ECCO
European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Knowledge-Sharing Webinar

Enhancing Supply Chain Security: Strategies, Case Studies and Roadmapping

June 14th 2024

Agenda

- Introduction (5 min)

- Securing Supply Chains: Assessing the Trustworthiness of Composite Suppliers’ Products (20 min) (Roland)

- Securing the Cyber Supply Chain: from exemplar cases to a possible roadmap (20 min) (Aaron)

- Q&A (15 min)

ECCO

European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Introduction

June 14th 2024

ECCO Community Working Groups

- Road-mapping
- Startups/Scaleups - SMEs support
- Human factors
- Skills
- Synergies on cybersecurity for Civilian and Space applications
- **Trusted supply chains**
  - **Chairs: Antonio Skarmeta and José Luis Hernández Ramos**
  - Participants: development of a "proto-community" based on the initial list of experts from ECSO and Pilots, and growing with additional people (44 members so far)
  - Objectives
    - Build community of experts on trusted supply chains and Strengthening Trusted and Resilient Supply Chain in Europe
    - Facilitate trusted information sharing about threats (to support prevention and response)
    - Propose a strategy, planning and recommendations to support the NCCs in the implementation of the Strategic Agenda's Action Plan

Enhancing Supply Chain Security: Strategies, Case Studies, and Roadmapping

- Webinar today focused on key strategies to secure supply chains against advanced cyberthreats, balancing industry-specific needs with standardized re-usability and:
  - Emphasizing compliance with regulations and certification schemes
  - Addressing challenges in securing complex attack surfaces and implementing current standards, with lessons from past experiences.

Planned webinars

- This event is part of a webinar series focused on European cybersecurity supply chain.

- List of webinars
  - Organizational and Operation Security in Trusted Supply Chains (March 19th)
  - Certification in the Lifecycle (May 7th)
  - Enhancing Supply Chain Security: Strategies, Case Studies, and Roadmapping (today)
  - Paradigm shift from cybersecurity to cyber resilience (expected by July)

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

Securing Supply Chain

Assessing the Trustworthiness of Composite Suppliers' Products

14 June 2024

ROLAND ATOUI - MANAGING DIRECTOR @RED ALERT LABS

RED ALERT LABS
IoT Security

Main Challenges

125 Bn+

OF CONNECTED DEVICES

IN 2030

>50%

VULNERABLES

62%

OF ATTACKS EXPLOIT THE CUSTOMERS' TRUST WITHIN THEIR SUPPLIERS

"The lack of **transparency and audits' inability** (expertise, time, costs) are causing a serious risk regarding the trust within the supply chain."

SUPPLY CHAIN REPORT, ENISA

"Attacks across the **supply chain** such as Solarwinds are worrying me, because I do not see at this stage how we can protect ourselves. Even for a company which strictly follows all **ANSSI's recommendations** - and this doesn't exist - it will still be very complicated."

GUILLAUME POUPARD, ANSSI EX-CEO

"Because of the **attacks' cascade effect** across the supply chain, malicious actors can create damages extended to both companies and their customers."

JUHAN LEPASSAR, ENISA CEO

"Lots of components made by companies all over the world are flowing across **many layers of suppliers and integrator** before until they are placed under a framework, tested and packed by OEM."

FINITE STATE REPORT

The CRA & NIS2

Both **Components** & **Products** must be assessed for conformity

Don’t just look at the screen.
Click and buy this IoT device! It’s very legit.
STOP STOP! It doesn't comply with the latest security standards!

Article 10 (4)

...manufacturers shall exercise **due diligence** when integrating **components sourced from third parties** in a manner that such components do not compromise the cybersecurity of **the product with digital elements**, including when integrating components of free and open-source software that have not been made available on the market in the course of a commercial activity.

What if you / your supplier doesn't comply ?

Financial Penalties

In the CRA, administrative fines can reach up to €15,000,000 or up to 2.5% of the total worldwide annual turnover

Reputational Damage

Loss of Trust, Negative Media, Investor Concerns, Competitive Disadvantage

Operational Disruptions

Non-compliance could lead to regulatory scrutiny, mandatory corrective actions, damaged trust in supply chains, market access restrictions, resource reallocation, and disruptions from implementing security measures

Increased Insurance Premiums

History of non-compliance can lead to higher cyber insurance premiums or lack of coverage

Non-compliance with cybersecurity regulations carries significant financial, reputational, operational, and insurance consequences.

Cybersecurity product compliance is challenging!

Technically **Complex**

Limited Resources

Expensive & Time **Consuming**

~30K€ per product compliance

4-24 weeks per certification

Lack of Visibility

Compliance Monitoring & **Maintenance**

Nightmare
To Keep up with Security Standards and meet increasing **Regulations** (CRA, RED, ...)

Panorama of Standards and Regulations for IoT

From Consumer to Industrial...

