

Development Centric DevSecOps



Executive Summary

Traditional software delivery has involved distinct teams with handshakes across application lifecycle from **Development**→**Testing**→**Security**→**Operations** which led to quarterly and half-yearly release cycles. With a need to accelerate time-to-market for software changes coupled with adhering to security guidelines especially in light of the increasing security threats facing the Travel industry and ensuring uptime for business applications, organizations have adopted DevOps and DevSecOps to transform their software delivery processes.

DevSecOps has been viewed as Security at the intersection of Development and Operations with security scans being triggered early in the application lifecycle. Typically, Development finds and resolves vulnerabilities, Operations blocks attacks and Security has visibility and control across the board as depicted in Figure 1.

While integration of tools tied to automation has been the driver for achieving DevSecOps, there are concerns over secure design, governance structures, developer responsibilities, and lack of skills in light of

increased exposure of travel applications to security breaches. Development centric approach to DevSecOps addresses these with an overlap on Engineering, Operations and Security Compliance.

Loopholes in design stem from interaction of crucial aviation systems with legacy technologies, leading to multiple vulnerable areas making Travel the 2nd most targeted sector for security attacks. Lack of skills leads to undesirable outcomes for DevSecOps adoption as referenced in DevSecOps Global Skills Survey. Further, 70% stated they have not received formal training making it difficult for them to be successful. While security is embedded early on to capture vulnerabilities with associated metrics, developers often look at these measures as hindrance which slows the pace of delivery often leading to concerns on developer responsibility and effectiveness of governance framework. The Sonatype DevSecOps Survey reveals 50% of developers know security is important but don't have enough time to spend on it.



Figure 1



Development centric DevSecOps

While automation ensures security leaks can be caught and resolved, however overall cycle time gets delayed primarily due to lack of clarity to developers around:

- Security guidelines with focus on 'Secure by Design'
- Governance metrics tracked using security gates
- Application security overlaps with IT Security, Operations and Engineering.

Approach is to enable the Development team with expertise from engineering (tooling), operations and IT security (compliance and governance standards) so that they are aware of the practices needed to be incorporated right from inception phase as depicted in Figure 2.

