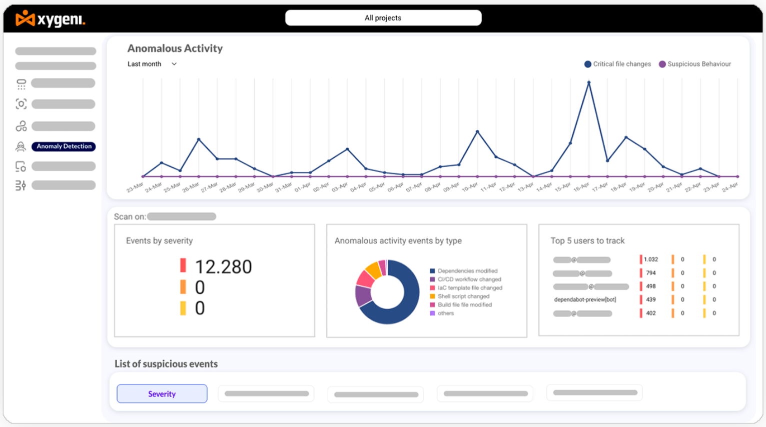
Anomaly Detection

Solution Brief

xygeni.

Real-Time Protection Against Exploits in Your Software Supply Chain

Xygeni's Anomaly Detection provides robust security by actively monitoring and addressing vulnerabilities and risks as they are detected. Our real-time analytics ensure that any attempt to exploit these vulnerabilities is identified and mitigated quickly, protecting the integrity and security of your software operations.



Scan on:

Events by severity

🟥	12.280
🟧	0
🟨	0

Top 5 users to track

[redacted]	1.032	0	0
[redacted]	794	0	0
[redacted]	498	0	0
dependabot-preview[bot]	439	0	0
[redacted]	402	0	0

List of suspicious events

About Company

Xygeni specializes in enhancing software development security and efficiency with our Application Security Posture Management (ASPM) platform. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Information Security Breaches Surveys in the U.K. highlight that the most severe security breaches often stem from critical file modifications and unauthorized activities. This revelation underscores the critical need for robust anomaly detection systems capable of identifying and responding to such unauthorized changes in real time.

Identity theft also poses a serious risk, often facilitated by insider threats and unauthorized access. In 2022, **81% of confirmed data breaches involved compromised credentials, emphasizing the vulnerability associated with weak configurations or stolen passwords.**

Xygeni's Anomaly Detection platform provides an additional layer of security by continuously monitoring and analyzing activities within your SCM and CI/CD infrastructure to identify and respond to unusual behavior quickly. Xygeni detects anomalies that indicate unauthorized modifications, access, or exploitations in real time. This proactive approach ensures that potential security breaches are addressed before they can escalate into serious threats.

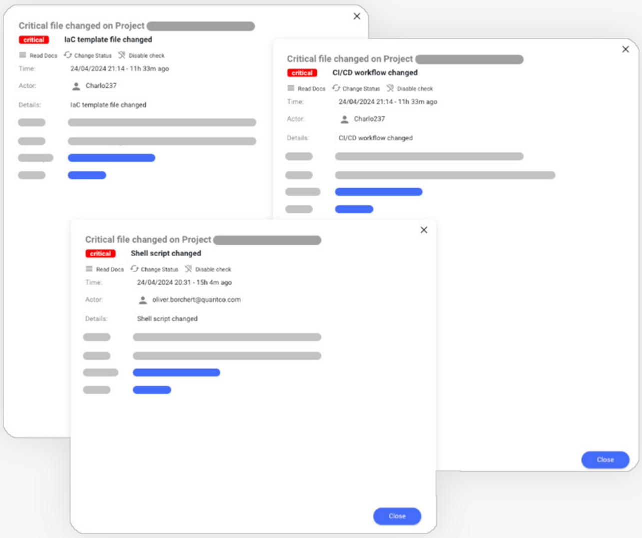
98% Cyberattacks prevented with basic security hygiene

Anomaly Detection

Solution Brief

Robust Code Tampering Protection

Xygeni's Code Tampering secures your applications by detecting unauthorized modifications in your codebase, pipelines, and configurations. It scans critical file changes, promptly identifies malicious alterations, and notifies findings for immediate action. Furthermore, it provides detailed insights including commit details and specific affected files, enhancing your response efficiency. Codetamper scanner is equipped with a variety of detectors designed to identify unauthorized modifications across several crucial areas:



