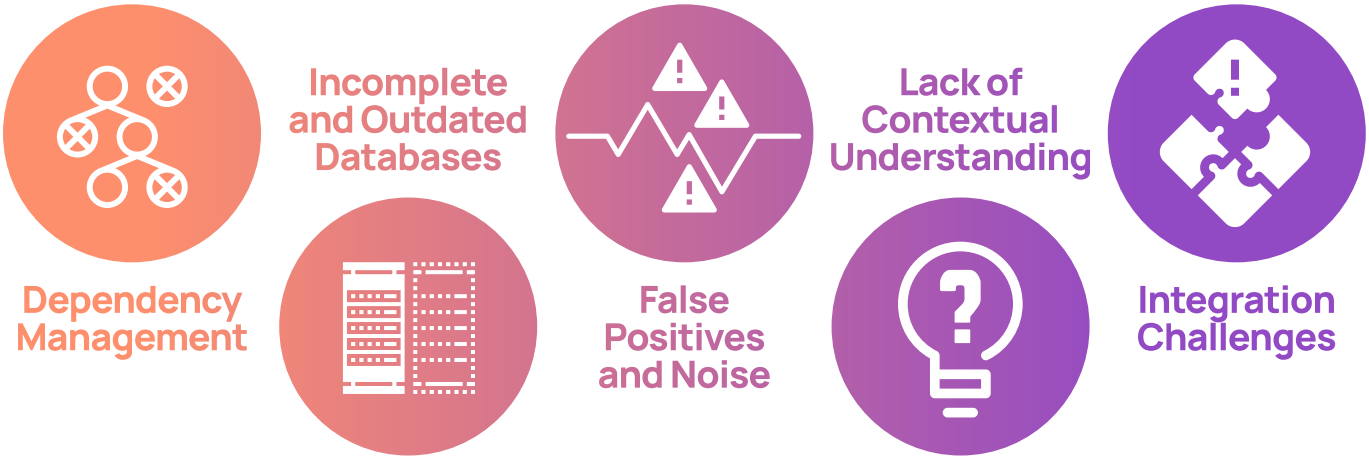
ox security

Choosing the Right SCA for Your Organization

Integrated SCA Shines a Light on Software Supply Chain Risk

Given the widespread use of third-party components in application development, identifying and remediating code vulnerabilities as early in development as possible is critical. However, traditional SCA tools fall short, providing superficial code analysis that overloads irrelevant or non-actionable alerts and false positives. Reasons for this can include:



Dependency Management

Modern applications often rely on a wide array of third-party components, each with its own transitive dependencies. Manually managing these dependencies can be daunting, leading to version conflicts, compatibility issues, and deployment bottlenecks, given a lack of awareness of how various libraries depend on one another. While SCA tools aim to provide visibility into these dependencies, the sheer volume and intricacy of modern software ecosystems make maintaining an accurate and up-to-date inventory challenging.

Incomplete and Outdated Databases

SCA tools rely heavily on databases of known vulnerabilities and open-source licenses to assess third-party components' security and compliance status. However, these databases often need to be completed or updated, leading to false positives, false negatives, and inaccurate risk assessments. Moreover, the delay between discovering a vulnerability and its inclusion in these databases can expose applications to potential threats, highlighting the need for real-time monitoring and proactive vulnerability management.

False Positives and Noise

One of the most common frustrations for developers using SCA tools is the prevalence of false positives and noise, as these tools often just look at vulnerabilities (CVEs) without understanding dependency relationships or usage within developer source code. SCA tools often flag insignificant or irrelevant issues, inundating developers with notifications and causing alert fatigue. Distinguishing genuine security threats from benign anomalies requires considerable time and effort, detracting from the overall effectiveness of the tool and leading to alert fatigue among development teams.

Lack of Contextual Understanding

While SCA tools excel at identifying vulnerabilities and license violations within third-party components, they often lack contextual understanding of how these components are used within the application. As a result, they may flag specific dependencies as problematic without considering that a developer may be using vulnerable components in a way that does not create a security risk. This lack of context can lead to misguided remediation efforts and unnecessary disruptions to the development process.

Integration Challenges

Integrating SCA tools into existing development workflows and toolchains can pose significant challenges for organizations. SCA must integrate seamlessly with a variety of development tools and processes to provide timely insights and facilitate proactive risk management. However, some SCA tools require agent installations and complex pipeline integrations, which can slow development productivity with excessive scan times.

OX's Integrated SCA Provides Better Visibility and More Accurate Prioritization

Through detailed discussions with dozens of DevOps and AppSec leaders and practitioners, OX Security has gained a deep understanding of the frustration these shortcomings have created.

