem was caused by an update to its antivirus software, which is designed to protect Microsoft Windows devices from malicious attacks.

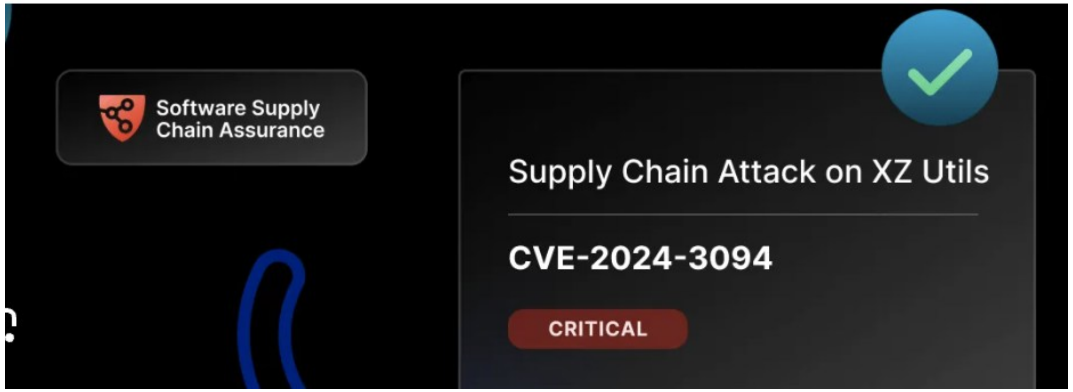


CVE-2024-3094 The targeted backdoor supply chain attack against XZ and liblzma

HTTPS://WWW.SONATYPE.COM/BLOG/CVE-2024-3094-THE-TARGETED-BACKDOOR-SUPPLY-CHAIN-ATTACK-AGAINST-XZ-AND-LIBLZMA

XZ Utils

one of the more complicated benevolent stranger malware injections to date, and deserves amplification.



Software Supply Chain Assurance

Supply Chain Attack on XZ Utils

CVE-2024-3094

CRITICAL

widely used components,
often
maintained by overworked and
underfunded teams, can
become entry points for malicious code.

uncovered by a curious developer who noticed that their ssh login was taking 500ms instead of 100ms.

Attack scenarios

Cyber-physical attack:

- IoT-based autonomous systems…

Data breaches

- General Data Protection Regulation (GDPR) non-compliance

Supply chain impersonation attack

- Impersonating trusted entity

Business identity theft

- Voice, credentials, video

What`s inside supply chain?

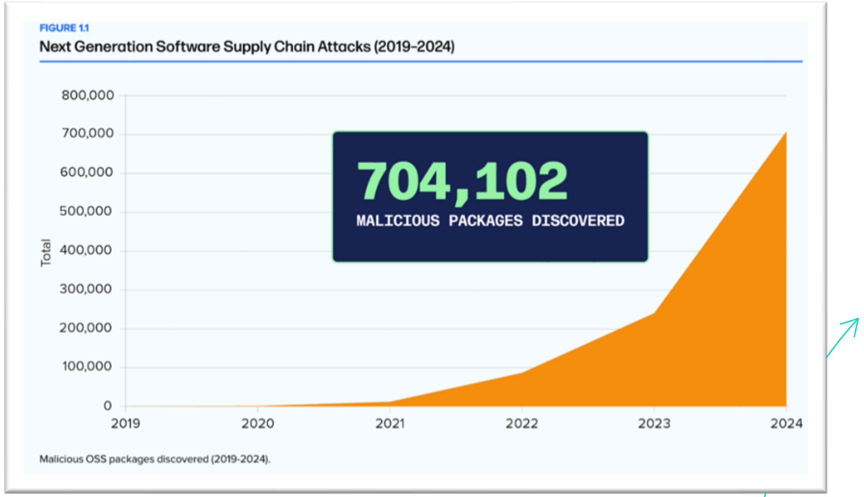


FIGURE 1.1

Next Generation Software Supply Chain Attacks (2019-2024)

Malicious OSS packages discovered (2019-2024).

Business continuity, safe operation

Data sharing - > 583 third parties in the supply chain

Business identity and trusted relationships

Challenges to SCC (supply chain cybersecurity)

Limited resources for cybersecurity

Different countries with disparate national legislations

Lack of transparency

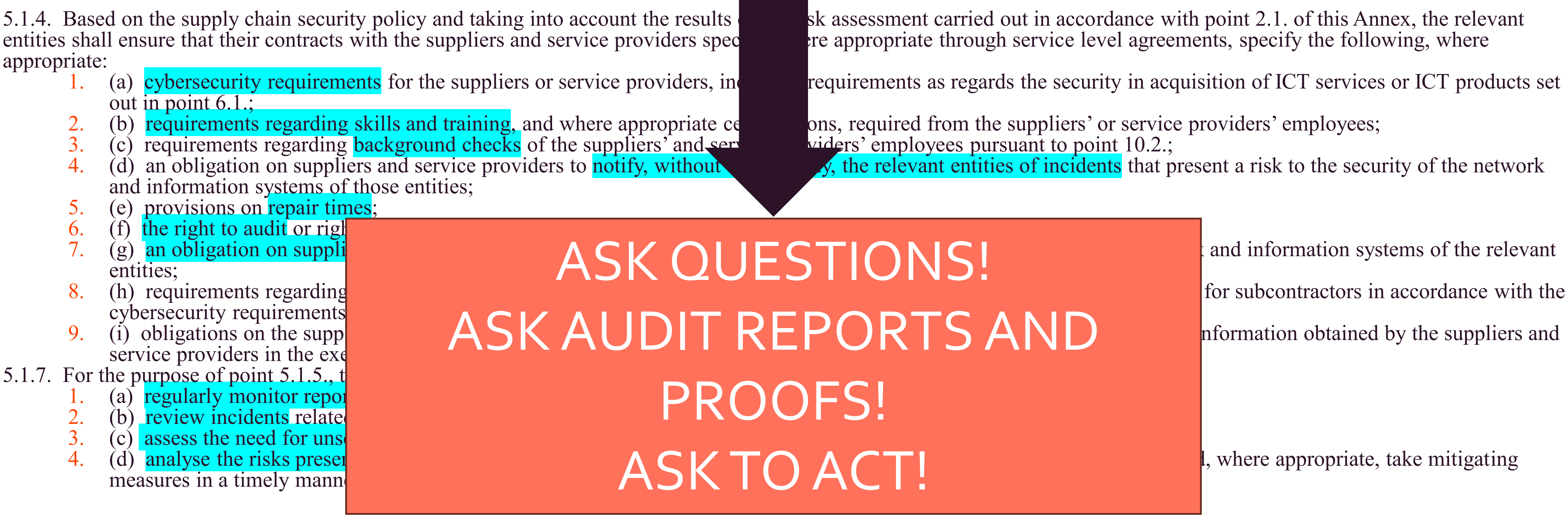
Finding solutions in supply chain security

- NIS2 obligations
- Buyer`s guide
- 3S of supply chain security

innovation
forward

How NIS2 supports you? Know your rights!

