oxsecurity

Integrated Software Composition Analysis (SCA)

Better insight, fewer false positives

Given the pervasive use of third-party components in application development, identifying and remediating code vulnerabilities as early in the development lifecycle as possible is critical. However, many SCA tools fall short, providing only superficial analysis that overloads teams with irrelevant or non-actionable alerts and false positives. Such tools tend to use a generic approach to prioritizing security issues, disregarding the context of vulnerabilities within the application and creating unnecessary noise and alert fatigue.

OX has integrated our proprietary SCA technology into the industry's first Active ASPM platform to provide a more intelligent approach to managing third-party code security and compliance challenges. Unlike traditional SCA tools, OX provides highly accurate risk prioritization, considering factors like reachability, exploitability, and damage potential of vulnerabilities. OX also consolidates related vulnerabilities based on root causes to reduce alert noise and presents a clear remediation path detailing resolved vulnerabilities and related information.

Comprehensive Risk Analysis and Remediation for Third-Party Code

The OX Active ASPM platform embeds proprietary SCA technology and can connect with your existing SCA tools to provide additional coverage.

- Integrated into OX's Active ASPM platform encompassing SAST, SCA, container security, SBOM, IaC, Git, and CI/CD posture, protecting secrets, PII, artifact integrity, and cloud security.
- Analyzes open-source packages and their licenses within the codebase to ensure compliance and manage security risks.
- Utilizes a 3-layer model to evaluate and prioritize vulnerabilities based on exploitability, reachability, and business impact, significantly reducing false positives by an average of 97%.
- Links container issues back to the code, turning traditional alerts into actionable items with clear paths to resolution.
- Facilitates comprehensive issue management by enriching issue reports with Software Bill of Materials (SBOM) information, including licensing, maintenance status, popularity, and code usage details.
- Provides detailed Dockerfile insights for base images, operating systems, and packages, enhancing container security.

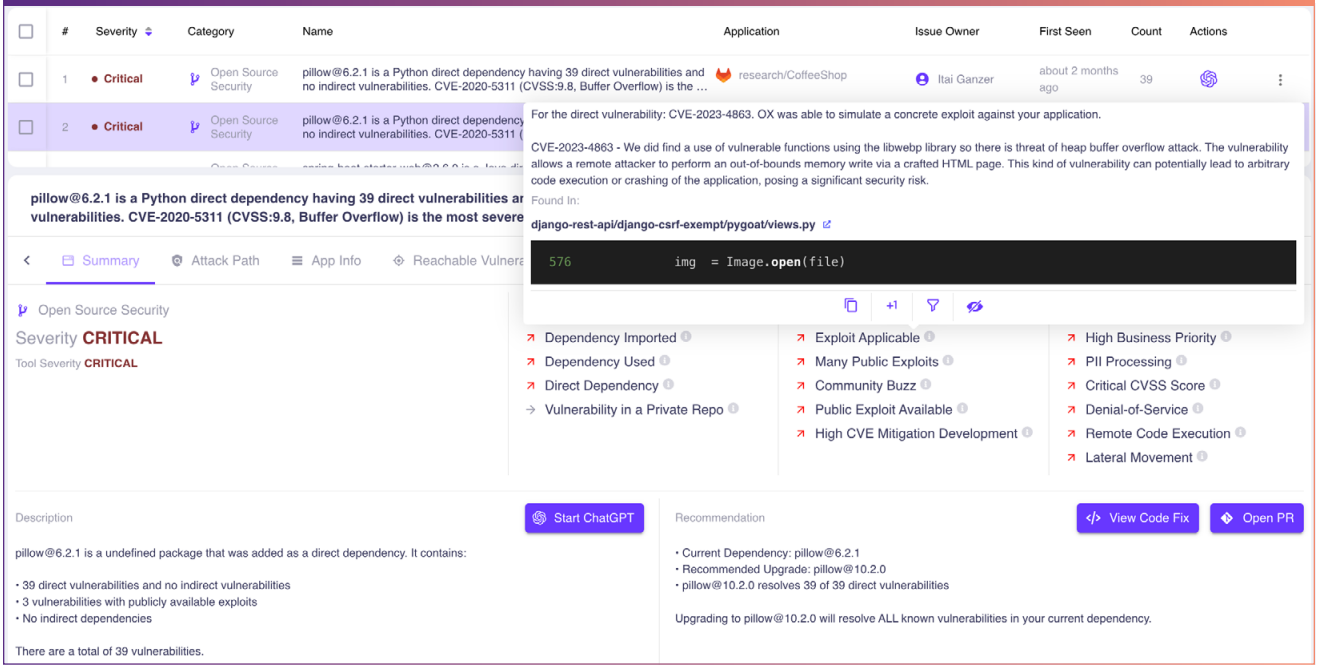
Superior Visibility, More Accurate Prioritization, and Faster Remediation

OX's Software Composition Analysis (SCA), integrated within our Active ASPM Platform, outperforms alternative SCA tools by providing deeper insights and eliminating inefficiencies. Through features like consolidated issue analysis and advanced dependency assessment, OX offers a smarter, actionable approach to navigating the complexities of third-party code components and streamlines the software development lifecycle.

