Kovair's DevSecOps: Making Security Testing Seamless in DevOps, with full PLM Transparency

By: Akshay Sharma,
CTO Kovair Software.

Kovair Software, Inc.

2410 Camino Ramon, STE 230
San Ramon, CA 94583
www.kovair.com
sales@kovair.com

© Kovair Software, Inc. All Rights Reserved. The Integrated ALM Company.

Kovair's DevSecOps

Integrating Security Testing within development and the operations teams is becoming the new norm, but this migration needs newer thinking, with newer processes, methods and tools. Full Product Lifecycle Management with Risk/Hazard Assessments are needed with Security in mind.

Security and risk management experts were once tasked occasionally, with consultants coming in annually, into typical organizations. What was once a silo'ed and occasional activity, are now engrained functions within all development and operations, including product management as all engineers need to be tasked with ensuring application and data security.

In this new world, all software engineers need to:

- Integrate security and compliance testing seamlessly into DevSecOps processes, within their continuous integration or continuous deployment toolchain environments.
- Scan for known vulnerabilities and misconfigurations in all open-source and third-party components, using vendors like HCL's Appscan and Veracode. Ideally, this is done with software composition analysis with hazard risk assessments, from vendors like Kovair, with product lifecycle management capabilities.
- Integrate Continuous Security Testing, with Shift-Left Testing concepts earlier in the development process, along with Shift-Right Testing in the field.
- Utilize security test automation scripts, templates, and test reports with the highest level of assurance with full transparency, within the entire product lifecycle.

According to Gartner:

"By 2023, more than 70% of enterprise DevSecOps initiatives will have incorporated automated security vulnerability and configuration scanning for open-source components and commercial packages, which is a significant increase from fewer than 30% in 2019."

Source: Gartner's report: **"12 Things to Get Right for Successful DevSecOps"**

According to this Gartner report, enterprises are looking to Agile, DevOps, and PLM solutions and all three require holistic applications security and data security testing and monitoring.