LEGISLATIONS AND OBLIGATIONS – FOR ICT SUPPLY CHAIN



5.1.4. Based on the supply chain security policy and taking into account the results o sk assessment carried out in accordance with point 2.1. of this Annex, the relevant entities shall ensure that their contracts with the suppliers and service providers spec re appropriate through service level agreements, specify the following, where appropriate:

1. (a) cybersecurity requirements for the suppliers or service providers, in requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1.;
2. (b) requirements regarding skills and training, and where appropriate ce ons, required from the suppliers' or service providers' employees;
3. (c) requirements regarding background checks of the suppliers' and ser viders' employees pursuant to point 10.2.;
4. (d) an obligation on suppliers and service providers to notify, without y, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;
5. (e) provisions on repair times;
6. (f) the right to audit or righ
7. (g) an obligation on suppli t and information systems of the relevant entities;
8. (h) requirements regarding for subcontractors in accordance with the cybersecurity requirements
9. (i) obligations on the supp nformation obtained by the suppliers and service providers in the exe

5.1.7. For the purpose of point 5.1.5., t

1. (a) regularly monitor repo
2. (b) review incidents relate
3. (c) assess the need for uns
4. (d) analyse the risks prese l, where appropriate, take mitigating measures in a timely mann

ASK QUESTIONS!

ASK AUDIT REPORTS AND PROOFS!

ASK TO ACT!

innovation forward

Buyer`s guide for software - 1

14 QUESTIONS FROM AGORIA: HTTPS://WWW.AGORIA.BE/NL/DIENSTEN/EXPERTISE/DIGITALISERING/CYBERSECURITY/BUYERS-GUIDE-SOFTWARE-SUPPLY-CHAIN-RISICOBEHEERSING

Security policy

- Do you have a formal security policy that is communicated and known?

Information Security Management System (ISMS):

- Do you follow the measures of a recognized ISMS framework, such as ISO27001, for example? Are you certified for this? Since when?

Incident Response:

- How do you respond to security incidents? Do you have a formal Incident Response plan? A Disaster Recovery plan? What is the potential impact on us as customers if you face a ransomware attack or hacking? Do you systematically inform your customers in the event of an incident?

Buyer`s guide for software - 2

14 QUESTIONS FROM AGORIA: HTTPS://WWW.AGORIA.BE/NL/DIENSTEN/EXPERTISE/DIGITALISERING/CYBERSECURITY/BUYERS-GUIDE-SOFTWARE-SUPPLY-CHAIN-RISICOBEHEERSING

Training:

- Does your development team receive regular training to keep abreast of the latest cyber threats and security practices in software? Is your development team trained to develop software according to the OWASP Secure Coding Best Practices?

Development methodology:

- Do you use a secure development life cycle (SDLC) methodology? How do you do quality assurance? Do you guys do threat modeling?

Automatic code review:

- Do you conduct regular code reviews? Do you use automated static code analysis tools to identify vulnerabilities?

Buyer`s guide for software - 3

14 QUESTIONS FROM AGORIA: HTTPS://WWW.AGORIA.BE/NL/DIENSTEN/EXPERTISE/DIGITALISERING/CYBERSECURITY/BUYERS-GUIDE-SOFTWARE-SUPPLY-CHAIN-RISICOBEHEERSING

Penetration testing:

- Do you perform penetration tests on your software products? If so, how often and are they performed internally or by outside parties? Do you have a Responsible Disclosure program?

Dependency tracking:

- In what ways do you ensure the security of external components or libraries used in your software? How do you ensure they are upto-date and secure?

Security updates:

- Do you have a procedure for timely updating and patching of software in response to discovered vulnerabilities? How do you communicate with customers about important security updates and patches? How long do you guarantee us security updates and patches?

Buyer`s guide for software - 4

14 QUESTIONS FROM AGORIA: HTTPS://WWW.AGORIA.BE/NL/DIENSTEN/EXPERTISE/DIGITALISERING/CYBERSECURITY/BUYERS-GUIDE-SOFTWARE-SUPPLY-CHAIN-RISICOBEHEERSING

Data storage and processing:

- Where and how is customer and user data stored and processed? Do you use data encryption? Does this comply with regional and international privacy laws?

Data access:

- How is access to customer and user data controlled by software developers and support personnel?

Software integrity:

- How do you ensure the integrity of your software throughout the development, distribution and update process? What tools and processes do you employ to ensure that the software that reaches the end user is authentic and unaltered?

Buyer`s guide for software - 5

14 QUESTIONS FROM AGORIA: HTTPS://WWW.AGORIA.BE/NL/DIENSTEN/EXPERTISE/DIGITALISERING/CYBERSECURITY/BUYERS-GUIDE-SOFTWARE-SUPPLY-CHAIN-RISICOBEHEERSING

Access to code:

- Do you have measures and procedures in place to ensure that only the software developers involved have access to the source code, and no one else?

Security Audits:

- Does your software regularly undergo security audits by outside organizations?

