












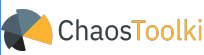














































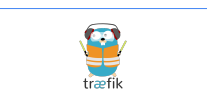






Name		Category	Description	Observations
Semgrep		SAST	Semgrep is a fast, open-source, static analysis tool for finding bugs and enforcing code standards at editor, commit, and CI time for many languages.	Semgrep analyzes code locally on your computer or in your build environment: code is never uploaded. Its rules look like the code you already write; no abstract syntax trees, regex wrestling, or painful DSLs. <a href="https://github.com/returntocorp/semgrep">https://github.com/returntocorp/semgrep</a>
AirIAM		IAM	AirIAM is an AWS IAM to least privilege Terraform execution framework. It compiles AWS IAM usage and leverages that data to create a least-privilege IAM Terraform that replaces the existing IAM management method.  AirIAM was created to promote immutable and version-controlled IAM management to replace today's manual and error prone methods.	<a href="https://github.com/bridgecrewio/AirIAM">https://github.com/bridgecrewio/AirIAM</a>
Amazon Firecracker		Sandboxing, Isolation	Firecracker is an open source virtualization technology that is purpose-built for creating and managing secure, multi-tenant container and function-based services that provide serverless operational models. Firecracker runs workloads in lightweight virtual machines, called microVMs, which combine the security and isolation properties provided by hardware virtualization technology with the speed and flexibility of containers.	<a href="https://firecracker-microvm.github.io">https://firecracker-microvm.github.io</a> <a href="https://github.com/firecracker-microvm/firecracker">https://github.com/firecracker-microvm/firecracker</a>
Anchore Grype		SAST	A vulnerability scanner for container images and filesystems. Easily install the binary to try it out. Works with Syft, the powerful SBOM (software bill of materials) tool for container images and filesystems.	<a href="https://github.com/anchore/grype">https://github.com/anchore/grype</a>
Anchore Syft		SCA	A CLI tool and go library for generating a Software Bill of Materials (SBOM) from container images and filesystems. Exceptional for vulnerability detection when used with a scanner tool like Grype.	* SBOM <a href="https://github.com/anchore/syft">https://github.com/anchore/syft</a>
Aporeto Trirame		Zero Trust Network	An open-source library curated by Aporeto to provide cryptographic isolation for cloud-native applications. Trirame-lib is a Zero-Trust networking library that makes it possible to setup security policies and segment applications by enforcing end-to-end authentication and authorization without the need for complex control planes or IP/port-centric ACLs and east-west firewalls. Trirame-lib supports both containers and Linux processes as well user-based activation, and it allows each application to enforce its own security policies.	* Uses the Zero-Trust Network approach to provide cryptographic isolation. * On November 2019 was acquired by Palo Alto Networks. <a href="https://github.com/aporeto-inc/trirame-lib">https://github.com/aporeto-inc/trirame-lib</a> <a href="https://www.aporeto.com/opensource">https://www.aporeto.com/opensource</a>
AppArmor		Linux Runtime Protection	AppArmor is an effective and easy-to-use Linux application security system. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing even unknown application flaws from being exploited. AppArmor security policies completely define what system resources individual applications can access, and with what privileges.	* Used with SELinux and Seccomp on Kubernetes to implement Security at Pod level ( <a href="https://kubernetes.io/docs/tasks/configure-pod-container/security-context">https://kubernetes.io/docs/tasks/configure-pod-container/security-context</a> ).  <a href="https://github.com/apparmor/apparmor/">https://github.com/apparmor/apparmor/</a> <a href="https://kubernetes.io/docs/tutorials/clusters/apparmor">https://kubernetes.io/docs/tutorials/clusters/apparmor</a> <a href="https://docs.docker.com/engine/security/apparmor">https://docs.docker.com/engine/security/apparmor</a>
AquaSec Kube-Bench		Security Audit	Checks whether Kubernetes is deployed according to security best practices as defined in the CIS Kubernetes Benchmark. Note that it is impossible to inspect the master nodes of managed clusters, e.g. GKE, EKS and AKS. It supports the tests for Kubernetes as defined in the CIS Benchmarks 1.3.0 to 1.5.0 respectively.	* CIS Benchmark <a href="https://github.com/aquasecurity/kube-bench">https://github.com/aquasecurity/kube-bench</a>
AquaSec Kuber-Hunter		DAST	It hunts for security weaknesses in Kubernetes clusters. The tool was developed to increase awareness and visibility for security issues in Kubernetes environments. Active hunting mode will exploit vulnerabilities it finds, in order to explore for further vulnerabilities. Normal hunting will never change state of the cluster, while Active hunting can potentially do state-changing operations on the cluster, which could be harmful.	<a href="https://github.com/aquasecurity/kube-hunter">https://github.com/aquasecurity/kube-hunter</a> <a href="https://aquasecurity.github.io/kube-hunter">https://aquasecurity.github.io/kube-hunter</a>
AquaSec Trivy		SAST	Trivy is a simple and comprehensive vulnerability scanner for containers, suitable for Continuous Integration (CI). Trivy detects vulnerabilities of OS packages (Alpine, RHEL, CentOS, etc.) and application dependencies (Bundler, Composer, npm, yarn etc.). Trivy is easy to use. Just install the binary and you're ready to scan. All you need to do for scanning is to specify an image name of the container.	* It is suitable for CI while others don't such as: Anchore Engine, Clair, etc. <a href="https://github.com/aquasecurity/trivy#comparison-with-other-scanners">https://github.com/aquasecurity/trivy#comparison-with-other-scanners</a> * SCA <a href="https://github.com/aquasecurity/trivy">https://github.com/aquasecurity/trivy</a>
Arachni		DAST	Arachni is a feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of modern web applications. The open-source security testing tool is capable of uncovering a number of vulnerabilities, including: Invalidated redirect, Local and remote file inclusion, SQL injection, XSS injection, etc.	<a href="https://www.arachni-scanner.com">https://www.arachni-scanner.com</a>