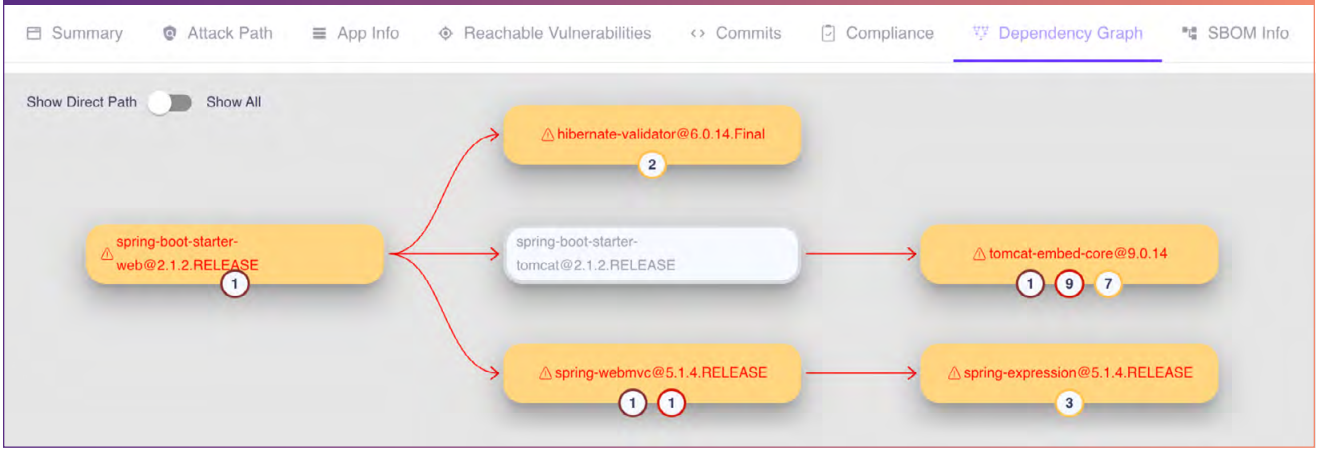
> **"Within five minutes, we connected GitLab, our main repository, to OX. Scanning started straight away, and it was just like Hallelujah!"**
>
> **Eric Austin**
> **Head of Security, Playbook Engineering**

Enter OX's SCA, a fully integrated component of our Active ASPM platform. By eschewing a generic, one-size-fits-all analysis model in favor of a more contextualized approach to AppSec, OX has redefined the standards for software composition analysis.

OX's SCA offering provides a comprehensive and efficient solution to the security and compliance challenges associated with open-source libraries and third-party dependencies in codebases. By architecting SCA as an agentless integration within the OX ecosystem rather than a third-party plug-in, OX addresses the shortcomings listed above in several key ways:

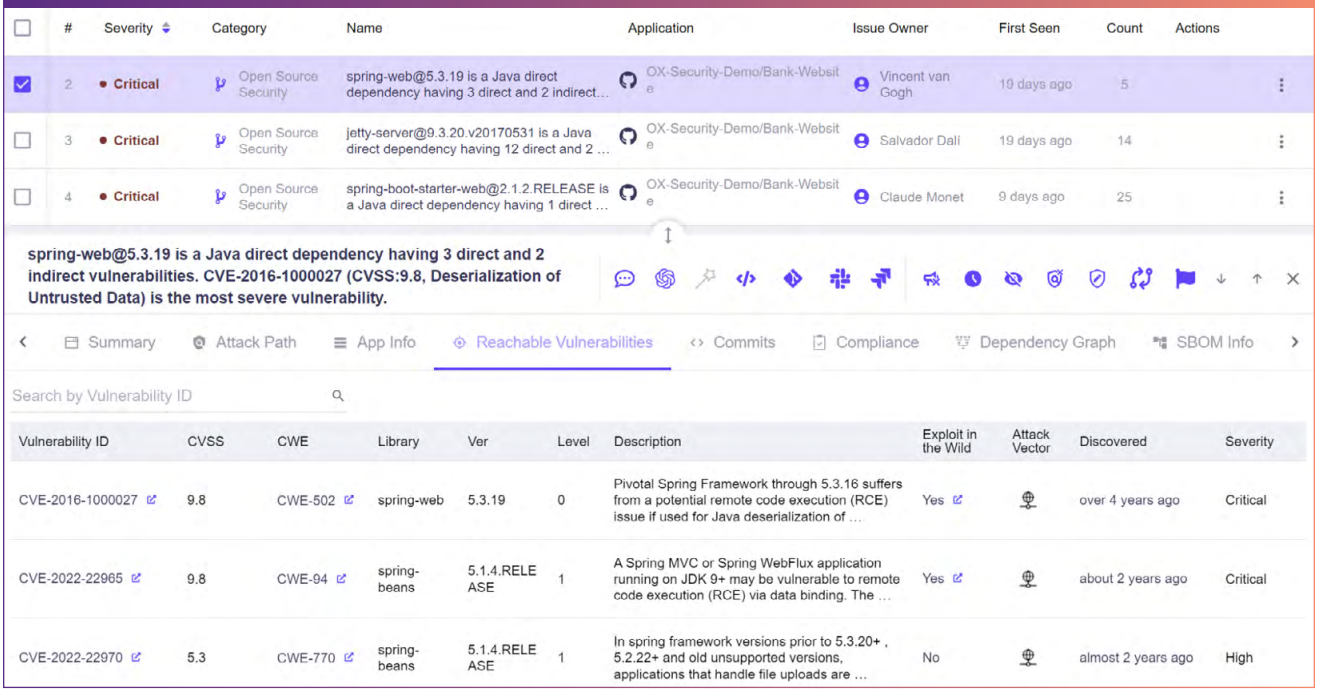
Advanced Dependency Assessment: OX SCA distinguishes between direct and indirect package dependencies, creating a dynamic visualization for both direct and indirect libraries. This enables users to understand the full scope of their project's dependencies at a glance, allowing them to view the entire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

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



Consolidated Issue Analysis: OX aggregates vulnerabilities across libraries and conducts root cause analysis. This approach consolidates multiple vulnerabilities into a single, actionable issue and dramatically reduces alert fatigue.

