CASE STUDY

oxsecurity

NAVIGATING VULNERABILITY PRIORITIZATION WITH OX:

Learn How a Leading Mobility-as-a-Service (MaaS) Provider Eliminated Irrelevant Alerts Through Intelligent Prioritization

CHALLENGE

Prioritize real threats vs. wasting resources on low-context vulnerabilities from a prior platform.

SOLUTION

A leading mobility-as-a-service (MaaS) provider deployed the OX platform to replace a legacy SCA solution with a streamlined approach that provided priorition based on correlation of risks and context.

With the OX Active ASPM Platform the organization achieved:

- Improved Efficiency
- Enhanced Security
- Better Resource Allocation

LEARN MORE AT WWW.OX.SECURITY

Background

A leading mobility-as-a-service (MaaS) provider, offers an urban mobility app used by over 1 billion users in more than 3,000 cities across 102 countries. Known for its comprehensive transit data and journey planning services, they are committed to improving the daily commute for people worldwide. As a publicly traded company the organization needs to ensure their security is focused on the most important proactive measures, especially in managing and prioritizing vulnerabilities.

The CISO was on a quest to streamline their security operations and enhance their overall security posture. Previously, they used another vendor for static code analysis but struggled with the overwhelming volume of irrelevant vulnerabilities reported and the lack of context for prioritization.

The challenge

The security team was inundated with the sheer number of vulnerabilities reported by a previous platform they were using, many of which lacked the necessary context to assess their actual risk. This led to inefficiencies and diverted valuable resources towards addressing non-critical issues.

Enter OX: contextual awareness for better AppSec

They decided to switch to OX, driven by the need for a more context-aware solution. OX's ability to integrate multiple static code analysis tools and provide a comprehensive, prioritized list of vulnerabilities was key to this decision. The detailed contextual information provided by OX allowed the team to focus on the most critical vulnerabilities that posed real risks to their operations. The team specifically liked that they could focus on what was important to their business.

> "Prior to OX, we were drowning in a sea of alerts. The platform's ability to accurately prioritize vulnerabilities based on context has been a game-changer. Now, we can effectively target the risks that pose the greatest threat to our business."

The organization deployed the OX platform, impressed by its ability to:

- **Correlate Risk and Context:** OX analyzes vulnerabilities from various static code analysis tools, prioritizing based on actual risk, not just volume.
- **Focus on Business Impact:** Detailed contextual information from OX empowered Eli's team to target vulnerabilities most critical to their business.

Seamless transition, dramatic results

The transition to OX was seamless. They replaced the other platform entirely with OX. The security team immediately noticed a significant reduction in the number of reported issues, with OX presenting 10% of vulnerabilities were critical compared to their previous solution. This reduction was due to OX's ability to contextualize vulnerabilities, eliminating false positives and highlighting only those that were exploitable and reachable.

Additional outcomes

- **Enhanced Team Efficiency:** Development teams were freed from non-essential fixes, focusing on core development tasks.
- **Improved Security Posture:** The organization addressed critical issues promptly, strengthening their overall security.
- **Optimized Resource Allocation:** The security team could strategically target impactful vulnerabilities.

KEY BENEFITS INCLUDE:

Contextual Prioritization: OX's ability to aggregate similar issues helped in reducing redundancy and streamlining the remediation process.

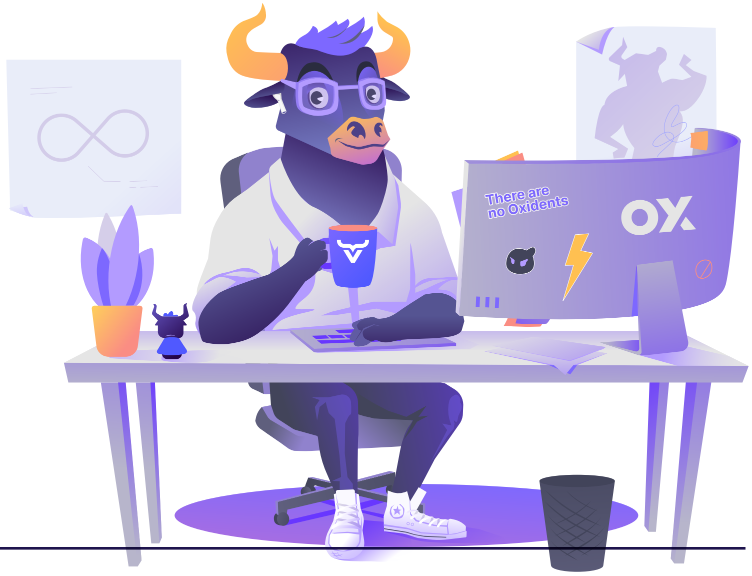
Aggregated Issues: OX's ability to aggregate similar issues helped in reducing redundancy and streamlining the remediation process.

Trust in the System: Despite initial fluctuations in the number of issues reported, the overall trust in OX's judgment and prioritization was high, supported by continuous validation from the security team.

Conclusion

OX has proven to be a valuable asset for the organization, significantly enhancing their ability to manage and prioritize security vulnerabilities. The transition from a previous solution to OX has resulted in improved efficiency, better resource allocation, and a stronger security posture. The organization's experience underscores the importance of contextual prioritization in cybersecurity and the value of a tool that adapts to the dynamic needs of modern enterprises.

> "OX has had a significant impact on our security operations. We've seen a dramatic reduction in wasted time and resources spent on irrelevant vulnerabilities, allowing us to focus on the threats that truly matter."



About OX Security

At OX Security, we're simplifying application security (AppSec) with the first-ever Active ASPM platform offering seamless visibility and traceability from code to cloud and cloud to code. Leveraging our proprietary AppSec Data Fabric, OX delivers comprehensive security coverage, contextualized prioritization, and automated response and remediation throughout the software development lifecycle. Recently recognized as a Gartner Cool Vendor and a SINET 16 Innovator, OX is trusted by dozens of global enterprises and tech-forward companies. Founded by industry leaders Neatsun Ziv, former VP of CheckPoint's Cyber Security business unit, and Lior Arzi from Check Point's Security Division, OX's Active ASPM platform is more than a platform; it empowers organizations to take the first step toward eliminating manual AppSec practices while enabling scalable and secure development.

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