

Xygeni Unveils Revolutionary SCA and ASPM Technologies at Black Hat USA 2024

Xygeni Introduces Streamlined Open Source Security, Advanced Malware Detection, and High-Performance AppSec Prioritization

LAS VEGAS, NEVADA, USA, August 8, 2024 /EINPresswire.com/ -- Xygeni, a leader in cybersecurity innovation, is excited to announce its participation in Black Hat USA 2024. As part of our commitment to advancing cybersecurity, we are proud to showcase our latest product launches designed to address the most pressing security challenges facing organizations today. Attendees will have the opportunity to explore our groundbreaking solutions, including XYGENI SCA, Xygeni Early Warning (MEW), and XYGENI ASPM.



Our MEW system embodies our proactive approach to cybersecurity, offering organizations an early warning system that keeps them one step ahead of cyber threats”

Jesus Cuadrado, CPO of Xygeni

Streamline Open Source Supply Chain with Reachability and Automated Remediation

[Xygeni Open Source Security](#) provides advanced SCA (Software Composition Analysis) capabilities including:

Reachability Analysis: Unlike conventional SCA tools, Xygeni integrates function-level reachability analysis, enabling security managers to understand the actual impact of vulnerabilities within their codebase. By identifying whether a vulnerability is reachable or exploitable, organizations can prioritize fixes more effectively.

Advanced Remediation: Xygeni increases the efficiency of the remediation process by automating actions to remove vulnerable dependencies or replace them with the safe version. In other cases, Xygeni provides the needed guidance for required manual actions, ensuring that vulnerabilities are addressed rapidly and minimizing exposition windows and potential attack vectors.

Pioneering Malware Detection with Xygeni Malware Early Warning (MEW)

The Xygeni Malware Early Warning (MEW) system is designed to detect and block unknown malware threats in Open Source packages before they can infect the customer application. As cyber threats evolve and attacks through the open-source supply chain grow, the need for

proactive measures becomes increasingly critical.

Unknown Malware Detection: MEW leverages advanced algorithms and code behavioral analysis to identify and mitigate zero-day malware not registered in any database. This approach improves protection beyond traditional protection based on CVEs and signatures.

Immediate Proactive Defense: By continuously monitoring the publication of new Open Source packages and new versions of existing ones, MEW analyzes them immediately and provides an early warning system that alerts security teams to potential threats before they use risky versions and block attempts to usage of malicious versions.

High Performing Prioritization across all your AppSec Tools with Xygeni ASPM

[Application Security Posture Management \(ASPM\)](#) is critical for reducing noise and fatigue by alerting and optimizing effort allocation for effective security posture improvement. Xygeni ASPM is designed to provide comprehensive oversight and management, ensuring security policies are effectively enforced across all applications.

Third-Party Integrations: Xygeni ASPM seamlessly integrates with a wide range of third-party tools, enhancing its capability to aggregate multiple security sources to remove any adoption barrier and accelerate integration in current operative environments with minimum effort and cost.. It ensures that organizations can leverage their existing security investments while benefiting from enhanced visibility and control.

Dynamic Prioritization Funnels: Our prioritization funnel technology allows security teams to configure the prioritization process according to their technical and business criteria. Automated calculation of contextual criteria enables a careful prioritization process with minimal effort. It ensures that the most critical issues are addressed first, optimizing resource allocation and response times.

"XYGENI ASPM is a game-changer for application security management, providing the tools and insights needed to maintain a robust security posture in today's dynamic environment" Jesus Cuadrado, CPO of Xygeni.

About Xygeni

Xygeni specializes in Application Security Posture Management (ASPM), using deep contextual insights to prioritize and manage security risks while minimizing noise and overwhelming alerts.

Our innovative technologies automatically detect malicious code in real-time upon new and updated components publication, immediately notifying customers and quarantining affected

components to prevent potential breaches.

With extensive coverage spanning the entire [Software Supply Chain](#)—including Open Source components, CI/CD processes and infrastructure, Anomaly detection, Secret leakage, Infrastructure as Code (IaC), and Container security—Xygeni ensures robust protection for your software applications.

Trust Xygeni to protect your operations and empower your team to build and deliver with integrity and security.

Fátima Said

Xygeni

fatima.said@xygeni.io

Visit us on social media:

[X](#)

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/733950321>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.