RED-DA
Delegated Regulation (EU) 2022/30 and cybersecurity compliance
02/2022

ETSI EN 303 645
Cybersecurity for the consumer Internet of Things: basic requirements
06/2020

NISTIR 8425
Profile of the IoT Core Baseline for Consumer IoT Products
final - 09/2022

IEC 62443
Safety of industrial automation and control systems
2019

Cybersecurity Act
and related schemes
06/2019

ISO 27402 + 04
Cybersecurity — IoT security and privacy — Device baseline requirements and certification scheme
Under development

Cyber Resilience Act
Supervises connected products and the services on which they depend
2025

EN 18031, EN 17640, EN 17927
Harmonised standards for RED-DA, FITCEM, SESIP

Essential Requirements

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
ANSI
Accredited Standards Committee X9
ISO
ITU
3GPP
W3C
fido ALLIANCE
IEEE
ETSI
Global Platform
OASIS
I E T F
CSA cloud security alliance
ISO
CSA cloud security alliance
NCCoE
Global Platform
cen
NIAP
PCI
CSTC
TRUSTED COMPUTING GROUP
NIAP
Federal Office for Information Security
EMVCo
ANSSI
enisa
Common Criteria
NIST
CSTC
CYBERSÉCURITÉ
CYBER SECURITY
OWASP
NIST
NIAP
PCI Security Standards Council
3GPP
KISA
NSR
IPA
CSA
EMVCo
Global Platform
TSE
CB
OC-CCN
FMV
ITSCC
商用密码检测中心 Commercial Cryptography Testing Center
SERTIT
TRUSTCB
CyberSecurity

> **The assessment of conformity of a product is carried out before this product is placed on the market and consists in demonstrating that it fulfils all the legislative requirements that apply to it**

ASSURANCE / PROOF

from meeting requirements to preparing for potential audits

Compliance is more than just ticking checkboxs

Compliance requires cyber resiliency in both technical solutions and business processes

Evidence of compliance readiness is key

Maintain documentation of compliance efforts and readiness for investigations

Compliance should focus on overall cyber resiliency and readiness for investigations, not just bare minimum technical requirements.

Why Composition ?

Cost-effective

A way to achieve cost-effective certification by reusing already certified components

Avoid fragmentation

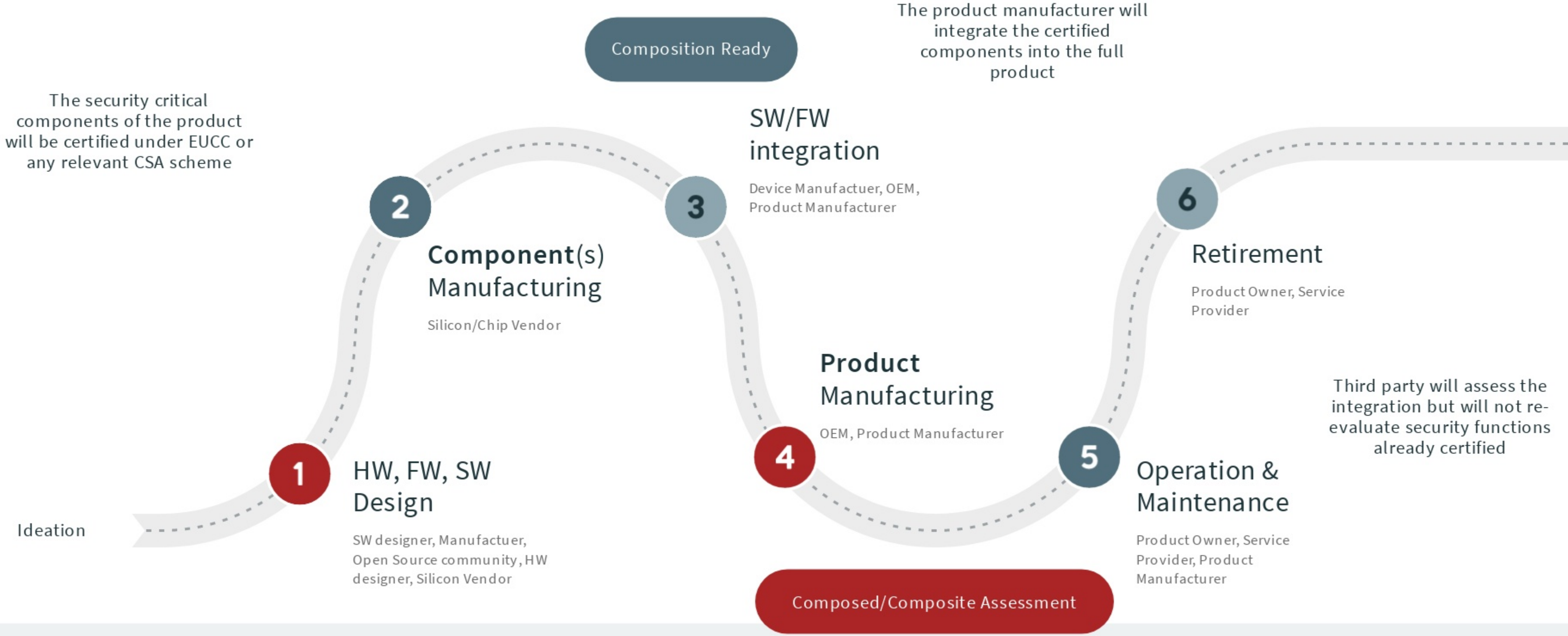
Composition helps avoid duplication and fragmentation across schemes

Build trusted infrastructure & supply chain

Enables building trusted and resilient multi-technology infrastructure and a trusted supply chain

Certification by composition is key to building trusted products ecosystems in a cost-effective way by reusing components across schemes.

