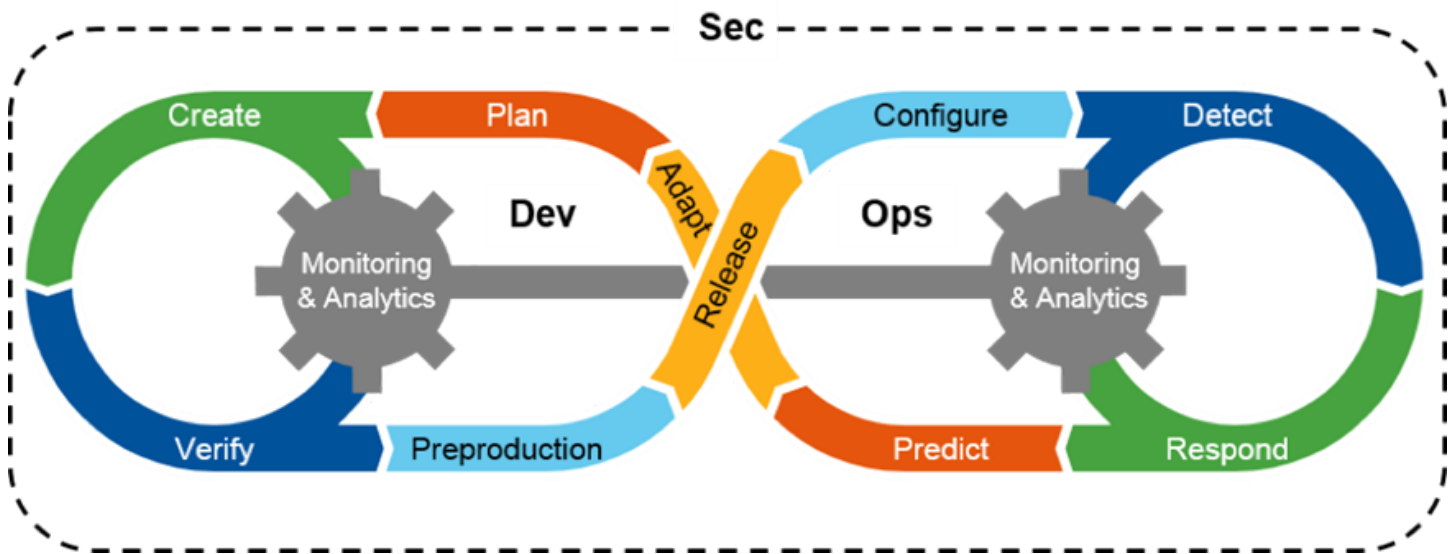


Ultimate DevSecOps library



This library contains list of tools and methodologies accompanied with resources. The main goal is to provide to the engineers a guide through opensource DevSecOps tooling. This repository covers only cyber security in the cloud and the DevSecOps scope.

Table of Contents

- [Definition](#)
- [Tooling](#)
- [Precommit and threat modeling](#)
- [SAST](#)
- [DAST](#)
- [Orchestration](#)
- [Supply chain and dependencies](#)
- [Infrastructure as code](#)
- [Containers security](#)
- [Kubernetes](#)
- [Cloud](#)
- [Chaos engineering](#)
- [Policy as code](#)
- [Methodologies](#)
- [Other](#)
- [License](#)

What is DevSecOps

DevSecOps focuses on security automation, testing and enforcement during DevOps - Release - SDLC cycles. The whole meaning behind this methodology is connecting together Development, Security and Operations. DevSecOps is methodology providing different methods, techniques and processes backed mainly with tooling focusing on developer / security experience.

DevSecOps takes care that security is part of every stage of DevOps loop - Plan, Code, Build, Test, Release, Deploy, Operate, Monitor.

Various definitions:




- <https://www.redhat.com/en/topics/devops/what-is-devsecops>
- <https://www.ibm.com/cloud/learn/devsecops>
- <https://snyk.io/series/devsecops/>
- <https://www.synopsys.com/glossary/what-is-devsecops.html>
- <https://spacelift.io/blog/what-is-devsecops>










Tooling











Pre-commit time tools

In this section you can find lifecycle helpers, precommit hook tools and threat modeling tools. Threat modeling tools are specific category by themselves allowing you to simulate and discover potential gaps before you start to develop the software or during the process.

