xygeni.

Adaion

Case Study

Adaion Minimizes Risk Prioritization Effort and Blocks Zero-Day Malware Attacks

About Adaion

Adaion is an interoperability cloud platform that leverages artificial intelligence (AI) to optimize data usage for energy grid operators, aiding in analysis and decision-making processes. Founded in 2021 by experts in data science and electricity grids, Adaion focuses on creating smart and sustainable grid solutions. Their team comprises specialists who use advanced technologies to guide companies toward effective energy transition.

Adaion's platform handles critical data for grid operators, making cybersecurity crucial for protecting sensitive information, maintaining grid operation integrity, and preventing disruptions from cyber threats. By applying AI to the energy grid, Adaion maximizes the value of available data, helping grid operators with precise analysis and informed decision-making.

The Challenge

Adaion faced significant challenges in ensuring the security of its software development lifecycle (SDLC). The primary concerns were:

- **The potential leakage of sensitive data.**
- **Overall security vulnerabilities within the development process.**

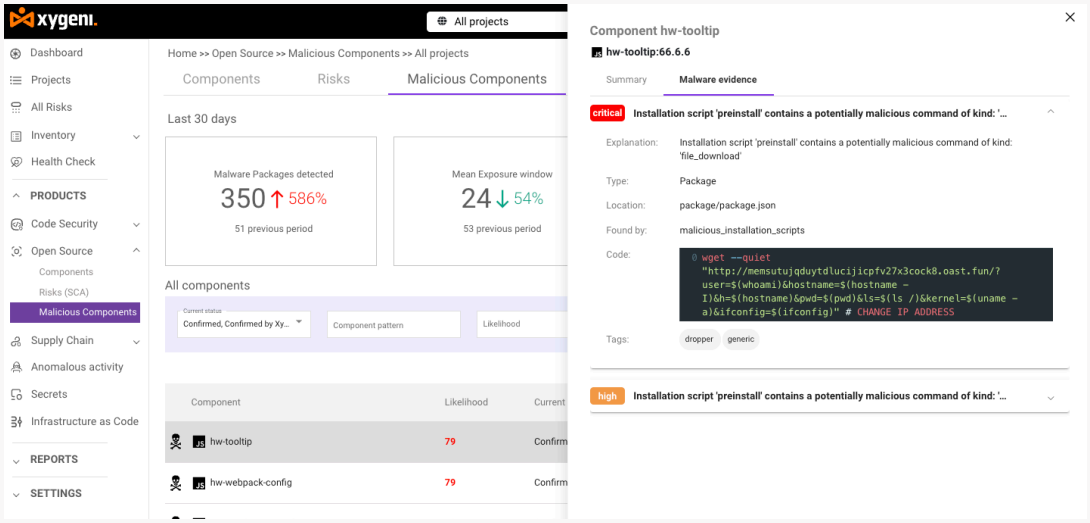
Their products are written in Python, and they use Azure DevOps as their CI/CD platform. As their product matured, securing the SDLC increased it became a priority. Adaion needed a solution to detect malware in open-source dependencies, ensure no secrets were published in source code, and gain visibility into their CI/CD infrastructure to identify and mitigate potential configuration vulnerabilities.

> **We needed to ensure our team and system could handle all security issues efficiently without slowing our operations**
>
> **Óscar J. García Pérez**
> CISO of Adaion

The Solution

After evaluating several options, Adaion chose Xygeni for its comprehensive security coverage and seamless integration capabilities. Xygeni provided the visibility and control needed over their SDLC, integrating seamlessly into Adaion's CI/CD pipelines. This integration allowed for:

- **Real-Time Malware Detection:** Xygeni enabled real-time malware detection in open-source dependencies, providing robust protection against zero-day threats.
- **Continuous Infrastructure Assessment:** Xygeni continuously asses the CI/CD infrastructure for configuration vulnerabilities, helping proactively identify and mitigate risks.
- **Prevention of Secrets Publication:** Xygeni ensured that no secrets were published in source code or any other file, maintaining the confidentiality and integrity of sensitive information.



