ASPM

Solution Brief

xygeni.

Unifying Risk Management from Code to Cloud

Minimize risks and protect your applications from malicious packages with Xygeni Early Malware Detection. Prioritize and address the vulnerabilities that matter most. Our comprehensive solution offers real-time monitoring of your dependencies to detect and mitigate threats before they impact your software.

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.

Managing security alerts is a critical challenge, especially when **48% of organizations receive over 10,000 alerts daily. Over half of these alerts (up to 52%) are false positives,** leading to alert fatigue and undermining confidence in security systems. Consequently, teams need help to sift through the noise, where critical and relevant vulnerabilities often get overlooked.

Implementing the latest technologies has demonstrated a potential to reduce false positives by up to 60%, significantly clarifying the security landscape and enabling teams to concentrate on genuine threats.

Xygeni's Application Security Posture Management (ASPM) helps address these challenges by integrating accurate proprietary scanning with advanced prioritization capabilities. By considering context information such as asset relationships, severity, exploitability, exposure, business impact, and other customer-defined criteria, **Xygeni reduces unnecessary noise, cutting down alerts by up to 90%.** This strategic focus enables teams to tackle the most pressing issues first, significantly enhancing security responsiveness and efficiency.

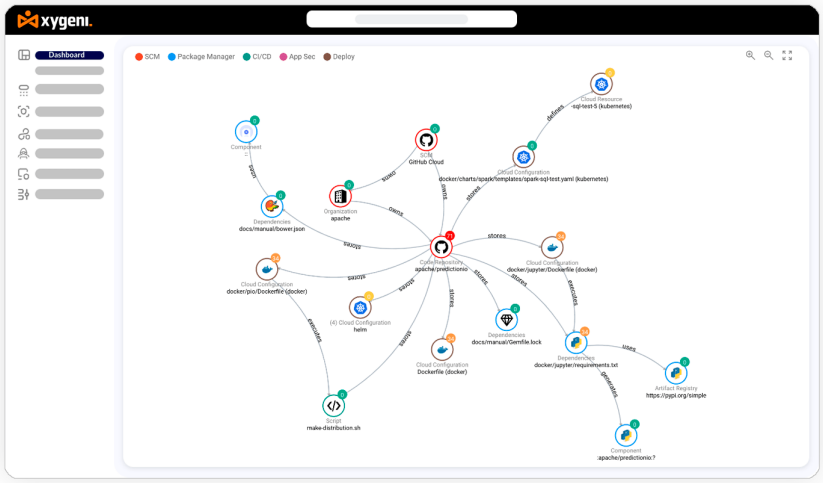
52% of Alerts Are False Positives

xygeni.

ASPM

Solution Brief

Automated Asset Discovery and Inventory Management:



Xygeni automates the identification and cataloging of every asset within your software supply chain, enhancing visibility and control over your development and deployment processes. From source control systems to build tools, CI/CD workflows, and distribution mechanisms, Xygeni captures a detailed inventory of assets including code repositories, open-source and private dependencies, package managers, pipelines and jobs, scripts and build files, plugins and tools, Infrastructure as Code (IaC) templates and cloud resources.

Furthermore, Xygeni automatically identifies and continuously monitors all assets, assessing their interdependencies and the individual and overall security posture of each asset, application, and customer-defined group or category.

Users and Contributors Analysis

Xygeni enhances its Inventory capabilities by integrating a comprehensive Collaborator Analysis feature. This analysis is crucial for managing administrative users, contributors, and collaborators associated with software repositories. By scanning and assessing the roles and activities of individuals involved in the development process, Xygeni supports organizations in achieving the least privilege approach by identifying and mitigating risks related to inactive or overprivileged users. Some key features are:

1. Comprehensive Permissions Review: Xygeni scans for all SCM (Source Control Management) user accounts that have read, write, or manage permissions on repositories. It includes permissions assigned directly to users or inherited from groups with access to the repositories.