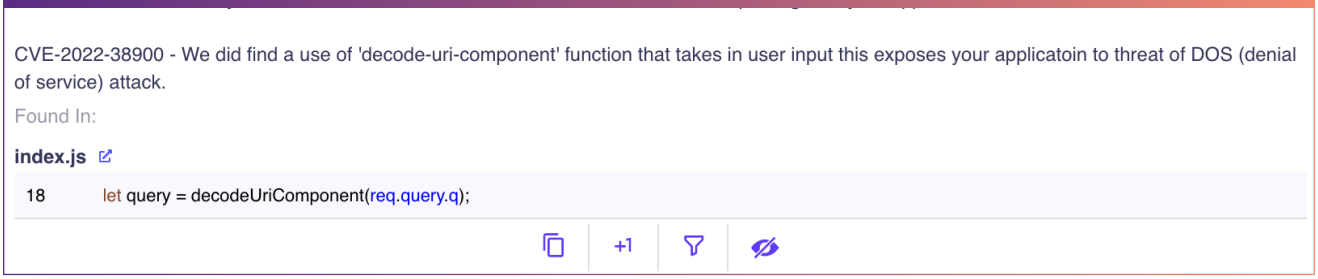
OX reduces the volume of alerts and simplified remediation by consolidating all of the vulnerabilities contributing to the root cause of a security issue.



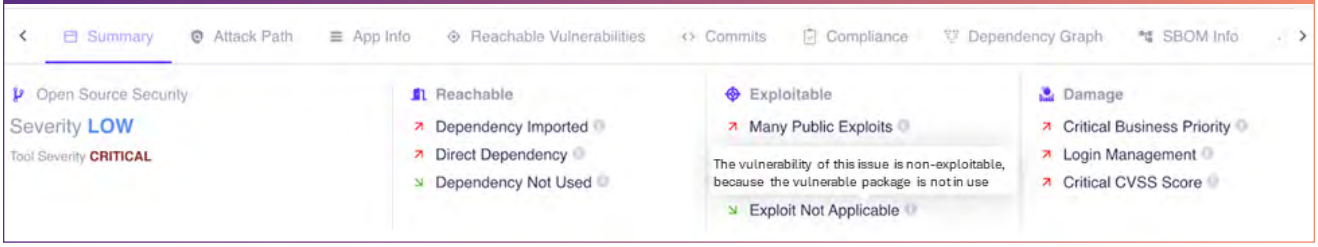
Context-Sensitive Prioritization: OX maximizes accuracy in prioritizing identified issues by applying a 3-layer contextual analysis. Each issue is analyzed based on reachability (can an attacker access the vulnerability), exploitability (if it is reachable, can the attacker take advantage of it), and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

For example, if a vulnerable library is incorporated into an application codebase but not used in an exploitable way, OX's analytics will assign a lower severity score. Other SCA tools simply do not apply this context and, therefore, cannot accurately assess and prioritize the risk.

Although this dependency was imported into the code, it is not actually being used and therefore poses a LOW risk rather than CRITICAL.



OX's automated triage has identified this library is being used in a way that poses a legitimate security risk.



Comprehensive Issue Management: OX enriches issue reports with Software Bill of Materials (SBOM) information, including licensing, maintenance status, popularity, and code usage details. We extend our analysis for containerized applications to base image vulnerabilities, offering comprehensive insights based on the Dockerfile. By recommending base image upgrades, we help resolve multiple vulnerabilities simultaneously, significantly reducing the attack surface.

Remediation-Focused Issue Resolution: OX's remediation approach prioritizes remedy over mere problem identification. We streamline the remediation process by consolidating issues based on their solutions rather than treating each problem separately. This method ensures that efforts are focused on effective vulnerability management, specifically tailored to the Software Composition Analysis (SCA) context, excluding container vulnerabilities for more targeted root cause analysis.

Conclusion

OX's embedded SCA functionality marks a significant leap forward in application security management. It underscores the critical need for tools that adapt to modern development environments' unique challenges and contexts. Our contextual analysis of third-party code and automated triage enhance the accuracy of critical issue identification and significantly cut down on response and remediation times.

If poor visibility and false alarms in your software supply chain are disrupting and delaying your development processes, see how OX's Active ASPM platform can eliminate the frustration of securing third-party libraries and open-source components.

About OX Security

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/

oxsecurity