Products' Typical Life-Cycle Phases



The security critical components of the product will be certified under EUCC or any relevant CSA scheme

Composition Ready

The product manufacturer will integrate the certified components into the full product

Ideation

1 HW, FW, SW Design

SW designer, Manufactuer, Open Source community, HW designer, Silicon Vendor

2 **Component**(s) Manufacturing

Silicon/Chip Vendor

3 SW/FW integration

Device Manufactuer, OEM, Product Manufacturer

4 **Product** Manufacturing

OEM, Product Manufacturer

5 Operation & Maintenance

Product Owner, Service Provider, Product Manufacturer

6 Retirement

Product Owner, Service Provider

Third party will assess the integration but will not re-evaluate security functions already certified

Composed/Composite Assessment

Products supply chain includes the actors, processes and assets that participate in the realization (e.g. development, design, maintenance, patch management) of all components.

Product/Component Level : 3 Types of Composition

Layered

Examples include an application using an operating system as its base component.

Network or bi-directional

An example is an application leveraging services from an external LDAP server.

Embedded

It's useful for developers creating libraries for future use across multiple products or for those providing foundational elements to other developers.

Composition Across Certification Schemes

EU cybersecurity certifications

EU has cybersecurity certification schemes like EUCC and EUCS

Product and process certification

EUCC certifies products, EUCS certifies services / secure data processing falling under the CRA

Leveraging certifications

A service can leverage a certified product for its own certification

The EU has complementary cybersecurity certifications for products and processes that can work together.

Composition Across Regulations...

RED

Both acts require risk assessments...

GDPR

interrelate with the Cyber Resilience Act on the aspect of data security and privacy protection for connected devices.

NIS2

As with the CSA, the Cyber Resilience Act would likely build on the NIS directive's objectives of ensuring a high common level of network and information system security.

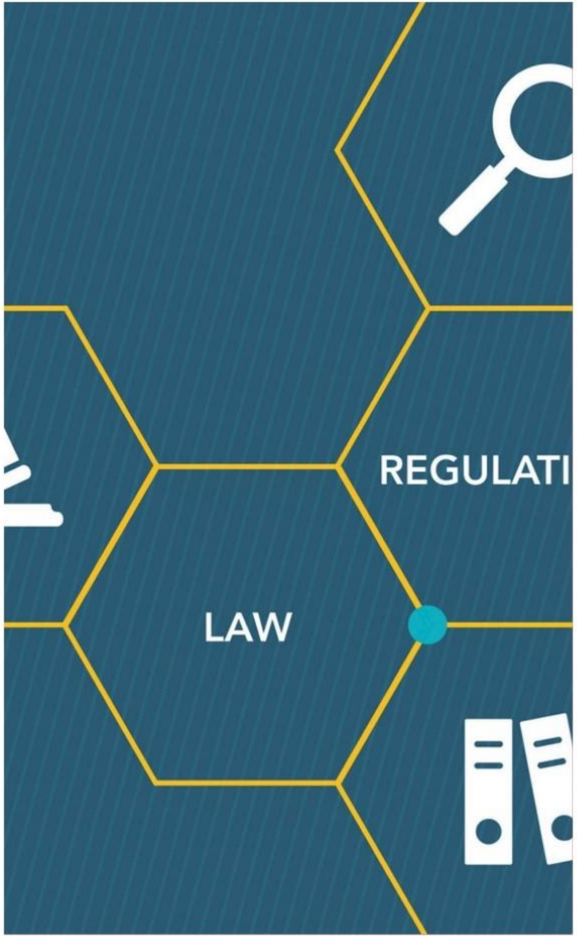
Market Surveillance and Enforcement

CSA

Both acts promote standards and certification to show compliance and cybersecurity.

AI

The CRA requires secure data processing for cybersecurity, complementing AI Act data governance.



Cybersecurity compliance is an ongoing process that requires continuous monitoring and adaptation to new threats and regulations.

Automation tools are critical to efficiently achieving and maintaining compliance over time.

What is CyberPass ?

CYBERPASS provides enterprises with a cost-effective and scalable AI-powered SaaS platform to assess and manage their manufactured or acquired connected **products' cybersecurity compliance**.

...the **Yuka** for Cybersecurity of Connected Products !

To Trust the Supply Chain You Need...