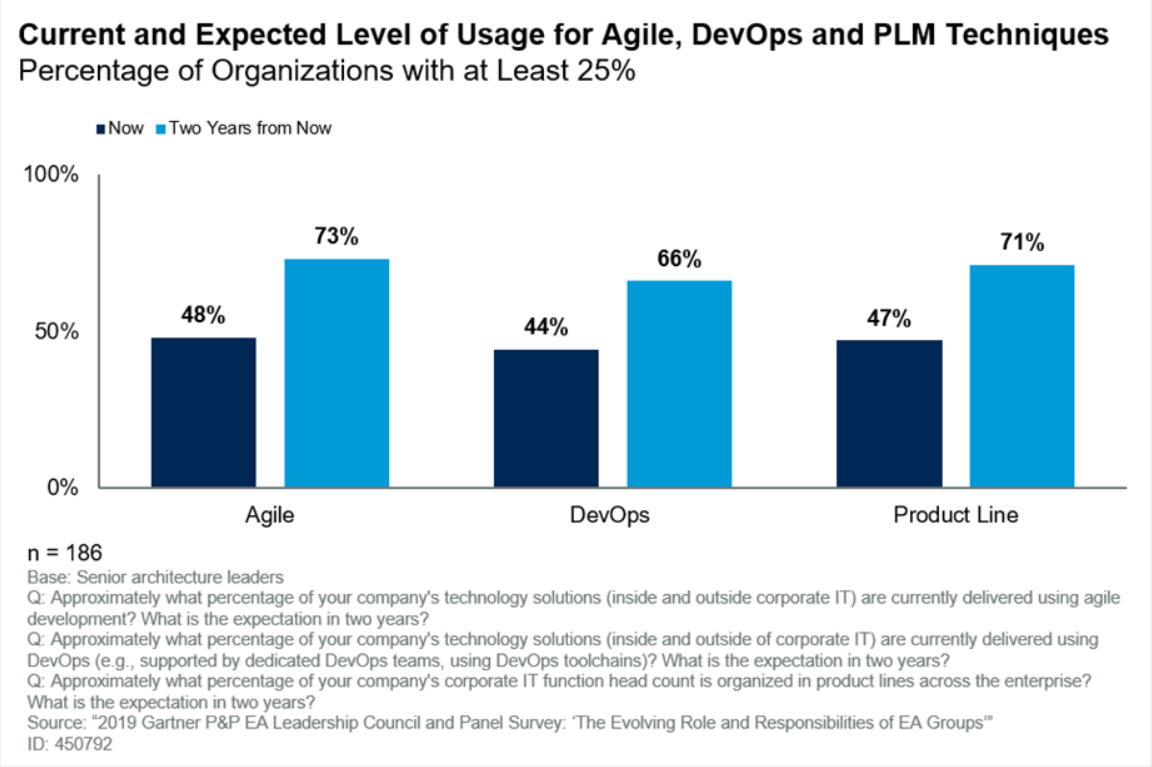

Fig:1

According to Gartner, Security doesn't stop in development (the left side of Figure 2). The entire DevOps life cycle needs to be secured, including when new services are deployed into runtime operation (the right side of Figure 2).

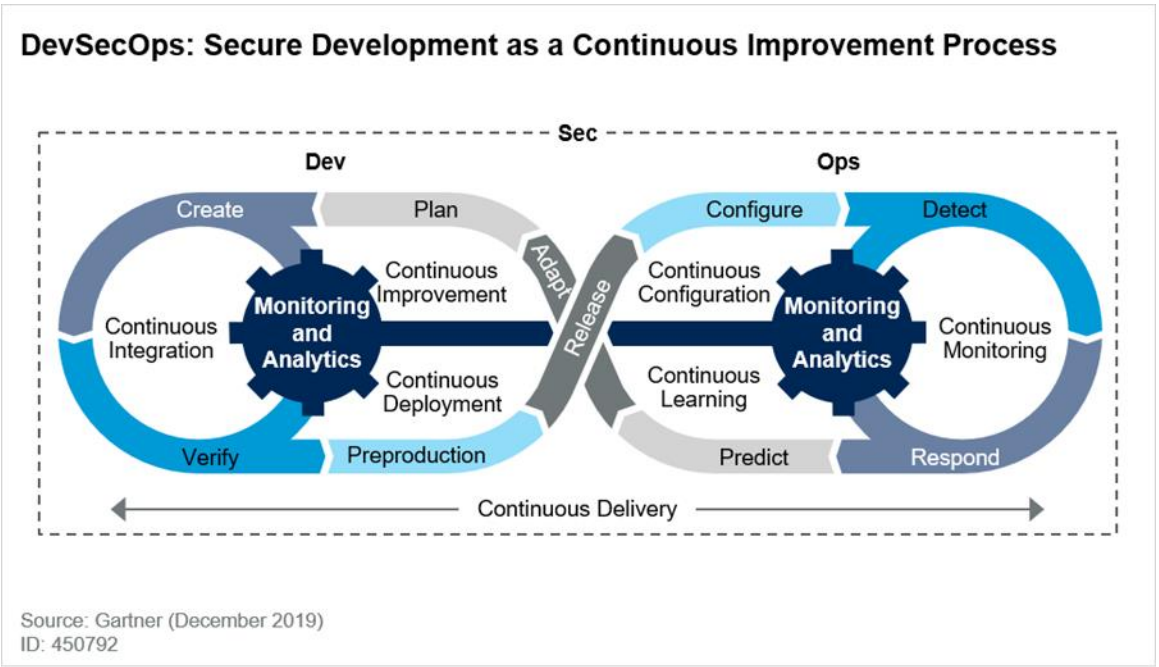

Fig:2

With Kovair's solutions, holistic DevSecOps with PLM can be achieved:

