# DevSecOps

Implanting security in the hyper fast DevOps environment

# What is DevSecOps & Why the Buzz?

In today's fast-paced world, organizations want to have the software products in their hands as early as possible. In order to keep up the pace, old methodologies such as Waterfall model of Software Development have been replaced with DevOps, which is complementary with Agile Software Development. DevOps is a unique style of Software Development that collaborates the Software Development teams and IT Operations team to cut down the Software Development Life Cycle duration by introducing Continuous Integration & Continuous Development (CI/CD) in the delivery of high-quality software.

DevOps, along with its speed and high-quality software delivery, brings an opportunity for hackers to attack the application at multiple phases in the CI/CD pipeline. This is where **DevSecOps** comes in the picture that provides automated security gates at multiple phases of DevOps.

**DevSecOps** is a transformational shift in DevOps, in which, every team involved in the process must be accountable for security of the application. DevSecOps necessarily means automating security checkpoints at multiple phases in the DevOps pipeline to secure the application without affecting the DevOps speed.

# Key Highlights of LTIMindtree DevSecOps

### Real-time Unified Dashboard
—
Real-time **Dashboard** to track AppSec progress

### Automated Assignment
—
**Assign** vulnerabilities and **track** remediation status

### Incremental Scans
—
**Dynamic Incremental scans** looking for New Attack Surface for vulnerabilities

### Reports
—
**Real-time & Customized** reporting

### Technical Debts
—
Up to **50%** Reduction in pre-existing technical debts

### PT Cost Reduction
—
Up to **20%** Penetration Test Cost reduction

### Vulnerability Correlation

**ML-driven Triaging** leads to >50% reduction in False Positives

### AppSec Tools Selection

**AI-enabled** automation & Centralized AppSec Tool Management

### Container Security

Discover, track, and continuously secure containers – from **build to runtime**

### Mean Time to Repair (MTTR)

Faster & prioritized remediation leading to **reduced MTTR**

### DAST Vulnerability Coverage
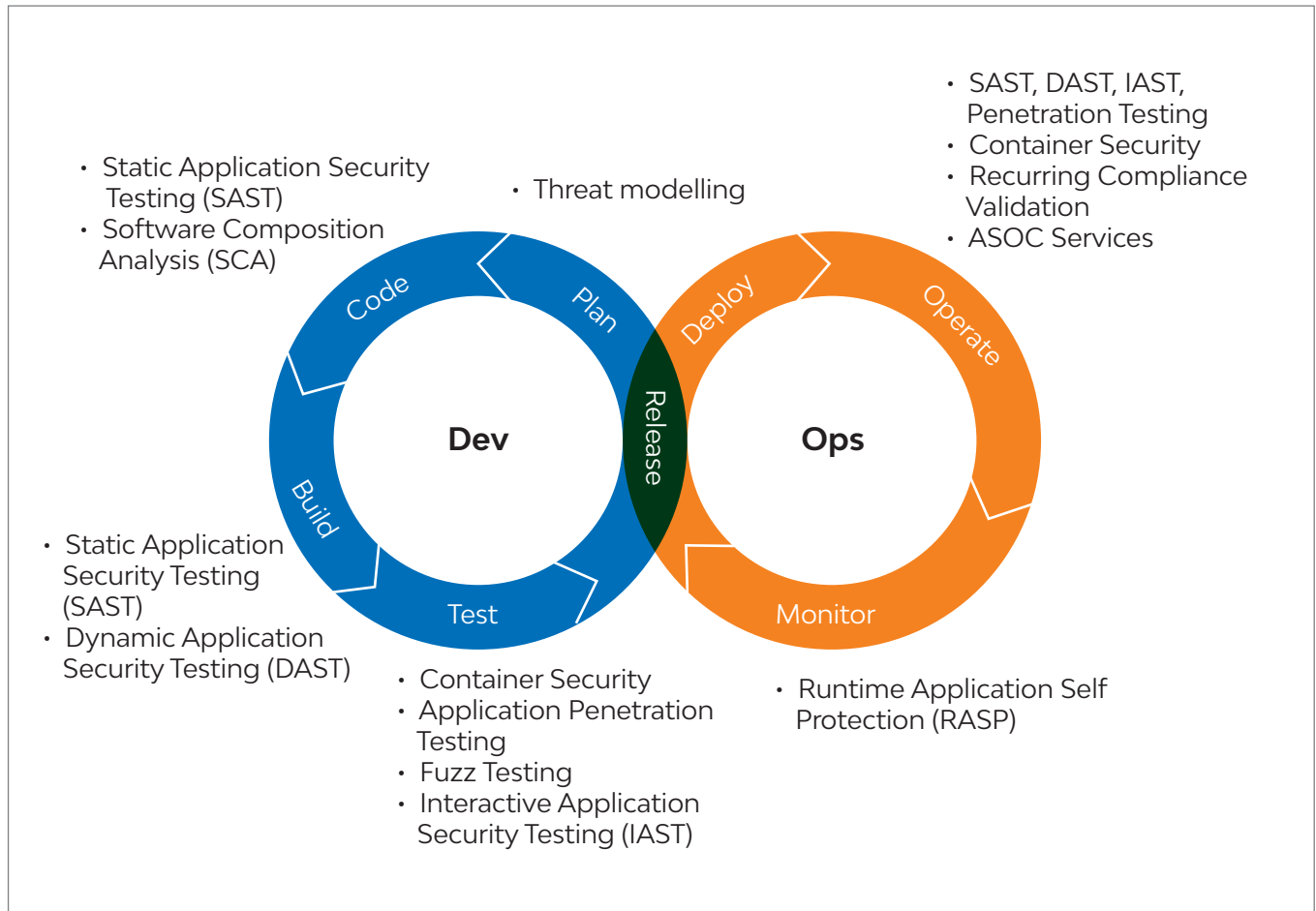
Crawls modern **frameworks** and **APIs**

### Compliance

**OWASP** Top 10 & **SANS** guidelines for Application Risk

# The LTIMindtree Way of Doing DevSecOps

A high-level view of the LTIMindtree DevSecOps services is as under:



