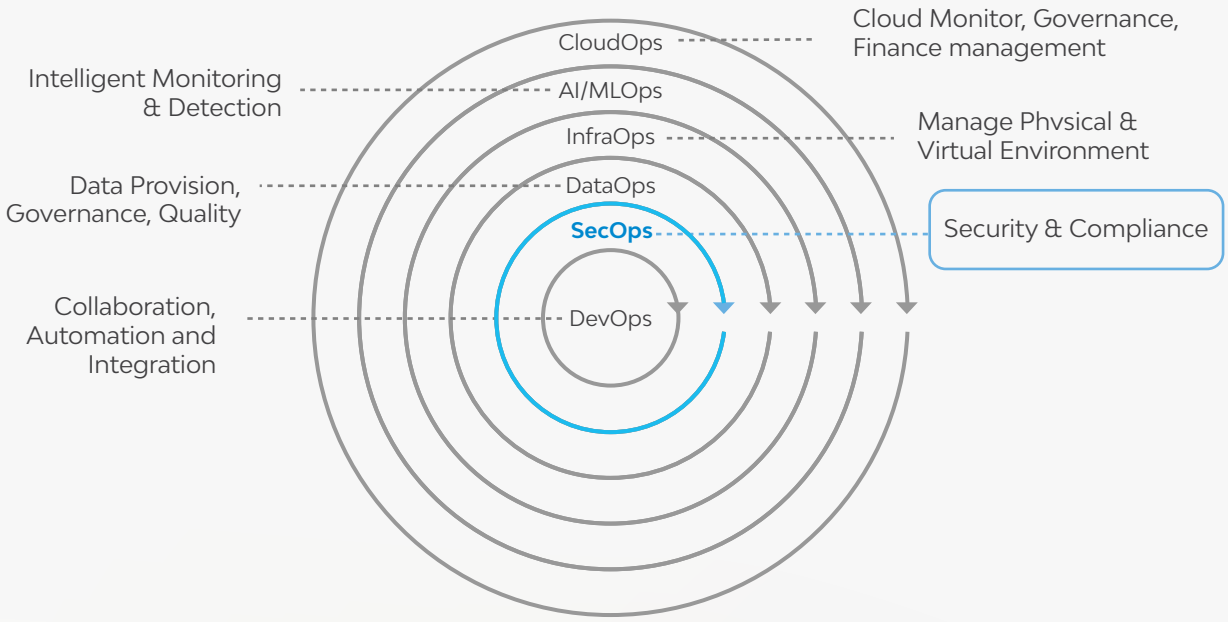
LTIMindtree

POV

XOps : Demystifying SecOps

Overview

SecOps is a transformational shift in DevOps that aims to automate crucial security tasks, to develop more secure applications and infrastructure. The prime motto is to automate security checkpoints at multiple phases of SDLC to secure the application and infrastructure without affecting the delivery speed. It facilitates the integration of tools, procedures, and technologies that safeguard the enterprise's application, data, and infrastructure and reduce the risk.



Need of SecOps

In today's scenario, software delivery speed and tool adoption are prioritized over security. Operations and development teams are often concerned with the speed of delivering the software applications and adopting tools that offer ease of implementation. When there isn't enough emphasis on security, an application can be vulnerable to attacks and can be compromised. With the advent of enhanced SDLC velocity and agile software models, there is also a high threat of losing sensitive and critical data. Indeed, according to "GitLab's Fifth Annual Global DevSecOps Survey conducted in 2020", DevOps practices have led to 60% of developers releasing code twice as quickly. Still, increased speed has always created a trade-off over security. According to another study conducted by "Synopsys, Inc. in 2020 ", nearly half of organizations consciously deploy vulnerable code because of delivery pressure.

One example of such a breach is the case of a major hotel chain. In February 2020, the hotel spokesperson confirmed the leak of personal details of more than 10.6 million guests. Their data was published on a hacking forum for sale. Security breaches happen every year because of the rise in cyber-attacks targeting influential organizations. However, a common element that stands out is that almost 85% of the violations fall in the OWASP Top 10 category (OWASP top 10 is a globally accepted security testing methodology).

By adopting SecOps, companies can inject security into the entire software delivery lifecycle. Approaching security with a shift-left approach allows project team members to emphasize how they securely design, develop, and deploy the software products to the market.