Modern DevSecOps tools allow using Threat modeling as code or generation of threat models based on the existing code annotations.







| Name | URL | Description | Meta |
|-------------|---|--|--|
| git-secrets | https://github.com/awslabs/git-secrets | AWS labs tool preventing you from committing secrets to a git repository |  12K |
| git-hound | https://github.com/tillson/git-hound | Searchers secrets in git |  1.1K |
| goSDL | https://github.com/slackhq/goSDL | Security Development Lifecycle checklist |  513 |


| Name | URL | Description | Meta |
|--------------------------------|---|--|--|
| ThreatPlaybook | https://github.com/we45/ThreatPlaybook | Threat modeling as code |  STARS 265 |
| Threat Dragon | https://github.com/OWASP/threat-dragon | OWASP Threat modeling tool |  STARS 745 |
| threatspec | https://github.com/threatspec/threatspec | Threat modeling as code |  STARS 297 |
| pytm | https://github.com/izar/pytm | A Pythonic framework for threat modeling |  STARS 608 |
| Threagile | https://github.com/Threagile/threagile | A Go framework for threat modeling |  STARS 530 |
| MAL-lang | https://mal-lang.org/#what | A language to create cyber threat modeling systems for specific domains |  STARS 22 |
| Microsoft Threat modeling tool | https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool | Microsoft threat modeling tool |  STARS 163 |
| Talisman | https://github.com/thoughtworks/talisman | A tool to detect and prevent secrets from getting checked in |  STARS 1.9K |
| 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 108 |

| Name | URL | Description | Meta |
|-----------------------|---|---|---|
| Sonarlint | https://github.com/SonarSource/sonarlint-core | Sonar linting utility for IDE |  STARS  |
| DevSkim | https://github.com/microsoft/DevSkim | DevSkim is a framework of IDE extensions and language analyzers that provide inline security analysis |  STARS  |
| detect-secrets | https://github.com/Yelp/detect-secrets | Detects secrets in your codebase |  STARS  |
| tflint | https://github.com/terraform-linters/tflint | A Pluggable Terraform Linter |  STARS  |
| Steampipe Code Plugin | https://github.com/turbot/steampipe-plugin-code | Use SQL to detect secrets from source code and data sources. |  Stars  |

Secrets management





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  |
| 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  |
| TruffleHog | https://github.com/trufflesecurity/truffleHog | TruffleHog is a scanning tool for detecting |  STARS  |

| Name | URL | Description | Meta |
|-------------------------------|---|---|--|
| | | hardcoded secrets | |
| Hashicorp Vault | https://github.com/hashicorp/vault | Hashicorp Vault secrets management |  STARS 29K |
| Mozilla SOPS | https://github.com/mozilla/sops | Mozilla Secrets Operations |  STARS 15K |
| AWS secrets manager GH action | https://github.com/marketplace/actions/aws-secrets-manager-actions | AWS secrets manager docs |  STARS 6.2 |
| GitRob | https://github.com/michenriksen/gitrob | Gitrob is a tool to help find potentially sensitive files pushed to public repositories on Github |  STARS 5.8K |
| git-wild-hunt | https://github.com/d1vious/git-wild-hunt | A tool to hunt for credentials in the GitHub |  STARS 38K |
| 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 8K |
| Knox | https://github.com/pinterest/knox | Knox is a service for storing and rotation of secrets, keys, and passwords used by other services |  STARS 1.2K |
| Chef vault | https://github.com/chef/chef-vault | allows you to encrypt a Chef Data Bag Item |  STARS 407 |
| Ansible vault | Ansible vault docs | Encryption/decryption utility for Ansible data files |  STARS 32K |