- SAST, DAST, IAST, Penetration Testing
- Container Security
- Recurring Compliance Validation
- ASOC Services

- Static Application Security Testing (SAST)
- Software Composition Analysis (SCA)

- Threat modelling

Code · Plan · Deploy · Operate · Release · Build · Test · Monitor

Dev · Ops

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)

- Container Security
- Application Penetration Testing
- Fuzz Testing
- Interactive Application Security Testing (IAST)

- Runtime Application Self Protection (RASP)

Securing applications in the DevOps pipeline

## The key services forming part of LTIMindtree DevSecOps Services are as under:

### ✓ Threat Modelling

Before starting the development of an application, LTIMindtree performs **Threat modelling** exercise that enables to identify the potential threats to applications.

### ✓ Static Application Security Testing (SAST)

In the Development phase, LTIMindtree looks at the code vulnerabilities which creep in as a result of not following secure code guidelines and best practices. LTIMindtree performs **Static Application Security Testing (SAST)** at IDE level and during Commit Time and Build Time.

### ✓ Software Composition Analysis (SCA)

LTIMindtree SAST is often clubbed with **Software Composition Analysis (SCA)** to identify the open source components present in the application and the vulnerable & deprecated open source components and their license risks.

### ✓ Container Security

After the application is packaged and built, Docker is used to create containers. At this stage, the container images may be vulnerable and hence LTIMindtree implements **Container Security** to scan the images, the running containers and their hosts for vulnerabilities.

### ✓ Dynamic Application Security Testing (DAST)

LTIMindtree performs **Dynamic Application Security Testing (DAST)** which identifies security vulnerabilities in a running application during post Build phase & QA phase. DAST is a Black-Box Testing technique to identify security vulnerabilities from an attacker's perspective.

### ✅ Application Penetration Testing

In order to make the application more secure, methods such as **Application Penetration Testing**, manual & automated and curated to the specific needs of the organization, are performed by LTIMindtree. LTIMindtree also performs Fuzz Testing in which invalid, unexpected, and random data are fed to the application to analyze its behavior and report the security vulnerabilities found.