Current/Future Trends:

As DevSecOps practices gather steam in 2022, several contemporary technology trends will likely expedite DevSecOps adoption. These trends will also aid teams as they integrate security and compliance into processes without slowing innovation or creating additional work for already time-strapped teams. This includes -

1. Hybrid Workplace

- Since the past year, the hybrid model of organization has given Security Operations Centers (SOCs) the new task of maintaining security for employees who operate from their homes and mobile devices. The traditional security methods are outdated since organizations have expanded to the personalized workspace. As a result, it has become necessary to implement best-in-class identity management to secure the data and code.
- Machine learning and automation are crucial to detecting malicious activities in the system and quickly mitigating risks, identifying threats regardless of the employee's location.

2. The Cloud Era

- The organizations are generating enormous data and are opting for cloud storage services over physical servers for its apparent benefits. This trend comes with security risks, as with increased usage and usership, cybercriminals are sure to migrate their attacks to the cloud. According to a study conducted by IDC (International Data Corporation), the world will have 175 zettabytes of data by 2025. Gartner predicts (Gartner Press release) that global cloud services spending will reach over $482 billion in 2022, a 54% increase from 2020.
- Organizations must find ways to keep scanning and monitoring their cloud storage and checking for any risks or potential threats. Before it turns into an attack, identifying risk can save them from costly and destructive data breaches. Some businesses choose to build an in-house hackers' team to get more eyes on potential vulnerabilities in their systems and fix them before an actual attack occurs.
- Adopting the principles of least privileges through Authorization and Authentication mechanisms for security in the cloud.

3. Increased Adoption Of Infrastructure As Code (IaC)

- According to a (Gartner Report) - By 2025, 60% of organizations will use infrastructure automation tools as part of their DevOps toolchains, improving application deployment efficiency by 25%."
- Codified infrastructure accelerates the adoption of SecOps practices to reduce the bugs and vulnerabilities of self-code, open-source code, third-party code or code libraries, and similar threats of application code.
- In December of 2021, for example, Log4Shell highlighted the importance of organizations monitoring code in development and production and the code of their partners and customers.
- "Wise developers don't reinvent the wheel: they use existing libraries and/or frameworks," wrote Nicolas Fränkel in the article You're running untrusted code! Published on Jan 2022. It also quotes that "From a security point of view, it means users of such third-party code should carefully audit it. We should look for flaws, both bugs, and vulnerabilities."

4. Intelligent AIOps Driven Systems

- To perform real-time monitoring and capture observable data, AIOps are a boon for this era. By analyzing data on activity in real-time, teams can unlock the insights developers need to accelerate innovation and a key for teams to integrate security verification to test code in development and continually identify new security vulnerabilities in production.

SecOps Lifecycle

SecOps is a practice that strives to automate essential security tasks. It involves introducing security measures early on or at each stage of the software development life cycle (SDLC). Building security starting from product conception decreases remediation time while making the product safer, lowering costs in the long run. Instead of measuring how long it takes for the pipeline to build, quality-test, and deploy software, DevOps organizations must start measuring the baseline with security activities included in the overall pipeline.