CLARITY

Buyers

- Centralize compliance
- Proactively manage risks and cut costs by 80%
- Track regulatory obligations

SIMPLICITY

Manufacturers

- Ai-powered compliance journey
- Extend market reach
- Reduce costs by 50% and accelerate timelines from weeks to days

EFFICENCY

Laboratories

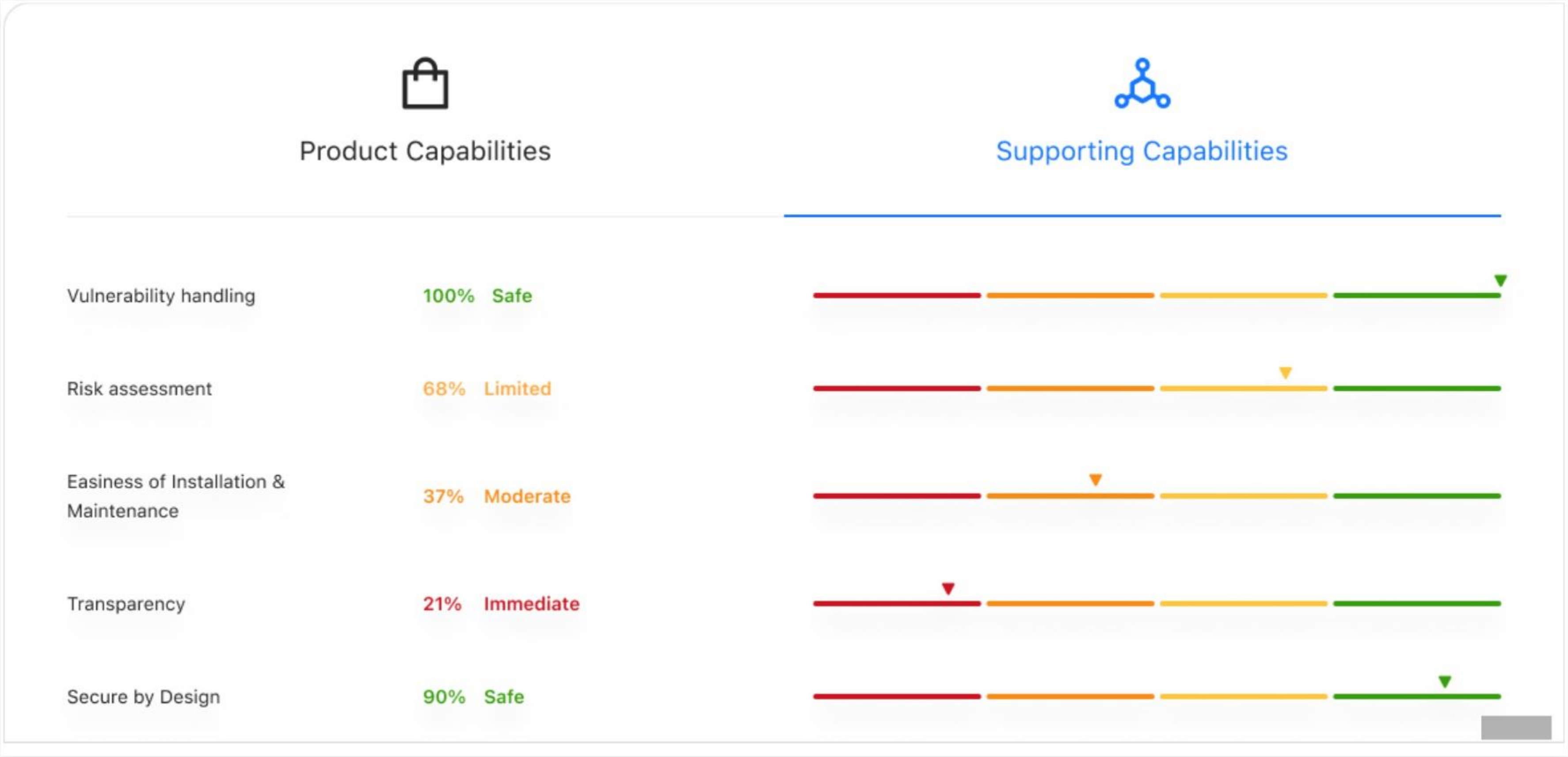
- Ai-powered evaluation assistance
- Expand market presence
- Improve communications

SCALABILITY

Scheme Owners

- Access APIs for interoperability
- Integrate with personalized schemes
- Manage certificate holders and labs

CYBERPASS
TRUST YOUR CONNECTED PRODUCTS



Vulnerability handling	100%	Safe
Risk assessment	68%	Limited
Easiness of Installation & Maintenance	37%	Moderate
Transparency	21%	Immediate
Secure by Design	90%	Safe

Key Takeaways

Proactivity & Automation

According to a study by Security Signals, only 39% of security teams' time is spent on prevention. This must change! Use Automated tools streamlining the conformity assessment process such as CyberPass (www.cyber-pass.eu)

Essential Requirement, Composition & Standards

Use the CRA essential requirements to derive security goals and sub-requirements. Rely on certified/compliant components and widely adopted standards such as the EN 303 645 or ISO 15408 to start now…

CRA as a cornerstone

The CRA should be the cornerstone of all cybersecurity regulation in the EU, providing horizontal principles and promoting consistency and harmonisation with existing and forthcoming legislation.

