verslag
buitenlandse zending

naam	Bert Huygens
zendingsactiviteit	Beurs cyber security2023
intern nummer bib	nvt

Inleiding

Het MT heeft beslist dat Bert Huygens als Verandermanager Informatieveiligheid het INBO zal vertegenwoordigen.

De Vlaamse overheid heeft een programma Informatieveiligheid uitgewerkt. Het biedt een antwoord op de uitdagingen en kansen voor een veilige informatieverwerking binnen de Vlaamse overheid, zoals de bescherming van persoonsgegevens of de toenemende dreiging van cybercriminelen. Hiervoor is het opportuun de kennis bij te schaven door het bijwonen van een beurs rond cybersecurity

Verslag

Session 1: Continuous Validation and Security Assessment

Risk Explorer for Software Supply Chain (Piergiorgio Ladisa from SAP France)

Open-Source Software (OSS) has become pervasive in contemporary applications, often comprising over 90% of the code in commercial software. Its widespread adoption spans the entire technology stack and the various stages of development and operations. Given the intricate nature of the modern software supply chain, malicious actors find numerous entry points to introduce harmful code into open-source components, thereby compromising downstream users.

During this presentation, we introduce the Risk Explorer for Software Supply Chains, a tool enabling interactive exploration of a comprehensive and technology-agnostic taxonomy

outlining methods through which attackers introduce malicious code in the software supply chain. We further showcase its practical applications in industrial contexts.

Security bill of materials and continuous threat analysis (Riccardo Scandariato from TUHH)

Architectural threat and risk analysis is one of the pillars of software security. However, integrating this practice in the context of continuous software development remains as a challenge. In this panel contribution, we will discuss how automatic techniques can be leveraged to seamlessly extract a so-called security bill of materials and to continuously link architectural security properties (as well as issues) to the code base.

Mandatory updates and EU Regulation (Prof. Fabio Massacci from VU Amsterdam)

The EU is implementing new regulations that require mandatory software updates. These regulations pose a challenge for software companies that need to keep up with the fast-paced development and use of multi-party open software and services. The AssureMOSS project is developing automated techniques to help companies comply with the new regulations and create more secure software.

Session 2: Code and Runtime Security Analysis with ML

Security Analysis of cloud infrastructure (Agathe Blaise from THALES)

In recent years, there has been an explosion of attacks directed at microservice-based platforms – a trend that follows closely the massive shift of the digital industries towards these environments. Two main types of approaches exist to provide a security assessment of deployed applications and services in such environments. The first one focuses on the mechanisms for analysis and validation of container images and orchestration deployment descriptions via static analysis and stress test procedures. The second one aims to provide methodologies to ensure the right behavior of microservices while in execution and eventually to detect anomalies in their behavior.

ML and Generative AI to address complexities surrounding supply chain vulnerabilities (Elisa Costante from FORESCOUT TECHNOLOGIES INC.):

Software supply chain vulnerabilities refer to security flaws within components that are integrated into various other software components and applications. These vulnerabilities pose significant challenges when it comes to identification and understanding their full scope upon disclosure. Particularly, in the context of lengthy supply chains, such as when a TCP/IP stack is utilized within an operating system, which is then incorporated into a Network Management Card, ultimately used in an Uninterruptible Power Supply (UPS), pinpointing affected products can be a time-consuming endeavor, often yielding only partial solutions. As a consequence, certain vendors may remain unaware of whether their products are impacted for an extended period following the initial disclosure of the vulnerability. In this presentation, I will delve into the complexities surrounding supply chain vulnerabilities and explore potential solutions leveraging Machine Learning (ML) and Generative AI to address some of these challenges.

LAZARUS – Enhancing Software Security (Adriana Freitas from APWG):

Discover how LAZARUS revolutionizes software security through advanced machine learning. Learn about its innovative cybersecurity approach throughout the software development lifecycle, including targeted security checks and valuable intelligence collection. Join us to witness LAZARUS bringing security to every step of software development SDLC.