### ✅ Interactive Application Security Testing (IAST)

LTIMindtree **Interactive Application Security Testing (IAST)** services combine the advantages of both SAST & DAST. LTIMindtree IAST services entails deployment of sensors and agents in the running application, actively monitoring and analyzing all application interactions & functionalities performed by automated and manual tests to identify security vulnerabilities in real-time.

### ✅ Runtime Application Self Protection (RASP)

LTIMindtree **Runtime Application Self Protection (RASP)** services include placing a RASP solution, also known as self-defense mechanism, within the application runtime that intercepts the interactions made to the application and blocks illegitimate requests. LTIMindtree RASP also provides logging visibility and exploit data with line of code details.

### ✅ Secure Coding Training

As a part of Shift-Left strategy, LTIMindtree encourages Secure Coding Trainings for developer enablement. To code in a secure manner, LTIMindtree provides gamified **Secure coding trainings** at the IDE level and remediation advisory. LTIMindtree provides training on security tools, standards and best practices including OWASP top 10, SANS top 25, PCI, etc. Scenario based training with code snippet for remediation are provided to quantify the developer's secure coding acumen.

✓ **Managed DevSecOps Services**

When applications are deployed in PROD (Production) environment, LTIMindtree performs managed SAST, SCA, DAST, IAST, Pen Testing services, etc. so that the applications are continuously tracked for new vulnerabilities. LTIMindtree's certified and well-trained engineers keep track of threats in applications and continuously interact with Dev & IT team to ensure a robust and secured application portfolio.

✓ **LTIMindtree Accelerator:** Application Security Orchestration and Correlation (ASOC) Services

For better vulnerability coverage, organizations use multiple security tools (Open-Source & Commercial) to scan the application. When multiple security tests like SAST, SCA, DAST etc. are performed, each testing tools throws a gigantic number of false positives and the security testing team ends up manually reviewing each issue, correlating them & confirming their validity.

LTIMindtree ASOC Services automatically correlates all the vulnerabilities from all tests and presents the security team a concise list of valid vulnerabilities. All security tools' scan results are ingested into the LTIMindtree ASOC platform which also provides a dynamic and drillable dashboard for tracking the issues & mitigation status of issues. LTIMindtree's ASOC platform automatically enables orchestration of security tools and provides a real-time view of the application security posture.

# Key Features & Business Benefits of LTIMindtree DevSecOps

| Features | Benefits |
| --- | --- |
| **Language Coverage** | • Broad language coverage such as Java, .NET, PHP, C++, etc. and major dynamic languages such as JavaScript/TypeScript, Go, Python, etc. |

| Features | Benefits |
|----------|----------|
| **Complete Integration in DevOps** | • Integration of Application Security tools with IDE<br>• Integration of Application Security tools in CI/CD pipeline at Commit, Build time, Containerization, QA phase, etc.<br>• Complete automation in the CI/CD pipeline (Jenkins, Azure DevOps, etc.)<br>• Integration with bug trackers |
| **Enhanced support** | • Manual source code review & false-positive analysis<br>• Remediation suggestion<br>• Specific to project methodologies<br>• Solutions to -<br>  o New/major enhancement<br>  o Minor enhancements<br>  o No enhancement |
| **Automated Compliance Checks** | • Enabling compliance with broad vulnerability coverage:<br>  o OWASP top 10, CWE/SANS top 25, PCI DSS, HIPAA, etc. |
| **Flexibility & Scalability** | • The Managed AppSec services are offered in:<br>  o On-premise<br>  o Cloud<br>• On-demand/automated AppSec scans<br>• Onboarding support for any no. of projects in CI/CD pipeline<br>• Report generation in multiple & customized formats |

| Features | Benefits |
|---|---|
| **ASOC Value Adds** | • Application security orchestration & correlation<br>• Triggering of application security scans from central platform<br>• Correlation & prioritization of vulnerabilities<br>• Better vulnerability coverage & deduplication of results<br>• Managing remediation with tools to assign and track vulnerability fixes |