Contribute to EU initiatives

Contribute to standards and guidance activities and initiatives such as the ones driven by ECCC, ECSO, Certify, Custodes, DOSS, Cobalt, Entrust, …

RED ALERT LABS
IoT Security

Thank You

Campus Cyber, 5 Rue Bellini, 92800 Puteaux , France

3 rue Parmentier, 94140, Alfortville, France

🌐 https://www.redalertlabs.com

☎ +33 9 51 79 07 87

@RedAlertLabs

/company/red-alert-labs

Enhancing Supply Chain Security

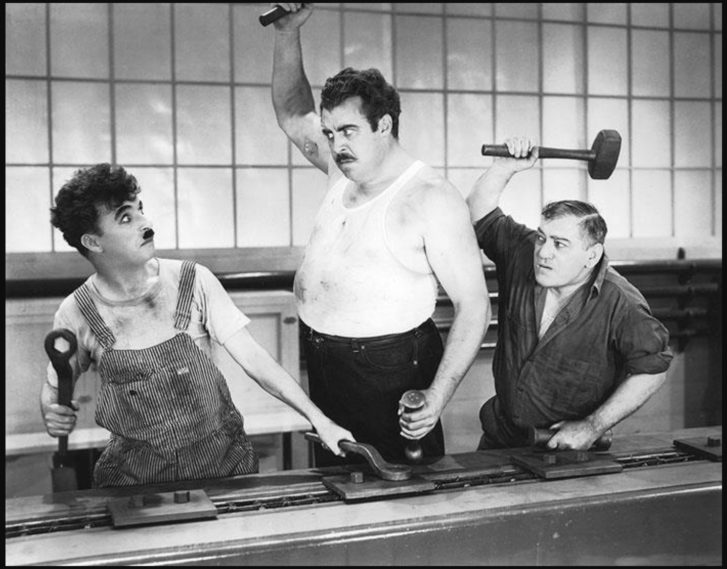
Corrado Aaron Visaggio

Department of Engineering- University of Sannio-CINI CyberSecurity National Lab

Chief Scientist Officer of DefenceTech

ECCO

European Cybersecurity COmmunity



14/06/2024

13/06/2024

Preliminary definitions

- “E-supply chains involve organizations using online information, to perform, rather than just support, some value-adding activities in the supply chain more efficiently and effectively” (Barlow and Li, 2007)
- “[Cyber supply chain is] the entire set of key actors and their organizational and process-level interactions that plan, build, manage, maintain, and defend the IT system infrastructure” (Boyson et al, 2009)
- Supply chain risk:
  - “The probability of loss arising because of incorrect, incomplete, or illegal access to information.” (Faisal et al., 2007)
  - “. . . degradation or disruption to a supply chain’s infrastructure or structural resources resulting from the successful exploitation of IT vulnerabilities by threats within an organization, within the supply chain network, or in the external environment” (Smith et al, 2007)

DragonFly 2.0 Attack - 2014

- A supply chain attack targeted updates of industrial control systems and supervisory control and data acquisition systems (**ICS and SCADA**)
- Legitimate updates to that software were infected with malware named "Havex" that allowed the attackers to create back doors and scan networks for more targets.
- Over 17,000 devices were infected in the US alone
- From 2014 to 2017 the crew moved on to "Dragonfly 2.0" and "transitioned to more targeted compromises that focused on specific energy sector entities and individuals and engineers who worked with ICS/SCADA system

Ccleaner – 2017...