The implementation process was straightforward and minimally intrusive. Adding the Xygeni scanner to their existing pipelines allowed Adaion to increase the number of applications and repositories analyzed gradually. This phased implementation was based on their capacity and priorities, ensuring a smooth transition and immediate benefits without disrupting their workflow.

Xygeni Support Products

Although Fintonic has tested all Xygeni products, increasing analysis coverage and issues detection, the focus and validated benefits during the PoC were concentrated on the following:

- **ASPM** to provide a single analysis and prioritization pane of glass to ensure maximum focus and impact of the remediation activities on the application's global security without increasing security team efforts.
- **Open Source Security** for certification of no secrets was exposed in any part of the current application and to validate control of leakages even before committing in the SCM.
- **Secrets Security** for certification of no secrets was exposed in any part of the current application and to validate control of leakages even before committing in the SCM.

The Results

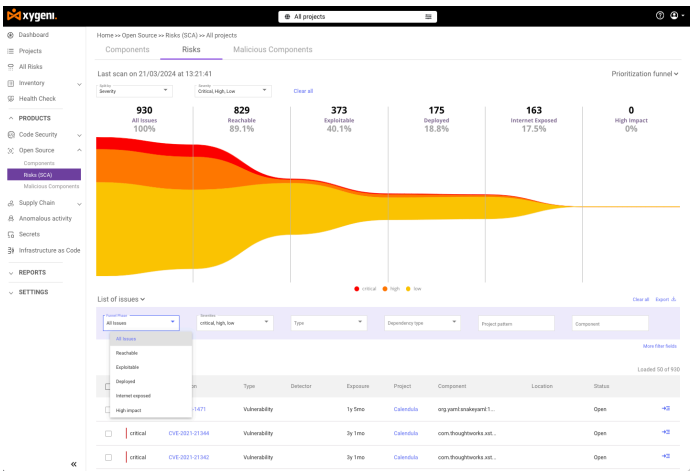
Since implementing Xygeni, Adaion has experienced significant improvements in its security processes. Key features of Xygeni have been particularly instrumental in this transformation:

Prioritization Made Easy

Xygeni Streamlines Adaion's Security Posture

Complete Visibility and Zero-Day Malware Protection

Xygeni helped Adaion achieve significant improvements in its security processes. The principal added value is the **complete visibility of their open-source dependencies, their vulnerabilities, and protection against zero-day malware attacks.** Xygeni provides effortless access to all direct and transitive dependencies, making it crucial to identify those affected by vulnerabilities and other risks immediately. By analyzing each newly published version and notifying Adaion if suspicious code is detected, **Xygeni adds an extra layer of security by blocking its use in automatic CI/CD processes.**



Continuous Assessment and Asset Inventory

Adaion now has visual and agile access to an inventory that is automatically and continuously updated with all development and delivery process assets. At a glance, they can see all repositories, libraries, automation, and cloud resources and how they relate. This continuous assessment allows for the **immediate identification of high-risk areas, saving the security team many hours in discovery and analysis**, and enabling them to focus directly on prioritization and remediation strategies.

Efficient Prioritization Process

The prioritization process has become very efficient, saving dozens of hours of manual work. It is based on a **dynamic funnel whose phases can be defined according to business processes and criteria**. In addition to the automatic calculations of each vulnerability's context, Adaion can add its prioritization criteria.

Peace of Mind with Secrets Protection

Finally, **Adaion enjoys peace of mind and confidence that the secrets of their infrastructure systems are perfectly protected**, with consequent time savings in invalidation and re-securing if such a leak occurs.

> Implementing Xygeni has transformed our approach to security. The visibility of our open-source dependencies and real-time detection of vulnerabilities have been invaluable. The ease of integration and the efficiency of the prioritization process have saved us countless hours. Xygeni's proactive analysis and notification of suspicious code give us peace of mind, ensuring our CI/CD processes are secure. I highly recommend Xygeni to any organization looking to bolster their SDLC security.
>
> **Óscar J. García Pérez**
> CISO of Adaion