Legit Security Adds Dashboard to ASPM Platform to Improve DevSecOps

Legit Security Adds Dashboard to ASPM Platform to Improve DevSecOps

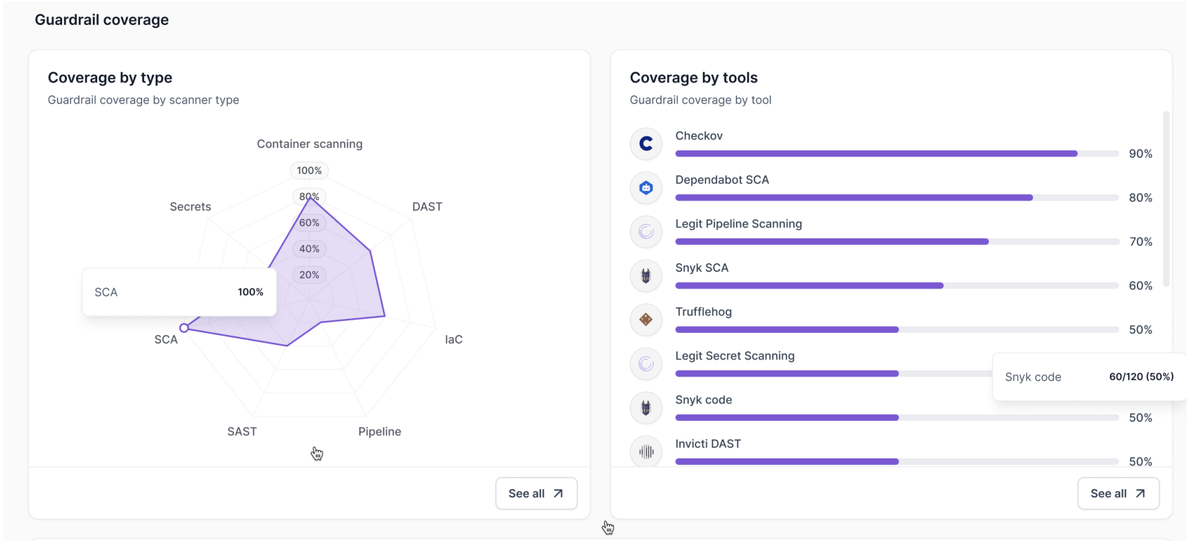
BY: MIKE VIZARD ON MARCH 29, 2025

Legit Security this week added a dashboard to its application security posture management (ASPM) platform that makes it simpler to correlate the creation of a vulnerability to a specific application development team.

Company CTO Liav Caspi said the risk prevention dashboard also makes it possible to identify missing guardrails, such as a static application security testing (SAST) tool, that might not have been turned on as code moved through a DevSecOps pipeline.

These insights create a teaching opportunity using, for example, gamification capabilities built into a software-as-a-service (SaaS) platform that can be used to further adoption of best DevSecOps practices, he added.

Finally, the dashboard also makes it possible to keep track of all the vulnerabilities that a DevSecOps team has prevented, to better surface the actual return on investment (ROI) being provided by remediation efforts, noted Caspi.



ASPM platforms have emerged as centralized platforms that employ large language models (LLMs) and heuristics to identify vulnerabilities in code before they wind up finding their way into a production environment. The overall goal is to correctly identify access keys, passwords, application programming interface (API) keys and other personally identifiable information (PII) that hopefully will no longer be exposed to cybercriminals after an application is deployed, he noted.

That capability is critical at a time when the volume of code being generated is dramatically increasing because of the rise of AI. Unfortunately, the AI platforms that create this code were trained using often flawed examples of code scraped from across the web. As a result, it's not uncommon for AI platforms to generate code that has known vulnerabilities.

Legit Security, in effect, is making a case for using AI to better identify vulnerabilities created by AI tools and humans alike in an era where cybercriminals are increasingly using the same capabilities to scan applications for those same vulnerabilities.

While a lot of progress has been made in terms of the adoption of best DevSecOps practices, there is clearly still much work to be done. A recent Futurum Research survey finds that over the next 12-18 months, organizations specifically plan to significantly increase software security spend on application programming interfaces (42%), DevOps toolchains (35%) incident response (34%) open source software (32%), software bill of materials (30%) and software composition analysis (27%) tools.

No application developer sets out to write insecure code, but expecting them to never make a mistake is unreasonable. It's always possible through training to teach developers to write better code, but in the rush to build software, there will inevitably be times when code may not have been properly reviewed. The simple truth of the matter is that no developer has the cognitive ability to identify every vulnerability that might find its way into a code base, noted Caspi.

The one thing that is certain, however, is that it's only a matter of time before a vulnerability is discovered in a production environment that is ultimately going to be more challenging and expensive to fix, as regulations continue to become more stringent.

FILED UNDER: BLOGS, BUSINESS OF DEVOPS, FEATURES, NEWS, SOCIAL - FACEBOOK, SOCIAL - LINKEDIN, SOCIAL - X
TAGGED WITH: AI, ASPM, CODE, LLMS, SAST

« Microsoft's Hyperlight Wasm: Bringing WebAssembly to Secure Micro-VMs

Five Great DevOps Job Opportunities »