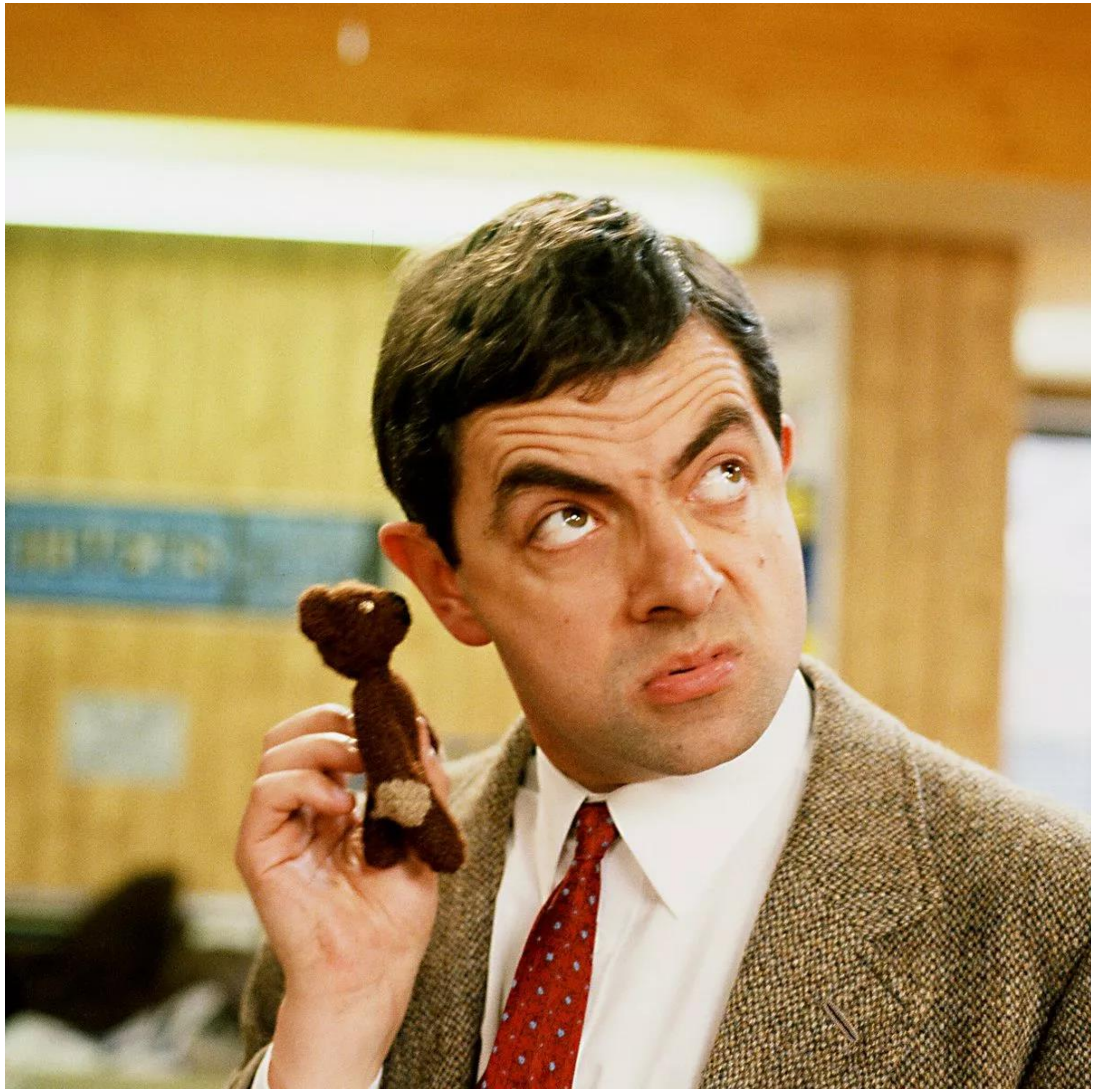
- Threat actors compromised the company's servers for more than a month and replaced the original version of the software with the malicious one.
- The malware attack infected over 2.3 million users who downloaded or updated their CCleaner app between August and September 2018 from the official website with the backdoored version of the software.
- Attackers first accessed an unattended workstation of one of the CCleaner developers, which was connected to Piriform network, using remote support software TeamViewer.
- The company believes attackers reused the developer's credentials obtained from previous data breaches to access the TeamViewer account
- Using the first machine, attackers penetrated into the second unattended computer connected to the same network and opened a backdoor through Windows RDP (Remote Desktop Service) protocol.

… Ccleaner – 2017

- Attackers infected the first computer with the older version of the second stage malware as well.
- Attackers compiled a customized version of ShadowPad, an infamous backdoor that allows attackers to download further malicious modules or steal data, and this payload the company believes was the third stage of the CCleaner attack.
- A few days later, attackers installed the 3rd stage payload on four computers in the Piriform network (as a mscoree.dll library) and a build server (as a .NET runtime library).
- Security company Avast acquired Piriform, the UK-based software development company behind CCleaner with more than 2 billion downloads.
- Attackers replaced the original version of CCleaner software from its official website with their backdoored version of CCleaner, which was distributed to millions of users.

SolarWinds - 2020

- The software builds for Orion versions 2019.4 HF 5 through 2020.2.1 that were released between March 2020 and June 2020 might have contained a trojanized component.
- The attackers managed to modify an Orion platform plug-in called SolarWinds.Orion.Core.BusinessLayer.dll that is distributed as part of Orion platform updates. The trojanized component is digitally signed and contains a backdoor that communicates with third-party servers controlled by the attackers.
- After an initial dormant period of up to two weeks, it retrieves and executes commands, called ‘Jobs,’ that include the ability to transfer files, execute files, profile the system, reboot the machine, and disable system services