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 | Met |
|-------------------------|---|---|---|
| CycloneDX | https://github.com/orgs/CycloneDX/repositories | CycloneDX format for SBOM |  |
| cdxgen | https://github.com/AppThreat/cdxgen | Generates CycloneDX SBOM , supports many languages and package managers. |  |
| SPDX | https://github.com/spdx/spdx-spec | SPDX format for SBOM - Software Package Data Exchange |  |
| Snyk | https://github.com/snyk/snyk | Snyk scans and monitors your projects for security vulnerabilities |  |
| vulncost | https://github.com/snyk/vulncost | Security Scanner for VS Code |  |
| Dependency Combobulator | https://github.com/apiiro/combobulator | Dependency-related attacks detection and prevention through heuristics and insight engine (support multiple |  |






| Name | URL | Description | Met |
|----------------------|---|--|---|
| | | dependency schemes) | |
| DependencyTrack | https://github.com/DependencyTrack/dependency-track | Dependency security tracking platform |  |
| DependencyCheck | https://github.com/jeremylong/DependencyCheck | Simple dependency security scanner good for CI |  |
| Retire.js | https://github.com/retirejs/retire.js/ | Helps developers to detect the use of JS-library versions with known vulnerabilities |  |
| PHP security checker | https://github.com/fabpot/local-php-security-checker | Check vulnerabilities in PHP dependencies |  |
| bundler-audit | https://github.com/rubysec/bundler-audit | Patch-level verification for bundler |  |
| 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 |  |

| Name | URL | Description | Met |
|---------------------|---|---|---|
| Renovatebot | https://github.com/renovatebot/renovate | Automated dependency updates, patches multi-platform and multi-language |  |
| npm-check | https://www.npmjs.com/package/npm-check | Check for outdated, incorrect, and unused dependencies. |  |
| 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. |  |
| Syft | https://github.com/anchore/syft | CLI tool and library for generating an SBOM from container images (and filesystems) |  |

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 229 |
| 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 174 |
| SLSA | Official GitHub link | Supply-chain Levels for Software Artifacts |  STARS 1.4K |
| kritis | https://github.com/grafeas/kritis | Solution for securing your software supply chain for Kubernetes apps |  STARS 684 |
| ratify | https://github.com/deislabs/ratify | Artifact Ratification Framework |  STARS 168 |

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 6.8K |
| Semgrep | https://semgrep.dev/ | Hi-Quality Open source, works on 17+ languages |  STARS 9.3K |
| Bandit | https://github.com/PyCQA/bandit | Python specific SAST tool |  STARS 5.8K |

| Name | URL | Description | Meta |
|---------------------|---|--|-------------|
| libsast | https://github.com/ajinabraham/libsast | Generic SAST for Security Engineers. Powered by regex based pattern matcher and semantic aware semgrep | STARS 11.2K |
| ESLint | https://eslint.org/ | Find and fix problems in your JavaScript code | |
| nodejsscan | https://github.com/ajinabraham/nodejsscan | NodeJs SAST scanner with GUI | STARS 2.3K |
| FindSecurityBugs | https://find-sec-bugs.github.io/ | The SpotBugs plugin for security audits of Java web applications | STARS 2.2K |
| SonarQube community | https://github.com/SonarSource/sonarqube | Detect security issues in code review with Static Application Security Testing (SAST) | STARS 8.4K |
| gosec | https://github.com/securego/gosec | Inspects source code for security problems by scanning the Go AST. | STARS 7.3K |
| Safety | https://github.com/pyupio/safety | Checks Python dependencies for known security vulnerabilities . | STARS 1.6K |

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 12K |
| Wapiti | https://github.com/wapiti-scanner/wapiti | Light pipeline ready scanning tool |  STARS 906 |
| Nuclei | https://github.com/projectdiscovery/nuclei | Template based security scanning tool |  STARS 16K |
| purpleteam | https://github.com/purpleteam-labs/purpleteam | CLI DAST tool incubator project |  STARS 109 |
| oss-fuzz | https://github.com/google/oss-fuzz | OSS-Fuzz: Continuous Fuzzing for Open Source Software |  STARS 9.4K |
| nikto | https://github.com/sullo/nikto | Nikto web server scanner |  STARS 7.5K |
| skipfish | https://code.google.com/archive/p/skipfish/ | Skipfish is an active web application security reconnaissance tool |  STARS 639 |





Continuous deployment security



















| Name | URL | Description | Meta |
|---------------|---|--|--|
| SecureCodeBox | https://github.com/secureCodeBox/secureCodeBox | Toolchain for continuous scanning of applications and infrastructure |  STARS 668 |



