DevSecOps-Vault

Collection of roadmaps, tools, best practice, resources about DevSecOps
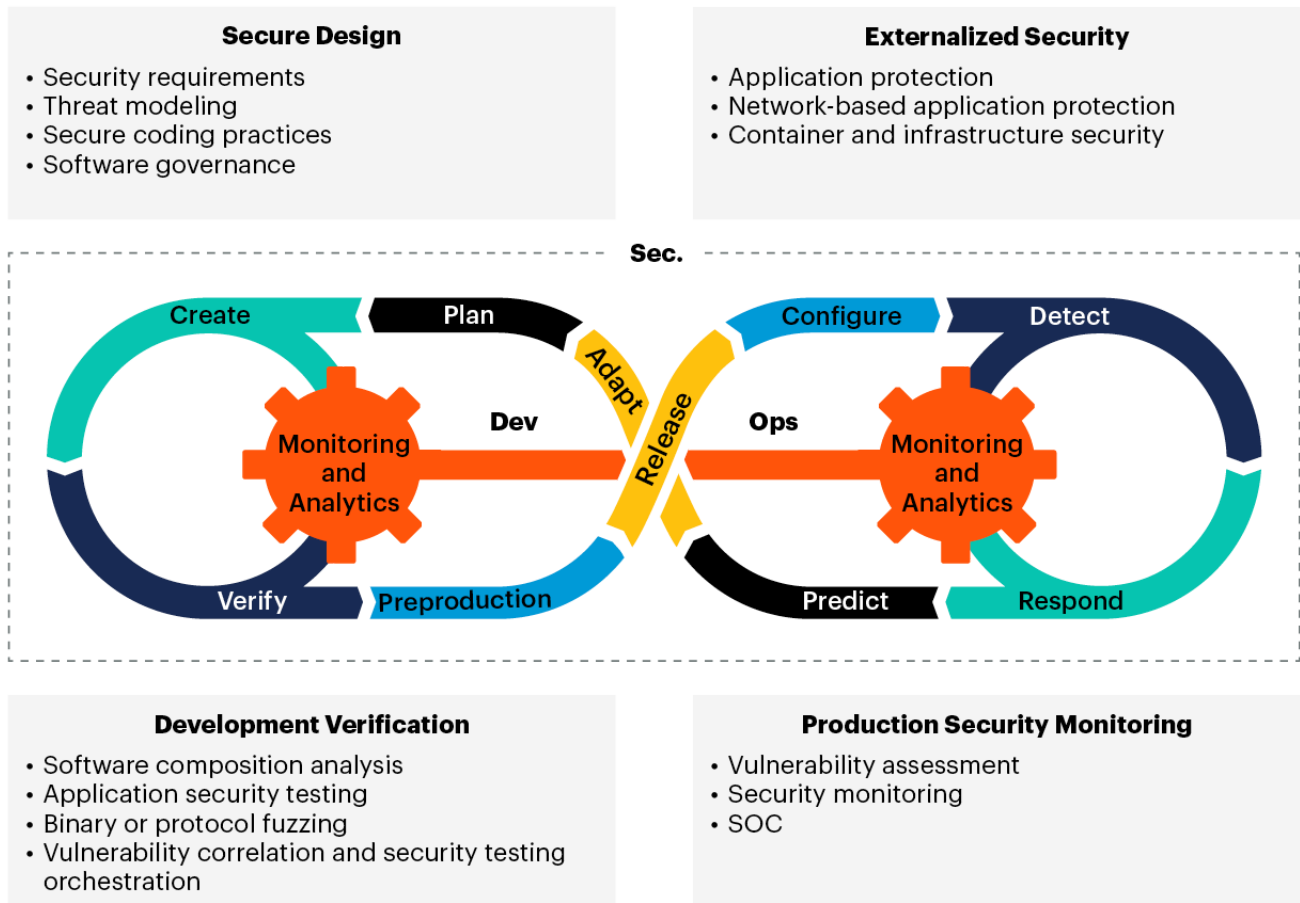
What is DevSecOps

DevSecOps is an approach to software development that integrates security into the entire software development lifecycle. It combines the principles of DevOps with security to create a culture of security that permeates the entire development process.

The goal of DevSecOps is to ensure that security is not an afterthought but is built into the development process from the very beginning. This approach emphasizes collaboration between development, operations, and security teams to ensure that security is a shared responsibility across the organization.

DevSecOps involves the implementation of security controls throughout the development lifecycle, from design to deployment, and beyond. This includes automated security testing, continuous monitoring, vulnerability assessments, and penetration testing.

By implementing DevSecOps practices, organizations can improve their overall security posture and reduce the risk of security breaches and vulnerabilities. This approach also helps to accelerate the delivery of secure software by integrating security into the development process, rather than treating it as a separate activity.

