EXEIN

Secure SDLC: A New Paradigm for the Future of IoT

Why it is crucial to act now and how Exein is pioneering this new paradigm

Exein S.p.A

Rome
Piazzale Flaminio 19,
00196, Italy

San Francisco
535 Mission St 14th floor,
94105, CA

WHITEPAPER

www.exein.io

Contents

1. Securing SDLC: Our Mission for the future of IOT

Traditional software development has primarily focused on ensuring quality, but security has often been **neglected**, being incorporated only during the **final stages** of development, when they are typically more complex to implement. This has increased the likelihood of incurring additional costs, longer development times, and even damaging the business's reputation.

Nowadays, with an increasing number of connected devices, it is imperative to emphasize the importance of security as a foundation of the **software development life cycle (SDLC).** The cybersecurity landscape has been plagued with numerous threats, making it crucial to integrate security into the software development methodology.

Apart from this, it is equally important to educate software developers about security best practices and the potential vulnerabilities that can arise from inadequate security measures. This will not only improve the overall security posture of the software but also ensure that developers are well-equipped to handle any security-related issues that may arise in the future.

In this white paper we describe the needs and benefits of integrating a security-first software development life cycle (SDLC), and how **Exein** is pioneering this fundamental aspect for the future of the Internet of Things (IoT).

2. The Cyber-Resilience Act

The European Commission published the Cyber Resilience Act on September 15, 2022. This new legislation, which will *be finalized by the end of 2023, aims to improve cybersecurity throughout the development and life cycle of products and establish* a clear compliance framework. Two primary objectives stand out regarding the SDLC:

> *"Create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle"*

> *Ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle"*

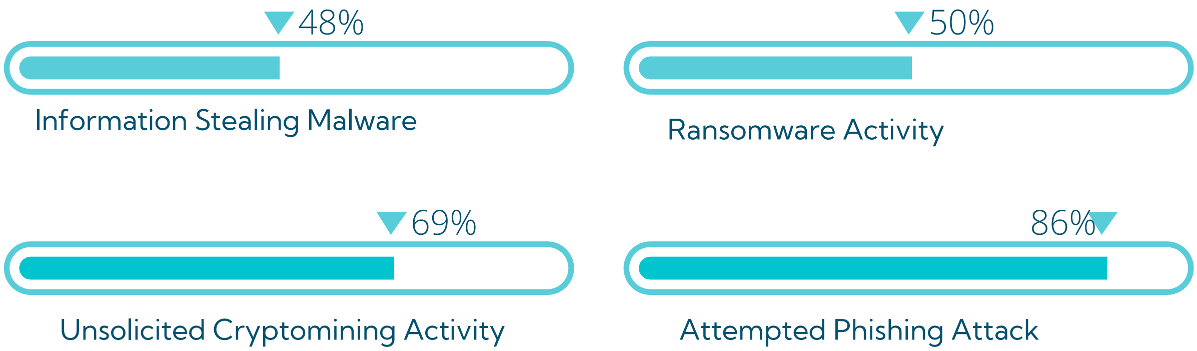
Should you be concerned? Absolutely, If you are involved in the production, import, or distribution of connected products with digital elements (e.g. smart sensors, smart cameras, mobile devices, network devices, etc.).

More info on the Cybersecurity Resilience Act from our Exein Blog.