AWS CloudFormation Linter		SAST	Validate AWS CloudFormation yaml/json templates against the AWS CloudFormation Resource Specification and additional checks. Includes checking valid values for resource properties and best practices.	<a href="https://github.com/aws-cloudformation/cfn-lint">https://github.com/aws-cloudformation/cfn-lint</a>
Bandit (Python)		SAST	Bandit is a tool designed to find common security issues in Python code. To do this Bandit processes each file, builds an AST from it, and runs appropriate plugins against the AST nodes. Once Bandit has finished scanning all the files it generates a report.  Bandit was originally developed within the OpenStack Security Project and later rehomed to PyCQA.	<a href="https://github.com/PyCQA/bandit">https://github.com/PyCQA/bandit</a>
Caddy Server		LB, Proxy, Ingress, Gateway	Caddy simplifies your infrastructure. It takes care of TLS certificate renewals, OCSP stapling, static file serving, reverse proxying, Kubernetes ingress, and more. Caddy runs great in containers because it has no dependencies—not even libc. Run Caddy practically anywhere.	<a href="https://caddyserver.com">https://caddyserver.com</a> <a href="https://github.com/caddyserver/caddy">https://github.com/caddyserver/caddy</a>
Capsule8 Sensor		HIDS, RASP	The Capsule8 Sensor, which is based on KProbes, performs advanced behavioral monitoring (in real-time) for cloud-native, containers, and traditional Linux-based servers. It is intended to be run on a Linux host persistently and ideally before the host begins running application workloads. It is designed to support API clients subscribing and unsubscribing from telemetry dynamically to implement various security incident detection strategies.	* It is a sensor and requires be integrated with existing tool (log aggregation, ingestion, persistency, alerting, correlation, etc.) to work as Host Intrusion Detection System (HIDS)  <a href="https://github.com/capsule8/capsule8">https://github.com/capsule8/capsule8</a>
Chaos Toolkit		Resilience	The Chaos Toolkit is an open-source and extensible tool that is written in Python. It uses platform-specific drivers to connect to your Kubernetes cluster and execute Chaos Experiments. Every experiment performed by Chaos Toolkit is written in JSON using a robust API. Experiments are made up of a few key elements that are executed sequentially and allow the experiment to bail out if any step in the process fails.	<a href="https://chaostoolkit.org">https://chaostoolkit.org</a>
Checkmarx KICS		SAST	Find security vulnerabilities, compliance issues, and infrastructure misconfigurations early in the development cycle of your infrastructure-as-code with KICS by Checkmarx.  KICS stands for Keeping Infrastructure as Code Secure, it is open source and is a must-have for any cloud native project.	IaC supported: Terraform (.tf, tfvars), CloudFormation (.json or .yaml), Ansible (.yaml), Dockerfile, K8s manifests, OpenAPI (.json or .yaml).  <a href="https://github.com/Checkmarx/kics">https://github.com/Checkmarx/kics</a>
Checkov		SAST	Checkov is a static code analysis tool for infrastructure-as-code.  It scans cloud infrastructure provisioned using Terraform, Terraform plan, Cloudformation, Kubernetes, Dockerfile, Serverless or ARM Templates and detects security and compliance misconfigurations using graph-based scanning.	<a href="https://github.com/bridgecrewio/checkov">https://github.com/bridgecrewio/checkov</a>
Cilium		Network Security	Cilium is an API-aware Networking and Security tool that uses eBPF and XDP. It secures transparently the network connectivity between application services deployed using Linux container management platforms like Docker and Kubernetes. Cilium works at Layer 3/4 to provide traditional networking and security services as well as Layer 7 to protect and secure use of modern application protocols such as HTTP, gRPC and Kafka.	* Implements Kubernetes SDN/CNI.  <a href="https://cilium.io">https://cilium.io</a> <a href="https://github.com/cilium/cilium">https://github.com/cilium/cilium</a> <a href="https://cilium.readthedocs.io/en/stable">https://cilium.readthedocs.io/en/stable</a>
Clair		SAST	Clair is an open source project for the static analysis of vulnerabilities in application containers (currently including AppC and Docker). Vulnerability data is continuously imported from a known set of sources (e.g. CVE) and correlated with the indexed contents of container images in order to produce lists of vulnerabilities that threaten a container.	* It is frequently used with Clair-Local-Scan ( <a href="https://github.com/arminc/clair-local-scan">https://github.com/arminc/clair-local-scan</a> ) and Clair-Scanner ( <a href="https://github.com/arminc/clair-scanner">https://github.com/arminc/clair-scanner</a> ) to perform scanning during CI/CD on premise (local).  <a href="https://github.com/quay/clair">https://github.com/quay/clair</a>

Cloudflare CFSSL		PKI	CFSSL is CloudFlare's PKI/TLS swiss army knife. It is both a command line tool and an HTTP API server for signing, verifying, and bundling TLS certificates.	<a href="https://cfssl.org">https://cfssl.org</a> <a href="https://github.com/cloudflare/cfssl">https://github.com/cloudflare/cfssl</a>
Cloudflare PAL		Zero Trust Network	PAL is a tool for provisioning secrets to docker containers in production. PAL uses a client/server architecture consisting of two components: a pal client which runs as the endpoint to a container, and pal, which is a daemon that runs outside of the container, accepts requests from pal instances over a unix domain socket, and makes access control decisions.	Embraces the Identity-based Security strategy. Provides a way to bootstrap identities in a Container-based Distributed Application.  <a href="https://github.com/cloudflare/pal">https://github.com/cloudflare/pal</a> <a href="https://blog.cloudflare.com/pal-a-container-identity-bootstrapping-tool">https://blog.cloudflare.com/pal-a-container-identity-bootstrapping-tool</a>
