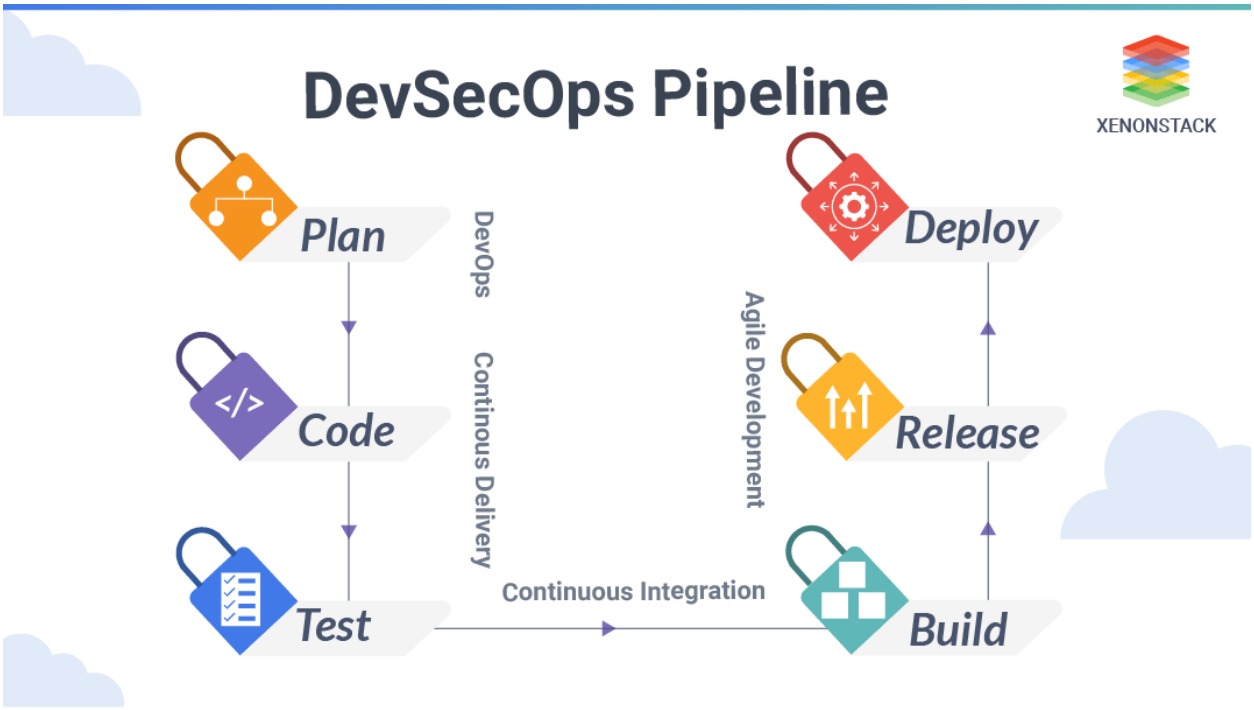
Definition of DevSecOps

DevSecOps is a cultural and technical practice that unifies software development (Dev), security (Sec), and operations (Ops) into a single, collaborative process. It "shifts left" security considerations—integrating them early and continuously throughout the software lifecycle—rather than treating security as a bolt-on at the end. In defense contexts, DevSecOps emphasizes secure, rapid delivery of mission-critical capabilities while maintaining compliance with standards like DoD's Risk Management Framework (RMF) and continuous Authorization to Operate (ATO). This approach reduces vulnerabilities, accelerates deployment (e.g., from months to days), and fosters resilience against cyber threats, which aligns with EADGE-T's goals of countering emerging adversaries through AI-augmented C2.