Take a look at links for detailed explanitation on DevSecOps:

- Redhat definitions
- IBM definitions
- Synk definitions
- Synopsys definitions
- Spacelift definitions

DevSecOps Security Checklist

Checklist Link

-
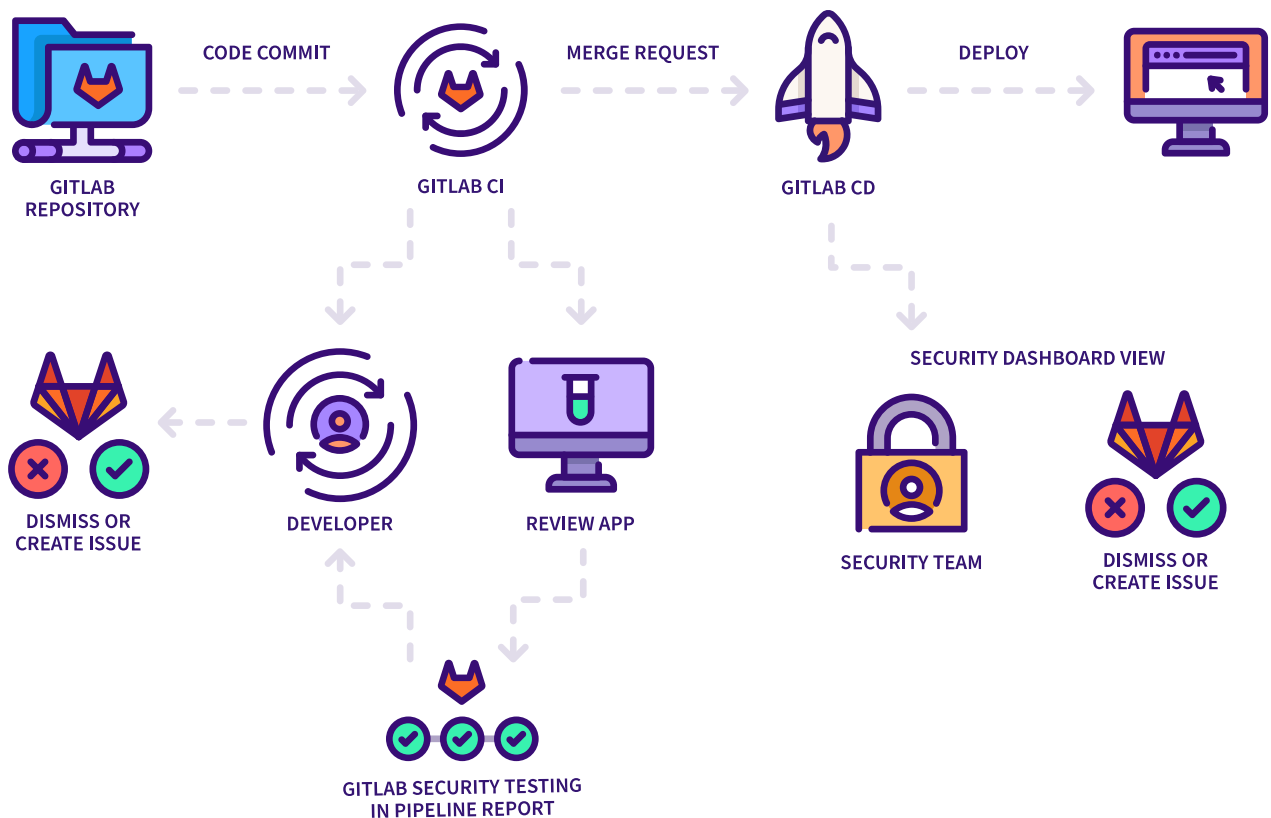
1. Design

- Development Lifecycle
    1. SDL(Secure Development Lifecycle) by Microsoft
    2. OWASP's Software Assurance Maturity Model
    3. Building Security In Maturity Model (BSIMM)
    4. NIST's Secure Software Developerment Framework
    5. DevSecOps basics: 9 tips for shifting left (Gitlab)
    6. 6 Ways to bring security to the speed of DevOps (Gitlab)
- Threat Model

1. What is Threat Modeling / Wikipedia
2. Threat Modeling by OWASP
3. Application Threat Modeling by OWASP
4. Agile Threat Modeling Toolkit
5. OWASP Threat Dragon

2. Develop

- Secure Coding
    1. Secure coding guide by Apple
    2. Secure Coding Guidelines for Java SE
    3. Go-SCP / Go programming language secure coding practices guide
    4. Android App security best practices by Google
    5. Securing Rails Applications

3. Build

- SAST(Static Application Security Testing)
    1. Scan Source Code using Static Application Security Testing (SAST) with SonarQube, Part 1
    2. Announcing third-party code scanning tools: static analysis & developer security training

4. Test

- DAST(Dynamic Application Security Testing)
    1. Dynamic Application Security Testing with ZAP and GitHub Actions
    2. Dynamic Application Security Testing (DAST) in Gitlab
    3. DAST using pdiscoveryio Nuclei (github action)
    4. ZAPCon 2021-Democratizing ZAP with test automation and domain specific languages
- Penetration testing
    1. Penetration Testing at DevSecOps Speed

5. Deploy

- Security Hardening & Config
    1. CIS Benchmarks
    2. DevSecOps in Kubernetes
- Security Scanning
    1. Best practices for scanning images (docker)

6. Operate and Monitor

- RASP(Run-time Application Security Protection)
    1. Runtime Application Self-Protection by rapid7
    2. Jumpstarting your devsecops - Pipeline with IAST and RASP
- Security Patch
    1. RASP(Runtime Application Self-Protection)
- Security Audit
- Security Monitor
    1. IAST(Interactive Application Security Testing)

      2. Metrics, Monitoring, Alerting
- Security Analysis
  1. [Attack Surface Analysis Cheat Sheet by OWASP](#)

Resources

Books

Books focussed around DevSecOps, bringing the security focus up front.