dapr		LB, Proxy, Ingress, Gateway	It works as sidecar. Dapr is a portable, serverless, event-driven runtime that makes it easy for developers to build resilient, stateless and stateful microservices that run on the cloud and edge and embraces the diversity of languages and developer frameworks.	 <a href="https://github.com/dapr/dapr">https://github.com/dapr/dapr</a>
Datawire Ambassador (CE)		LB, Proxy, Ingress, Gateway	Ambassador is an open source Kubernetes-native API Gateway built on Envoy, designed for microservices. Ambassador essentially serves as an Envoy ingress controller.	<a href="https://www.getambassador.io">https://www.getambassador.io</a> <a href="https://github.com/datawire/ambassador">https://github.com/datawire/ambassador</a>
DEX		IAM	Dex is an identity service that uses OpenID Connect to drive authentication for other apps. Dex acts as a portal to other identity providers through "connectors." This lets dex defer authentication to LDAP servers, SAML providers, or established identity providers like GitHub, Google, and Active Directory. Clients write their authentication logic once to talk to dex, then dex handles the protocols for a given backend.	* Used frequently in Kubernetes.  <a href="https://github.com/dexidp/dex">https://github.com/dexidp/dex</a>
Dockle		SAST	Dockle is a container image Linter for security, detect container's vulnerabilities, helps build best-practice Dockerfile, supports CIS Benchmarks and DevSecOps practices (suitable for CI such as Travis CI, CircleCI, Jenkins, etc.).	* CIS Benchmark  <a href="https://github.com/goodwithtech/dockle">https://github.com/goodwithtech/dockle</a>
Envoy Proxy		LB, Proxy, Ingress, Gateway	Envoy is a high performance C++ distributed L7 proxy designed for single services and applications, as well as a communication bus and "universal data plane" designed for large microservice "service mesh" architectures. Built on the learnings of solutions such as NGINX, HAProxy, hardware and cloud LB, Envoy runs alongside every application and abstracts the network by providing common features, even Security, in a platform-agnostic manner.	<a href="https://www.envoyproxy.io">https://www.envoyproxy.io</a> <a href="https://github.com/envoyproxy/envoy">https://github.com/envoyproxy/envoy</a>
Ghostunnel Proxy		Proxy	Ghostunnel is a simple TLS proxy with mutual authentication support for securing non-TLS backend applications.	<a href="https://github.com/square/ghostunnel">https://github.com/square/ghostunnel</a>
Gloo Open Source		LB, Proxy, Ingress, Gateway	Gloo is a cloud-native API Gateway and Ingress Controller built on Envoy Proxy to connect, secure and control traffic across all your application services. Modernize to microservices architecture and scale your edge operations with a lightweight, yet powerful control plane for distributed environments.	* The WAF features are WIP.  <a href="https://gloo.solo.io">https://gloo.solo.io</a> <a href="https://github.com/solo-io/gloo">https://github.com/solo-io/gloo</a>
GolangCI-Lint		SAST	golangci-lint is a fast Go linters runner. It runs linters in parallel, uses caching, supports yaml config, has integrations with all major IDE and has dozens of linters included.	<a href="https://github.com/golangci/golangci-lint">https://github.com/golangci/golangci-lint</a>
Google gVisor		Sandboxing, Isolation	gVisor is a user-space kernel, written in Go, that implements a substantial portion of the Linux system surface. It includes an Open Container Initiative (OCI) runtime called runc that provides an isolation boundary between the application and the host kernel. The runc runtime integrates with Docker and Kubernetes, making it simple to run sandboxed containers.	<a href="https://github.com/google/gvisor">https://github.com/google/gvisor</a> <a href="https://gvisor.dev/docs">https://gvisor.dev/docs</a>
GoSec		SAST	Inspects source code for security problems by scanning the Go AST.	<a href="https://github.com/securego/gosec">https://github.com/securego/gosec</a>
Grafeas		Software Supply Chain	Grafeas is an open-source artifact metadata API that provides a uniform way to audit and govern your software supply chain. It defines an API spec for managing metadata about software resources (container images, VMs, JAR, and scripts). You can use Grafeas to define and aggregate information about your project's components.	* Grafeas and Kritis integration: <a href="https://www.infoq.com/presentations/supply-grafeas-kritis">https://www.infoq.com/presentations/supply-grafeas-kritis</a>  <a href="https://grafeas.io">https://grafeas.io</a> <a href="https://github.com/grafeas/grafeas">https://github.com/grafeas/grafeas</a>
HAProxy Ingress Controller		LB, Proxy, Ingress, Gateway	An ingress controller is a Kubernetes resource that routes traffic from outside your cluster to services within the cluster. Features: Secure communication with built-in SSL termination, rate limits based on whitelisting IP, multiple load-balancing algorithms, Layer 7 observability with the HAProxy Stats page and Prometheus metrics, able to set maximum connection limits to backend servers to prevent overloading services, etc.	* HA Proxy has a Enterprise version. * NGINX and HA Proxy are Proxies most used solutions to be used as LB, Proxy in Container-based Applications.  <a href="https://github.com/haproxytech/kubernetes-ingress">https://github.com/haproxytech/kubernetes-ingress</a>
Hashicorp Consul Connect		LB, Proxy, Ingress, Gateway	Consul Connect provides service-to-service connection authorization and encryption using mutual Transport Layer Security (TLS). Applications can use sidecar proxies in a service mesh configuration to establish TLS connections for inbound and outbound connections without being aware of Connect at all. Applications may also natively integrate with Connect for optimal performance and security. Connect can help you secure your services and provide data about service-to-service communications.	<a href="https://www.consul.io/docs/connect/index.html">https://www.consul.io/docs/connect/index.html</a> <a href="https://www.consul.io/docs/connect/security.html">https://www.consul.io/docs/connect/security.html</a>
Hashicorp Vault Open Source		PKI, Secrets Management	Vault is a tool for securely accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, and more. Vault provides a unified interface to any secret, while providing tight access control and recording a detailed audit log.	* The Enterprise version includes HSM, MFA, Disaster Recovery, FIPS 140, etc.  <a href="https://github.com/hashicorp/vault">https://github.com/hashicorp/vault</a>