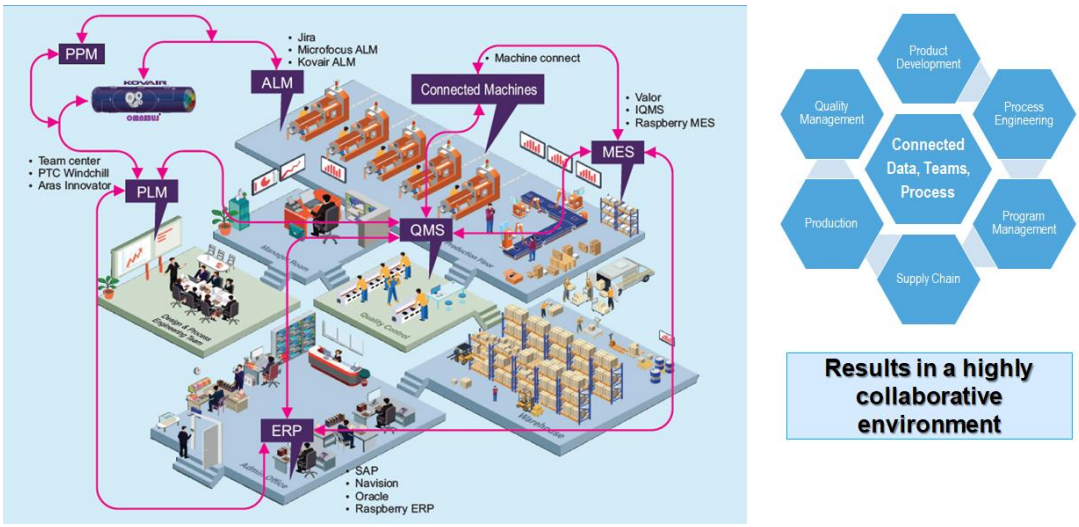

Fig:3

Kovair's Critical DevSecOps capabilities include:

- **Creation, orchestration, and management** of complex software release pipelines, of Kubernetes deployments, and legacy ALM systems with Security process adherence and configurations through task based configurable pipelines, that can be made concurrent, within a drag-and-drop workflow editor.
- **Execution of both automated and manual tasks**, on-demand, as part of the DevSecOps pipeline flow, for all Kubernetes solutions, as well as legacy ALM applications, with complete Project Lifecycle Management, Risk and Hazard Management Reports.
- **Execution of custom commands** managing dependency between custom applications, system commands and microservices across the complete Continuous Delivery pipeline for security testing. Kovair provides integration with security testing tools like HCL AppScan and Veracode.
- **Execution of Tasks on any host** removing the dependency of having security testing tools in one single server or in Kovair DevOps application server enabling hybrid multi-cloud environment.
- **In-depth visibility** into release pipeline and progress across all environments for all teams in a real-time manner through pre-defined reports and dashboards facilitating early detection of security flaws.

- **Security Test Execution across multiple environments** - cloud, VMs, containers, and traditional environments having any operating systems.
- **Application Performance Monitoring** with the help of Dynatrace or any other APM tool as per requirements whereby issues are reported and can be raised as a defect in Kovair's defect management tool.

Next Steps for Project Leaders:

Enterprise DevSecOps offered by Kovair facilitates the concept of continuous delivery pipelines with continuous Security Testing through automation of different activities involved in the delivery cycle. With this launch, Kovair will now start offering a full Enterprise DevSecOps workflow to its prospects and customers, with integrated solutions from it's partners.

Conclusion

CIOs and Software Architects of Enterprises embarking on Digital Transformation projects should explore Kovair's latest DevSecOps-based offerings as they re-vector to newer hybrid multi-cloud datacenters offering newer services: with security vulnerability assessments built-in, via integrated partners.

Here we have discussed all the migration strategies and best practices. Follow-on blogs will include Use Case Scenarios, and further benefits of the Kovair solution set.