xenonstack.com

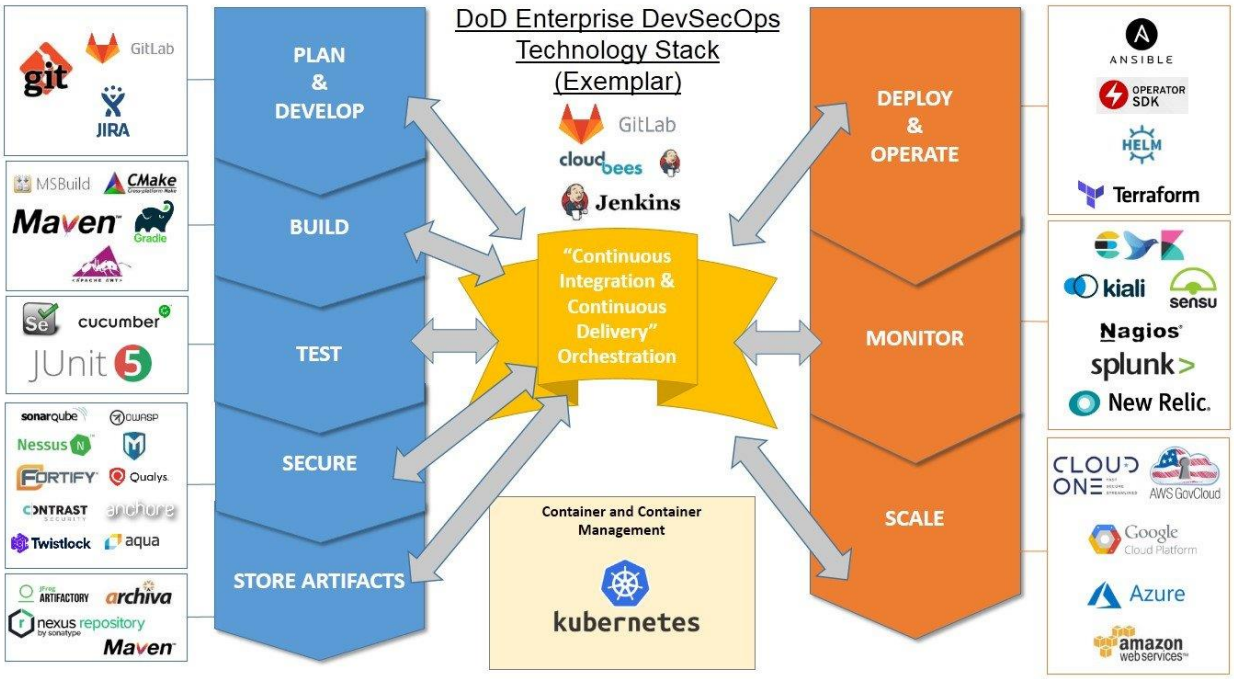
DevSecOps Pipeline - A Complete Overview | 2024

Key DevSecOps Practices

Based on DoD and industry standards, here are core practices tailored to defense systems like EADGE-T. These build on Phase 1's cybersecurity (e.g., SIEM in Section 3.3,

vulnerability scanning in Section 3.6) and DevOps elements, enabling secure TR2 enhancements.

- **Shift Left Security**: Embed security requirements and automated checks (e.g., static/dynamic code analysis, threat modeling) from the planning phase. In TR2, this could mean scanning AI/ML models for vulnerabilities during development in the SDC.
- **Automated Pipelines (CI/CD with Security Gates)**: Use tools like Jenkins, GitLab CI, or Kubernetes for automated builds, testing, and deployments, with integrated security scans (e.g., SAST/DAST, container vulnerability checks). Defense adaptations include compliance-as-code for RMF controls, ensuring zero-downtime updates in MOSA architectures.
- **Infrastructure as Code (IaC)**: Treat infrastructure (e.g., networks, servers) as versioned code, scanned for misconfigurations. Phase 1's Juniper Apstra (Section 5.3.1) for intent-based networking can extend here for secure, automated provisioning.
- **Continuous Monitoring and Feedback**: Implement real-time logging, anomaly detection, and incident response (e.g., via SIEM tools from Phase 1 Section 3.3). In defense, this includes ATO monitoring and integration with tools like ELK Stack or Splunk for audit trails.
- **Collaboration and Culture**: Foster cross-functional teams (dev, sec, ops) with shared responsibilities. DoD emphasizes training and metrics like deployment frequency and mean time to recovery (MTTR) to measure success.
- **Compliance and Risk Management**: Automate adherence to standards (e.g., NIST, STIGs from Phase 1). In classified environments like EADGE-T's RED/Pink domains, this includes secure supply chain practices to mitigate export/ITAR risks.



infoq.com

The Defense Department's Journey with DevSecOps - InfoQ

Relevance to TR2 and Derived Stakeholder Needs

DevSecOps directly supports the Phase 1 bullet on architectural transformation for modular/open solutions and continuous deployment, ensuring these are secure-by-design. It enhances TR2's AI integrations (e.g., secure data pipelines in TR2-AI-NEED-007) and MOSA (TR2-AI-NEED-009) by preventing vulnerabilities in third-party UAE AI solutions. Without DevSecOps, risks like supply chain attacks could undermine CDS integration (Need Area 1) or site expansions (Need Area 6).