- [DevOpsSec](#)
- [Docker Securitiy - Quick Reference](#)
- [Holistic Info-Sec for Web Developers](#)
- [Securing DevOps](#)
- [The DevOps Handbook (Section VI)](#)

Conferences

A body of knowledge for combining DevOps and Security has been delivered via conferences and meetups. This is a short list of the venues that have dedicated a portion of their agenda to it.

- [AWS re:Inforce](#)
- [AWS re:Invent](#)
- [DevSecCon](#)
- [DevOps Connect](#)
- [DevOps Days](#)
- [Goto Conference](#)
- [IP Expo](#)
- [ISACA Ireland](#)
- [RSA Conference](#)
- [All Day DevOps](#)

Training

DevSecOps requires an appetite for learning and agility to quickly acquire new skills. We've collected these links to help you learn how to do DevSecOps with us.

Labs

Labs are hands-on learning opportunities to grow your skills in Dev, Sec, and Ops. All skills are useful and need to be grown so that you can have the empathy, knowledge and trade to operate DevSecOps style.

- [DevSecOps Bootcamp](#)
- [Exercism](#)
- [Infoseclabs](#)
- [Infrastructure Monitoring](#)
- [Pentester Lab](#)
- [Vulnhub](#)

Vulnerable Test Targets

It's important to build up knowledge by learning how to break applications left vulnerable by security mistakes. This section contains a list of vulnerable apps that can be deployed to learn what not to do. These same apps can be made safe by remediating the intentional vulnerabilities to learn how to prevent attackers from gaining access to underlying infrastructure or data.

- Damn Vulnerable Web Application (PHP/MySQL)
- LambHack (Lambda)
- Metasploitable (Linux)
- Mutillidae (PHP)
- NodeGoat (Node)
- OWASP Damn Vulnerable Serverless Application (DVSA) (AWS Serverless)
- OWASP Juice Shop (NodeJS/Angular)
- RailsGoat (Rails)
- WebGoat (Web App)
- WebGoat.Net (.NET)
- WebGoatPHP (PHP)

Security of CI/CD

DO NOT FORGET MANY DEVSECOPS PIPELINE SUFFER FROM SECURITY VULNEBILITIES

- Github Actions
    1. Security hardening for GitHub Actions
    2. Github Actions Security Best Practices
    3. GitHub Actions Security Best Practices [cheat sheet included]
- Jenkins
    1. Securing Jenkins
    2. Securing Jenkins CI Systems by SANS
    3. DEPRECATED/chef-jenkins-hardening

Tools and Links for DevSecOps
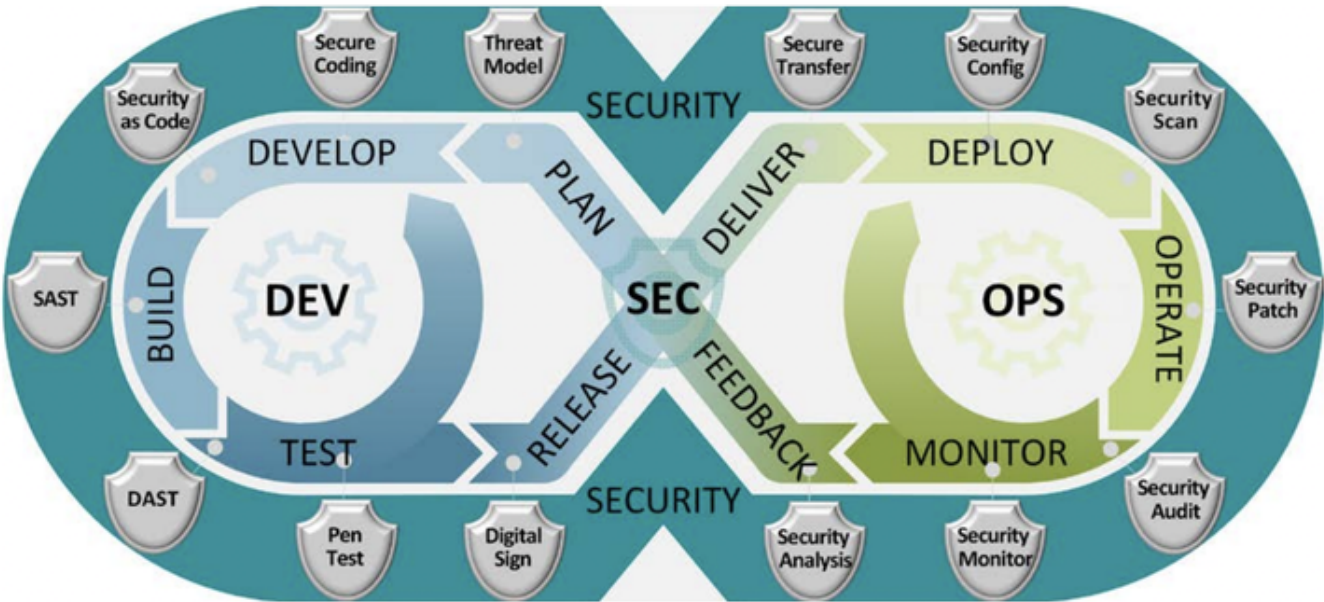
DevOps loop contains ==> Plan, Code, Build, Test, Release, Deploy, Operate, Monitor.

