

DevSecOps as a Service (DSOaaS)

- [DSOaaS Overview](#)
- [Getting Started with DSOaaS](#)
- [DSOaaS Methods](#)
- [How Our DSOaaS Works](#)
- [DSOaaS Deliverables](#)
- [DSOaaS SLA](#)
- [DSOaaS FAQ](#)

DSOaaS Overview

What is DSOaaS?

GrintOps DSOaaS embeds security controls into your CI/CD pipeline, ensuring vulnerabilities are caught before production.

Ideal For

- Teams handling sensitive user data
- Compliance-driven environments (ISO, HIPAA)
- DevOps teams needing security hardening

Plans

- Starter: SAST + container scan
- Pro: Add DAST, secrets detection, SBOM
- Enterprise: Custom policy engine + compliance reporting

Getting Started with DSOaaS

Step 1 – Assessment

We analyze your code stack & pipeline to match relevant security scanners.

Step 2 – Pipeline Integration

Security stages added as pre-deploy & post-build checks.

Step 3 – Reporting & Alerts

All findings accessible via portal or sent to your DevSecOps Slack/Email channels.

DSOaaS Methods

Common Integrations

- GitHub/GitLab runners
- Terraform modules
- Dockerfile linters

Security Layers

- SAST (CodeQL, SonarQube)
- DAST (OWASP ZAP, Nikto)
- SCA (Grype, Trivy)
- Secrets/Key Leak Detection

Compliance Ready

- SBOM generation
- CVE linkbacks
- OWASP mapping

How Our DSOaaS Works

Steps

1. GrintOps evaluates your pipeline & codebase
2. We add security gates:
 - Pre-commit hooks
 - CI/CD stage scanners
3. Alerts & reports delivered per commit or on schedule

DSOaaS Deliverables

Deliverable Items

- Security pipeline config (modular YAML)
- Findings summary (HTML, JSON)
- SBOM & CVSS scorecards
- GitHub Action / GitLab CI snippets
- Risk remediation checklist

DSOaaS SLA

Service Level Agreements

Tier	Response Time	Onboarding Time	Alerts
Starter	≤ 48h	3-5 days	Weekly
Pro	≤ 24h	2-4 days	Daily
Enterprise	≤ 12h	1-3 days	Realtime + SIEM export

DSOaaS FAQ

Frequently Asked Questions

Q: Will this slow down my pipeline?

A: No, scans are optimized to run asynchronously or in parallel depending on your tier.

Q: Does this replace pentesting?

A: No, DSOaaS is preventive. Pentest (PTaaS) is complementary for real-world exploitation checks.

Q: Can I customize security rules?

A: Yes, especially in Enterprise plans with policy-as-code support.

Q: What languages are supported?

A: Most popular stacks: JS, Python, Go, Java, PHP, Ruby. Others can be configured on request.