How to implement supply chain security

SOLUTIONS ARE THERE

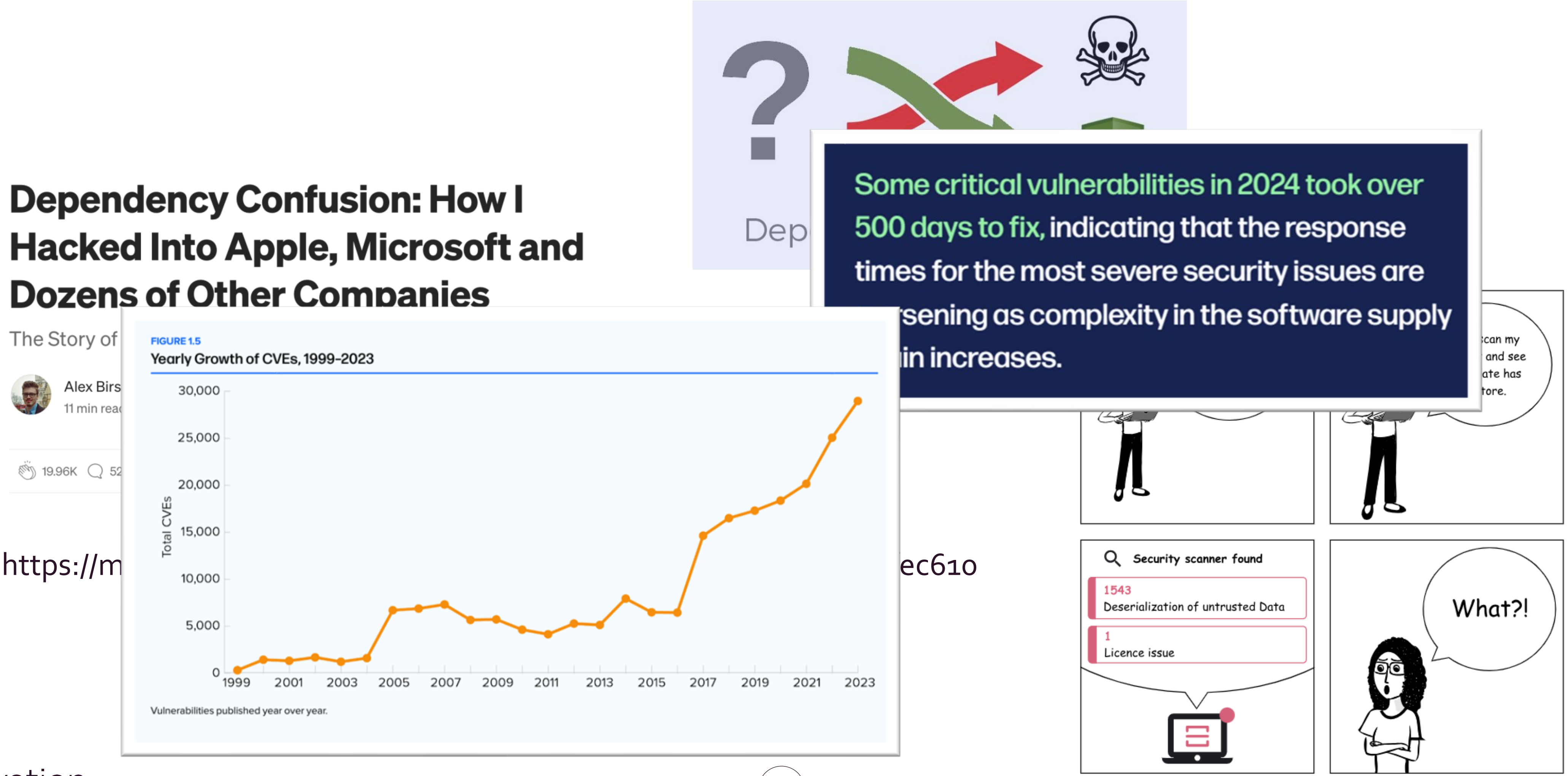
Controls	Tools
1. Policy and strategy, Risk management, mitigating the risks from outside threats	NIST cybersecurity supply chain risk management: https://csrc.nist.gov/projects/cyber-supply-chain-risk-management Threat modelling
2. Components analysis Checking the code not written by you con	SBOM (software bill of materials), Inventory
3. S into pip	
4. P	

6.1.2. For the purpose of point 6.1.1., the processes and procedures referred to in point 6.1.1. shall include:

1. (a) security requirements to apply to the ICT services or ICT products to be acquired;
2. (b) requirements regarding security updates throughout the entire lifetime of the ICT services or ICT products, or replacement after the end of the support period;
3. (c) information describing the hardware and software components used in the ICT services or ICT products;
4. (d) information describing the implemented cybersecurity functions of the ICT services or ICT products and the configuration required for their secure operation;
5. (e) assurance that the ICT services or ICT products comply with the security requirements according to point (a);
6. (f) appropriate methods for validating that the delivered ICT services or ICT products are compliant to the stated security requirements, as well as documentation of the results of the validation.

Software composition analysis:

ARE YOUR DEPENDENCIES SECURE?



Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of

Alex Birs

11 min rea

19.96K 52

https://m

ec610

FIGURE 1.5

Yearly Growth of CVEs, 1999-2023

Vulnerabilities published year over year.

Some critical vulnerabilities in 2024 took over 500 days to fix, indicating that the response times for the most severe security issues are
sening as complexity in the software supply
in increases.

Security scanner found

1543
Deserialization of untrusted Data

1
Licence issue

SBOM – managing dependencies transparently

HTTPS://SYSDIG.COM/BLOG/SBOM-101-SOFTWARE-BILL-OF-MATERIALS/

A Software Bill of Materials (SBOM) is a formal record containing the details and supply chain relationships of various components used in building software. These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or cess-restricted.

In an ideal world, **every software company would attach an SBOM to each del erable**, and everyone would have full visibility to the components used in software and know exactly which vulnerab ies are impacting that software.

if package *libfoobar-1.5.3-r3-u8* is part of t ackage name, version, license, etc. used to assemble *libfoobar-1.5.3-r3-u8*, and the co n a multi-level tree where each node is decomposed into its dependencies.

Traceability
Security of components
Visibility

WHAT VULNERABILITIES IMPACT MY SOFTWARE?

Software Bill of Materials (SBOM)

What is SBOM?

A SBOM is a nested inventory, a list of ingredients that make up software components.

Allow software users and vendors to know which components are problematic and remediate

OWASP CycloneDX is a full-stack BOM standard that provides advanced supply chain capabilities for cyber risk reduction.

