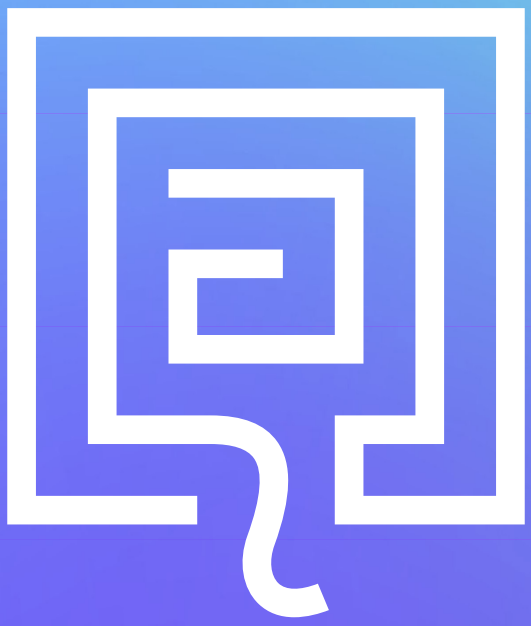


ARIANNA

leads the way

The product security management platform designed by experts

ARIANNA is a product by SECURITY PATTERN

ARIANNA

Leads the way

ARIANNA is a product security management platform for connected devices and systems. Built upon the principles of a robust vulnerability management process, ARIANNA supports device manufacturers to identify, triage, address and report vulnerabilities.

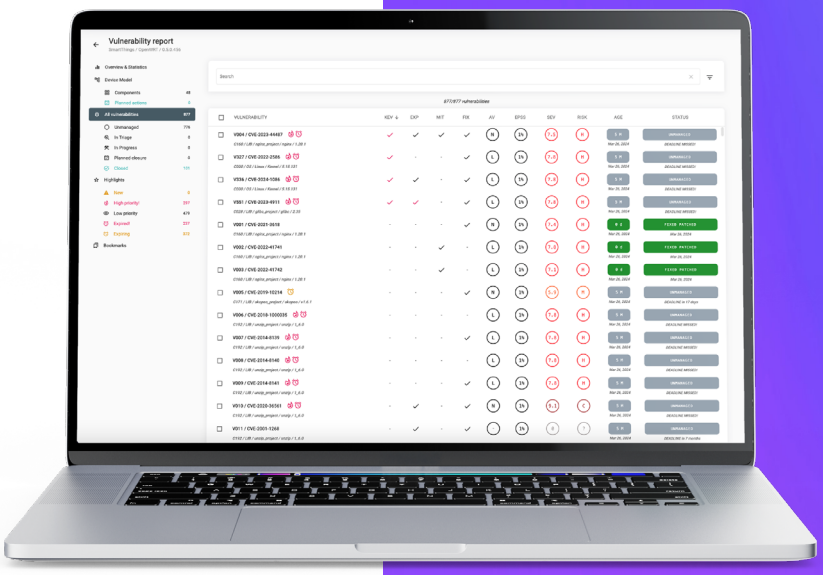
The aim of vulnerability management is not to reach zero vulnerabilities. The aim is to gain visibility into the vulnerabilities and keep them under control. Manage risk according to your use case and the product's intended environment.

ARIANNA analyzes build artifacts to obtain the most accurate Device Model. The Device Model is a complete list of components, both hardware (HBOM[1]) and software (SBOM[2]).

ARIANNA's clear user interface helps device manufacturers understand and prioritize vulnerabilities. Our platform helps the user to make informed decisions by considering the risk a vulnerability will be exploited in their specific system.

Power up your product security

- Experience based
- Human-centered
- Robust



[1] Hardware Bill of Materials

[2] Software Bill of Materials

A compliance journey

Regulations and Standards

The right fit for your industry

Medical
IEC 81001
FDA Pre-Market Submission
MDR (EU 2017/745)

Industrial Automation & Control Systems (IACS)
ISA/IEC 62443

Automotive
ISO/SAE 21434
UN R155 and R156

Consumer Electronics
ETSI EN 303 645
UK PSTI Act

SBOM is an important artifact requested by various regulations and standards. Creating, maintaining and sharing SBOMs are important practices to improve supply chain transparency.

Our SBOMs are compliant with all main regulations and standards.

Our SBOMs are compliant with all main regulations and standards. The SBOM is downloadable in machine-readable formats such as CycloneDX and SPDX. In addition, the SBOM stays up to date with any software versioning changes or component removal/additions.

ARIANNA is unique

Our differentiators

Designed by cybersecurity experts

ARIANNA is born out of a clear need for vulnerability management, witnessed firsthand. Security Pattern's cybersecurity experts noticed this while providing consultancy services to device manufacturers around the globe. ARIANNA has been developed by experts and side by side with the final user: device manufacturers who wish to get more grip on product security.