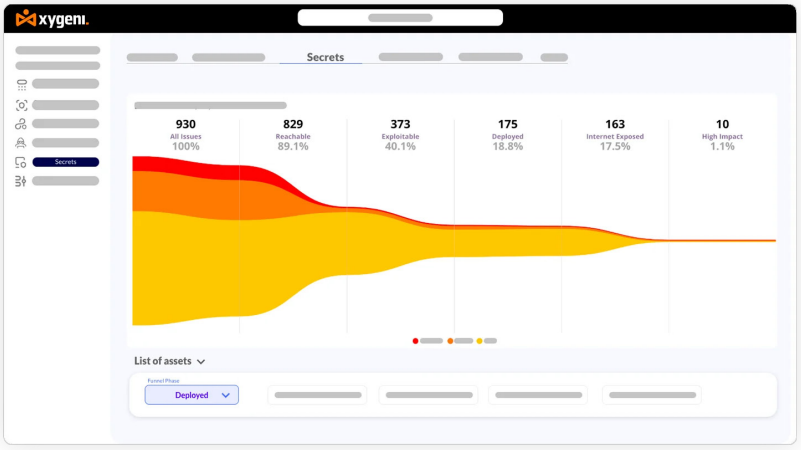
2. Group and User Tracking: The system registers all SCM groups, including any users with significant permissions, ensuring that all potential access points are monitored and controlled.

3 Non-SCM Contributors: Xygeni also identifies git users who are not linked to an SCM account but have made commits to the git history. Xygeni tracks contributions across all branches, providing a complete picture of who has influenced the codebase.

ASPM

Solution Brief

Advanced Dynamic Prioritization:



Xygeni's prioritization capabilities go beyond standard methods by incorporating dynamic funnels that allow for extensive customization and precise filtering. Customers can define up to eight stages in their prioritization funnel, tailored not only by severity but also by issue type and category. This flexibility ensures that each organization can focus on the vulnerabilities that pose the highest risk according to their specific security policies and operational needs.

The funnel system supports the integration of customer-defined properties alongside pre-configured stages such as reachability or exploitability, among others. This allows organizations to refine their security focus further and manage vulnerabilities more effectively based on unique criteria important to their environment. By utilizing Xygeni's dynamic funnels, teams can optimize their security efforts, ensuring that critical issues are quickly identified and addressed.

Integration of Third-Party Security Reports:

Xygeni's Application Security Posture Management (ASPM) platform enhances its capabilities by easily integrating reports from third-party security tools, including Static Application Security Testing (SAST) and Software Composition Analysis (SCA) tools. This integration allows organizations to leverage their existing technology stack, providing a comprehensive view of security threats across different tools and platforms. By consolidating and correlating these reports, Xygeni helps teams understand their security posture in a unified context, ensuring that all potential vulnerabilities are identified, prioritized, and addressed efficiently. Key benefits of this integration include:

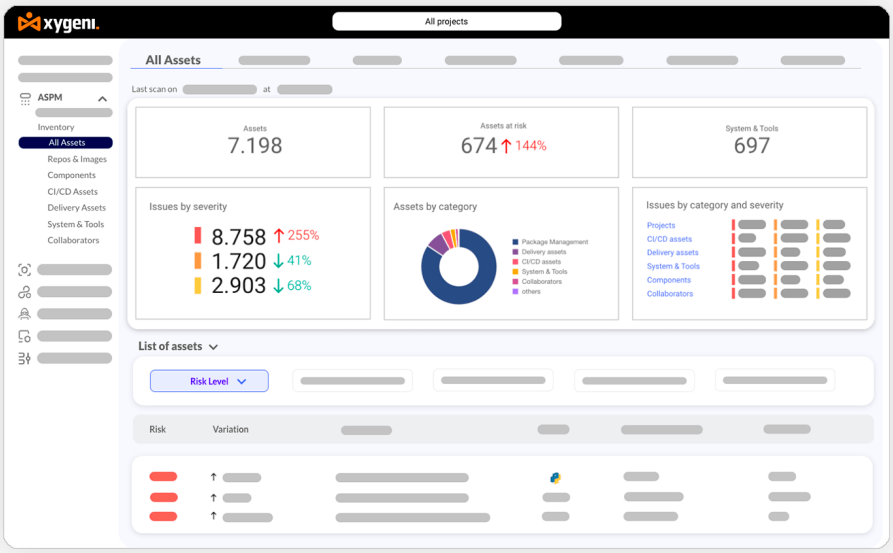
- **Unified Security Dashboard:** Consolidates findings from various tools into a single, comprehensive dashboard for easy monitoring and analysis.
- **Enhanced Threat Detection:** Combines data from multiple sources to provide a more complete assessment of security risks.
- **Efficient Remediation:** Enables quicker and more coordinated responses to security issues by providing centralized management of vulnerabilities.