CycloneDX

SPDX

SWID TAGS

Traceability
Security of components
Visibility

- Other SBOM tools:
  - Anchore, Rezilion
  - FOSSA, SPDX SBOM Generator (Opensource)
  - Mend, Tern Project, TauruSeer

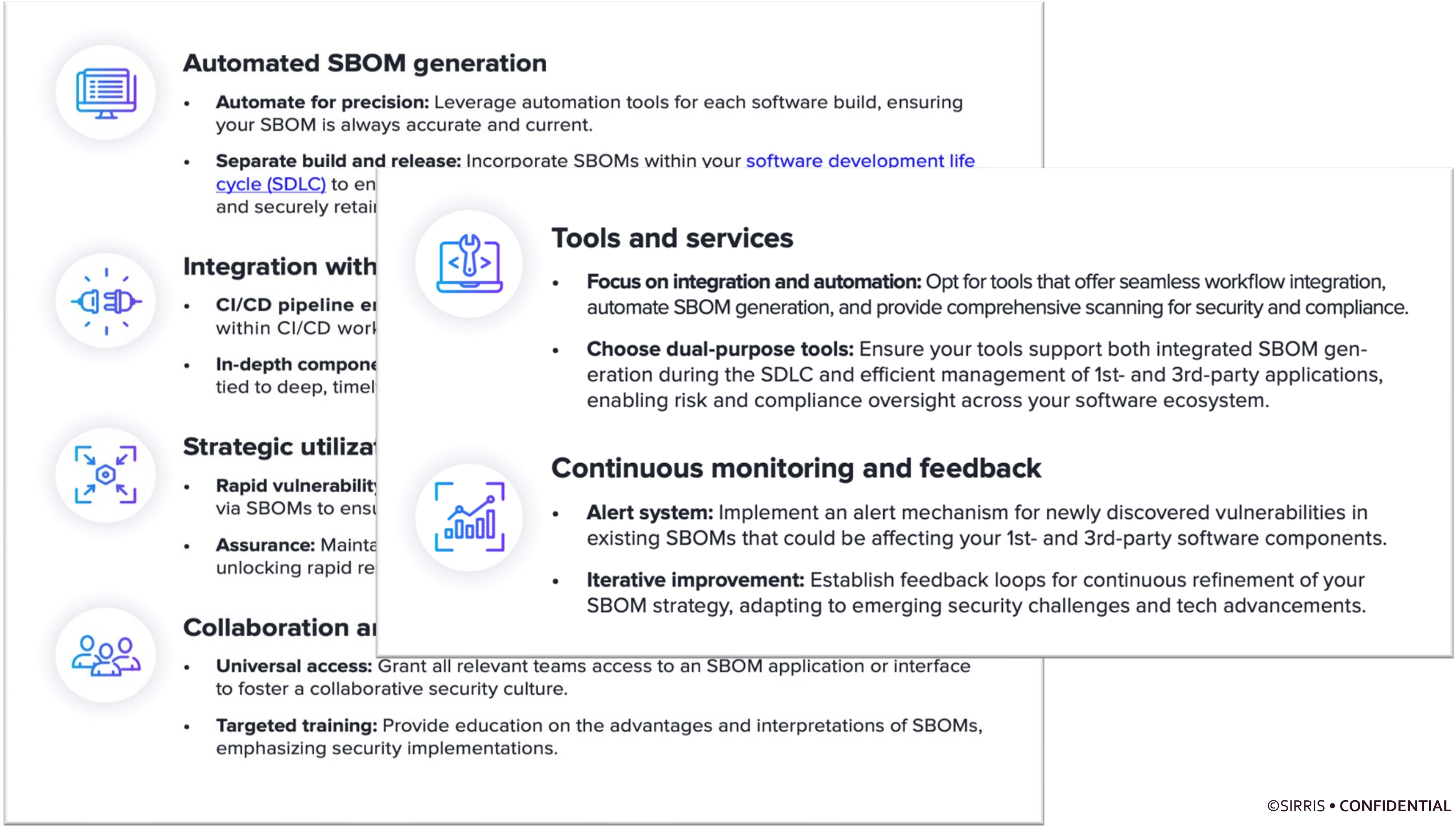
sonatype SBOM manager

JFrog

oxsecurity

SBOM cheat sheet

HTTPS://WWW.SONATYPE.COM/HUBFS/1-2023%20NEW%20SITE%20ASSETS/CHEAT%20SHEETS/SBOM_CHEAT_SHEET_REV-041724.PDF



Automated SBOM generation

- **Automate for precision:** Leverage automation tools for each software build, ensuring your SBOM is always accurate and current.
- **Separate build and release:** Incorporate SBOMs within your software development life cycle (SDLC) to en and securely retai

Integration with

- **CI/CD pipeline e** within CI/CD work
- **In-depth compone** tied to deep, timel

Strategic utiliza

- **Rapid vulnerabilit** via SBOMs to ens
- **Assurance:** Mainta unlocking rapid re

Collaboration a

- **Universal access:** Grant all relevant teams access to an SBOM application or interface to foster a collaborative security culture.
- **Targeted training:** Provide education on the advantages and interpretations of SBOMs, emphasizing security implementations.

Tools and services

- **Focus on integration and automation:** Opt for tools that offer seamless workflow integration, automate SBOM generation, and provide comprehensive scanning for security and compliance.
- **Choose dual-purpose tools:** Ensure your tools support both integrated SBOM generation during the SDLC and efficient management of 1st- and 3rd-party applications, enabling risk and compliance oversight across your software ecosystem.

Continuous monitoring and feedback

- **Alert system:** Implement an alert mechanism for newly discovered vulnerabilities in existing SBOMs that could be affecting your 1st- and 3rd-party software components.
- **Iterative improvement:** Establish feedback loops for continuous refinement of your SBOM strategy, adapting to emerging security challenges and tech advancements.