huskyCI		SAST	huskyCI is an open source tool that orchestrates security tests and centralizes all results into a database for further analysis and metrics. It can perform static security analysis in Python (Bandit and Safety), Ruby (Brakeman), JavaScript (Npm Audit and Yarn Audit), Golang (Gosec), Java (SpotBugs plus Find Sec Bugs), and HCL (TFSec). It can also audit repositories for secrets like AWS Secret Keys, Private SSH Keys, and many others using GitLeaks.	<a href="https://github.com/globocom/huskyCI">https://github.com/globocom/huskyCI</a>
In-toto		Software Supply Chain	A framework to secure the integrity of software supply chains. in-toto is designed to ensure the integrity of a software product from initiation to end-user installation. It does so by making it transparent to the user what steps were performed, by whom and in what order. As a result, with some guidance from the group creating the software, in-toto allows the user to verify if a step in the supply chain was intended to be performed, and if the step was performed by the right actor.	<a href="https://in-toto.io">https://in-toto.io</a> <a href="https://github.com/in-toto/in-toto">https://github.com/in-toto/in-toto</a>
Istio		LB, Proxy, Ingress, Gateway	Istio lets you connect, secure, control, and observe services. Istio makes it easy to create a network of deployed services with load balancing, service-to-service authentication, monitoring, and more, with few or no code changes in service code. You add Istio support to services by deploying a special sidecar proxy throughout your environment that intercepts all network communication between microservices, then configure and manage Istio using its control plane functionality.	* Istio uses Envoy Proxy in different way to implement Sidecar, API Gateway and Ingress Controller, which are the way to deliver security controls over the data plane. * Istio includes a CA and SPIFFE specs to implement Identity-based Security ( <a href="https://istio.io/docs/concepts/security">https://istio.io/docs/concepts/security</a> ).  <a href="https://istio.io">https://istio.io</a> <a href="https://istio.io/docs/concepts/security">https://istio.io/docs/concepts/security</a>
JetStack Cert Manager		PKI	Cert-Manager is a Kubernetes add-on to automate the management and issuance of TLS certificates from various issuing sources. It will ensure certificates are valid and up to date periodically, and attempt to renew certificates at an appropriate time before expiry.	<a href="https://cert-manager.io">https://cert-manager.io</a> <a href="https://github.com/jetstack/cert-manager">https://github.com/jetstack/cert-manager</a>

KeyCloak		IAM	Add authentication to applications and secure services with minimum fuss. No need to deal with storing users or authenticating users. It's all available out of the box. You'll even get advanced features such as User Federation, Identity Brokering and Social Login.	Can be integrated with K8s: <a href="https://medium.com/@sagarpatkeat/kubernetes-with-keycloak-eca47f86abec">https://medium.com/@sagarpatkeat/kubernetes-with-keycloak-eca47f86abec</a> <a href="https://blog.codecentric.de/en/2019/05/configuring-kubernetes-login-keycloak/">https://blog.codecentric.de/en/2019/05/configuring-kubernetes-login-keycloak/</a> <a href="https://www.keycloak.org">https://www.keycloak.org</a>
Kritis		Software Supply Chain	Kritis is an open-source solution for securing your software supply chain for Kubernetes applications. Kritis enforces deploy-time security policies using the Google Cloud Container Analysis API, and in a subsequent release, Grafeas.	* Grafeas and Kritis integration: <a href="https://www.infoq.com/presentations/supply-grafeas-kritis">https://www.infoq.com/presentations/supply-grafeas-kritis</a> * In Kubernetes, Kritis works as an Admission Controller. <a href="https://github.com/grafeas/kritis">https://github.com/grafeas/kritis</a>
KubeSec.io		Risk Analysis	Security risk analysis for Kubernetes resources.	<a href="https://kubesecc.io">https://kubesecc.io</a> <a href="https://github.com/controlplaneio/kubesecc">https://github.com/controlplaneio/kubesecc</a>
Linkerd		LB, Proxy, Ingress, Gateway	Linkerd is a service mesh, designed to give platform-wide observability, reliability, and security without requiring configuration or code changes.	* Linkerd is a Cloud Native Computing Foundation (CNCF) project. <a href="https://github.com/linkerd/linkerd2">https://github.com/linkerd/linkerd2</a>
Litmus Chaos		Resilience	Litmus is a toolset to do cloud-native chaos engineering. Litmus provides tools to orchestrate chaos on K8s to help SREs find weaknesses in their deployments. SREs use Litmus to run chaos experiments initially in the staging environment and eventually in production to find bugs, vulnerabilities. Fixing the weaknesses leads to increased resilience of the system. Chaos is orchestrated using the following Kubernetes Custom Resource Definitions (CRDs).	<a href="https://github.com/litmuschaos/litmus">https://github.com/litmuschaos/litmus</a> <a href="https://litmuschaos.io">https://litmuschaos.io</a>
ModSecurity		WAF	ModSecurity is an open source, cross platform web application firewall (WAF) engine for Apache, IIS and Nginx that is developed by Trustwave's SpiderLabs. It has a robust event-based programming language which provides protection from a range of attacks against web applications and allows for HTTP traffic monitoring, logging and real-time analysis.	* For Kubernetes, it should be integrated to NGINX Ingress Controller. <a href="https://modsecurity.org">https://modsecurity.org</a> <a href="https://kubernetes.github.io/ingress-nginx/user-guide/third-party-addons/modsecurity">https://kubernetes.github.io/ingress-nginx/user-guide/third-party-addons/modsecurity</a>
Moloch		NIDS	Moloch augments your current security infrastructure to store and index network traffic in standard PCAP format, providing fast, indexed access. An intuitive and simple web interface is provided for PCAP browsing, searching, and exporting. Moloch exposes APIs which allow for PCAP data and JSON formatted session data to be downloaded and consumed directly.	<a href="https://molo.ch">https://molo.ch</a> <a href="https://github.com/aol/moloch">https://github.com/aol/moloch</a>
