SAST vs DAST vs SCA

Which Security Testing Methodology is Right for You?

SAST
Static Application Security Testing

DAST
Dynamic Application Security Testing

SCA
Software Composition Analysis

What is it?

SAST

Analyzes the source code for potential security vulnerabilities without running the application.

DAST

Simulates an attack on the running application to find vulnerabilities.

SCA

Analyzes third-party software used in an application to identify security vulnerabilities and licensing compliance issues.

When to use

SAST	During development.
DAST	Post-development, during testing or production.
SCA	During development and throughout the software development life cycle.

Advantages

SAST
Able to find security issues before application deployment. Easy integration with development toolchain.

DAST
Identifies vulnerabilities in the running applications.

SCA
Identifies vulnerable third-party software.

Disadvantages

SAST

- Generates a high number of false positives.
- Not suitable for identifying runtime issues or vulnerabilities that arise during the execution.

DAST

- May miss some vulnerabilities.
- Can generate false positives.
- Slows down the application during testing.

SCA

- Does not identify issues inside the code.
- Limited scope around third-party software.

Cost

SAST	Moderate to high.
DAST	Moderate to high.
SCA	Low to moderate.

Examples of tools

SAST	SonarQube, Veracode, Checkmarx, Fortify
DAST	IBM AppScan, HP WebInspect, Acunetix, Qualys Web Application Scanning
SCA	Whitesource, Snyk, Black Duck, OpenHub, Sonatype Nexus Lifecycle

Use case scenario

SAST
- Detecting common coding errors.
- Finding vulnerabilities within your codebase.
- Ensuring code adherence to security standards.

DAST
- Identifying vulnerabilities in web applications, web services, and APIs.
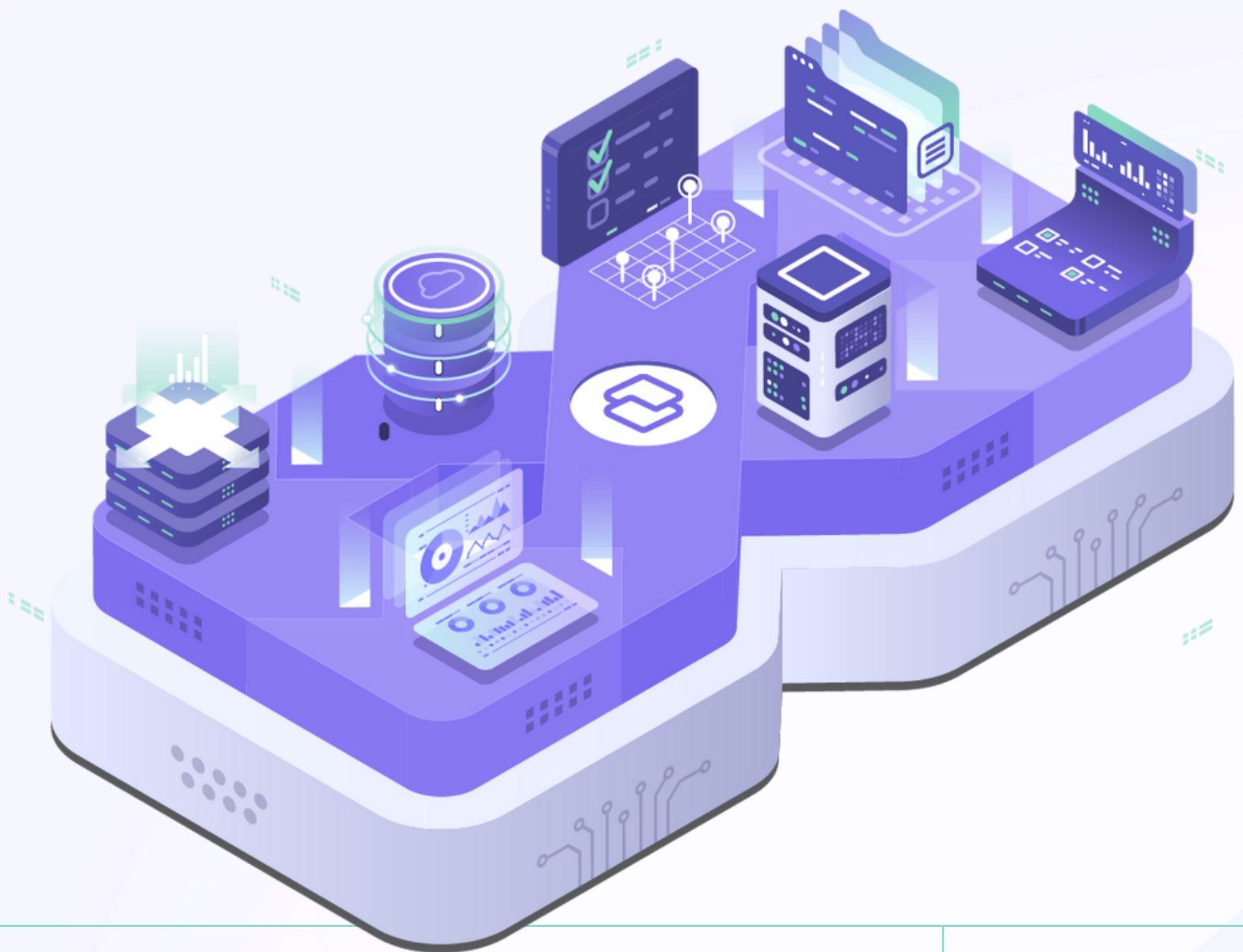- Simulating real-world attacks.

SCA
- Promoting license and policy compliance.
- Identifying open-source component risks.
- Protecting against supply chain attacks.
- Checking dependencies for vulnerabilities.

Level up your DevSecOps skills with us!

Certified DevSecOps Professional Course

Link in the description

Practical DevSecOps

Making Product Security Accessible to Everyone