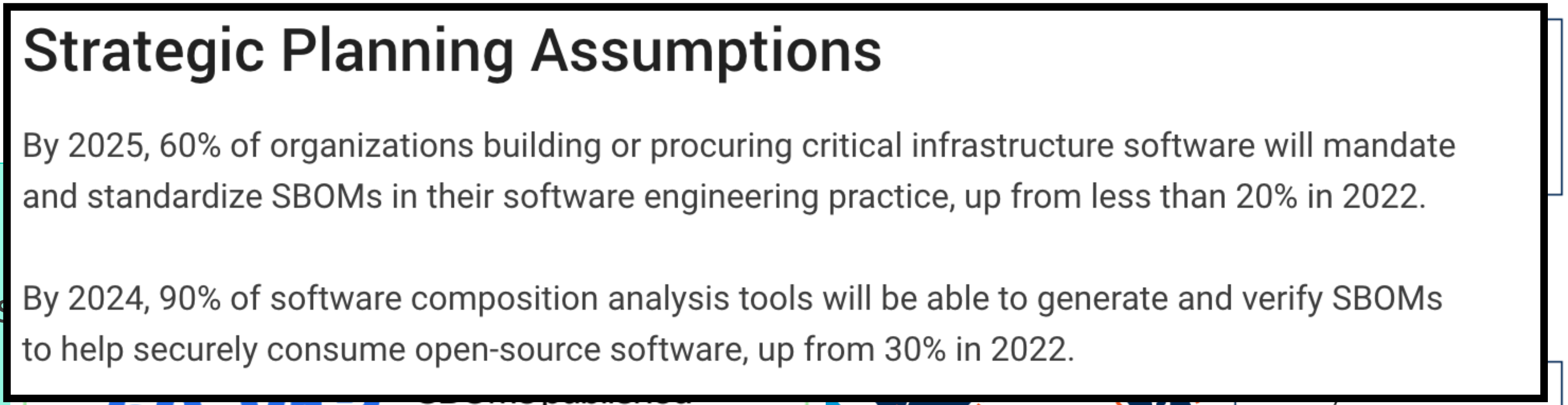
Gartner report

Keeping software bills of materials (SBOMs) data in sync with corresponding software artifacts presents a key challenge.

BUT:

projects using a Software Bill of Materials (SBOM) t manage OSS dependencie showed a 264-day reduction in mean time to remediate (MTTR) compared to those that di not.

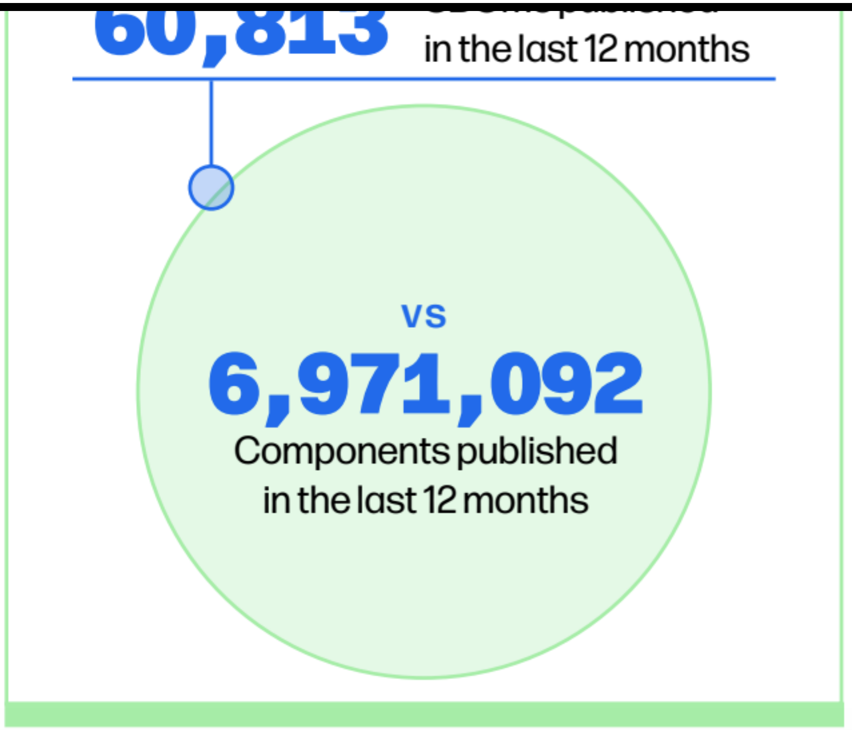
Integrate SBOM Workflows as Part of the Software Development Life Cycle

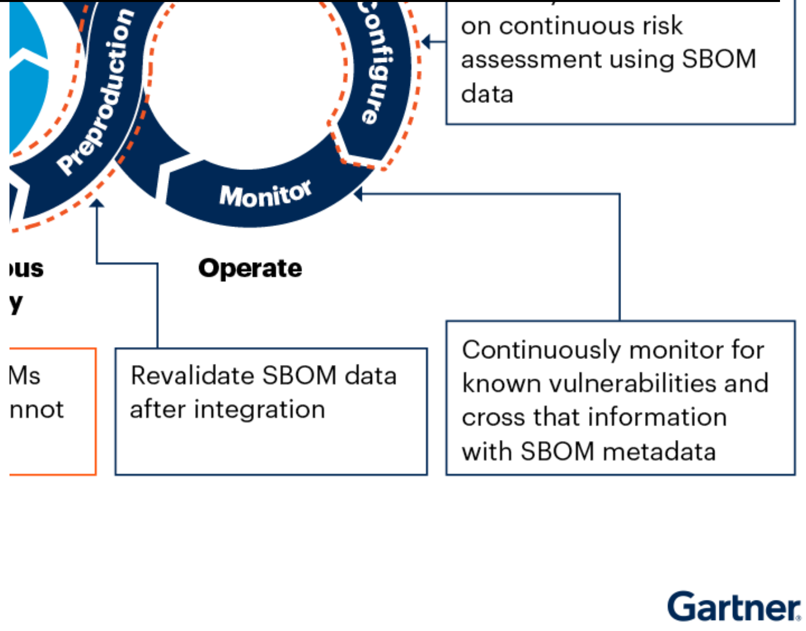


Strategic Planning Assumptions

By 2025, 60% of organizations building or procuring critical infrastructure software will mandate and standardize SBOMs in their software engineering practice, up from less than 20% in 2022.

By 2024, 90% of software composition analysis tools will be able to generate and verify SBOMs to help securely consume open-source software, up from 30% in 2022.





