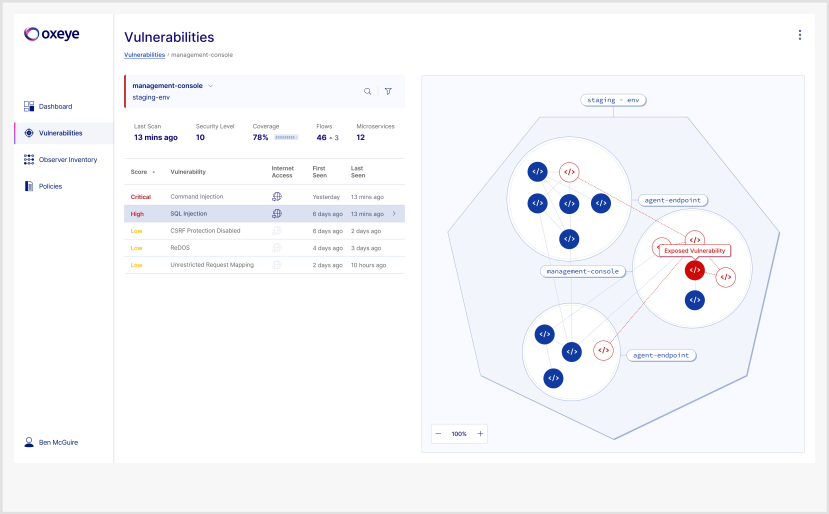
Oxeye Targets Millions of Insecure Cloud Native Applications with CNAST Platform

Advanced Solution Analyzes Code-level Vulnerabilities to Deliver Contextualized Risk Assessment for Cloud Native Applications



TEL AVIV, ISRAEL, December 7, 2021 /EINPresswire.com/ -- Oxeye, a technology innovator in cloud-native application security testing, today announced the company's Cloud Native Application Security Testing Platform (CNAST). The new platform identifies code vulnerabilities, open-source vulnerabilities, and secrets to highlight the most critical issues in the software development lifecycle, delivering clear guidance for fast and accurate remediation.

According to Gartner's 2021 Magic Quadrant for Application Security Testing, "Modern application design and the continued adoption of DevSecOps are expanding the scope of the AST market. Security and risk management leaders can meet tighter deadlines and test more complex applications by seamlessly integrating and automating AST in the software delivery life cycle."

> The Oxeye platform provides a single unified platform for modern application security testing, providing highly accurate vulnerability testing prior to cloud native app production."
>
> *Dean Agron, Co-Founder and CEO of Oxeye*

However, unlike traditional AST, cloud native application security testing necessitates a different approach. One that provides context via enrichment of the surrounding application components. Unlike SAST, DAST, IAST and SCA, the Oxeye CNAST approach is focused on contextual analysis to point out the exploitable vulnerabilities and secrets. This includes analyzing all potential risks, deep mapping of all app components and how they communicate with each other, lightweight fuzzing for active validation and enrichment of the underlying container, cluster and cloud configurations.

Oxeye CNAST is centered on the cloud native segment of the AST market, which is rapidly accelerating as AppSec and DevSecOps professionals scramble to protect more than 500 million cloud-native apps expected to be deployed by 2023. To secure these applications, developers will need to conduct testing and be absolutely sure they remain safe throughout deployment. Oxeye supports scalable, ever-changing environments and automatically adapts to changes for an agile testing scope without changes to code or the need to manually intervene.

Oxeye's vulnerability profiling helps prioritize the most urgent areas to focus on, leveraging powerful capabilities that include:
- Complete Cloud Native Application Security Testing for Modern Architectures – Oxeye analyzes code across microservices to identify code vulnerabilities and other critical issues as part of the software development lifecycle for clear guidance that enables accurate remediation.
- Multi-Layer/Multi-Service Identification of Exploitable Vulnerabilities - Provides Runtime Code Analysis without the need for changes to application code, Vulnerable Flow Analysis to detect vulnerabilities across application microservices, and Active Validation with automatic creation and execution of security tests to validate vulnerabilities prior to reporting.
- Contextual Risk Assessment - Enriches data with infrastructure configuration information from the container, cluster, and cloud layers to calculate risks based on Internet accessibility, sensitive data processing, flawed configuration, etc.
- Clear Remediation Guidance for Developers – Provides developers with application analysis in runtime to reproduce each step of vulnerability exploitation, delivery of the exact line of code where the vulnerability has been executed, and vulnerability flow visibility for accurate execution flow tracing that allows for fast identification and remediation of actual issues.

"Pieces of code are located literally everywhere throughout cloud native applications," said Dean Agron, Co-Founder and CEO of Oxeye. "The Oxeye platform provides a single unified platform for modern application security testing, providing highly accurate vulnerability testing prior to production. With it, users gain access to the most prominent, automated security risk testing solution for all important stages of software development."

Pricing and Availability
Oxeye Cloud Native AST will be generally available in Q1, 2022. Oxeye invites IT professionals interested in learning more to visit https://www.oxeye.io/solution or to schedule a personalized demo at https://www.oxeye.io/get-a-demo.

Resources:
- Follow Oxeye on Twitter at @OxeyeSecurity
- Join Oxeye on LinkedIn at https://www.linkedin.com/company/oxeyeio/
- Visit Oxeye online at http://www.oxeye.io

About Oxeye

Oxeye provides a cloud-native application security testing solution designed specifically for modern architectures. The company enables customers to identify and resolve the most critical code vulnerabilities as an integral part of the software development lifecycle, unding Round as Company disrupting traditional application security testing (AST) approaches by offering a contextual, effortless, and comprehensive solution that ensures no vulnerable code ever reaches production. Built for Dev and AppSec teams Oxeye helps to shift security to the left while accelerating development cycles, reducing friction, and eliminating risks. To learn more, please visit www.oxeye.io.

Joe Austin
Public Relations
email us here
Visit us on social media:
Twitter
LinkedIn