NAXSI		WAF	It is an open-source, high performance, low rules maintenance WAF for NGINX. NAXSI means Nginx Anti XSS & SQL Injection. Technically, it is a third party nginx module, available as a package for many UNIX-like platforms. This module, by default, reads a small subset of simple (and readable) rules containing 99% of known patterns involved in website vulnerabilities.	* It should be adapted to work in Kubernetes. <a href="https://github.com/nbs-system/naxsi">https://github.com/nbs-system/naxsi</a>
NGINX Ingress Controller		LB, Proxy, Ingress, Gateway	Ingress Controller for Kubernetes based on NGINX.	<a href="https://kubernetes.github.io/ingress-nginx">https://kubernetes.github.io/ingress-nginx</a> <a href="https://github.com/kubernetes/ingress-nginx">https://github.com/kubernetes/ingress-nginx</a>
Notary		Software Supply Chain	Notary is a project that allows anyone to have trust over arbitrary collections of data. Publishers can digitally sign collections and consumers can verify integrity and origin of content. This ability is built on a straightforward key management and signing interface to create signed collections and configure trusted publishers. With Notary anyone can provide trust over arbitrary collections of data. Using The Update Framework (TUF) as the underlying security framework, Notary takes care of the operations necessary to create, manage, and distribute the metadata necessary to secure the integrity of the data.	* The Notary project has officially been accepted in to the Cloud Native Computing Foundation (CNCF). * It can be integrated into K8s through Admission Controller specific implementation like IBM Portieris ( <a href="https://github.com/IBM/portieris">https://github.com/IBM/portieris</a> ). * 'Single Source of Truth for 'Software Supply Chain' <a href="https://github.com/IBM/portieris">https://github.com/IBM/portieris</a>
Open Policy Agent (OPA)		Security Policy	OPA is an open source, general-purpose policy engine that unifies policy enforcement across the stack. OPA provides a high-level declarative language that let's you specify policy as code and simple APIs to offload policy decision-making from your software. You can use OPA to enforce policies in microservices, Kubernetes, CI/CD pipelines, API gateways, and more.	* Falco and OPA are usually used together. * OPA is hosted by the Cloud Native Computing Foundation (CNCF). <a href="https://www.openpolicyagent.org">https://www.openpolicyagent.org</a>
OpenAM		IAM	Open Access Management (OpenAM) is an access management solution that includes Authentication, SSO, Authorization, Federation, Entitlements and Web Services Security. Cross Domain Single Sign On (CDSSO), SAML 2.0, OAuth 2.0 & OpenID Connect ensure that OpenAM integrates easily with legacy, custom and cloud applications without requiring any modifications. It's a developer-friendly, open-source control solution that allows you to own and protect your users digital identities.	<a href="https://github.com/OpenIdentityPlatform/OpenAM">https://github.com/OpenIdentityPlatform/OpenAM</a>
OpenSCAP		DAST	With oscap you can check security configuration settings of a system, and examine the system for signs of a compromise by using rules based on standards and specifications. The oscap uses SCAP which is a line of specifications maintained by the NIST which was created to provide a standardized approach for maintaining system security. The oscap mainly processes the XCCDF which is a standard way of expressing a checklist content and defines security checklists. It also combines with other specifications such as CPE, CCE and OVAL to create a SCAP content.	* The SCAP Workbench is a graphical utility that offers an easy way to perform common oscap tasks. <a href="https://www.open-scap.org">https://www.open-scap.org</a>
OpenUnison		IAM	OpenUnison combines the identity services that are most used by applications into a single system that is quick to deploy, easy to use, and simple to maintain. The identity services provided by OpenUnison include: Authentication - Who are you? How do we know that?, Session Management - How did you login? What do you have access to?, Identity Federation - SSO across domains, User Provisioning - Creating and managing identity data in systems and applications and Access Request Management - Why do you have access?.	<a href="https://github.com/TremoloSecurity/OpenUnison">https://github.com/TremoloSecurity/OpenUnison</a> <a href="https://github.com/TremoloSecurity/openunison-k8s-operator">https://github.com/TremoloSecurity/openunison-k8s-operator</a> <a href="https://github.com/TremoloSecurity/openunison-qs-kubernetes">https://github.com/TremoloSecurity/openunison-qs-kubernetes</a>
OSSEC HIDS		HIDS	OSSEC is an Open Source Host-based Intrusion Detection System. It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows.	* If you want to explore the strategies to use OSSEC on Public Cloud Infrastructures, I recommend reading this: <a href="https://atomicorp.com/ossec-con2019">https://atomicorp.com/ossec-con2019</a> <a href="https://www.ossec.net">https://www.ossec.net</a> <a href="https://www.ossec.net/docs">https://www.ossec.net/docs</a> <a href="https://github.com/ossec">https://github.com/ossec</a>
OWASP Dependency-Track		SCA	Dependency-Track is an intelligent Supply Chain Component Analysis platform that allows organizations to identify and reduce risk from the use of third-party and open source components. Dependency-Track monitors component usage across all versions of every application in its portfolio in order to proactively identify risk across an organization. The platform has an API-first design and is ideal for use in CI/CD environments.	* SBOM <a href="https://dependencytrack.org">https://dependencytrack.org</a>
OWASP Zed Attack Proxy (ZAP)		DAST	Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible. At its core, ZAP is what is known as a "man-in-the-middle proxy." It can be used as a stand-alone application, and as a daemon process.	* Webapp Security Proxy <a href="https://www.zaproxy.org">https://www.zaproxy.org</a> <a href="https://github.com/zaproxy/zaproxy">https://github.com/zaproxy/zaproxy</a>