Critical file changed on Project

IaC template file changed

Time: 24/04/2024 21:14 - 11h 33m ago

Actor: Charlo237

Details: IaC template file changed

Critical file changed on Project

CI/CD workflow changed

Time: 24/04/2024 21:14 - 11h 33m ago

Actor: Charlo237

Details: CI/CD workflow changed

Critical file changed on Project

Shell script changed

Time: 24/04/2024 20:31 - 15h 4m ago

Actor: oliver.borchert@quantco.com

Details: Shell script changed

- **CI/CD:** Detects changes in build and workflow files.
- **Context-Aware Prioritization:** Monitors modifications in CODEOWNERS, configuration, environment files, and shell scripts.
- **Descriptor:** Scans for unauthorized changes in dependency descriptor files.
- **Infrastructure as Code (IaC):** Identifies modifications in IaC templates.
- **Policy:** Tracks changes in security policy files.
- **Security Tool Configuration:** Detects alterations in the configuration of security tools.
- **Custom Critical Files:** Alerts on changes to files designated as critically important by the user.

Real-Time Alerting for Anomalies

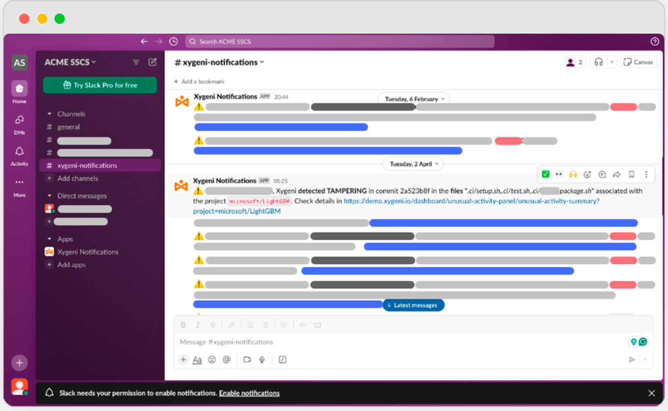
Xygeni ensures proactive security by providing real-time alerts for detected anomalies, allowing your team to respond quickly to potential threats. Alerts can be sent directly via email, a webhook, or integrated into messaging platforms like Slack, ensuring that your teams receive immediate notifications. This rapid alerting system is equipped to deliver crucial context about each incident, enabling a quick and informed response to protect your operations.

Anomaly Detection

Solution Brief

Detect Suspicious Activities in Real-Time

Xygeni's Unusual Activity Detection leverages advanced sensors to provide continuous monitoring and real-time alerts for suspicious behaviors across your software development platforms. This feature is designed to identify and alert on anomalies by analyzing usage patterns and detecting deviations from established normal behaviors, ensuring rapid response to potential security threats. Our system employs a comprehensive set of detectors categorized by the target resource:



Xygeni Notifications APP 20:44

Xygeni Notifications APP 05:25

⚠ [redacted], Xygeni detected TAMPERING in commit 2a523b8f in the files ".ci/setup.sh,.ci/test.sh,.ci/[redacted]package.sh" associated with the project `microsoft/LightGBM`. Check details in https://demo.xygeni.io/dashboard/unusual-activity-panel/unusual-activity-summary?project=microsoft/LightGBM

Slack needs your permission to enable notifications. Enable notifications

- **Organization Detectors:** Monitor changes in configurations, compliance frameworks, and administrative privileges.
- **Repository Detectors:** Detect unusual repository operations such as anomalous merges, deletions, and permission changes.
- **Branch Detectors:** Focus on commits that bypass protections, along with branch setting alterations.
- **Jenkins Detectors:** Track suspicious login behaviors and unusual plugin installations or build durations.

Customize Anomaly Detection Rules

Adapt your anomaly detection strategy to your environment's specific needs with Xygeni's customizable rulesets. Tailor rules align with your organization's unique risk profile, ensuring that alerts are relevant and timely. This customization capability allows you to fine-tune the sensitivity and specificity of the detection system, enhancing the relevance of alerts and improving overall security posture.

Book Your Demo Now - Transform Your Approach to Cybersecurity!