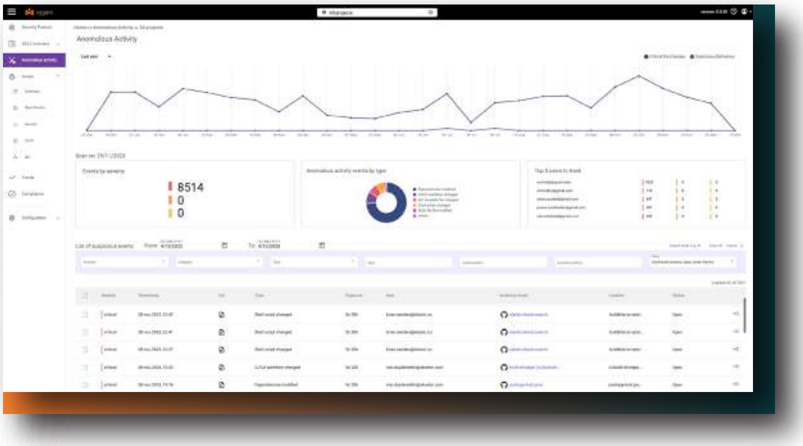
Solution Brief

Xygeni Anomaly Detection

xygeni

Real-time Anomaly Detection for a Secure Software Supply Chain

Secure your Software Supply Chain against unauthorized code modifications, identity theft risks, and other malicious activities. Proactively monitor, assess, and address irregularities in real-time to safeguard your software development and deployment processes.



Effective anomaly detection in the Software Supply Chain is crucial for mitigating insider-related and identity theft risks. It provides an additional layer of security by monitoring for signs of unusual activities that could indicate malicious intent or policy violations, helping to protect the organization's assets and reputation.

Xygeni Anomaly Detection tool responds to the growing need for vigilant monitoring regarding irregularities and unauthorized activities, Xygeni's Anomaly Detection provides an essential safeguard against the risks of unauthorized code modifications and other malicious activities that could compromise the integrity of software development and deployment processes.

Xygeni's Anomaly Detection is a solution designed to proactively identify and address irregularities within the Software Supply Chain. The Xygeni sensor captures activity events in the CI/CD infrastructure, intelligently assesses risks, and identifies potential threats in real time. Xygeni is uniquely equipped to monitor permissions and user activities and extends its vigilance to the entire operational spectrum, including critical events during pipeline execution.

This suite of detectors is intricately classified to target specific areas, ensuring nuanced and effective security oversight.

98%

Cyberattacks prevented with basic security hygiene

Solution Brief

Xygeni Anomaly Detection

Whether it's an attempt to skip code review, unusual code repository or pipeline modifications, or unexpected CI/CD system security configuration changes, Xygeni's Anomaly Detection ensures that such activities are promptly identified and notified to rapid response and potential thread containment and mitigation from the SOC team.

Organizational Sphere

In the Organizational Sphere, the detectors are adept at monitoring critical configurations and operational settings. They watch auditing configurations, CI/CD token scopes, and compliance frameworks, ensuring that any modifications align with the organization's security policies and regulatory standards. The system diligently tracks environment protections and feature flag updates, which are essential for maintaining the organization's operational integrity and security posture.

Repository Level

At the Repository Level, Xygeni's detectors are designed to identify anomalies in code management and user permissions. They alert on unusual pull requests activities, such as anomalous forks or merges bypassing status checks, and monitor for unauthorized or suspicious changes in repository settings, including archiving, deletion, or renaming. This level of monitoring is critical for protecting the integrity of code repositories against unauthorized access and potential code tampering.

CI/CD Environments

For CI/CD Environments, the detectors extend their surveillance to login activities and plugin management. They provide insights into failed login attempts, unusual login patterns, and critical indicators of unauthorized access attempts or compromised credentials. Additionally, monitoring plugin installations ensures that only authorized and vetted plugins are integrated into the Jenkins environment, safeguarding against potential vulnerabilities introduced by third-party tools.

Branch-level monitoring

Branch-level monitoring focuses on the integrity of commits and branch protection protocols. The detectors are configured to alert on unauthorized changes to branch protections, updates to default branches, and modifications to status check requirements. The system ensures that all commits adhere to established security practices, including detecting unsigned commits, which are vital for traceability and accountability in code changes.

CI/CD Project Monitoring

CI/CD Project Monitoring involves monitoring the build process, with detectors specifically tailored to identify unusual build durations. This monitoring aspect is essential in identifying operational inefficiencies or security concerns that might manifest during the build process.

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