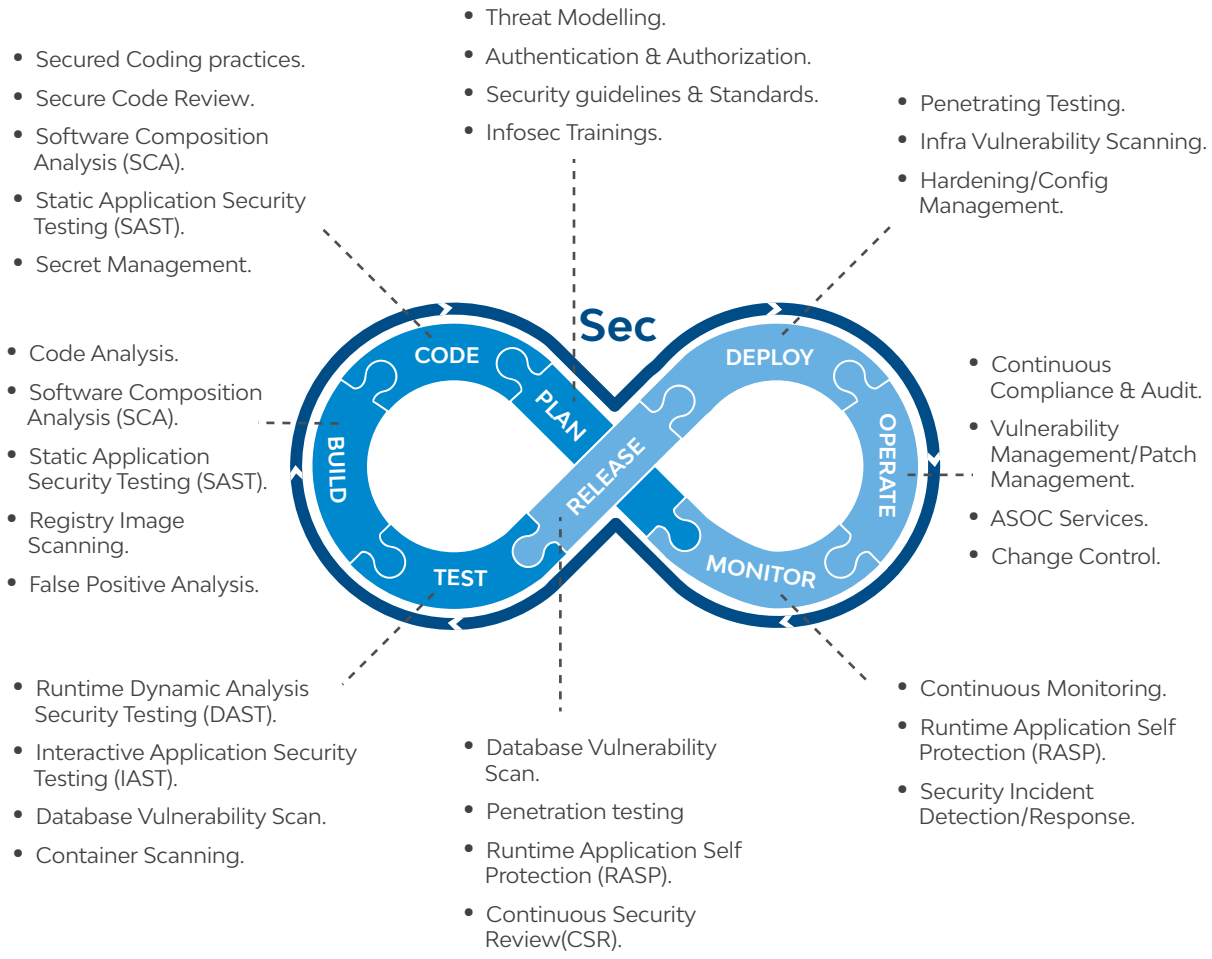


Fig. Integrated security across the DevOps lifecycle

Measurements Of SecOps And Business Benefits

Measuring Success:

Several measurements can be considered in SecOps. Below are some of the key metrics.

- Number of system vulnerabilities.
- Security Technical Debt.
- Number of false positives.
- Number of security defects and incidents.

Business Outcomes:

IT organizations that successfully implement the SecOps methodology can experience various business benefits. Highlighting some of the critical outcomes, which include-

- Reduced security vulnerabilities.
- Highly secured software or products.
- Improved productivity.
- Reduced security technical debt.
- Faster time-to-market.

Our Accelerator/Framework:

Organizations use multiple security tools (open-source and commercial) to scan the application for better vulnerability coverage. When numerous security tests like SAST, SCA, DAST, etc., are performed, each testing tool throws many false positives. The security testing team manually reviews each issue, correlating them and confirming their validity.

LTIMindtree has its in-house accelerator known as **Application Security Orchestration and Correlation (ASOC),** enabling the orchestration of security tools and providing a real-time view of the application security posture. LTIMindtree ASOC Services automatically correlates all the vulnerabilities from all tests and presents the security team with 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 and mitigation status of cases.

Key feature highlights include:

- One-stop security platform.
- One-click onboarding and execution.
- AI-leaded SecOps tool mapping.
- Consolidated SecOps dashboards.
- Correlation and de-duplication.
- Better vulnerability coverage and de-duplication of results.

About the Authors

S. Rakesh Kumar DevOps Architect

Rakesh is a DevOps Architect for Cloud Practice at LTIMindtree. He has 12+ years of IT experience and transformed into a SME in DevSecOps, Container and multi-Cloud technologies. Rakesh helps enterprise customers in transforming their DevOps journey, leveraging his experience and DevOps best practices. Outside of work, Rakesh enjoys canvas painting and playing sports.

Karan Vora DevOps Architect

Karan is a DevSecOps Architect for Cloud Practice at LTIMindtree. He has 9+ years of IT experience with a rich background in implementing DevSecOps solutions for multiple application technology on both on-premises and cloud platforms. He has experience in DevSecOps transformation via Consulting & Architecting assignment around Cloud/DevSecOps for enterprise customers. Beyond work he likes cooking, dancing, travelling, trekking and music.