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

Kubernetes





| Name | URL | Description | Meta |
|-----------|---|---|---|
| KubiScan | https://github.com/cyberark/KubiScan | A tool for scanning Kubernetes cluster for risky permissions |  |
| Kubeaudit | https://github.com/Shopify/kubeaudit | Audit Kubernetes clusters for various different security concerns |  |
| 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®. |  |








| Name | URL | Description | Meta |
|------------------|---|--|--|
| kubesecc | https://github.com/controlplaneio/kubesecc | Security risk analysis for Kubernetes resources |  STARS 1.1K |
| kube-bench | https://github.com/aquasecurity/kube-bench | Kubernetes benchmarking tool |  STARS 6.5K |
| kube-score | https://github.com/zegl/kube-score | Static code analysis of your Kubernetes object definitions |  STARS 2.5K |
| kube-hunter | https://github.com/aquasecurity/kube-hunter | Active scanner for k8s (purple) |  STARS 4.5K |
| Calico | https://github.com/projectcalico/calico | Calico is an open source networking and network security solution for containers |  STARS 5.3K |
| Krane | https://github.com/appvia/krane | Simple Kubernetes RBAC static analysis tool |  STARS 648 |
| Starboard | https://github.com/aquasecurity/starboard | Starboard integrates 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 3.4K |
| Inspektor-gadget | https://github.com/kinvolk/inspektor-gadget | Collection of tools (or gadgets) to debug and inspect k8s |  STARS 1.7K |

| Name | URL | Description | Meta |
|-------------------------|---|---|---|
| kube-linter | https://github.com/stackrox/kube-linter | Static analysis for Kubernetes |  STARS  |
| 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  |
| HelmSnyk | https://github.com/snyk-labs/helm-snyk | The Helm plugin for Snyk provides a subcommand for testing the images. |  Stars  |
| Kubewarden | https://github.com/orgs/kubewarden/repositories | Policy as code for kubernetes from SUSE. |  Stars  |
| Kubernetes-sigs BOM | https://github.com/kubernetes-sigs/bom | Kubernetes BOM generator |  Stars  |
| Capsule | https://github.com/clastix/capsule | A multi-tenancy and policy-based framework for Kubernetes |  Stars  |
| Badrobot | https://github.com/controlplaneio/badrobot | Badrobot is a Kubernetes Operator audit tool |  Stars  |
| kube-scan | https://github.com/octarinesec/kube-scan | k8s cluster risk assessment tool |  STARS  |
| Istio | https://istio.io | Istio is a service mesh based on Envoy. Engage |  Stars  |




| Name | URL | Description | Meta |
|-----------------------|---|---|--|
| | | encryption, role-based access, and authentication across services. | |
| Kubernetes Insights | https://github.com/turbot/steampipe-mod-kubernetes-insights | Visualize Kubernetes inventory and permissions through relationship graphs. |  Stars 24 |
| Kubernetes Compliance | https://github.com/turbot/steampipe-mod-kubernetes-compliance | Check compliance of Kubernetes configurations to security best practices. |  Stars 30 |



Containers

| Name | URL | Description | Meta |
|------------------------|---|---|--|
| Harbor | https://github.com/goharbor/harbor | Trusted cloud native registry project |  STARS 22K |
| Anchore | https://github.com/anchore/anchore-engine | Centralized service for inspection, analysis, and certification of container images |  STARS 1.6K |
| Clair | https://github.com/quay/clair | Docker vulnerability scanner |  STARS 22K |
| Deepfence ThreatMapper | https://github.com/deepfence/ThreatMapper | Apache v2, powerful runtime vulnerability scanner for kubernetes, virtual |  STARS 4.5K |

| Name | URL | Description | Meta |
|--------------|---|--|---|
| | | machines and serverless. | |
| Docker bench | https://github.com/docker/docker-bench-security | Docker benchmarking against CIS |  STARS 22K |
| Falco | https://github.com/falcosecurity/falco | Container runtime protection |  STARS 6.6K |
| Trivy | https://github.com/aquasecurity/trivy | Comprehensive scanner for vulnerabilities in container images |  STARS 20K |
| Notary | https://github.com/notaryproject/notary | Docker signing |  STARS 3.1K |
| Cosign | https://github.com/sigstore/cosign | Container signing |  STARS 3.9K |
| watchtower | https://github.com/containrrr/watchtower | Updates the running version of your containerized app |  STARS 16K |
| Grype | https://github.com/anchore/grype | Vulnerability scanner for container images (and also filesystems). |  STARS 7.1K |






