DevSecOps Ecosystem Security Phase 1: State of the Art & Security Requirements

Radu Darius Razvan

Roman Alisa-Dariana

DevSecOps Ecosystem Overview

Core Technologies: GitHub Actions, Git, CI/CD Pipelines, Issue Tracking

Implementation: GitHub Actions (Primary CI/CD Platform)

Security Focus Areas:

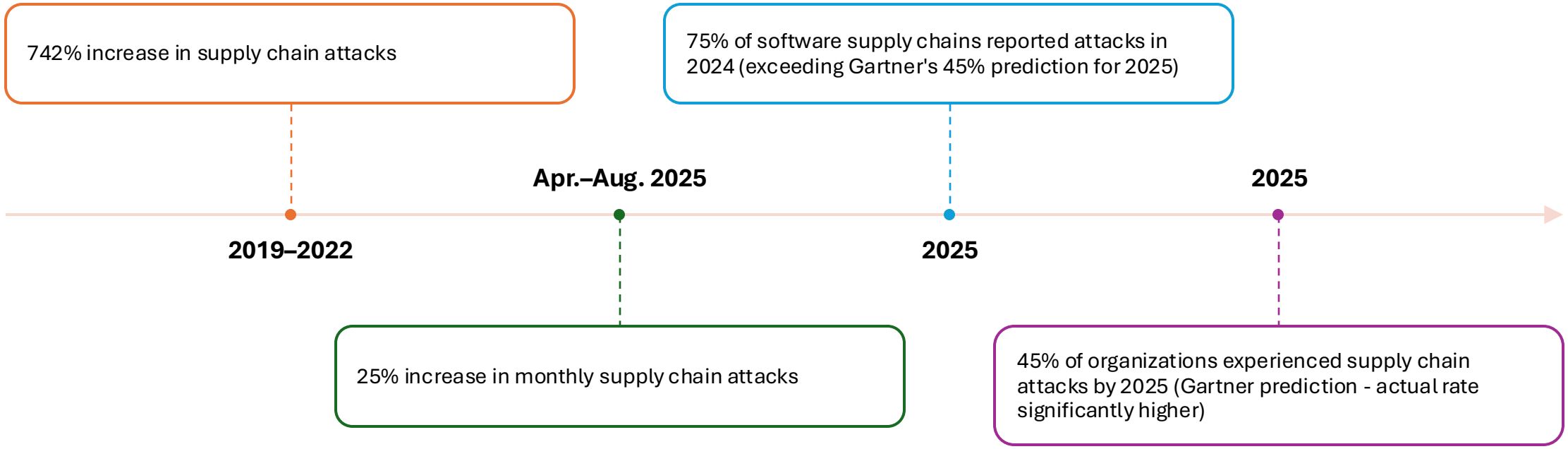
Secret management and credential protection

Pipeline hardening and integrity

Access control and authentication

Supply chain security

Critical Statistics



Recent Critical Breaches (2024-2025)

1. **1. tj-actions/changed-files Supply Chain Attack (March 2025)**
    1. **CVE-2025-30066** (CVSS: 8.6)
    2. **Impact**: 23,000+ repositories affected
    3. **Method**: Compromised GitHub Personal Access Token (PAT)
    4. **Result**: CI/CD secrets exposed in workflow logs (AWS keys, GitHub tokens, npm tokens, SSH keys)
    5. **Added to CISA KEV catalog** - Active exploitation confirmed
2. **reviewdog/action-setup Compromise (March 2025)**
    1. **Cascading supply chain attack** targeting v1 tag
    2. Malicious Base64-encoded payload injected
    3. Affected downstream dependencies including tj-actions
3. **Git Security Vulnerabilities (January 2025)**
    1. **CVE-2024-50349** and **CVE-2024-52006**
    2. ANSI escape sequence exploitation
    3. Credential theft through misleading prompts

Threat Landscape & Attack Vectors

OWASP Top 10 CI/CD Security Risks

CICD-SEC-1: Insufficient Flow Control Mechanisms

CICD-SEC-2: Inadequate Identity and Access Management

CICD-SEC-3: Dependency Chain Abuse

And 7 more ...

Common Attack Methods

Credential theft via exposed secrets in logs

Malicious commits to trusted repositories

Pipeline poisoning through pull request manipulation

Dependency confusion and typosquatting

Token compromise for unauthorized access

Applicable Security Standards & Frameworks

SLSA (Supply-chain Levels for Software Artifacts): Framework for securing build integrity and verifying artifact provenance across four maturity levels.

NIST SSDF (SP 800-218): Defines secure software development practices across four groups—PO, PS, PW, and RV—for end-to-end software assurance.

NIST SP 800-204D: Guides integration of software supply chain security into DevSecOps pipelines through secure builds and artifact attestations.

OWASP Top 10 CI/CD Security Risks: Community-driven list of the most critical CI/CD pipeline vulnerabilities and recommended mitigations.

CIS Benchmarks: Prescriptive hardening standards for Docker, Kubernetes, and cloud platforms to secure CI/CD environments.

CI/CD Security Requirements

Confidentiality

Protect secrets, credentials, code, and customer data through encrypted storage, RBAC, and OIDC short-lived tokens.

Enforce secret masking and environment-scoped access for least-privilege control.

Integrity

Ensure artifact and code integrity with hash verification, SLSA provenance, signed commits, and protected branches.

Maintain immutable logs and verified dependencies via SBOM and pinning.

Availability

Maintain pipeline resilience with redundant runners, retry logic, and continuous monitoring.

Apply rate limiting, resource quotas, and DDoS protection for CI/CD uptime.