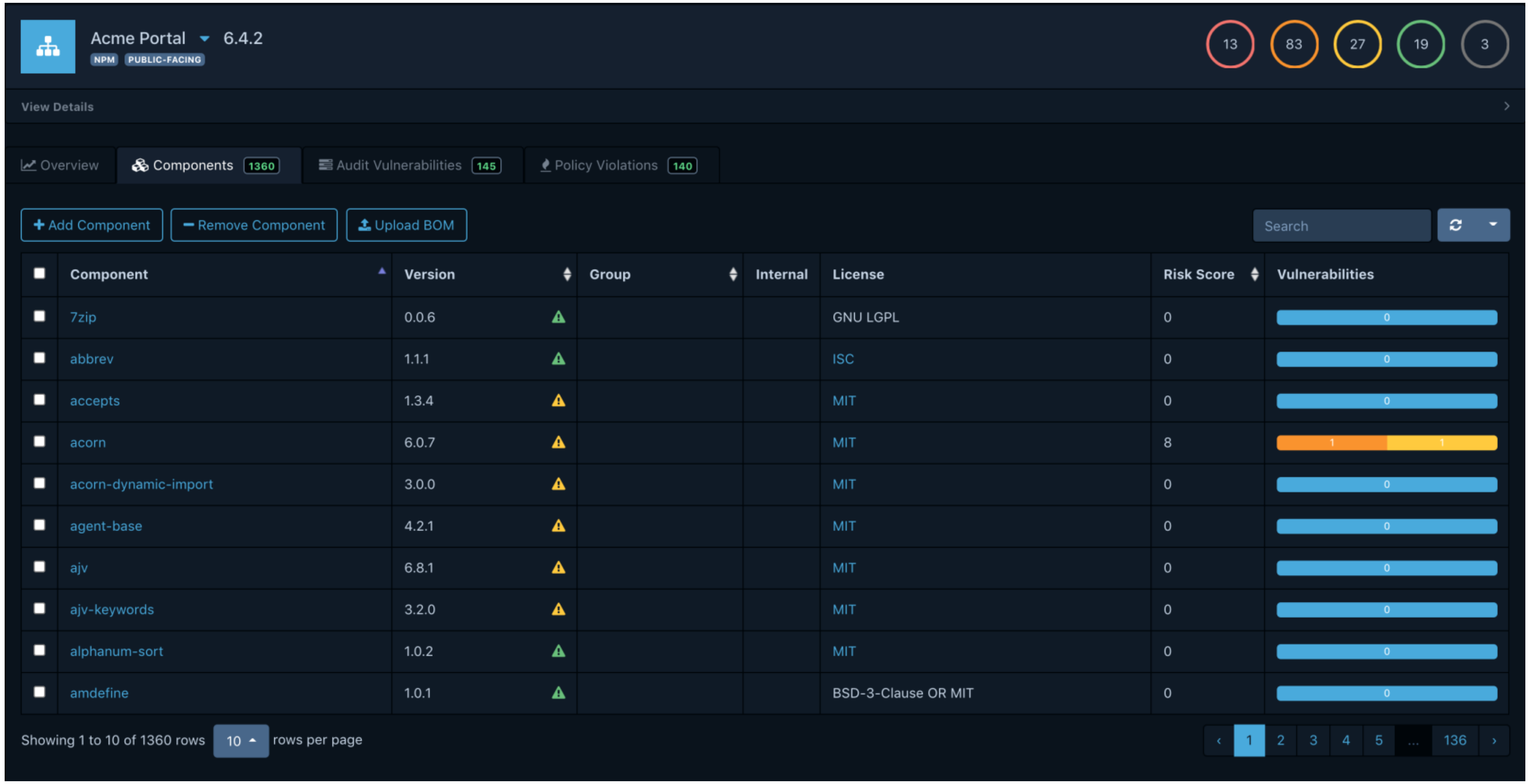
on continuous risk assessment using SBOM data

Revalidate SBOM data after integration

Continuously monitor for known vulnerabilities and cross that information with SBOM metadata