Multi-Cloud

| Name | URL | Description | Meta |
|----------------|---|---|---|
| Cloudsploit | https://github.com/aquasecurity/cloudsploit | Detection of security risks in cloud infrastructure |  STARS 3K |
| ScoutSuite | https://github.com/nccgroup/ScoutSuite | NCCgroup mutlicloud scanning tool |  STARS 6K |
| CloudCustodian | https://github.com/cloud-custodian/cloud-custodian/ | Multicloud security analysis framework |  STARS 5.1K |









| Name | URL | Description | Meta |
|------------|---|--|---|
| CloudGraph | https://github.com/cloudgraphdev/cli | GraphQL API + Security for AWS, Azure, GCP, and K8s |  STARS 861 |
| Steampipe | https://github.com/turbot/steampipe | Instantly query your cloud, code, logs & more with SQL. Build on thousands of open-source benchmarks & dashboards for security & insights. |  Stars 6.1k |

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 REPO NOT FOUND |
| Prowler | https://github.com/toniblyx/prowler | Prowler is a command line tool that helps with AWS security assessment, auditing, hardening and incident response. |  STARS 9.1K |
| aws-inventory | https://github.com/nccgroup/aws-inventory | Helps to discover all AWS resources created in an account |  STARS 689 |
| PacBot | https://github.com/tmobile/pacbot | Policy as Code Bot (PacBot) |  STARS 1.3K |
| Komiser | https://github.com/mlabouardy/komiser | Monitoring dashboard for |  STARS 3.9K |




| Name | URL | Description | Meta |
|----------------|---|---|---|
| | | costs and security | |
| Cloudsplaining | https://github.com/salesforce/cloudsplaining | IAM analysis framework |  STARS 1.9K |
| ElectricEye | https://github.com/jonrau1/ElectricEye | Continuously monitor your AWS services for configurations |  STARS 830 |
| Cloudmapper | https://github.com/duo-labs/cloudmapper | CloudMapper helps you analyze your Amazon Web Services (AWS) environments |  STARS 5.8K |
| cartography | https://github.com/lyft/cartography | Consolidates AWS infrastructure assets and the relationships between them in an intuitive graph |  STARS 2.8K |
| policy_sentry | https://github.com/salesforce/policy_sentry | IAM Least Privilege Policy Generator |  STARS 1.9K |
| AirIAM | https://github.com/bridgecrewio/AirIAM | IAM Least Privilege analyzer and Terraformer |  STARS 747 |
| StreamAlert | https://github.com/airbnb/streamalert | AirBnB serverless, real-time data analysis framework which empowers you to ingest, analyze, and alert |  STARS 2.9K |
| CloudQuery | https://github.com/cloudquery/cloudquery/ | AirBnB serverless, real-time data analysis framework which empowers you to ingest, analyze, and alert |  STARS 5.4K |
| S3Scanner | https://github.com/sa7mon/S3Scanner/ | A tool to find open S3 buckets and |  STARS 2.3K |

| Name | URL | Description | Meta |
|----------------------------------|---|---|--|
| | | dump their contents | |
| 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 2.1K |
| 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 205 |
| Parliment | Parliment | Parliament is an AWS IAM linting library |  STARS 972 |
| Yor | Yor | Adds informative and consistent tags across infrastructure-as-code frameworks such as Terraform, CloudFormation, and Serverless |  STARS 748 |
| AWS Insights | https://github.com/turbot/steampipe-mod-aws-insights | Visualize AWS inventory and permissions through relationship graphs. |  Stars 84 |
| AWS Compliance | https://github.com/turbot/steampipe-mod-aws-compliance | Check compliance of AWS |  Stars 334 |

| Name | URL | Description | Meta |
|------|-----|--|------|
| | | configurations to security best practices. | |