Pre-commit tools

DevSecOps pre-commit tools are a critical part of the software development lifecycle, particularly for organizations that prioritize security in their development processes. These tools help ensure that security considerations are integrated into every step of the development process, from coding to deployment.

Here are some reasons why DevSecOps pre-commit tools are important:

Early detection of security vulnerabilities: Pre-commit tools can identify security issues early in the development process, before code is even committed to the repository. This allows developers to address security concerns immediately, rather than discovering them later in the development process when they can be much more difficult and expensive to fix.

Consistent security standards: Pre-commit tools can enforce consistent security standards across the development team, ensuring that security best practices are followed by all developers.

Reduced risk of security breaches: By catching security issues early, pre-commit tools can help reduce the risk of security breaches and protect sensitive data.

Improved efficiency: Pre-commit tools can help developers catch security issues before they become more complex and time-consuming to fix, which can ultimately lead to more efficient development processes.

Enhanced collaboration: Pre-commit tools can help facilitate collaboration between developers and security teams by providing a common language and set of standards for discussing security issues.

Overall, DevSecOps pre-commit tools play a critical role in ensuring that security is integrated into the software development lifecycle. By catching security issues early and enforcing consistent standards, these tools help organizations build more secure and efficient software.

Name	URL	Description	Meta

Name	URL	Description	Meta
git-secrets	https://github.com/awslabs/git-secrets	AWS labs tool preventing you from committing secrets to a git repository	STARS 11K
git-hound	https://github.com/tillson/git-hound	Searchers secrets in git	STARS 981
goSDL	https://github.com/slackhq/goSDL	Security Development Lifecycle checklist	STARS 501
ThreatPlaybook	https://github.com/we45/ThreatPlaybook	Threat modeling as code	STARS 249
Threat Dragon	https://github.com/OWASP/threat-dragon	OWASP Threat modeling tool	STARS 495
threatspec	https://github.com/threatspec/threatspec	Threat modeling as code	STARS 260
pytm	https://github.com/izar/pytm	A Pythonic framework for threat modeling	STARS 677
Threagile	https://github.com/Threagile/threagile	A Go framework for threat modeling	STARS 443
MAL-lang	https://mal-lang.org/#what	A language to create cyber threat modeling systems for specific domains	STARS 21
Microsoft Threat modeling tool	https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool	Microsoft threat modeling tool	STARS 145
Talisman	https://github.com/thoughtworks/talisman	A tool to detect and prevent secrets from getting checked in	STARS 1.7K
SEDATED	https://github.com/OWASP/SEDATED	The SEDATED® Project (Sensitive Enterprise Data Analyzer To Eliminate Disclosure) focuses on preventing sensitive data such as user credentials and tokens from being pushed to Git.	STARS 101
Sonarlint	https://github.com/SonarSource/sonarlint-core	Sonar linting utility for IDE	STARS 205
DevSkim	https://github.com/microsoft/DevSkim	DevSkim is a framework of IDE extensions and language analyzers that provide inline security analysis	STARS 781

Name	URL	Description	Meta
detect-secrets	https://github.com/Yelp/detect-secrets	Detects secrets in your codebase	STARS 2.8K
tflint	https://github.com/terraform-linters/tflint	A Pluggable Terraform Linter	STARS 3.7K

## Secrets management

#TODO: Add explaination here

Secrets management includes managing, versioning, encryption, discovery, rotating, provisioning of passwords, certificates, configuration values and other types of secrets.

Name	URL	Description	Meta
GitLeaks	https://github.com/zricethezav/gitleaks	Gitleaks is a scanning tool for detecting hardcoded secrets	STARS 12K
ggshield	https://github.com/gitguardian/ggshield	GitGuardian shield (ggshield) is a CLI application that runs in your local environment or in a CI environment and helps you detect more than 350+ types of secrets and sensitive files.	STARS 1.3K
TruffleHog	https://github.com/trufflesecurity/truffleHog	TruffleHog is a scanning tool for detecting hardcoded secrets	STARS 11K
Hashicorp Vault	https://github.com/hashicorp/vault	Hashicorp Vault secrets management	STARS 27K
Mozilla SOPS	https://github.com/mozilla/sops	Mozilla Secrets Operations	STARS 12K
AWS secrets manager GH action	https://github.com/marketplace/actions/aws-secrets-manager-actions	AWS secrets manager docs	STARS 55
GitRob	https://github.com/michenriksen/gitrob	Gitrob is a tool to help find potentially sensitive files pushed to public repositories on Github	STARS 5.6K
git-wild-hunt	https://github.com/d1vious/git-wild-hunt	A tool to hunt for credentials in the GitHub	STARS 268
aws-vault	https://github.com/99designs/aws-vault	AWS Vault is a tool to securely store and access AWS credentials in a development environment	STARS 7.3K

Name	URL	Description	Meta
Knox	https://github.com/pinterest/knox	Knox is a service for storing and rotation of secrets, keys, and passwords used by other services	STARS 1.1K
Chef vault	https://github.com/chef/chef-vault	allows you to encrypt a Chef Data Bag Item	STARS 410
Ansible vault	Ansible vault docs	Encryption/decryption utility for Ansible data files	STARS 300

OSS and Dependency management

Dependency security testing and analysis is very important part of discovering supply chain attacks. SBOM creation and following dependency scanning (Software composition analysis) is critical part of continuous integration (CI). Data series and data trends tracking should be part of CI tooling. You need to know what you produce and what you consume in context of libraries and packages.