OWASP dependency track

HTTPS://OWASP.ORG/WWW-PROJECT-DEPENDENCY-TRACK/

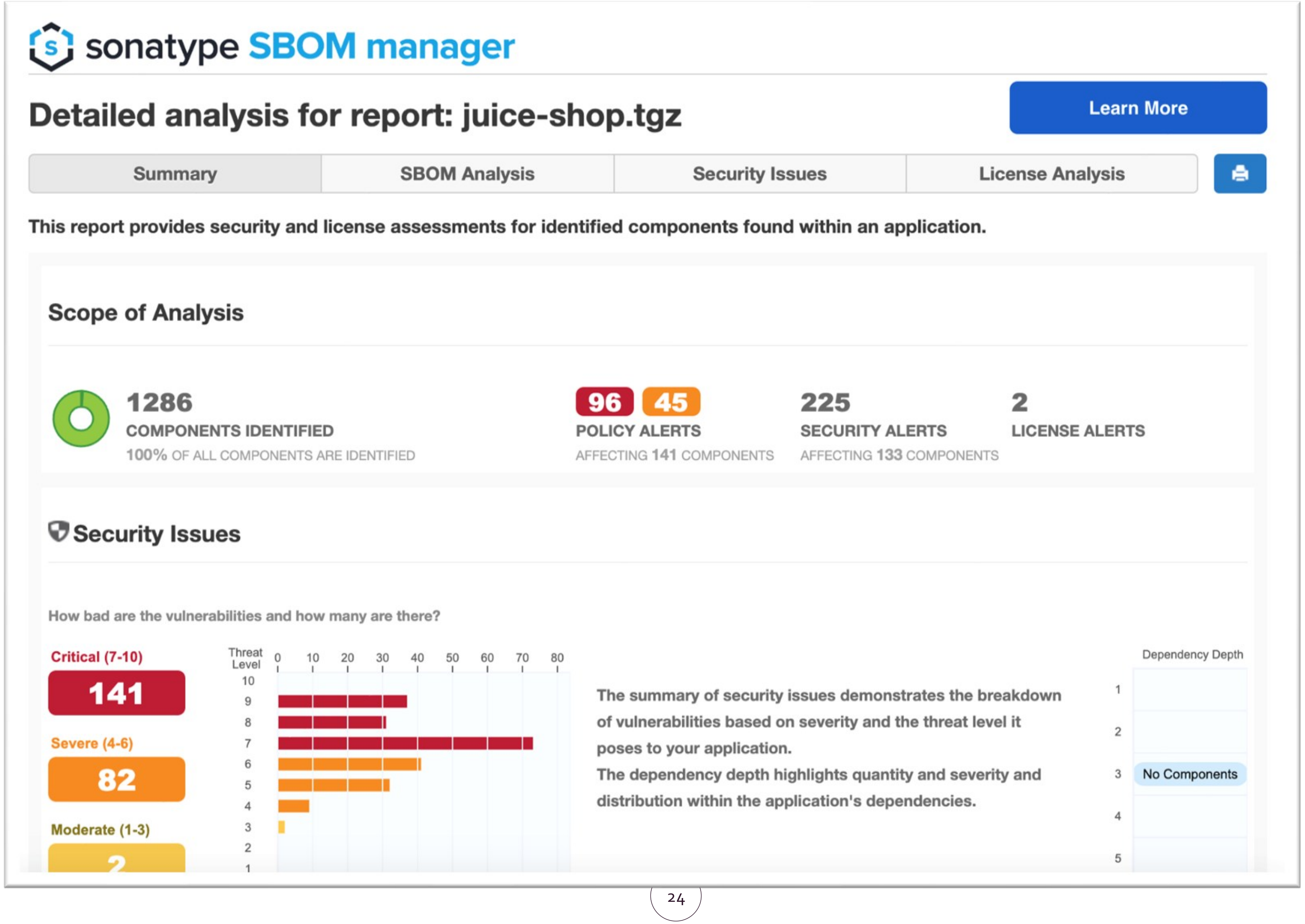


☐	Component	Version		Group	Internal	License	Risk Score	Vulnerabilities
☐	7zip	0.0.6	⚠			GNU LGPL	0	0
☐	abbrev	1.1.1	⚠			ISC	0	0
☐	accepts	1.3.4	⚠			MIT	0	0
☐	acorn	6.0.7	⚠			MIT	8	1 1
☐	acorn-dynamic-import	3.0.0	⚠			MIT	0	0
☐	agent-base	4.2.1	⚠			MIT	0	0
☐	ajv	6.8.1	⚠			MIT	0	0
☐	ajv-keywords	3.2.0	⚠			MIT	0	0
☐	alphanum-sort	1.0.2	⚠			MIT	0	0
☐	amdefine	1.0.1	⚠			BSD-3-Clause OR MIT	0	0

Showing 1 to 10 of 1360 rows 10 rows per page

- intelligent Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.
- leverages the capabilities of Software Bill of Materials (SBOM).

Sonatype SBOM manager



sonatype SBOM manager

Detailed analysis for report: juice-shop.tgz

Learn More

Summary | SBOM Analysis | Security Issues | License Analysis

This report provides security and license assessments for identified components found within an application.

Scope of Analysis

1286 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE IDENTIFIED

96 45 POLICY ALERTS
AFFECTING 141 COMPONENTS

225 SECURITY ALERTS
AFFECTING 133 COMPONENTS

2 LICENSE ALERTS

Security Issues

How bad are the vulnerabilities and how many are there?

Critical (7-10)
141

Severe (4-6)
82

Moderate (1-3)
2

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application.
The dependency depth highlights quantity and severity and distribution within the application's dependencies.

Sigstore

HTTPS://WWW.SIGSTORE.DEV/

Sigstore is an open source project for improving software supply chain security.

Empowers software developers and consumers to securely sign and verify software artifacts such as release files, container images, binaries, software bills of materials (SBOMs), and more.

Signatures are generated with ephemeral signing keys so there’s no need to manage keys.

Signing events are recorded in a tamper-resistant public log so software developers can audit signing events.

Minimize the contents

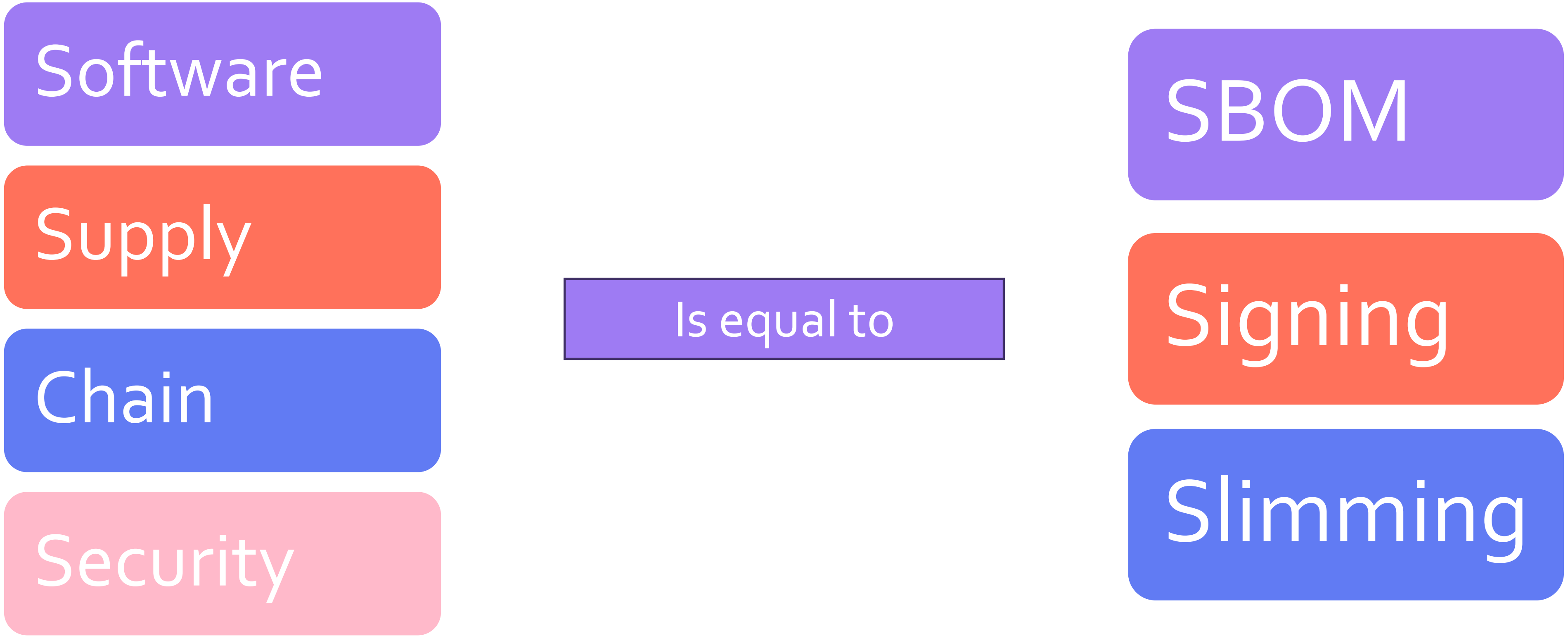
HTTPS://THENEWSTACK.IO/THE-3-SS-OF-SOFTWARE-SUPPLY-CHAIN-SECURITY-SBOMS-SIGNING-SLIMMING/

