LEGIT

Application Security Acronyms Cheat Sheet

Definitions

SAST (Static Application Security Testing):

SAST or static analysis tests the security of software from the inside out. This type of testing analyzes the software code to identify known vulnerabilities, such as SQL injection and cross-site scripting.

Static analysis looks at code early in the development lifecycle, before it becomes a running application.

DAST (Dynamic Application Security Testing):

DAST or dynamic analysis tests the security of software from the outside in. This type of testing analyzes the actions of a running application to identify vulnerabilities such as misconfigurations or authentication issues.

SCA (Software Composition Analysis):

SCA identifies and tests the security and legality of open source software in a codebase. This type of testing identifies known vulnerabilities, such as SQL injection and cross-site scripting, and existing licenses in open source code.

Cloud-Native Application Protection Platform (CNAPP)

CNAPP is a security solution focused on the security of cloud environments. These solutions aim to monitor, detect, and remediate cloud security threats and vulnerabilities.

Application Security Orchestration and Correlation (ASOC)

ASOC is a solution that helps facilitate vulnerability testing and remediation. These solutions correlate scan data from various sources, including SAST, DAST, IAST, and SCA tools. These tools are typically limited to helping with aggregation, prioritization, de-duplication of results, and alert orchestration. This category has some overlap with RBVM or Risk Based Vulnerability Management.

ASPM (Application Security Posture Management)

ASPM gives security teams a clear view of the full software factory, its assets, its owners, its security controls, its vulnerabilities, and how all are related. With this view, security teams can ensure the integrity, governance, and compliance of every software release.

Gartner defines ASPM as a solution that “analyzes security signals across software development, deployment and operation to improve visibility, better manage vulnerabilities and enforce controls.” (Gartner® Report: Innovation Insight For Application Security Posture Management (ASPM))

ASPM Comparisons

ASPM vs. SAST, DAST, and SCA

Static analysis (SAST), dynamic analysis (DAST), and software composition analysis (SCA) scan source code for vulnerabilities in different phases of code development.

Solely scanning source code for application security falls short because its focus is too narrow, it lacks context, and it produces a variety of results without correlation.

In addition, source code scanners only look at application risk and largely ignore the risk found in the software factory, like weaknesses in the CI/CD pipeline. This focus leads to blind spots in the area that’s currently causing and producing the most devastating attacks seen in the wild.

ASPM Definitions

Deduplication: When two or more application security tools in the same category (i.e., SAST, SCA, DAST, secrets, etc.) find the same vulnerability or issue in the same application/repo/file, ASPM solutions will highlight the duplication and help with prioritization.

Correlation:
Can refer to a few things:

- Matching a singular issue between different tools (i.e., SAST and DAST)
- Identifying the same issue in different areas (i.e., same secret in different files)
- Mapping child issues back to a parent issue (i.e., vulnerabilities in transitive dependency A, B, and C all map to dependency “Package A”)

Root cause analysis: This is true issue origination identification, where multiple issues are tied back to a singular fix.

Toxic combination: This refers to the ability to tie different types of risks together in a way that shows an attack path or an elevated combined risk.

ASPM vs. ASOC

ASPM is a more comprehensive security solution than ASOC. While ASOC is focused on integrating vulnerability data from application scanning tools, ASPM is focused on the entire software factory – from code to pipelines, pathways, and assets. ASPM will include all of the ASOC value proposition, but then also bring in additional value through the visibility, correlation, and risk granularity that is missing from ASOC platforms.

ASPM vs. CNAPP

CNAPP is solely focused on runtime protection of cloud-native applications, while ASPM is centered on application security across the SDLC.

Get more details on ASPM. Contact us to get more information or Request a demo.

About Legit Security

Legit is a new way to manage your application security posture for security, product, and compliance teams. With Legit, enterprises get a cleaner, easier way to manage and scale application security and address risks from code to cloud. Built for the modern SDLC, Legit tackles the most challenging problems facing security teams, including GenAI usage, proliferation of secrets, and an uncontrolled dev environment. Fast to implement and easy to use, Legit lets security teams protect their software factory from end to end, gives developers guardrails that let them do their best work safely, and delivers metrics that prove the security program's success. This new approach means teams can control risk across the business – and prove it.