ASPM

Solution Brief

Audit Trail of Security Events

Xygeni's Application Security Posture Management platform includes a robust security audit trail feature that provides a comprehensive timeline of events associated with each asset. This feature tracks and logs all significant activities, such as changes, updates, and security incidents, ensuring that users have a clear and detailed view of the security history for each asset within their software environment. The most relevant capabilities of our security audit trail are:



- **Event Login:** Every modification, update, or security event related to an asset is meticulously logged, creating a chronological record that can be crucial for troubleshooting, compliance audits, and security investigations.
- **Comprehensive Coverage:** The audit trail captures a wide range of events, from code commits and build configurations to deployment activities and configuration modifications, ensuring that all aspects of the asset lifecycle are monitored.
- **Easy Access and Visualization:** Users can easily access and visualize the audit trails through Xygeni's intuitive interface to quickly find specific events or patterns.
- **Enhanced Security and Compliance:** By maintaining a detailed record of all actions taken on each asset, organizations can enhance their security posture and compliance with regulatory requirements, making it easier to verify that proper processes are followed and to detect potential security breaches early.

Quick and Efficient Remediation Process

Xygeni's ASPM platform optimizes the remediation process by providing detailed guidelines and automated actions for addressing risks and vulnerabilities. It offers clear, actionable steps tailored to each specific issue, enabling quick and effective resolutions. Integration with ticketing and tracking tools facilitates easy updates to workflows, ensuring vulnerabilities are promptly managed

ASPM

Solution Brief

xygeni.

Integration of 3rd-party security reports

Xygeni Xygeni's platform allows for uploading reports from both third-party tools and Xygeni scans. This is accomplished using the report-upload command, which facilitates the integration of external scan results into the Xygeni ecosystem for comprehensive analysis and management.

Upon uploading, the command validates and normalizes the findings, converting them into Xygeni's standard format. This standardization allows for consistent processing of findings across different tools, enhancing the platform's prioritization, filtering, and remediation workflows.

Users can specify the report file and its format, which helps accurately process the report. If the format is not explicitly provided, it can be automatically inferred. Additionally, users can specify custom properties such as business value or architectural significance, which can influence how findings are prioritized and handled within the platform.

Xygeni integrates with a wide range of third-party security tools, enhancing our platform's capability to manage various security assessments. Here's a summarized overview of the supported scanners and formats:

Types of Analysis Supported:

- Software Composition Analysis (SCA)
- Static Application Security Testing (SAST)
- Infrastructure as Code (IaC) Flaws
- Secrets Detection

Supported Tools:

- Checkmarx (SCA, SAST, IaC)
- Fortify (SAST)
- Snyk (SCA)
- Checkov (IaC)
- KICS (IaC)
- GitLeaks (Secrets)

Supported Formats:

- SARIF (Standard format for multiple analysis types)
- JSON (Widely used for all types of analysis)
- XML (Specifically for certain SAST tools like Checkmarx)
- .fpr and .fvdl (Specific to Fortify SAST)

Book Your Demo Now - Transform Your Approach to Cybersecurity!