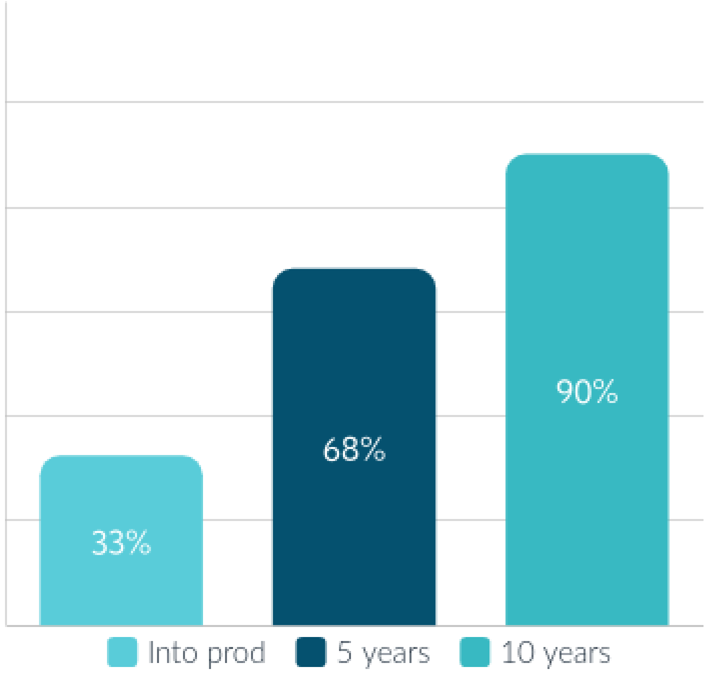
3. Numbers don't lie

Or why we need to take actions

Percentage of organizations subjected to cyber attacks



% of applications with flaws



When application move into production, nearly one-third contain at least one security flaw

88%

Organizations plan to increase cybersecurity

45B+

Connected devices by 2025

4. Securing the SDLC

Key steps and best practices

Securing the SDLC requires a set of established processes and best practices to ensure that security is integrated into every phase of software development. These steps are iterative and should be followed throughout the entire software development lifecycle, in order to create more robust and secure software applications.

1 Requirement Gathering and Threat Modeling

- Clearly define the security requirements and objectives for the software. This includes identifying potential threats, risks, and compliance requirements.
- Perform a thorough analysis of the software design and architecture to identify potential security vulnerabilities and threats. Create a threat model that documents these risks and helps prioritize security controls.

2 Secure Design and Secure Coding

- Develop a secure software design that incorporates appropriate security controls. This involves selecting secure coding practices, secure architecture patterns, and encryption mechanisms.
- Implement secure coding practices during the development phase. This includes following secure coding guidelines, avoiding common vulnerabilities (e.g., buffer overflows, SQL injections), and utilizing secure libraries and frameworks.

3 Static Code Analysis and Testing

- Conduct static code analysis using specialized tools to identify security flaws, vulnerabilities, and coding errors. This helps catch potential issues early in the development process.
- Perform various security testing techniques, such as penetration testing, vulnerability scanning, and security code reviews. These tests validate the effectiveness of security controls and identify any remaining vulnerabilities.

4 Secure Deployment

- Implement secure deployment practices to ensure the software is securely installed and configured in the target environment. This involves securely configuring servers, databases, and other components.

5 Continuous Monitoring and Incident Response

- Establish mechanisms to continuously monitor the software's security in production. This includes logging security-related events, implementing intrusion detection systems, and performing regular security assessments.
- Develop an incident response plan to handle security incidents effectively. This includes defining roles and responsibilities, establishing communication channels, and having procedures to investigate and respond to security breaches.

6 Patch Management and Secure Retirement

- Regularly update and patch the software to address newly discovered vulnerabilities. Maintain an up-to-date inventory of software dependencies and third-party components to ensure timely updates.
- Plan for the secure retirement of the software by following appropriate procedures for data disposal, securely archiving data, and closing any remaining security loopholes.

5. Pioneering Secure SDLC

Exein's Quest for IoT Security Excellence

Since its funding Exein's mission has always been to equip security to all the devices that are connected, across various industries including computers and electronics, manufacturing, automotive, health and medical devices.

We have made significant strides in our efforts to establish a unified, secure ecosystem. Our key achievements include:

- **Runtime Security on All Linux Devices:** We have successfully implemented Runtime Security on a wide range of Linux devices. Our solutions are tailored to optimize performance taking into account the specific resource power and architectures of each device. This includes ARM 64, x86-64 devices and support for different kernel versions.
- **Support Container applications (incl. Docker):** our Runtime and Analyzer solutions support container applications including Docker.
- **Support for Android and Windows Devices (Upcoming):** Our focus extends beyond Linux devices to encompass the ever-expanding Android ecosystem and, in our ongoing commitment to broad compatibility, to include Windows devices.
- **Real-Time Operating Systems (RTOS):** We have recognized the significance of real-time operating systems and we support different flavours of RTOS.
- **Yocto Platinum Membership:** We are proud to be a Platinum Member of the Yocto Project, an open-source collaboration that provides tools and resources for creating custom Linux-based systems.