We don't ignore vulnerable hardware

Security is a combination of hardware, software and procedures. Even though the increased focus on SBOM is a great step toward supply chain security and transparency, it is not enough. Hardware can be vulnerable too. We propose hardware mitigations when the product is already on the market. While during the development of a product, HBOMs and related vulnerabilities can lead to design adjustments.

We build the most accurate Device models

To obtain all the components a device consists of, we analyze artifacts coming from the build procedure. We don't need access to source code, nor do we perform binary analysis. We optimized the Device Model Creation process to be non-intrusive and extremely accurate, minimizing wasting time on false positives.

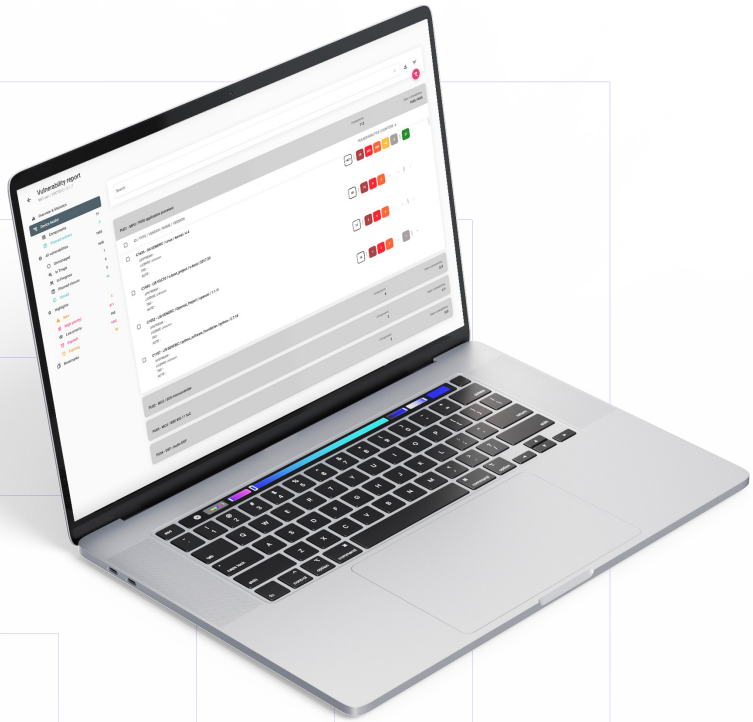
ARIANNA has been developed by experts and side by side with the final user

Your complete solution

Key features

Vulnerability Management

Manage identified vulnerabilities using a robust vulnerability management process. ARIANNA shows all the identified vulnerabilities, and gives remediation and mitigation options. Assign a status to each vulnerability and keep track of all open and closed vulnerabilities. Assign a policy to each project, view vulnerability deadlines and close vulnerabilities in time.



1. **Vulnerability Identification**
   Continuous monitoring and reporting of vulnerabilities: ARIANNA provides the most accurate results through improved vulnerability mapping, identifying false positives and automatically closing patched vulnerabilities.

2. **Vulnerability Triaging and Prioritisation**
   Automated pre-triage using our proprietary engine reduces the vulnerabilities to be analyzed by an order of magnitude or more. In addition, ARIANNA provides all relevant information to assess vulnerabilities, such as available exploits, severity, and EPSS score.

3. **Vulnerability Mitigation and Remediation**
   Review available mitigations and fixes using the original source URLs. This can significantly speed up the time to address a vulnerability.

SBOM / HBOM Management

Get accurate insight into all the components present in your product, both third-party and proprietary components. ARIANNA is unique because it monitors both software and hardware components. By using ARIANNA platform, your SBOM and HBOM always stay up to date, even after changes to the software stack or after addition/removal of components. Automate maintenance by using APIs or manage it directly on the platform.

Compliance

Satisfy requirements from standards and regulations in your industry such as FDA pre-market application, IEC 62443, ISO/SAE 21434, ETSI 303 645, RED, IEC TR 60601-4-5, UL2900 and MDR EU 2017/745.

Exporting & Sharing

Download the SBOM & HBOM in CycloneDX and SPDX, or copy to clipboard. Share results within or outside your organization.

Exploit Intelligence

We highlight four levels of exploit maturity, including actively exploited vulnerabilities from CISA's KEV. Use this information to prioritize vulnerabilities efficiently.

ARIANNA is a product by SECURITY PATTERN

We help creators of smart and connected devices to design, implement, and operate their systems with a sustainable security level.

Security Pattern
www.securitypattern.com
hello@securitypattern.com