OwlH Net		NIDS	OwlH was born to help security engineers to manage, analyze and respond to network threats and anomalies using Open Source Network IDS Suricata and Zeek, offering: Centralized Rule management and Network IDS nodes Configuration Management, Software TAP to capture cloud and distributed traffic in cloud and hybrid dispersed environments, Traffic Forensics with Moloch, Centralized Visualization and Compliance Mapping.	<a href="https://www.owlh.net">https://www.owlh.net</a> <a href="https://github.com/OwlH-net">https://github.com/OwlH-net</a> <a href="http://documentation.owlh.net">http://documentation.owlh.net</a>
PHPStan		SAST	PHPStan focuses on finding errors in your code without actually running it. It catches whole classes of bugs even before you write tests for the code. It moves PHP closer to compiled languages in the sense that the correctness of each line of the code can be checked before you run the actual line.	<a href="https://github.com/phpstan/phpstan">https://github.com/phpstan/phpstan</a>
PowerfulSeal		Resilience	PowerfulSeal adds chaos to your Kubernetes clusters, so that you can detect problems in your systems as early as possible. It kills targeted pods and takes VMs up and down. It follows the Principles of Chaos Engineering, and is inspired by Chaos Monkey. Watch the Seal at KubeCon 2017 Austin.	<a href="https://github.com/bloomberg/powerfulseal">https://github.com/bloomberg/powerfulseal</a>

Project Calico		Network Security	Calico is an open source networking and network security solution for containers, virtual machines, and native host-based workloads. Calico supports a broad range of platforms including Kubernetes, OpenShift, Docker EE, OpenStack, and bare metal services.	* SDN <a href="https://www.projectcalico.org">https://www.projectcalico.org</a>
Pylint (Python)		SAST	Pylint is a tool that checks for errors in Python code, tries to enforce a coding standard and looks for code smells. It can also look for certain type errors, it can recommend suggestions about how particular blocks can be refactored and can offer you details about the code's complexity.	<a href="https://www.pylint.org">https://www.pylint.org</a>
Rancher Load Balancer Controller		LB, Proxy, Ingress, Gateway	L7 Load Balancer service managing load balancer provider configured via load balancer controller. Pluggable model allows different controller and provider implementation. v0.1.0 has support for Kubernetes ingress as a controller, and Rancher Load Balancer as a provider. Rancher provider is a default one, although you can develop and deploy your own implementation (nginx, traefik, etc).	<a href="https://github.com/rancher/lb-controller">https://github.com/rancher/lb-controller</a>
Safety (Python)		SCA	Safety checks your installed dependencies for known security vulnerabilities.  By default it uses the open Python vulnerability database Safety DB, but can be upgraded to use pyup.io's Safety API using the --key option.	<a href="https://github.com/pyupio/safety">https://github.com/pyupio/safety</a>
SELinux		Linux Runtime Protection	SELinux is a security enhancement to Linux which allows users and administrators more control over access control. SELinux adds finer granularity to access controls. Instead of only being able to specify who can read, write or execute a file, for example, SELinux lets you specify who can unlink, append only, move a file and so on. SELinux allows you to specify access to many resources other than files as well, such as network resources and interprocess communication (IPC).	* Used frequently with AppArmor and Seccomp on Kubernetes to implement Security at Pod level ( <a href="https://kubernetes.io/docs/tasks/configure-pod-container/security-context">https://kubernetes.io/docs/tasks/configure-pod-container/security-context</a> ). <a href="https://selinuxproject.org">https://selinuxproject.org</a> <a href="https://github.com/SELinuxProject">https://github.com/SELinuxProject</a> <a href="https://kubernetes.io/docs/concepts/policy/pod-security-policy">https://kubernetes.io/docs/concepts/policy/pod-security-policy</a>
Skyscanner CFripper		SAST	CFRipper is a Library and CLI security analyzer for AWS CloudFormation templates. You can use CFRipper to prevent deploying insecure AWS resources into your Cloud environment. You can write your own compliance checks by adding new custom plugins.	* CloudFormation Lint implemented in Python <a href="https://github.com/Skyscanner/cfripper">https://github.com/Skyscanner/cfripper</a>
Snort IDS		IDS	Snort's open source network-based intrusion detection/prevention system (IDS/IPS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching and matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, semantic URL attacks, buffer overflows, server message block probes, and stealth port scans. <i>Snort can work as sniffer, packet logger, and snort.</i>	<a href="https://www.snort.org">https://www.snort.org</a>
SonarQube CE		SAST	In addition to exposing vulnerabilities, it is used to measure the source code quality of a web application. Despite being written in Java, SonarQube is able to carry out analysis of over 20 programming languages. Furthermore, it gets easily integrated with continuous integration tools to the likes of Jenkins.	<a href="https://www.sonarqube.org">https://www.sonarqube.org</a>
SPIFFE		Zero Trust Network	SPIFFE, the Secure Production Identity Framework For Everyone, provides a secure identity, in the form of a specially crafted X.509 certificate, to every workload in a modern production environment. SPIFFE removes the need for application-level authentication and complex network-level ACL configuration.	* It is used by The SPIRE Project, Istio Citadel, Envoy Proxy, Pinterest, Kong Kuma, Hashicorp Consul, The Ghostunnel proxy, etc. <a href="https://spiffe.io">https://spiffe.io</a>
SPIRE		Zero Trust Network	SPIRE is a production-ready implementation of the SPIFFE ( <a href="https://spiffe.io">https://spiffe.io</a> ) APIs that performs node and workload attestation in order to securely issue SVIDs to workloads, and verify the SVIDs of other workloads, based on a predefined set of conditions.	<a href="https://spiffe.io/spire">https://spiffe.io/spire</a> <a href="https://scytale.io/opensource-spiffe">https://scytale.io/opensource-spiffe</a>