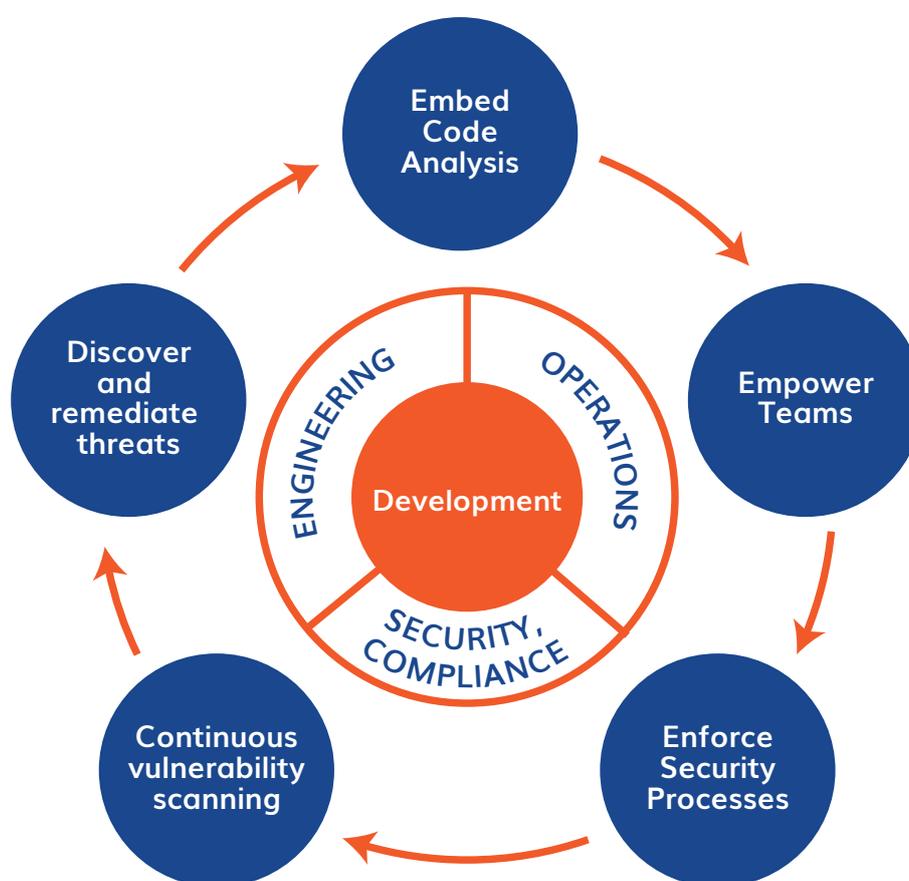


Figure 2

Embedding Code Analysis does not just involve integrating plugins into IDE and continuous integration; it goes beyond that to educate developers around OWASP Top 10 vulnerabilities, security rules and best coding practices from security perspective. Awareness and training around these make sure the rules and coding practices are followed right during design and development thereby reducing iterations.

Development teams are free to question specific rules / practices and in consultation with supporting teams can update and refine the rules database thereby marking certain non-essential security rules false positives.

Security process includes governance metrics like Defect Density (number of vulnerabilities per component), Defect Burn Rate (vulnerabilities resolution), Top Vulnerability types and Recurring Bugs, Adversaries per Application and Adversary Return Rate that are published frequently and tracked to closure. Benchmarks are discussed and agreed among the development, security and operation teams thereby reducing technical debt.

While tools are in play from operations perspective to discover and remediate threats, the root cause is fed into development teams to ensure such attacks are dealt while designing and developing the applications. Development teams are part of the root cause findings and preventive actions. This ensures such vulnerabilities are considered while designing the applications.

Continuous vulnerability scans are triggered periodically on both the source code and the running applications with insights being shared with operations, development, security and engineering teams, findings of which help the respective teams to take corrective actions either in code, infrastructure or tooling.

Benefits

Such an approach results in:

- Ensuring 'Secure by Design' principle is followed by empowering and educating development together with effective collaboration with security, operations and engineering teams.
- Positive customer perception around secure delivery, resulting in becoming a trusted partner.
- Early detection and resolution of security issues together with speed in delivery leading to cost optimization.
- Increased ability to measure vulnerabilities that helps in constant iterative improvements.
- Improved overall security coupled with reduction in vulnerabilities, increased code coverage tied to automation.

Conclusion

While automation is the underlying foundation for adopting DevSecOps, it's the Development centric approach to DevSecOps that has been a catalyst to accelerate adoption at IGT Solutions and has helped teams to work towards a common and shared goal of building, delivering and maintaining secure applications.



References

- IBM. "IBM X-Force Threat Intelligence Index" | <https://www.ibm.com/security/data-breach/threat-intelligence>. 2019
- Veracode and DevOps.com. " DevSecOps Global Skills Survey" | <https://info.veracode.com/analyst-report-devsecops-global-skill-survey.html>
- Sonatype. "DevSecOps Community Survey" | <https://cdn2.hubspot.net/hubfs/1958393/DevSecOps%20Survey/Sonatype%20DevSecOps%20Survey%202017.pdf?t=1492464912432>. 2017

About the Author



Mitul Jain

Author leads DevOps (Cloud, Agile) and Testing Services at IGT Solutions. He brings 17 years of rich experience in DevOps, Cloud, Agile and Automation while architecting various solutions, models and frameworks using cutting-edge innovative technologies. He has significant exposure in adopting industry's best practices for multiple customers in Travel and Hospitality, Transportation, BFSI, Telecom, and Manufacturing sector.



IGT Solutions (IGT) is a leading Technology, BPM, and Digital Services and Solutions Company committed to deliver innovation and business excellence across the entire spectrum of Travel, Transportation and Hospitality domain.

Established in 1998, with 100% focused on the Travel industry, we have more than 70+ marquee customers globally. IGT serves 4 in top 5 Airlines, Top 5 Travel Companies, 4 in Top 5 Hospitality companies. We provide digital contact center services, travel technology and innovative digital services and solutions for 100+ travel processes including Reservations and Sales, Customer Service, IROPS Management, Baggage Helpdesk, Crew Helpdesk, Chatbots, Robotic Process Automation, Travel Analytics and Social Media Services.



IGT Solutions Pvt. Ltd.

Echelon Building, Plot No. 49,
Sector-32, Gurgaon - 122 001,
Haryana, India

T +91 (0)124 458 7000
F +91 (0)124 458 7198
mktg@igtsolutions.com
www.igtsolutions.com