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 |
|----------------|---|--|--|
| Forseti | https://github.com/forseti-security/forseti-security | Complex security orchestration and scanning platform |  1.3K |
| GCP Insights | https://github.com/turbot/steampipe-mod-gcp-insights | Visualize GCP inventory and permissions through relationship graphs. |  8 |
| GCP Compliance | https://github.com/turbot/steampipe-mod-gcp-compliance | Check compliance of GCP configurations to security best practices. |  28 |

Microsoft Azure

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

| Name | URL | Description | Meta |
|------------------|---|--|--|
| Azure Insights | https://github.com/turbot/steampipe-mod-azure-insights | Visualize Azure inventory and permissions through relationship graphs. |  8 |
| Azure Compliance | https://github.com/turbot/steampipe-mod-azure-compliance | Check compliance of Azure configurations to security best practices. |  49 |

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 5.9K |
| Kyverno | https://github.com/kyverno/kyverno | Kyverno is a policy engine designed for Kubernetes |  STARS 4.8K |
| 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 2.8K |
| Cloud Formation guard | https://github.com/aws-cloudformation/cloudformation-guard | Cloud Formation policy as code |  STARS 1.2K |
| 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 221 |

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 6.2K |
| 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 1.4K |
| 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 66 |
| chaoskube | https://github.com/linki/chaoskube | Test how your system behaves under arbitrary pod failures. |  STARS 1.7K |
| Kube-Invaders | https://github.com/lucky-sideburn/KubeInvaders | Gamified chaos engineering tool for Kubernetes |  STARS 950 |
| kube-monkey | https://github.com/asobti/kube-monkey | Gamified chaos engineering tool for Kubernetes |  STARS 2.9K |

| Name | URL | Description | Meta |
|-----------------|---|---|---------------------------|
| 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. | <small>STARS</small> 4.1K |
| Gremlin | https://github.com/gremlin/gremlin-python | Chaos engineering SaaS platform with free plan and some open source libraries | <small>STARS</small> 55 |
| AWS FIS samples | https://github.com/aws-samples/aws-fault-injection-simulator-samples | AWS Fault injection simulator samples | <small>STARS</small> 31 |
| CloudNuke | https://github.com/gruntwork-io/cloud-nuke | CLI tool to delete all resources in an AWS account | <small>STARS</small> 2.6K |

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 | <small>STARS</small> 1.8K |
| Checkov | https://github.com/bridgecrewio/checkov | Checkov is a static code analysis tool for infrastructure-as-code | <small>STARS</small> 6.3K |
| tfsec | https://github.com/aquasecurity/tfsec | tfsec uses static analysis of your terraform templates to spot potential security issues. Now with terraform CDK support | <small>STARS</small> 6.4K |
| terrascan | https://github.com/accurics/terrascan | Terrascan is a static code analyzer for | <small>STARS</small> 4.4K |

| Name | URL | Description | Meta |
|--------------------------------|---|--|---|
| | | Infrastructure as Code | |
| cfsec | https://github.com/aquasecurity/cfsec | cfsec scans CloudFormation configuration files for security issues |  STARS 59 |
| cfn_nag | https://github.com/stelligent/cfn_nag | Looks for insecure patterns in CloudFormation |  STARS 1.2K |
| Sysdig IaC scanner action | https://github.com/sysdiglabs/cloud-iac-scanner-action | Scans your repository with Sysdig IAC Scanner and report the vulnerabilities. |  STARS 4 |
| Terraform Compliance for AWS | https://github.com/turbot/steampipe-mod-terraform-aws-compliance | Check compliance of Terraform configurations to AWS security best practices. |  Stars 23 |
| Terraform Compliance for Azure | https://github.com/turbot/steampipe-mod-terraform-azure-compliance | Check compliance of Terraform configurations to Azure security best practices. |  Stars 6 |
| Terraform Compliance for GCP | https://github.com/turbot/steampipe-mod-terraform-gcp-compliance | Check compliance of Terraform configurations to GCP security best practices. |  Stars 2 |
| Terraform Compliance for OCI | https://github.com/turbot/steampipe-mod-terraform-oci-compliance | Check compliance of Terraform configurations to OCI security best practices. |  Stars 2 |