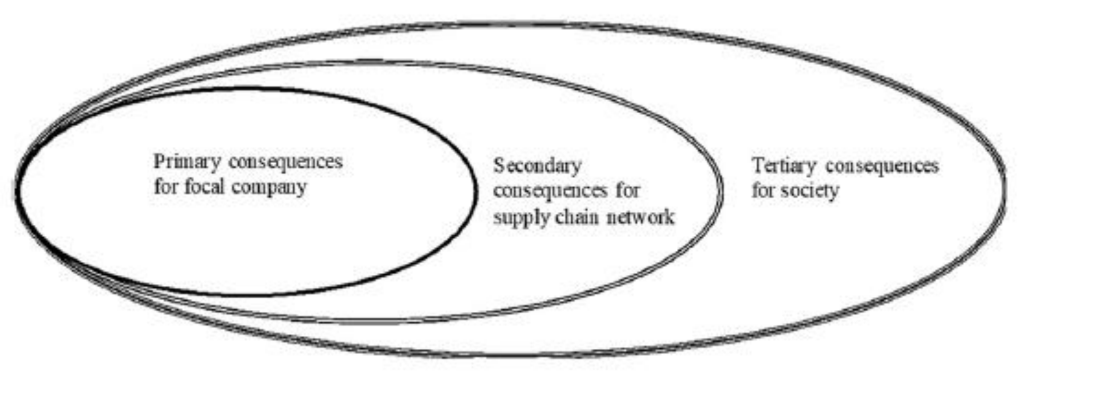


Log4j-2021

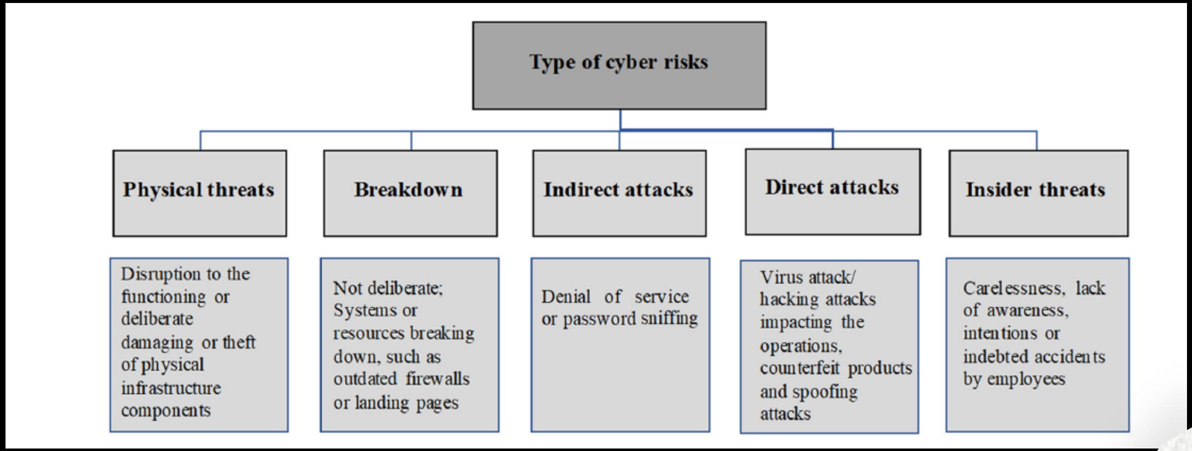
- Log4Shell (CVE-2021-44228) is a zero-day vulnerability in Log4j, a popular Java logging framework, involving arbitrary code execution.
- Apache gave Log4Shell a CVSS severity rating of 10
- The exploit was simple to execute and is estimated to have had the potential to affect hundreds of millions of devices
- We didn’t know where log4j was.
- Cybersecurity company Tenable said the exploit was "the single biggest, most critical vulnerability ever," Ars Technica called it "arguably the most severe vulnerability ever“ and The Washington Post said that descriptions by security professionals "border on the apocalyptic."

Penetration & Propagation

- Technical points : all IT-related assets, including system, software, personnel and equipement
  - Poor maintenance, not reliable outsourcing
- Human points: future cyber risks, and especially intended attacks, are expected to exploit human PoPs rather than, hitherto, focus on the technical domain.
- Physical points: physical objects such as buildings, machines and other surroundings

