EINPRESSWIRE

Oxeye Reveals Application Security Predictions for 2023

Security Experts Cite the Shift to Cloud Native Applications as the Driver Significant Opportunities and Challenges

TEL AVIV, ISRAEL, December 20, 2022 /EINPresswire.com/ -- Oxeye, the provider of award-winning cloud-native application security, today announced five predictions expected to shape enterprise security spending in 2023. The predictions follow industry-wide research which shows the industry is shifting away from legacy software infrastructure and standardizing on cloud native applications – resulting in the need for new and more effective approaches to cloud native application security.

The 2022 ISG Provider Lens™ Cloud Native Services and Solutions report for the U.S. stated, “The U.S. ecosystem around containers, Kubernetes and related services is entering a more mature phase as developers and the IT community reach a deeper understanding of the benefits and challenges that come with cloud-native technologies. In addition, traditional security systems based on protecting a perimeter around the enterprise also fall short with cloud-native architectures. Multi-developer, multi-platform environments made up of widely distributed software components require specialized security solutions.”

Oxeye, a leading cloud native application security provider has seen this change reflected in its own operations. Based on feedback from deployments over the past 12 months, the company is making several predictions on the trends it sees enterprise organizations prioritizing in 2023. The five forecasts made by Oxeye for 2023 include:

1. Application security and cloud security will converge:
Over the next 12 months, more applications will be built using a cloud native approach than the traditional, monolithic architecture. Distributed applications that use containers will be impacted by an increasing number of vulnerabilities that span microservices and traverse the infrastructure layer. The distinction between application security and cloud security has clearly blurred as application security is now affected by the underlying cloud infrastructure, while cloud security professionals now have to take the application layer into account in their attack path

analysis. For application security professionals, this means they must now learn to perform an accurate analysis of cloud native applications, which combine analysis of code, container, cluster, cloud and their connections and communications. For cloud security professionals, this means finding a way to add application layer analysis into their existing security posture.

2. 'Shift left' will become 'Shift everywhere'
For the last decade, people have been talking about shifting left. The truth is, the more static your analysis is, the more false positives you will get, along with alert fatigue. Running a SAST tool doesn't actually tell you what your application risk is, only that you have a bunch of vulnerabilities, some real, some not. There's a real need to tie runtime analysis to signals that you're getting from your static scanners, so that contextual knowledge is provided of what's happening within applications. Intelligent analysis that combines user derived signals from static analysis with signals that you get from runtime analysis (shifting to the right) will provide greater truth about the vulnerabilities in your applications, and a true understanding of how they contribute to overall risk.

3. Greater C-Suite demand for visibility into risk contributions of apps and the teams that build them
The days when the greatest challenge for the appsec team was 'What vulnerabilities are in our applications, and how do we remediate them?' will go away. This will be replaced by the need to establish and report metrics on the risk contribution of each application, and the chain of accountability to the teams that are responsible for their production and security. Leaders will want to know this so they can allocate resources accordingly to lower their overall risk exposure. This will force appsec teams to find tools that provide detailed, high fidelity risk profiles for each application within their care that include the 'risk score' of their applications (calculated from the total, type, and severity levels of the vulnerabilities that are left without remediation), the type of data that these applications collect, transfer and store, and the number of records that are collected, among others.

4. There will be a demand for clearer prioritization data, making the Vulnerability Exploitability Exchange (VEX) more popular
Vulnerability management typically means sorting through a mountain of noise to figure out what really needs to be remediated, and what doesn't, then prioritizing remediation efforts. Appsec professionals will increase their demands on tool vendors to provide clear data on the relative levels of risk that each vulnerability presents, so that they're not left guessing what to remediate and left to assign precious resources to manual prioritization efforts. This shift will call for a clear, consistent data format for communicating the prioritization information that is machine readable to enable automations and integrations. The Vulnerability Exploitability Exchange (VEX) will become more popular as a result.

5. Software supply chain security will finally have a clear definition
But it's not a simple one. Ask 10 different people what software supply chain security is and you're likely to get 10 different answers, with some of them being lengthy and confusing. As

software supply chain security continues to receive more scrutiny, a more precise and consistent definition will emerge. It will not likely be a simple, one-sentence definition, but clearly defined categories where each have their own definitions and requirements.

“Cloud-native applications are game-changers when it comes to business agility, but the protection of these platforms introduce new challenges, restrictions and requirements that restrict traditional application security solutions from functioning effectively in these environments,” said Ron Vider, CTO and Co-founder, Oxeye Security. “As this is a rapidly evolving space, the shift to cloud-native application security demands a new approach that holistically looks at all software components and the underlying infrastructure to ensure resilient operations.”

If interested in learning more about how Oxeye can assist with cloud-native application security challenges, please visit https://www.oxeye.io/contact to contact us.

Resources:
- Take a deeper dive into the vulnerability by reading the blog entry on Oxeye’s website at: https://www.oxeye.io/blog
- Follow Oxeye on Twitter at @OxeyeSecurity
- Follow 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 solution designed specifically for modern container and Kubernetes-based architectures. The company enables customers to quickly identify and resolve all application-layer risks as an integral part of the software development lifecycle by offering a seamless, comprehensive, and effective solution that ensures touchless assessment, focus on the exploitable risks, and actionable remediation guidance. 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
Media
+1 818-332-6166
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/607242954

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.