SpotBugs (Java)		SAST	SpotBugs is a program which uses static analysis to look for bugs in Java code. SpotBugs is the spiritual successor of FindBugs, carrying on from the point where it left off with support of its community. Please check the official manual for details. SpotBugs requires JRE (or JDK) 1.8.0 or later to run. However, it can analyze programs compiled for any version of Java, from 1.0 to 1.9.	<a href="https://github.com/spotbugs/spotbugs">https://github.com/spotbugs/spotbugs</a>
Stelligent cfn_nag		SAST	The cfn-nag tool looks for patterns in CloudFormation templates that may indicate insecure infrastructure. Roughly speaking, it will look for:  IAM rules that are too permissive (wildcards) Security group rules that are too permissive (wildcards) Access logs that aren't enabled <i>Enabling that isn't enabled</i>	* CloudFormation Lint implemented in Ruby <a href="https://github.com/stelligent/cfn_nag">https://github.com/stelligent/cfn_nag</a>
Suricata-IDS		NIDS	It is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing. Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats.	<a href="https://suricata-ids.org">https://suricata-ids.org</a>
Sysdig Falco		HIDS, RASP	Falco is a behavioral activity monitor designed to detect anomalous activity in your applications. Falco audits a system at the most fundamental level, the kernel. Falco then enriches this data with other input streams such as container runtime metrics, and Kubernetes metrics. Falco lets you continuously monitor and detect container, application, host, and network activity -all in one place- from one source of data, with one set of rules.	<a href="https://falco.org">https://falco.org</a> <a href="https://github.com/falcosecurity/falco">https://github.com/falcosecurity/falco</a>
Sysdig Inspect		HIDS, RASP	Sysdig is a full-system exploration, troubleshooting and debugging tool for Linux systems. It records all system calls made by any process, allowing SysAdmins to debug the operating system or any processes running on it. - Cysdig is a simple, intuitive, and fully customizable curses UI for Sysdig. - Sysdig Inspect is a powerful web interface for container troubleshooting and security investigation.	<a href="https://github.com/draios/sysdig">https://github.com/draios/sysdig</a> <a href="https://github.com/draios/sysdig-inspect">https://github.com/draios/sysdig-inspect</a>
tfsec (Terraform)		SAST	tfsec uses static analysis of your terraform templates to spot potential security issues. Now with terraform CDK support. It was integrated into AquaSec products by 2021/0712.	<a href="https://github.com/aquasecurity/tfsec">https://github.com/aquasecurity/tfsec</a>
Traefik		LB, Proxy, Ingress, Gateway	Traefik (pronounced traffic) is a modern HTTP reverse proxy and load balancer that makes deploying microservices easy. Traefik integrates with your existing infrastructure components (Docker, Swarm mode, Kubernetes, Marathon, Consul, Etcd, Rancher, Amazon ECS, ...) and configures itself automatically and dynamically. Pointing Traefik at your orchestrator should be the only configuration step you need.	<a href="https://containo.us/traefik">https://containo.us/traefik</a> <a href="https://github.com/containous/traefik">https://github.com/containous/traefik</a>
w3af		DAST	w3af is an open source web application security scanner which helps developers and penetration testers identify and exploit vulnerabilities in their web applications. The scanner is able to identify 200+ vulnerabilities, including Cross-Site Scripting, SQL injection and OS commanding.	<a href="http://w3af.org">http://w3af.org</a> <a href="https://github.com/andresriancho/w3af">https://github.com/andresriancho/w3af</a>
Wapiti		DAST	Wapiti allows you to audit the security of your websites or web applications. It performs "black-box" scans (it does not study the source code) of the web application by crawling the webpages of the deployed webapp, looking for scripts and forms where it can inject data. Once it gets the list of URLs, forms and their inputs, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable.	<a href="https://wapiti.sourceforge.io">https://wapiti.sourceforge.io</a> <a href="https://sourceforge.net/p/wapiti/git/ci/master/tree">https://sourceforge.net/p/wapiti/git/ci/master/tree</a>
Wazuh HIDS		HIDS	Wazuh provides a security solution capable of monitoring your infrastructure, detecting threats, intrusion attempts, system anomalies, poorly configured applications and unauthorized user actions. It also provides a framework for incident response and regulatory compliance.	* It is a fork of OSSEC. * It can be integrated with Splunk, ELK, EFK and provides an RESTful API. <a href="https://wazuh.com">https://wazuh.com</a> <a href="https://github.com/wazuh/wazuh-kubernetes">https://github.com/wazuh/wazuh-kubernetes</a> <a href="https://github.com/wazuh/wazuh-docker">https://github.com/wazuh/wazuh-docker</a>

Weave Net		Network Security	Weave Net creates a virtual network that connects Docker containers across multiple hosts and enables their automatic discovery. With Weave Net, portable microservices-based applications consisting of multiple containers can run anywhere: on one host, multiple hosts or even across cloud providers and data centers.	* SDN <a href="https://www.weave.works/oss/net">https://www.weave.works/oss/net</a> <a href="https://github.com/weaveworks/weave">https://github.com/weaveworks/weave</a>
Yor		Tagging	Yor is an open-source tool that helps add informative and consistent tags across infrastructure-as-code frameworks such as Terraform, CloudFormation, and Serverless.  Yor is built to run as a GitHub Action automatically adding consistent tagging logics to your IaC. Yor can also run as a pre-commit hook and a standalone CLI.	<a href="https://github.com/bridgecrewio/yor">https://github.com/bridgecrewio/yor</a> <a href="https://bridgecrew.io/blog/announcing-yor-open-source-iac-tag-trace-cloud-resources/">https://bridgecrew.io/blog/announcing-yor-open-source-iac-tag-trace-cloud-resources/</a>