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 5.8K |
| Camunda | https://github.com/camunda/camunda-bpm-platform | Workflow and process automation |  STARS 3.7K |
| DefectDojo | https://github.com/DefectDojo/django-DefectDojo | Security orchestration and vulnerability management platform |  STARS 3.3K |
| Faraday | https://github.com/infobyte/faraday | Security suite for Security Orchestration, vulnerability management and centralized information |  Stars 4.4k |

Methodologies, whitepapers and architecture

List of resources worth investigating:

- https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf
- <https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsStrategyGuide.pdf>
- <https://csrc.nist.gov/publications/detail/sp/800-204c/draft>
- <https://owasp.org/www-project-devsecops-maturity-model/>
- <https://www.sans.org/posters/cloud-security-devsecops-best-practices/>

AWS DevOps whitepapers:

- <https://d1.awsstatic.com/whitepapers/aws-development-test-environments.pdf>
- https://d1.awsstatic.com/whitepapers/AWS_DevOps.pdf
- https://d1.awsstatic.com/whitepapers/AWS_Blue_Green_Deployments.pdf
- <https://d1.awsstatic.com/whitepapers/DevOps/import-windows-server-to-amazon-ec2.pdf>
- https://d1.awsstatic.com/whitepapers/DevOps/Jenkins_on_AWS.pdf
- <https://d1.awsstatic.com/whitepapers/DevOps/practicing-continuous-integration-continuous-delivery-on-AWS.pdf>
- <https://d1.awsstatic.com/whitepapers/DevOps/infrastructure-as-code.pdf>

- <https://d1.awsstatic.com/whitepapers/microservices-on-aws.pdf>
- <https://d1.awsstatic.com/whitepapers/DevOps/running-containerized-microservices-on-aws.pdf>
- <https://d1.awsstatic.com/Marketplace/solutions-center/downloads/AppSec-DevSecOps-AWS-SANS-eBook.pdf> (AWS + SANS whitepaper)

AWS blog:

- <https://aws.amazon.com/blogs/devops/building-end-to-end-aws-devsecops-ci-cd-pipeline-with-open-source-sca-sast-and-dast-tools/>
- <https://aws.amazon.com/blogs/devops/building-an-end-to-end-kubernetes-based-devsecops-software-factory-on-aws/>

Microsoft whitepapers:


- https://azure.microsoft.com/mediahandler/files/resourcefiles/6-tips-to-integrate-security-into-your-devops-practices/DevSecOps_Report_Tips_D6_fm.pdf
- <https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/devsecops-in-azure>
- <https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/devsecops-in-github>



GCP whitepapers:

- <https://cloud.google.com/architecture/devops/devops-tech-shifting-left-on-security>
- <https://cloud.google.com/security/overview/whitepaper>
- https://services.google.com/fh/files/misc/security_whitepapers_march2018.pdf
- <https://cloud.google.com/security/encryption-in-transit/application-layer-transport-security>
- <https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf>

Other

Here are the other links and resources that do not fit in any previous category. They can meet multiple categories in time or help you in your learning.

| Name | URL | Description | Meta |
|---------------------------------|---|---|---|
| Automated Security Helper (ASH) | https://github.com/aws-samples/automated-security-helper | ASH is a one stop shop for security scanners, and does not require any installation. It will identify the different frameworks, and download the relevant, up to date tools. ASH is running on isolated Docker containers, keeping the user environment clean, with a |  281 |

| Name | URL | Description | Meta |
|---------------------------|---|---|--|
| | | single aggregated report. The following frameworks are supported: Git, Python, Javascript, Cloudformation, Terraform and Jupyter Notebooks. | |
| Mobile security framework | https://github.com/MobSF/Mobile-Security-Framework-MobSF | SAST, DAST and pentesting tool for mobile apps |  STARS 14K |
| Legitify | https://github.com/Legit-Labs/legitify | Detect and remediate misconfigurations and security risks across all your GitHub and GitLab assets |  STARS 693 |

Training - <https://www.practical-devsecops.com/devsecops-university/>

DevSecOps videos - [Hackitect playground](#)

License

MIT license

Marek Šottl (c) 2022