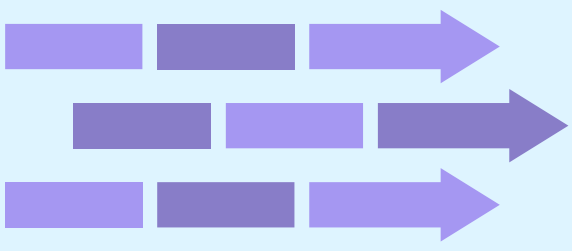
6 Steps to Implementing DevSecOps

DevSecOps brings security and operations into the development process and helps ensure that everyone within an organization is responsible for security and compliance. A DevSecOps culture has become a must in order to maintain speed, agility, and innovation while simultaneously meeting regulations and staying ahead of attacks. Making the shift can seem complicated and confusing, but a few practical tips can get you headed in the right direction.

Here are six steps you can follow to start baking security into the DNA of your organization.

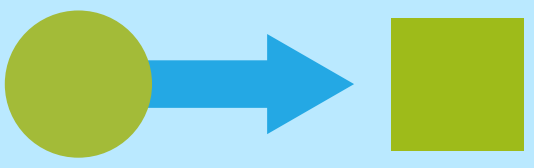
1 CODE ANALYSIS

Deliver code in small, frequent releases to make it easier to quickly check for vulnerabilities, while also embedding code analysis into the quality assurance process



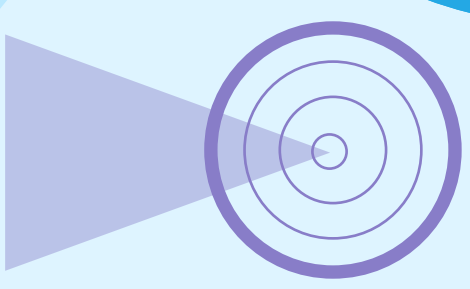
2 CHANGE MANAGEMENT

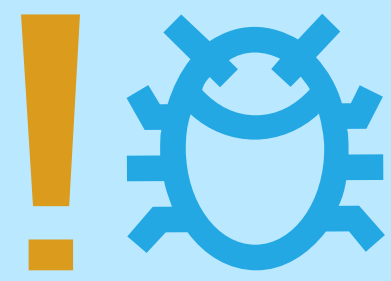
Make the change management process more efficient by allowing any developer at any time to suggest a mission critical security change – and make the approved changes within 24 hours



6 SECURITY TRAINING FOR ENGINEERS

Empower engineers with security-specific coding training by sending them to industry conferences or by investing in security certifications





3 COMPLIANCE MONITORING

Gather evidence of compliance while you're starting to code or make changes so you will be in a continuous state of compliance

5 VULNERABILITY MANAGEMENT & ASSESSMENT

Even after you've released the code and done vulnerability checks, it's important to conduct periodic scans and do code reviews and penetration tests

4 THREAT INVESTIGATION

Discover, investigate, and remediate threats or vulnerabilities that have emerged based on the changes you've made to the organization with newly delivered code

sumologic™

Let Sumo Logic give you the visibility you need on your journey to DevSecOps.

Try it out for free

www.sumologic.com/start-free