SECURITY INNOVATION

DevOps Solutions

DON'T LET SECURITY SLOW YOU DOWN

DevOps is built on the premise of accelerated development to get features to the market quickly. This requires collaboration between software developers and IT infrastructure staff throughout an application's lifecycle.

Security Innovation helps client realize Secure DevOps via technical assessments, process reviews, and awareness and specialized training.

PLAN & ASSESS

Secure DevOps requires continuous and iterative assessment. Design analysis sets the foundation; mapping security requirements to code identifies potential automation points; and understanding how testing points can drive configuration changes lets you use existing technology wisely.

Security Innovation can conduct assessments at any phase of development and on any application type.

SDLC GAP ANALYSIS

Leveraging our proprietary Application Security Maturity Model (ASM) and expertise in popular industry methodologies, our team will analyze your processes, skillsets, and tools. We make specific recommendations and construct a roadmap for you to move from your current state to continuous Secure DevOps.

SECURE DESIGN REVIEW

To properly plan for security and component reuse, it's important to identify insecure APIs and frameworks. Securing these components enables recycling and minimized new development. A Security Design Review ensures security-sensitive elements (e.g. password requirements, user authentication mechanisms) and secure deployment options are defined so they can be coded properly.

SOFTWARE SECURITY CODE REVIEW

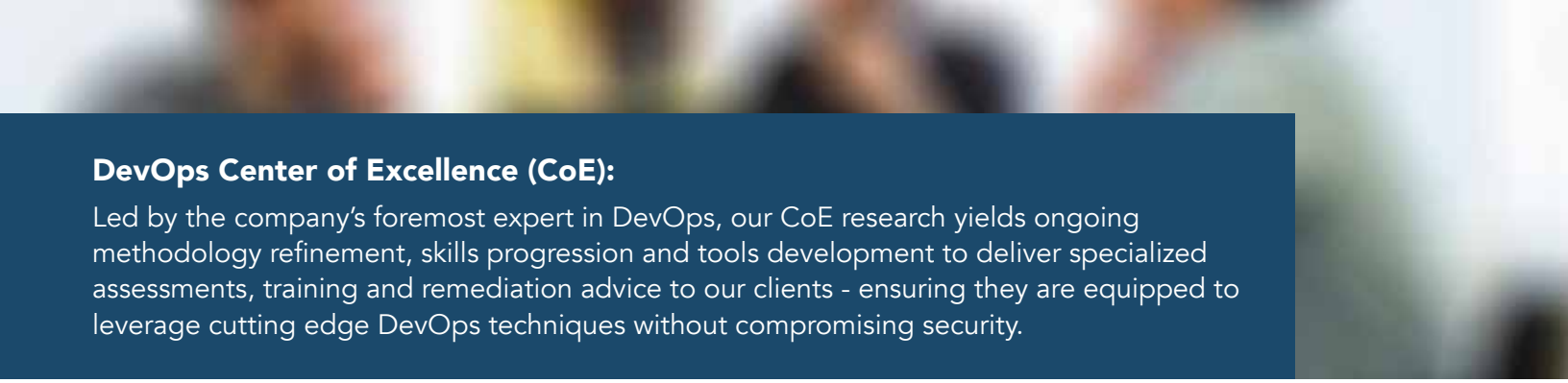
DevOps calls for rapid code reviews in small chunks, analyzing only newly or re-written code. While this makes it easy for developers to push modular code to production, certain features need to undergo deeper inspection before deployment. To facilitate continuous review as part of DevOps cycles, we focus on "hot spots" in code bases, frameworks and components, offering both rapid and deeper-level

SOFTWARE SECURITY ASSESSMENT

Software should be assessed regularly to provide an immediate feedback loop to development. Leveraging scanners for breadth and specialized tools for depth, we can conduct recurring analysis on regularly updated code and more sophisticated attacks for new or higher risk features. To ensure problems are fixed correctly, we provide detailed platform and technology specific remediation guidance.

INFRASTRUCTURE ATTACK SIMULATION

Unlike a penetration test, malicious hackers don't just probe for vulnerabilities in deployed software – they constantly scan, test, and attack all layers of your organization. Our Attack Simulation does the same, assessing your entire organization's resilience against persistent external attack to identify vulnerabilities that can lead to a breach or be used to traverse to other more valuable assets.



DevOps Center of Excellence (CoE):

Led by the company's foremost expert in DevOps, our CoE research yields ongoing methodology refinement, skills progression and tools development to deliver specialized assessments, training and remediation advice to our clients - ensuring they are equipped to leverage cutting edge DevOps techniques without compromising security.

TRAIN

IT security and software security go hand in hand. DevOps emphasizes cross-training so each person has skills in multiple areas to minimize information silos.

With the industry's largest application security training library comprising 100-400 level courses, we offer progressive training for all major roles, technologies and platforms.

"It is not enough to do your best; you must know what to do, and then do your best."

W. Edwards Deming

BY PLATFORM

Mobile, Android, iOS, AWS Database, Oracle, SQL, Automotive, Cloud, Azure, Embedded, Windows

BY TECHNOLOGY

.NET, C#, Java, PHP, C/C++, Objective-C, Web 2.0, AJAX, HTML 5.0, SAP, Ruby on Rails

BY COMPLIANCE

PCI DSS, OWASP, CWE, HIPAA, NIST

- **MANAGERS**
  Learn basic security practices and how they build off each other in subsequent phases
- **ARCHITECTS**
  Learn how to assess design components, re-use secure elements, threat model and reduce your attack surface
- **DEVELOPERS**
  Learn how to code defensively and remediate vulnerabilities in specific languages, and conduct rapid security code review techniques for iterative testing that consider deployment configurations
- **TESTERS**
  Learn how to leverage completed threat model and security architecture and requirements to drive test planning and penetration testing for applications and application defenses, e.g., WAFs
- **OPERATIONS/IT**
  Learn secure configuration skills for cloud services, databases, and infrastructure defenses, as well as knowledge