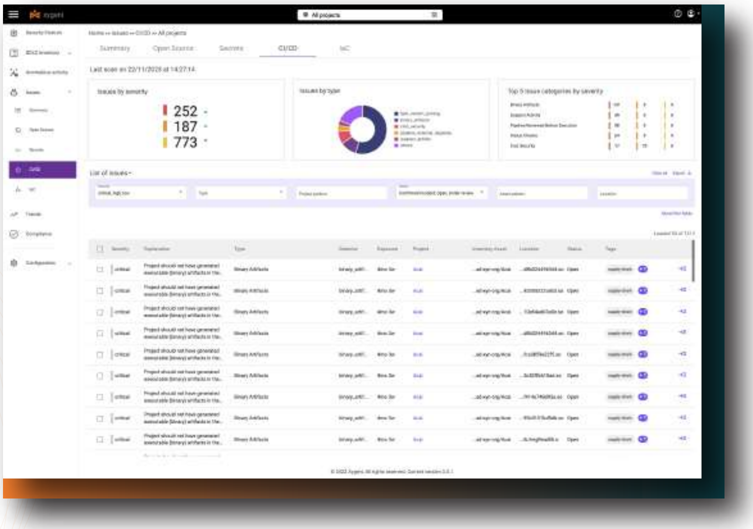
Solution Brief

Xygeni CI/CD Security

Comprehensive Defense for Your CI/CD Pipeline Security

CI/CD Security stands as a sentinel, protecting the CI/CD pipeline and ensuring compliance with the stringent standards required in today's fast-paced, security-conscious development environments.



In a landscape increasingly threatened by 'poisoned pipeline' attacks, as emphasized in a recent study by the European Union Agency for Cybersecurity (ENISA), which found that 60% of supply chain attacks “took advantage” of customer trust in their supplier, and 42% to unknown sources, Xygeni launchs its CI/CD Security solution. This innovative platform directly responds to the growing trend of exploiting vulnerabilities in CI/CD environments, including source code management (SCM) repositories, to launch supply chain attacks. Notable incidents like the SolarWinds, Codecov, and Kaseya breaches have starkly illustrated the risks, with attackers compromising CI/CD environments to gain access to production areas and further propagate attacks.

Xygeni's CI/CD Security offers a comprehensive defense mechanism tailored to safeguard the CI/CD pipeline, a critical component in modern software development. This advanced platform is engineered for real-time detection and response to threats that target vital pipeline tools and configurations. It vigilantly monitors SCM &CI/CD systems, including Jenkins, Tekton, and others, effectively preventing unauthorized access and malicious activities.

Xygeni's CI/CD Security suite offers a robust array of misconfiguration detectors meticulously engineered to safeguard the entire DevOps ecosystem against a broad spectrum of security vulnerabilities. These detectors are strategically categorized to provide targeted and effective monitoring across various aspects of CI/CD and SCM systems, ensuring a fortified and resilient development environment.

60%

of supply chain attacks “took advantage” of customer trust in their supplier*

*ENISA

Solution Brief

Xygeni CI/CD Security

The distinctive mark of Xygeni's CI/CD Security lies in its ability to seamlessly blend comprehensive security scanning with the dynamic nature of CI/CD pipelines. Unlike conventional security tools, it offers an automated, holistic approach to pipeline security, encompassing continuous threat scanning and immediate decision and action. This proactive stance on security is coupled with a deep understanding of common pipeline vulnerabilities, ensuring that both configuration errors and unauthorized alterations are swiftly identified and blocked if desired. Xygeni's CI/CD Security stands as a sentinel, protecting the CI/CD pipeline and ensuring compliance with the stringent standards required in today's fast-paced, security-conscious development environments.

CI/CD Security Domain

Xygeni's CI/CD Security offers a comprehensive defense mechanism tailored to safeguard the CI/CD pipeline, a critical component in modern software development. This advanced platform is engineered for real-time detection and response to threats that target vital pipeline tools and configurations. It vigilantly monitors SCM &CI/CD systems, including Jenkins, Tekton, and others, effectively preventing unauthorized access and malicious activities.

Xygeni's CI/CD Security suite offers a robust array of misconfiguration detectors meticulously engineered to safeguard the entire DevOps ecosystem against a broad spectrum of security vulnerabilities. These detectors are strategically categorized to provide targeted and effective monitoring across various aspects of CI/CD and SCM systems, ensuring a fortified and resilient development environment.

Webhook and Plugin Security

Detectors monitor for the use of secure webhook URLs and guard against the deployment of deprecated or vulnerable plugins, which are potential vectors for security breaches. Additionally, the suite ensures secure communication with remote repositories, advocating for using HTTPS to protect data in transit.

CI/CD Tool-Specific Security

Xygeni's detectors extend their vigilance to include administrative monitoring, workflow permissions, and the implementation of essential security tools like SAST and fuzzing. This ensures that every operational aspect of CI/CD tools is scrutinized for potential misconfigurations, from token permissions to secure communication protocols, thereby safeguarding the integrity of the CI/CD pipeline.

Package Managers and Release Processes

The suite includes detectors that ensure the security of package registries, verify the signing of releases, and advise against using insecure URL dependencies and public repositories. This level of monitoring is crucial for maintaining the security of dependencies and third-party packages integral to the development process.

Source Code Management

Xygeni's detectors focus on preserving code repositories' sanctity. This includes monitoring for binary artifacts, ensuring rigorous code review processes, managing repository access controls, enforcing compliance with organizational security policies such as MFA requirements, and verifying signed commits.

xygeni

Xygeni protects the security and integrity of the CI/CD processes and infrastructure and any software components throughout the entire SDLC. Xygeni shields your Software Supply Chain from unseen threats, providing comprehensive visibility and control throughout the entire SDLC. Our platform enables systematic risk assessment, prioritizes threatened components, and enhances your global security posture, all with unmatched efficiency and cost-effectiveness.

in X

Schedule demo