Name	URL	Description	Meta
CycloneDX	https://github.com/orgs/CycloneDX/repositories	CycloneDX format for **SBOM**	STARS 155
cdxgen	https://github.com/AppThreat/cdxgen	Generates CycloneDX **SBOM**, supports many languages and package managers.	STARS 178
SPDX	https://github.com/spdx/spdx-spec	SPDX format for **SBOM** - Software Package Data Exchange	STARS 216
Snyk	https://github.com/snyk/snyk	Snyk scans and monitors your projects for security vulnerabilities	STARS 4.4K
vulncost	https://github.com/snyk/vulncost	Security Scanner for VS Code	STARS 194

Name	URL	Description	Meta
Dependency Combobulator	https://github.com/apiiro/combobulator	Dependency-related attacks detection and prevention through heuristics and insight engine (support multiple dependency schemes)	STARS 83
DependencyTrack	https://github.com/DependencyTrack/dependency-track	Dependency security tracking platform	STARS 1.7K
DependencyCheck	https://github.com/jeremylong/DependencyCheck	Simple dependency security scanner good for CI	STARS 4.9K
Retire.js	https://github.com/retirejs/retire.js/	Helps developers to detect the use of JS-library versions with known vulnerabilities	STARS 3.2K
PHP security checker	https://github.com/fabpot/local-php-security-checker	Check vulnerabilities in PHP dependencies	STARS 1K
bundler-audit	https://github.com/rubysec/bundler-audit	Patch-level verification for bundler	STARS 2.5K
gemnasium	https://gitlab.com/gitlab-org/security-products/analyzers/gemnasium	Dependency Scanning Analyzer based on Gemnasium	
Dependabot	https://github.com/dependabot/dependabot-core	Automated dependency updates built into GitHub providing security alerts	STARS 3.2K

| Name	URL	Description	Meta
Renovatebot	https://github.com/renovatebot/renovate	Automated dependency updates, patches multi-platform and multi-language	STARS 12K
npm-check	https://www.npmjs.com/package/npm-check	Check for outdated, incorrect, and unused dependencies.	STARS 6.4K
Security Scorecards	https://securityscorecards.dev	Checks for several security health metrics on open source libraries and provides a score (0-10) to be considered in the decision making of what libraries to use.	STARS 3.3K
Syft	https://github.com/anchore/syft	CLI tool and library for generating an SBOM from container images (and filesystems).	STARS 3.9K

Supply chain specific tools

Supply chain is often the target of attacks. Which libraries you use can have a massive impact on security of the final product (artifacts). CI (continuous integration) must be monitored inside the tasks and jobs in pipeline steps. Integrity checks must be stored out of the system and in ideal case several validation runs with comparison of integrity hashes / or attestation must be performed.

Name	URL	Description	Meta
Tekton chains	https://github.com/tektoncd/chains	Kubernetes Custom Resource Definition (CRD) controller that allows you to manage your supply chain security in Tekton.	STARS 198
in-toto	https://github.com/in-toto/attestation/tree/v0.1.0/spec	An in-toto attestation is authenticated metadata about one or more software artifacts	STARS 106

Name	URL	Description	Meta
SLSA	[Official GitHub link](#)	Supply-chain Levels for Software Artifacts	`STARS 1.1K`
kritis	https://github.com/grafeas/kritis	Solution for securing your software supply chain for Kubernetes apps	`STARS 646`
ratify	https://github.com/deislabs/ratify	Artifact Ratification Framework	`STARS 107`

SAST

Static code review tools working with source code and looking for known patterns and relationships of methods, variables, classes and libraries. SAST works with the raw code and usually not with build packages.

Name	URL	Description	Meta
Brakeman	https://github.com/presidentbeef/brakeman	Brakeman is a static analysis tool which checks Ruby on Rails applications for security vulnerabilities	`STARS 6.6K`
Semgrep	https://semgrep.dev/	Hi-Quality Open source, works on 17+ languages	`STARS 7.9K`
Bandit	https://github.com/PyCQA/bandit	Python specific SAST tool	`STARS 5K`
libsast	https://github.com/ajinabraham/libsast	Generic SAST for Security Engineers. Powered by regex based pattern matcher and semantic aware semgrep	`STARS 99`
ESLint	https://eslint.org/	Find and fix problems in your JavaScript code	
nodejsscan	https://github.com/ajinabraham/nodejsscan	NodeJs SAST scanner with GUI	`STARS 2.1K`
FindSecurityBugs	https://find-sec-bugs.github.io/	The SpotBugs plugin for security audits of Java web applications	`STARS 2K`
SonarQube community	https://github.com/SonarSource/sonarqube	Detect security issues in code review with Static Application Security Testing (SAST)	`STARS 7.6K`
gosec	https://github.com/securego/gosec	Inspects source code for security problems by scanning the Go AST.	`STARS 6.6K`

Name	URL	Description	Meta
Safety	https://github.com/pyupio/safety	Checks Python dependencies for known security vulnerabilities .	`STARS 1.5K`

Note: Semgrep is free CLI tool, however some rulesets (https://semgrep.dev/r) are having various licences, some can be free to use and can be commercial.