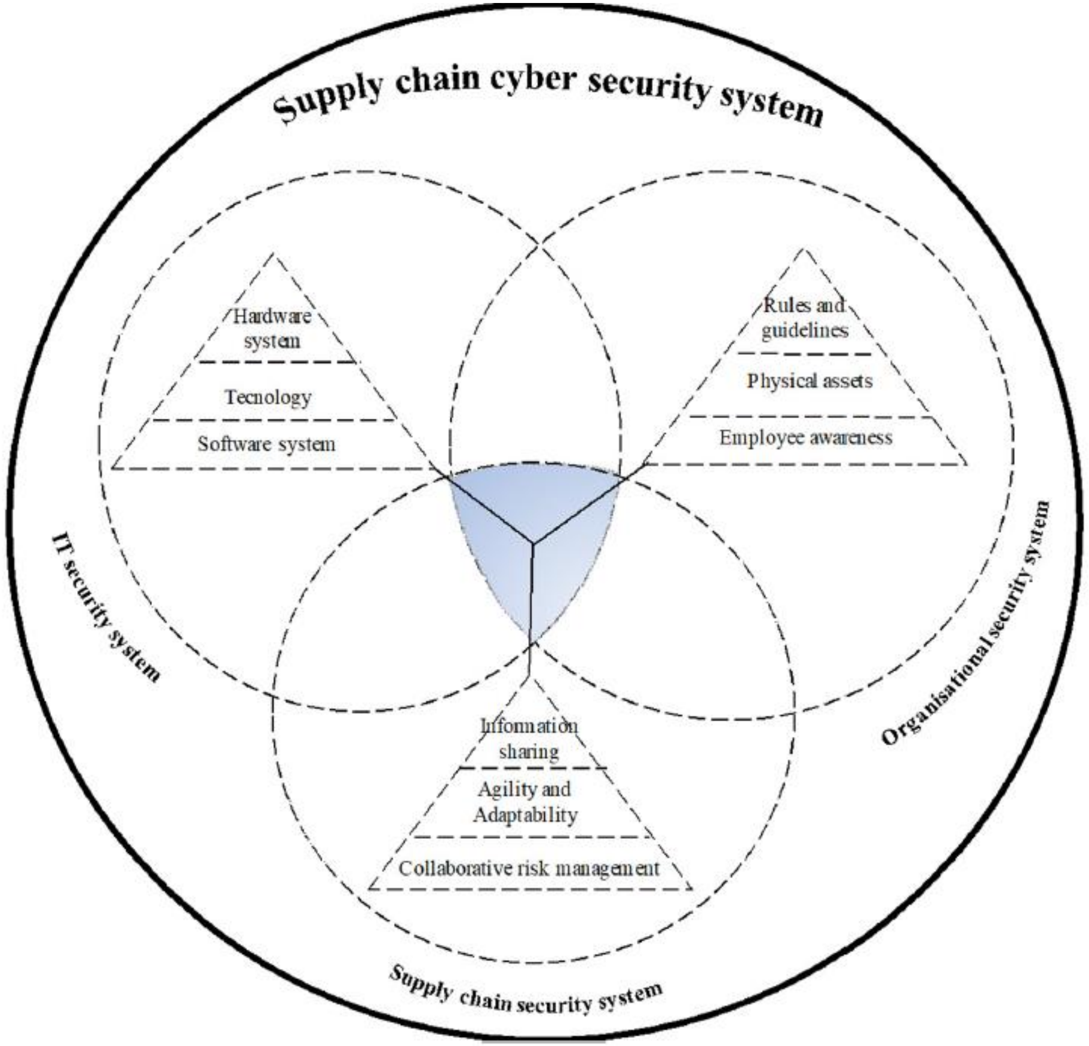

Primary consequences for focal company
Secondary consequences for supply chain network
Tertiary consequences for society

Classification of Cyber Risks



Type of cyber risks

Physical threats	Breakdown	Indirect attacks	Direct attacks	Insider threats
Disruption to the functioning or deliberate damaging or theft of physical infrastructure components	Not deliberate; Systems or resources breaking down, such as outdated firewalls or landing pages	Denial of service or password sniffing	Virus attack/ hacking attacks impacting the operations, counterfeit products and spoofing attacks	Carelessness, lack of awareness, intentions or indebted accidents by employees


Supply chain cyber security system
Hardware system
Tecnology
Software system
Rules and guidelines
Physical assets
Employee awareness
Information sharing
Agility and Adaptability
Collaborative risk management
IT security system
Organisational security system
Supply chain security system

Conclusions

- Secure Patching Management
- Software Composition Analysis
- SBOM
- Monitoring of vulnerabilities
- Asset Inventory
- Protection of development and production ecosystem (Code base, development codebase, deployment, software distribution)
- Signed Software updates and versioning
- Certifications
- Frequent and independent Vulnerability assessments of software
- Ad-hoc sandboxes for static and dynamic verification of security requirements of software
- Standard Guidelines for SC collaboration
- Incident Management
- Formal agreements between SC partners

Reference

- Barlow, A. and Li, F. (2007), “E-supply chains: understanding current and future opportunities and barriers”, International Journal of Information Technology and Management, Vol. 6 Nos 2/3/4, pp. 286-298.

- Boyson, S., Corsi, T. and Rossman, H. (2009), “Building a cyber supply chain assurance reference model”, Science Applications InternationalCorporation (SAIC).

- Faisal, M.N., Banwet, D.K. and Shankar, R. (2007), “Information risks management in supply chains: an assessment and mitigation framework”, Journal of Enterprise Information Management, Vol. 20No. 6, pp. 677-699.

- Smith, G.E., Watson, K.J., Baker, W.H. and Pokorski Ii, J.A. (2007), “A critical balance: collaboration and security in the IT-enabled supply chain”, International Journal of Production Research, Vol. 45No. 11, pp. 2595-2613.

- Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. Supply Chain Management: An International Journal, 25(2), 223-240.

Contacts

- Corrado aaron visaggio
- mail: visaggio@unisannio.it
- Linkedin: https://www.linkedin.com/in/corrado-aaron-visaggio-629839/

Thank you