Slimming is identifying what is in your software containers and minimizing the content to only that which is required to run in production, thereby minimizing attack surface. While this process is often manual, labor-intensive, and requires specialized knowledge, AI helps to automate it.

“Complex systems are inherently riskier; with that in mind, **leverage technology to simplify a scenario rather than overcomplicate it.**”

Takeaway

ADOPT 3S



Software

Supply

Chain

Security

Is equal to

SBOM

Signing

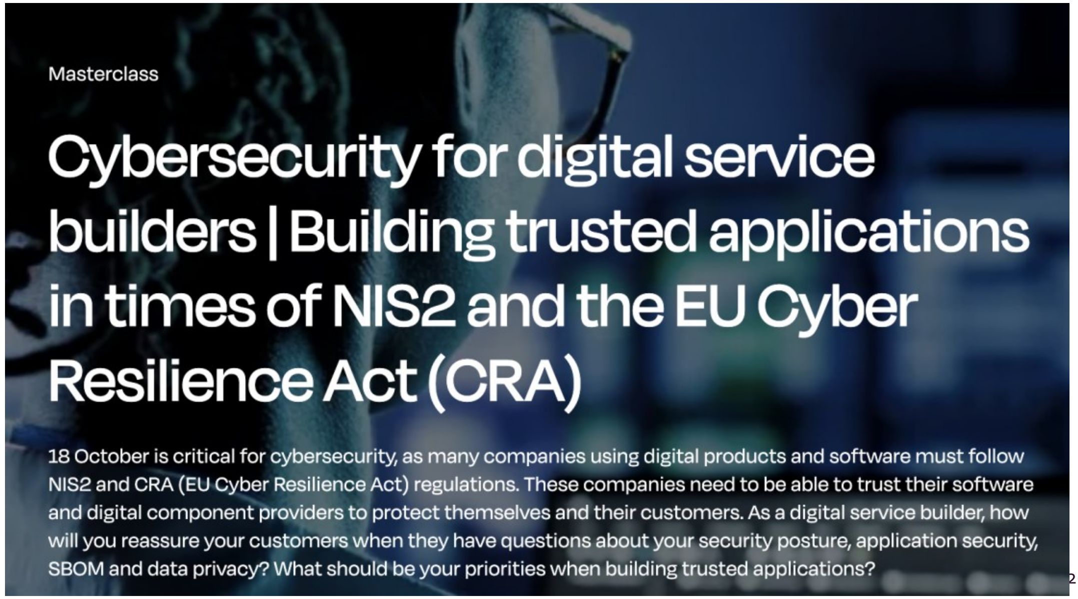
Slimming

Our collective offerings in CS

MASTERCLASSES, LEARNING NETWORK, LIGHTWEIGHT TRAINING

- CYBERACTIVE: FREE lightweight webinars and trainings:
  - For SMEs in digital and manufacturing sector
  - Online or physical
  - 3 languages, all over Belgium

- VLAIO-IP: SUBSIDIZED 1 day in-depth masterclass
  - Flemish and Brussels companies
  - 28.11 – digital.



Masterclass

Cybersecurity for digital service builders | Building trusted applications in times of NIS2 and the EU Cyber Resilience Act (CRA)

18 October is critical for cybersecurity, as many companies using digital products and software must follow NIS2 and CRA (EU Cyber Resilience Act) regulations. These companies need to be able to trust their software and digital component providers to protect themselves and their customers. As a digital service builder, how will you reassure your customers when they have questions about your security posture, application security, SBOM and data privacy? What should be your priorities when building trusted applications?

Our individual coaching offerings in CS

1-3 DAYS COMPACT COACHING

- Focus: manufacturing and digital service SMEs NIS2 pre-compliance
- Maturity scan for digital – software security maturity, threat modelling, preparation to NIS2 self-assessment
- Typically : 1 to 3 days
- Deliverable: list of tools&advises, action plan, maturity report
- Possible Modalities:
  - Flanders companies VLAIO-IP2 (when elligible)
  - Brussel companies via STIG/Innoviris convention (when eligible)

Useful resources

NIS 2.0: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

https://cybersec4europe.eu/

Study and recommendations in cybersecurity: https://www.agoria.be/nl/studie-Cybersecurity-in-de-maakindustrie

Web-site of Vlaio initiatives: https://www.digitaletoekomst.be/nl/cyber-security/

https://blog.cybersecuritycoalition.be/webcasts/the-nis2-directive-a-high-common-level-of-cybersecurity-in-the-eu/

https://blog.cybersecuritycoalition.be/wp-content/uploads/20221205_NIS2-Directive_CCB.pdf

https://ccb.belgium.be/en/cyberfundamentals-framework

https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

3 Pillars of NIS2+extended scope : https://blog.cybersecuritycoalition.be/wp-content/uploads/20221205_NIS2-Directive_CCB.pdf

Exact amounts and dates : https://www.devoteam.com/expert-view/ensure-compliance-with-the-sri2-nis2/

Cyberfundamentals : https://atwork.safeonweb.be/fr/tools-resources/cyberfundamentals-framework

innovation
forward

Feedback & Questions

THANK YOU!