OWASP curated list of SAST tools : https://owasp.org/www-community/Source_Code_Analysis_Tools

DAST

Dynamic application security testing (DAST) is a type of application testing (in most cases web) that checks your application from the outside by active communication and analysis of the responses based on injected inputs. DAST tools rely on inputs and outputs to operate. A DAST tool uses these to check for security problems while the software is actually running and is actively deployed on the server (or serverless function).

Name	URL	Description	Meta
Zap proxy	https://owasp.org/www-project-zap/	Zap proxy providing various docker containers for CI/CD pipeline	`STARS 11K`
Wapiti	https://github.com/wapiti-scanner/wapiti	Light pipeline ready scanning tool	`STARS 577`
Nuclei	https://github.com/projectdiscovery/nuclei	Template based security scanning tool	`STARS 12K`
purpleteam	https://github.com/purpleteam-labs/purpleteam	CLI DAST tool incubator project	`STARS 96`
oss-fuzz	https://github.com/google/oss-fuzz	OSS-Fuzz: Continuous Fuzzing for Open Source Software	`STARS 8.5K`
nikto	https://github.com/sullo/nikto	Nikto web server scanner	`STARS 6.5K`
skipfish	https://code.google.com/archive/p/skipfish/	Skipfish is an active web application security reconnaissance tool	`STARS 585`

Continuous deployment security

Name	URL	Description	Meta
SecureCodeBox	https://github.com/secureCodeBox/secureCodeBox	Toolchain for continuous scanning of applications and infrastructure	`STARS 575`

Name	URL	Description	Meta
OpenSCAP	https://github.com/OpenSCAP/openscap	Open Source Security Compliance Solution	`STARS 1.1K`
ThreatMapper	https://github.com/deepfence/ThreatMapper	ThreatMapper hunts for vulnerabilities in your production platforms, and ranks these vulnerabilities based on their risk-of-exploit.	`STARS 3.3K`

Kubernetes

Name	URL	Description	Meta
KubiScan	https://github.com/cyberark/KubiScan	A tool for scanning Kubernetes cluster for risky permissions	`STARS 1.1K`
Kubeaudit	https://github.com/Shopify/kubeaudit	Audit Kubernetes clusters for various different security concerns	`STARS 1.6K`
Kubescape	https://github.com/armosec/kubescape	The first open-source tool for testing if Kubernetes is deployed according to the NSA-CISA and the MITRE ATT&CK®.	`STARS 8.1K`
kubesec	https://github.com/controlplaneio/kubesec	Security risk analysis for Kubernetes resources	`STARS 917`
kube-bench	https://github.com/aquasecurity/kube-bench	Kubernetes benchmarking tool	`STARS 5.7K`
kube-score	https://github.com/zegl/kube-score	Static code analysis of your Kubernetes object definitions	`STARS 2.2K`
kube-hunter	https://github.com/aquasecurity/kube-hunter	Active scanner for k8s (purple)	`STARS 4.2K`
Calico	https://github.com/projectcalico/calico	Calico is an open source networking and network security solution for containers	`STARS 4.4K`
Krane	https://github.com/appvia/krane	Simple Kubernetes RBAC static analysis tool	`STARS 579`

Name	URL	Description	Meta
Starboard	https://github.com/aquasecurity/starboard	Starboard inegrates security tools by outputs into Kubernetes CRDs	STARS 1.3K
Gatekeeper	https://github.com/open-policy-agent/gatekeeper	Open policy agent gatekeeper for k8s	STARS 3K
Inspektor-gadget	https://github.com/kinvolk/inspektor-gadget	Collection of tools (or gadgets) to debug and inspect k8s	STARS 1.3K
kube-linter	https://github.com/stackrox/kube-linter	Static analysis for Kubernetes	STARS 2.2K
mizu-api-traffic-viewer	https://github.com/up9inc/mizu	A simple-yet-powerful API traffic viewer for Kubernetes enabling you to view all API communication between microservices to help your debug and troubleshoot regressions.	stars 8.5k
HelmSnyk	https://github.com/snyk-labs/helm-snyk	The Helm plugin for Snyk provides a subcommand for testing the images.	stars 37
Kubewarden	https://github.com/orgs/kubewarden/repositories	Policy as code for kubernetes from SUSE.	stars 57
Kubernetes-sigs BOM	https://github.com/kubernetes-sigs/bom	Kubernetes BOM generator	stars 211
Capsule	https://github.com/clastix/capsule	A multi-tenancy and policy-based framework for Kubernetes	stars 1.1k
Badrobot	https://github.com/controlplaneio/badrobot	Badrobot is a Kubernetes Operator audit tool	stars 191
Istio	https://istio.io	Istio is a service mesh based on Envoy. Engage encryption, role-based access, and authentication across services.	