AWS CloudFormation Guard		Security Policy	Guard offers a policy-as-code domain-specific language (DSL) to write rules and validate JSON- and YAML-formatted data such as CloudFormation Templates, K8s configurations, and Terraform JSON plans/configurations against those rules.	<a href="https://github.com/aws-cloudformation/cloudformation-guard">https://github.com/aws-cloudformation/cloudformation-guard</a>
AWS Serverless Rules		SAST	The Serverless Rules are a compilation of rules to validate infrastructure as code template against recommended practices. This currently provides a module for cfn-lint and a plugin for tfint.  You can use those rules to get quick feedback on recommended practices while building a serverless application, as part of automated code review process, or as guardrails before deployment to production.	<a href="https://github.com/awslabs/serverless-rules">https://github.com/awslabs/serverless-rules</a>
Dagda		SAST	Dagda is a tool to perform static analysis of known vulnerabilities, trojans, viruses, malware & other malicious threats in docker images/containers and to monitor the docker daemon and running docker containers for detecting anomalous activities. In order to fulfill its mission, first the known vulnerabilities as CVEs, BIDs (Bugtraq IDs), RHSAs and RHBAs, and the known exploits from Offensive Security database are imported into a MongoDB to facilitate the search of these vulnerabilities and exploits when your analysis are in progress.	<a href="https://github.com/eliasgranderubio/dagda">https://github.com/eliasgranderubio/dagda</a>
Docker Bench		Security Audit	The Docker Bench for Security is a script that checks for dozens of common best-practices around deploying Docker containers in production. The tests are all automated, and are inspired by the CIS Docker Benchmark v1.2.0.	* CIS Benchmark <a href="https://github.com/docker/docker-bench-security">https://github.com/docker/docker-bench-security</a>
Grabber		DAST	Grabber is a web application scanner. Basically it detects some kind of vulnerabilities in your website.  Grabber is simple, not fast but portable and really adaptable. This software is designed to scan small websites such as personals, forums etc. absolutely not big application: it would take too long time and flood your network.	<a href="http://rgaucher.info/beta/grabber">http://rgaucher.info/beta/grabber</a>
Heptio Ironclad		WAF	This is a reference configuration for running a web application firewall (WAF) on Kubernetes. It is a container build of ModSecurity+Nginx running the ModSecurity Core Rule Set along with a Go helper.  The Ironclad container runs as a sidecar for your application. It proxies inbound requests to your application over localhost within the confines of a single Kubernetes Pod.	* "Take this with a grain of salt because this project is not actively maintained. I think the sidecar approach has benefits, especially if you have a lot of application-specific rules/exceptions that you want to version alongside each application." * <a href="https://www.youtube.com/watch?v=xVEWYgF4deg">https://www.youtube.com/watch?v=xVEWYgF4deg</a> <a href="https://github.com/heptiolabs/ironclad">https://github.com/heptiolabs/ironclad</a>
Kube-Monkey		Resilience	kube-monkey is an implementation of Netflix's Chaos Monkey for Kubernetes clusters. It randomly deletes Kubernetes (K8s) pods in the cluster encouraging and validating the development of failure-resilient services.	* It injects faults in K8s killing pods. <a href="https://github.com/asobit/kube-monkey">https://github.com/asobit/kube-monkey</a>
NeuVector Kubernetes CIS Benchmark		Security Audit	A set of scripts inspired by CIS Kubernetes Benchmark that checks best-practices of Kubernetes installations	* CIS Benchmark <a href="https://github.com/neuvector/kubernetes-cis-benchmark">https://github.com/neuvector/kubernetes-cis-benchmark</a>
Regula		Security Policy	Regula is a tool that evaluates CloudFormation and Terraform infrastructure-as-code for potential AWS, Azure, and Google Cloud security and compliance violations prior to deployment. Regula includes a library of rules written in Rego, the policy language used by the Open Policy Agent (OPA) project. Regula works with your favorite CI/CD tools such as Jenkins, Circle CI, and AWS CodePipeline.	<a href="https://github.com/fugue/regula">https://github.com/fugue/regula</a>
Seccomp		Linux Runtime Protection	Seccomp filtering provides a means for a process to specify a filter for incoming system calls. The filter is expressed as a Berkeley Packet Filter (BPF) program, as with socket filters, except that the data operated on is related to the system call being made: system call number and the system call arguments. This allows for expressive filtering of system calls using a filter program language with a long history of being exposed to userland and a straightforward data set.	* Used frequently with AppArmor and SELinux on Kubernetes to implement Security at Pod level ( <a href="https://kubernetes.io/docs/tasks/configure-pod-container/security-context">https://kubernetes.io/docs/tasks/configure-pod-container/security-context</a> ). <a href="https://www.kernel.org/doc/Documentation/prctl/seccomp_filter.txt">https://www.kernel.org/doc/Documentation/prctl/seccomp_filter.txt</a> <a href="https://kubernetes.io/docs/concepts/policy/pod-security-policy">https://kubernetes.io/docs/concepts/policy/pod-security-policy</a>
Terraform Linter (tfint)		SAST	TFLint is a framework and each feature is provided by plugins, the key features are as follows: - Find possible errors (like illegal instance types) for Major Cloud providers (AWS/Azure/GCP). - Warn about deprecated syntax, unused declarations. - Enforce best practices, naming conventions.	<a href="https://github.com/terraform-linters/tflint">https://github.com/terraform-linters/tflint</a>
User Account and Authentication (UAA) Server		IAM	The primary role of UAA is as an OAuth2 provider, issuing tokens for client apps to use when they act on behalf of CFAR users. In collaboration with the login server, UAA can authenticate users with their CFAR credentials, and can act as an SSO service using those, or other, credentials.	* Generally UAA and DEX are integrated to Kubernetes API Server. <a href="https://docs.cloudfoundry.org/concepts/architecture/uaa.html">https://docs.cloudfoundry.org/concepts/architecture/uaa.html</a>