Reduce noise and remediate faster with consolidated issue analysis

OX aggregates vulnerabilities across libraries and conducts root cause analysis. This approach consolidates multiple vulnerabilities into a single actionable issue, dramatically reducing alert fatigue by focusing on effective remediation rather than merely identifying problems.

OX maximizes accuracy in prioritizing identified issues by applying a 3-layer contextual analysis.



Navigate complex dependencies with advanced dependency assessment

AppSec Professionals frequently dedicate substantial time to validating the significance of specific Software Composition Analysis (SCA) findings before delegating remediation tasks to developers. Key questions include whether a vulnerable dependency is in use and, if so, whether it interacts safely with developer code. Leveraging OX's expertise in various application security testing technologies can significantly streamline this process. OX is adept at determining whether developer code is using—or not using—a dependency in ways that could potentially be exploited. This capability can save considerable time and enhance security efficacy.

OX SCA distinguishes between direct and indirect package dependencies, creating a dynamic visualization for both direct and indirect libraries. This enables users to understand the full scope of their project's dependencies at a glance, allowing them to view the entire graph or just the direct paths. It serves as visual proof of our deep analysis capabilities, enabling informed decision-making on security priorities.

Focus on the risks that matter most with context-sensitive prioritization

OX maximizes accuracy in prioritizing identified issues by applying a 3-layer contextual analysis. Each issue is analyzed based on reachability (can the vulnerability be accessed by an attacker), exploitability (if it is reachable, can the attacker take advantage of it), and damage (is malicious behavior such as remote code execution possible by exploiting the vulnerability).

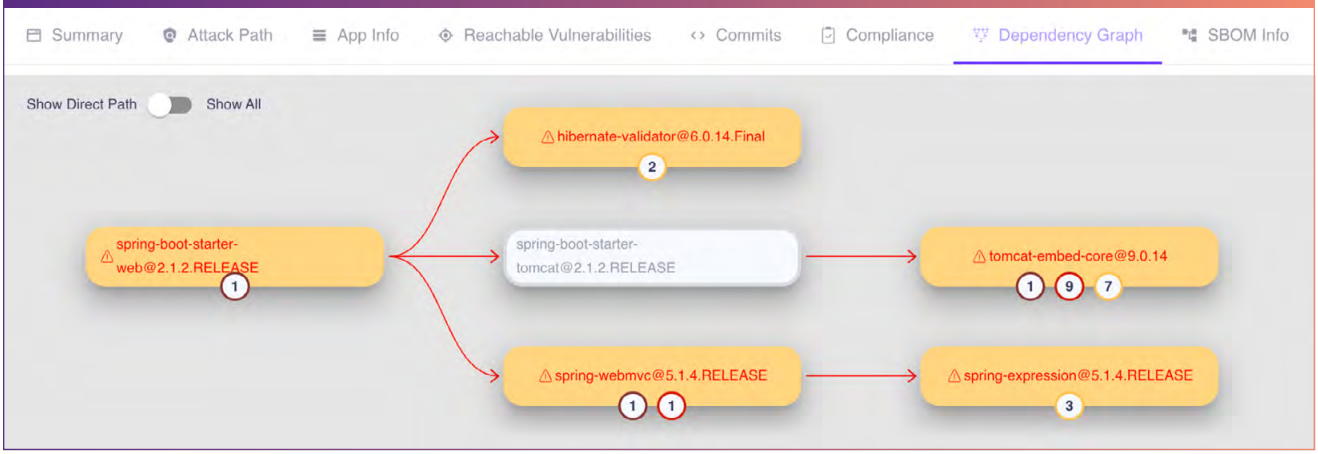
Get ahead of compliance requirements with comprehensive issue management

OX links SCA issues to software bill of materials (SBOM), assessing compliance standards, package maintenance, popularity, and actual code usage. This holistic view clearly explains each issue's impact and compliance implications.

Save time and automate manual tasks with an efficient remediation path

OX presents a clear remediation path and developer guidance detailing resolved vulnerabilities and related information. It allows users to open pull requests (PRs) directly from the interface with a single click and create no-code automated workflows to facilitate immediate action.

OX maps the dependencies between multiple security issues into a single, actionable alert.



oxsecurity

Founded by Neatsun Ziv and Lion Arzi, two former Check Point executives, OX is the first and only Active Application Security Posture Management (ASPM) Platform, consolidating disparate application security tools (ASPM+AST and SSC) into a single console. By merging an AppSec data fabric with a user-centric approach tailored for developers, OX offers complete visibility, prioritization, and automated remediation of security issues throughout the development cycle, enabling organizations to release secure products quickly.

INTERESTED IN LEARNING MORE VISIT: WWW.OX.SECURITY/BOOK-A-DEMO/