Containers

Name	URL	Description	Meta
Harbor	https://github.com/goharbor/harbor	Trusted cloud native registry project	STARS 20K
Anchore	https://github.com/anchore/anchore-engine	Centralized service for inspection, analysis, and certification of container images	STARS 1.5K
Clair	https://github.com/quay/clair	Docker vulnerability scanner	STARS 20K
Deepfence ThreatMapper	https://github.com/deepfence/ThreatMapper	Apache v2, powerful runtime vulnerability scanner for kubernetes, virtual machines and serverless.	STARS 3.3K
Docker bench	https://github.com/docker/docker-bench-security	Docker benchmarking against CIS	STARS 20K
Falco	https://github.com/falcosecurity/falco	Container runtime protection	STARS 5.7K
Trivy	https://github.com/aquasecurity/trivy	Comprehensive scanner for vulnerabilities in container images	STARS 17K
Notary	https://github.com/notaryproject/notary	Docker signing	STARS 3K
Cosign	https://github.com/sigstore/cosign	Container signing	STARS 3.2K
watchtower	https://github.com/containrrr/watchtower	Updates the running version of your containerized app	STARS 13K
Grype	https://github.com/anchore/grype	Vulnerability scanner for container images (and also filesystems).	STARS 5.4K

Multi-Cloud

Name	URL	Description	Meta
Cloudsploit	https://github.com/aquasecurity/cloudsploit	Detection of security risks in cloud infrastructure	STARS 2.5K
ScoutSuite	https://github.com/nccgroup/ScoutSuite	NCCgroup mutlicloud scanning tool	STARS 5.2K
CloudCustodian	https://github.com/cloud-custodian/cloud-custodian/	Multicloud security analysis framework	STARS 4.7K

Name	URL	Description	Meta
CloudGraph	https://github.com/cloudgraphdev/cli	GraphQL API + Security for AWS, Azure, GCP, and K8s	`STARS 820`

AWS

AWS specific DevSecOps tooling. Tools here cover different areas like inventory management, misconfiguration scanning or IAM roles and policies review.

Name	URL	Description	Meta
Dragoneye	https://github.com/indeni/dragoneye	Dragoneye Indeni AWS scanner	`STARS 29`
Prowler	https://github.com/toniblyx/prowler	Prowler is a command line tool that helps with AWS security assessment, auditing, hardening and incident response.	`STARS 7.9K`
aws-inventory	https://github.com/nccgroup/aws-inventory	Helps to discover all AWS resources created in an account	`STARS 660`
PacBot	https://github.com/tmobile/pacbot	Policy as Code Bot (PacBot)	`STARS 1.2K`
Komiser	https://github.com/mlabouardy/komiser	Monitoring dashboard for costs and security	`STARS 3.1K`
Cloudsplaining	https://github.com/salesforce/cloudsplaining	IAM analysis framework	`STARS 1.7K`
ElectricEye	https://github.com/jonrau1/ElectricEye	Continuously monitor your AWS services for configurations	`STARS 727`
Cloudmapper	https://github.com/duo-labs/cloudmapper	CloudMapper helps you analyze your Amazon Web Services (AWS) environments	`STARS 5.4K`
cartography	https://github.com/lyft/cartography	Consolidates AWS infrastructure assets and the relationships between them in an intuitive graph	`STARS 2.6K`
policy_sentry	https://github.com/salesforce/policy_sentry	IAM Least Privilege Policy Generator	`STARS 1.8K`
AirIAM	https://github.com/bridgecrewio/AirIAM	IAM Least Privilege anmalyzer and Terraformer	`STARS 688`

Name	URL	Description	Meta
StreamAlert	https://github.com/airbnb/streamalert	AirBnB serverless, real-time data analysis framework which empowers you to ingest, analyze, and alert	STARS 2.8K
CloudQuery	https://github.com/cloudquery/cloudquery/	AirBnB serverless, real-time data analysis framework which empowers you to ingest, analyze, and alert	STARS 4.1K
S3Scanner	https://github.com/sa7mon/S3Scanner/	A tool to find open S3 buckets and dump their contents	STARS 2K
aws-iam-authenticator	https://github.com/kubernetes-sigs/aws-iam-authenticator/	A tool to use AWS IAM credentials to authenticate to a Kubernetes cluster	STARS 2K
kube2iam	https://github.com/jtblin/kube2iam/	A tool to use AWS IAM credentials to authenticate to a Kubernetes cluster	STARS 1.9K
AWS open source security samples	Official AWS opensource repo	Collection of official AWS open-source resources	AMAZON AWS
AWS Firewall factory	Globaldatanet FMS automation	Deploy, update, and stage your WAFs while managing them centrally via FMS	STARS 121
Parliment	Parliment	Parliament is an AWS IAM linting library	STARS 916
Yor	Yor	Adds informative and consistent tags across infrastructure-as-code frameworks such as Terraform, CloudFormation, and Serverless	STARS 634

Google cloud platform

GCP specific DevSecOps tooling. Tools here cover different areas like inventory management, misconfiguration scanning or IAM roles and policies review.

