Newsletter 1

February 2024

In this Issue

Overview

RESCALE (**Revolutionised Enhanced Supply Chain Automation with Limited Threats Exposure**) is a European Union project under the HORIZON-CL3-2022-CS-01 2022 programme that was launched on October 2023. RESCALE has 3-years duration and aims at designing, building, and demonstrating secure-by-design supply chains.

KPIs

- >95% resilience on cyberattacks
- >98% accuracy of vulnerability assessment algorithms
- >3 software and hardware TBOM files
- >20 papers in journals and conferences
- detect 0-day exploits

RESCALE will:

- Design and develop a toolbox to audit and increase the security of supply chain based emerging technologies for both hardware and software modules.
- Detect and safeguard the hardware elements of supply chain systems.
- Provide a Trusted BOM approach that will infuse trust in software and hardware supply chain and promote trusted updates.
- Demonstrate and validate the effectiveness of the proposed solutions in 2 complementary use cases.
- Ensure wide visibility and raise awareness on the security of software and hardware components in supply chains.

Validation

2 real-world pilots

Auto-Placement Security Aware Augmented Data-Flow and Infrastructure

Privacy-by-Design Distributed Cloud

Goals

- ✓ **Automation**: Automate the evaluation processes of both software and hardware components.
- ✓ **No vulnerabilities**: Ensure that third party segments are free from vulnerabilities.
- ✓ **Audit**: Offer effective audit procedures for cybersecurity testing.
- ✓ **Secure systems**: Enable the construction of secure systems with the strongest possible guarantees.

Kick Off Meeting

- ✓ **Location**: Athens, Greece
- ✓ **Date**: 4-5 October 2023
- ✓ **Number of Partners**: 15
- ✓ **Number of Countries**: 11

Supply Chain Cybersecurity Market Trends

The supply chain cybersecurity market size is expected to grow in the coming years due to the threat landscape and the integration of supply chain solutions.

- The supply chain cybersecurity market size exceeded 2 billion USD in 2022 and is forecasted to register more than a 11% Compound Annual Growth Rate (CAGR) from 2022 to 2027, reaching a value of approximately USD 3.5 billion by 2027.
- This growth is attributed to the growing adoption of cloud-based solutions, integration of third-party supply chain solutions, the rising demand for high visibility and transparency in supply chain processes and the increase in supply chain cyberattacks.
- Cyberattacks on software supply chains have surged by 742% in the years 2020 to 2023, highlighting a significant threat vector within the cybersecurity landscape, where attackers increasingly exploit vulnerabilities in software supply chains.
- 49% of organizations have experienced a data breach caused by a third-party vendor in the last 12 months based on data leading up to 2023.

Issues in Supply Chains

Issue 1 – Third Party Risks

Supply chains often involve multiple third-party vendors, each with their own cybersecurity practices. If a vendor has weak security measures, it can become a point of entry for cyberattacks, affecting all businesses within the supply chain.

Issue 2 – Lack of Visibility and Transparency

Many organizations lack visibility into their supply chain's security practices. Without this visibility, it's challenging to assess risks and ensure that all parts of the supply chain meet the required cybersecurity standards.

Issue 3 – Software Supply Chain Attacks

Attackers increasingly target software supply chains, exploiting vulnerabilities in third-party software, open-source libraries, or development tools to distribute malicious code or gain unauthorized access.

Issue 4 – Complex Compliance Requirements

With the global nature of supply chains, organizations must navigate a complex landscape of regulatory and compliance requirements. Ensuring compliance with all relevant cybersecurity standards across different jurisdictions can be challenging.

Issue 5 – Counterfeit Components

Cybersecurity supply chains are also at risk from counterfeit hardware and software components, which may contain malicious functionalities or vulnerabilities that can be exploited by cybercriminals.

Issue 6 – Inadequate Security Standards and Practices

Not all organizations and their supply chain partners maintain high cybersecurity standards. Inconsistent or inadequate security practices across the supply chain increase the risk of cyberattacks.

Supply Chain Cyberattacks Statistics [ENISA, Understanding the increase in Supply Chain Security Attacks (2021)]

The supply chain cybersecurity market is experiencing significant growth, driven by the increasing reliance on third-party logistics solutions providers and the rising need for robust security measures across supply chains due to cyberattacks.

Supply chain security is crucial to protect against disruptions, non-malicious failures and cyberattacks, which can lead to significant financial losses, reputational damage, and risks to public safety.

Implementing supply chain security protects against attacks that can compromise data integrity and confidentiality, especially in a world where supply chains are increasingly digital and interconnected. The growth of the market is facilitated by advancements in technology, such as AI, IoT, and blockchain, which are optimizing supply chain operations and creating new opportunities for supply chain security.

Contact Project Coordinator: Dr. Apostolos Fournaris, Industrial Systems Institute (ISI), fournaris@isi.gr
General inquiries: info@rescale-project.eu

RESCALE WWW rescale-project.eu @Rescale_Horizon Rescale Project Horizon EU

This project has received funding from the European Union's Horizon Europe Research and Innovation program under grant agreement No **101120962**.