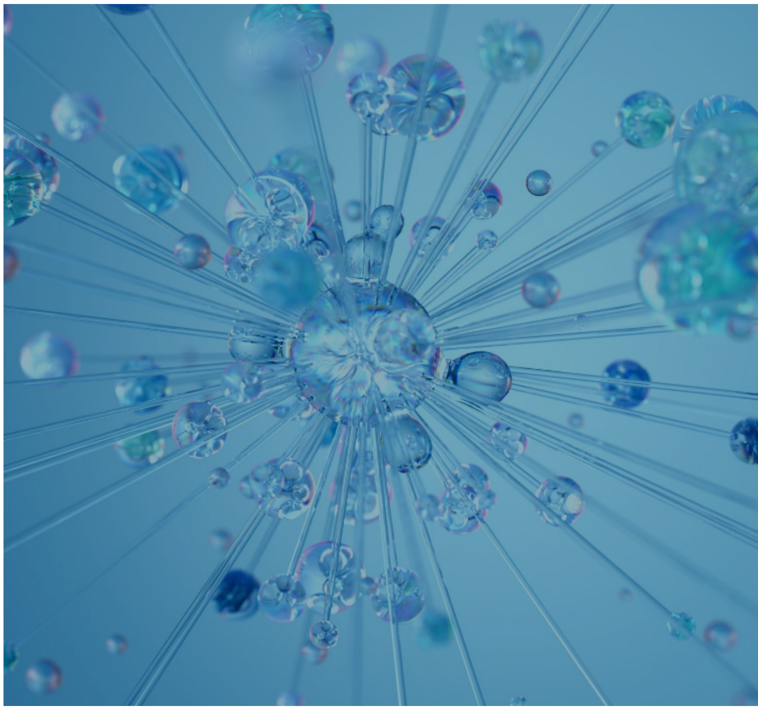
6. The Key Role of Artificial Intelligence

Integrating AI In the SDLC

AI can play a fundamental role in securing the SDLC, where it can be used to identify and reduce potential security vulnerabilities and threats, without the need for human intervention.

This can help to reduce development times and costs, while also improving the overall security posture of the software.

Exein is actively working on integrating generative AI into their upcoming products, demonstrating their commitment to advancing state-of-the-art technology. These are some of the initiatives:



- **Code Fixing and Debugging**: using generative AI to minimize the risk of introducing CVEs during software development.

- **Patch Creation**: prompting generative AI to create and apply patches with build system (e.g. Yocto).

- **Firmware Generation**: generate updated firmware tailored to specific hardware architectures leveraging a wizard-like interface to simplify a secure firmware generation process

- **AI Assistant Functionality**: an intelligent assistant that understands context, educates users about potential threats, and guides them in responding efficiently to security incidents.

- **Automated Security Policy Decisions**: create and apply automated security policy decisions. The AI algorithms can comprehend the appropriate actions to take in response to security events and can apply new static rules to proactively detect and halt attacks, bolstering the security defenses of software systems.

3. Exein Enterprise Security Toolset

- Sofware BOM
- CVE Search Check
- Static Code Analysis
- Malware Scan
- Weak Password Hash findings

Included in

Exein Analyzer

- Managing multiple
- system, including
- Linux, RTOS, UEFI,
- Docker, Android,
- Uboot
- Kernel Security
- Binary Analysis

Included in

Exein Analyzer

- Automatic Report Creation
- Security Firmware Rating
- Workspace Report Management

Included in

Exein Analyzer

- Real-time activity Monitoring
- Fleet Management
- Fast deployment
- Flexible & Cross-platform

Included in

Exein Runtime

- AI-Assisted Control Panel
- AI-based threats and Anomaly Detection
- Custom Policy and Rules Enforcement

Included in

Exein Runtime

More To Come

7. Contact us

Throughout this white paper, we explored the concept of Secure SDLC as a new paradigm for the future of IoT and discussed crucial reasons why it is imperative to act now.

We recognize that every organization has unique security needs,
which is why our solution is customizable to meet those specific requirements.
Our team of experts will work with you to understand your project requirements
and provide a proof of concept (POC) that is entirely free of charge.

During the POC, we will discuss how our technology can help
solve your security problems and provide an opportunity to see it in action.

Contact us at hello@exein.io