Name	URL	Description	Meta

Name	URL	Description	Meta
Forseti	https://github.com/forseti-security/forseti-security	Complex security orchestration and scanning platform	`STARS` `1.3K`

Policy as code

Policy as code is the idea of writing code in a high-level language to manage and automate policies. By representing policies as code in text files, proven software development best practices can be adopted such as version control, automated testing, and automated deployment. (Source: https://docs.hashicorp.com/sentinel/concepts/policy-as-code)

Name	URL	Description	Meta
Open Policy agent	https://github.com/open-policy-agent/opa	General-purpose policy engine that enables unified, context-aware policy enforcement across the entire stack	`STARS` `7.8K`
Kyverno	https://github.com/kyverno/kyverno	Kyverno is a policy engine designed for Kubernetes	`STARS` `3.6K`
Inspec	https://github.com/inspec/inspec	Chef InSpec is an open-source testing framework for infrastructure with a human- and machine-readable language for specifying compliance, security and policy requirements.	`STARS` `2.6K`
Cloud Formation guard	https://github.com/aws-cloudformation/cloudformation-guard	Cloud Formation policy as code	`STARS` `1.1K`
cnspec	https://github.com/mondoohq/cnspec	cnspec is a cloud-native and powerful Policy as Code engine to assess the security and compliance of your business-critical infrastructure. cnspec finds vulnerabilities and misconfigurations on all systems in your infrastructure including: public and private cloud environments, Kubernetes clusters, containers, container registries, servers and endpoints, SaaS products, infrastructure as code, APIs, and more.	`STARS` `124`

Chaos engineering

Chaos Engineering is the discipline of experimenting on a system in order to build confidence in the system's capability to withstand turbulent conditions in production.

Reading and manifestos: https://principlesofchaos.org/

Name	URL	Description	Meta
chaos-mesh	https://github.com/chaos-mesh/chaos-mesh	It is a cloud-native Chaos Engineering platform that orchestrates chaos on Kubernetes environments	`STARS` `5.6K`
Chaos monkey	https://netflix.github.io/chaosmonkey/	Chaos Monkey is responsible for randomly terminating instances in production to ensure that engineers implement their services to be resilient to instance failures.	`STARS` `13K`
Chaos Engine	https://thalesgroup.github.io/chaos-engine/	The Chaos Engine is a tool that is designed to intermittently destroy or degrade application resources running in cloud based infrastructure. These events are designed to occur while the appropriate resources are available to resolve the issue if the platform fails to do so on it's own.	`STARS` `60`
chaoskube	https://github.com/linki/chaoskube	Test how your system behaves under arbitrary pod failures.	`STARS` `1.6K`
Kube-Invaders	https://github.com/lucky-sideburn/KubeInvaders	Gamified chaos engineering tool for Kubernetes	`STARS` `875`
kube-monkey	https://github.com/asobti/kube-monkey	Gamified chaos engineering tool for Kubernetes	`STARS` `2.7K`
Litmus Chaos	https://litmuschaos.io/	Litmus is an end-to-end chaos engineering platform for cloud native infrastructure and applications. Litmus is designed to orchestrate and analyze chaos in their environments.	`STARS` `3.6K`
Gremlin	https://github.com/gremlin/gremlin-python	Chaos enginnering SaaS platform with free plan and some open source libraries	`STARS` `48`
AWS FIS samples	https://github.com/aws-samples/aws-fault-injection-simulator-samples	AWS Fault injection simulator samples	`STARS` `26`
CloudNuke	https://github.com/gruntwork-io/cloud-nuke	CLI tool to delete all resources in an AWS account	`STARS` `2.3K`

Infrastructure as code security

Scanning your infrastructure when it is only code helps shift-left the security. Many tools offer in IDE scanning and providing real-time advisory do Cloud engineers.

Name	URL	Description	Meta
KICS	https://github.com/Checkmarx/kics	Checkmarx security testing opensource for IaC	STARS 1.5k
Checkov	https://github.com/bridgecrewio/checkov	Checkov is a static code analysis tool for infrastructure-as-code	STARS 5.4K
tfsec	https://github.com/aquasecurity/tfsec	tfsec uses static analysis of your terraform templates to spot potential security issues. Now with terraform CDK support	STARS 5.7K
terrascan	https://github.com/accurics/terrascan	Terrascan is a static code analyzer for Infrastructure as Code	STARS 3.9K
cfsec	https://github.com/aquasecurity/cfsec	cfsec scans CloudFormation configuration files for security issues	STARS 57
cfn_nag	https://github.com/stelligent/cfn_nag	Looks for insecure patterns in CloudFormation	STARS 1.1K
Sysdig IaC scanner action	https://github.com/sysdiglabs/cloud-iac-scanner-action	Scans your repository with Sysdig IAC Scanner and report the vulnerabilities.	STARS 3

Orchestration

Event driven security help to drive, automate and execute tasks for security processes. The tools here and not dedicated security tools but are helping to automate and orchestrate security tasks or are part of most modern security automation frameworks or tools.

Name	URL	Description	Meta
StackStorm	https://github.com/StackStorm/st2	Platform for integration and automation across services and tools supporting event driven security	STARS 5.4K
Camunda	https://github.com/camunda/camunda-bpm-platform	Workflow and process automation	STARS 3.2K
DefectDojo	https://github.com/DefectDojo/django-DefectDojo	Security orchestration and vulnerability management platform	STARS 2.7K
Faraday	https://github.com/infobyte/faraday	Security suite for Security Orchestration, vulnerability management and centralized information	stars 3.8k

#TODO: REFACTOR UNDER THESE SECTIONS

Monitoring

Name	URL	Description	Meta