Tooling:

Pre-commit time tools:

Tool	Definition	Strength	Advantage	Utility
git-secrets	Prevents committing secrets (API keys, passwords) into Git repositories.	Detects secrets in Git commits	Protects against accidental exposure of secrets by blocking their inclusion in commits	Secrets
git-hound	Scans Git repositories for secrets and sensitive information.	Effective detection of secrets and sensitive information	Identifies and prevents the exposure of secrets in Git repositories	Secrets
goSDL	Automates the Security Development Lifecycle (SDL) process in Go.	Automates SDL processes	Integrates security into the software development lifecycle	Security
ThreatPlaybook	Threat modeling tool that automatically generates security tests based on threat scenarios.	Automatic generation of security tests based on threat models	Automates security testing based on threat models	Testing
Threat Dragon	Visual threat modeling tool for creating threat and risk diagrams.	Visual creation of threat models	Visualizes and analyzes potential threats using diagrams	Visualization
threatspec	Integrates threat modeling into code	Integrates threat	Ensures that threat modeling is part	Integration

	and testing processes.	modeling into development processes	of the code and testing processes	
pytm	Python-based tool for creating threat models.	Creates threat models using Python	Automates and facilitates threat modeling through Python scripts	Modeling
Threagile	Agile threat modeling tool designed to be lightweight and flexible.	Lightweight and flexible threat modeling	Adapts to agile methodologies and provides flexibility in threat modeling	Agile
MAL-lang	Language for modeling attacks and threats	Specialized in attack and threat modeling	Models and analyzes attack scenarios to understand risks	Attacks
Microsoft Threat Modeling Tool	Microsoft tool for graphical threat modeling.	Graphical interface for creating threat models	Provides a graphical interface for visualizing and documenting threats	Visualization
Talisman	Analyzes files for secrets before commits to prevent their inclusion.	Prevents secrets from being committed by analyzing files	Prevents accidental exposure of secrets by analyzing files before commits	Secrets
SEDATED	Detects leaks of sensitive data in files.	Detects leaks of sensitive data	Prevents sensitive data leaks by scanning files	Leaks
Sonarlint	Real-time code analysis tool that detects security issues and bugs.	Real-time static code analysis	Provides suggestions for fixing code issues and improves code quality and	Code Quality

			security	
DevSkim	Static analysis tool that detects security issues and vulnerabilities in code.	Detects security vulnerabilities and issues in code	Identifies security issues during code writing	Security
detect-secrets	Detects secrets in code repositories by scanning commits.	Detects secrets in code repositories	Prevents accidental inclusion of secrets in repositories	Secrets

Secrets management

Tool	Definition	Strength	Advantage	Utility
GitLeaks	Tool to detect secrets in Git repositories.	Detects secrets in Git repositories	Protects against accidental secret exposure by scanning Git repositories	Secrets
HashiCorp Vault	Secrets management solution for securely storing and controlling access to secrets.	Centralized secrets management	Provides robust security and controlled access to secrets	Secrets
Mozilla SOPS	Tool for encrypting configuration files with secrets.	Encryption of configuration files	Protects secrets by encrypting them in configuration files	Encryption
Chef Vault	Chef extension for managing secrets and sensitive data.	Integration with Chef for secrets management	Manages secrets within Chef environments	Management
Ansible Vault	Ansible tool for encrypting sensitive data in playbooks.	Encryption of data in Ansible playbooks	Protects sensitive information by encrypting it in playbooks	Encryption

OSS and Dependency management

Tool	Definition	Strength	Advantage	Utility
Snyk	Tool for detecting and fixing vulnerabilities in open source dependencies.	Detection and remediation of vulnerabilities	Enhances the security of open source dependencies by detecting and fixing vulnerabilities	Security
Dependency Combobulator	Tool for analyzing and visualizing project dependencies.	Visualization of dependencies	Helps understand and manage dependencies by providing an overview of their relationships	Visualization
DependencyTrack	Platform for managing dependencies and monitoring vulnerabilities.	Dependency management and vulnerability tracking	Provides detailed information on vulnerabilities and their management	
DependencyCheck	Dependency analysis tool for detecting vulnerabilities and security issues.	Vulnerability detection in dependencies	Identifies vulnerabilities and security issues in dependencies	Security
PHP Security Checker	Tool for analyzing the security of PHP projects by checking for	PHP-specific security analysis	Helps secure PHP projects by detecting specific vulnerabilities	PHP

	vulnerabilities.			
npm-check	Tool for checking updates of dependencies in npm projects.	Checking for dependency updates	Facilitates npm dependency management by checking for available updates	Updates

Supply chain specific tools:

Tool	Definition	Strength	Advantage	Utility
Tekton Chains	Tool for managing supply chain in CI/CD pipelines with digital signatures.	Supply chain management with digital signatures	Ensures the integrity and traceability of artifacts throughout the delivery chain	Integrity
SLSA	Framework for software supply chain security, establishing standards for secure production.	Security standards for software production	Provides security practices to ensure trust in the software supply chain	Security
Ratify	Tool for validating artifact provenance and ensuring compliance with security policies.	Validation of artifact provenance	Ensures artifacts come from trusted sources and adhere to security policies	Compliance
chain-bench	Tool for assessing supply chain compliance with SLSA standards.	Assessment of compliance with SLSA standards	Helps verify that supply chains meet SLSA security standards	Assessment

SAST

Tool	Definition	Strength	Advantage	Utility
ESLint	Tool for static analysis of JavaScript code and detection of quality issues.	Static analysis of JavaScript code	Improves code quality by detecting errors, inconsistencies, and style issues	Quality
nodejsscan	Tool for detecting vulnerabilities in Node.js applications.	Detection of Node.js-specific vulnerabilities	Identifies security vulnerabilities in Node.js applications	Security
SonarQube	Platform for continuous code quality analysis and issue management.	Continuous code quality analysis	Provides a comprehensive view of code quality and security issues	Quality
Semgrep	Tool for pattern searching and vulnerability detection in code.	Pattern searching and vulnerability detection	Allows creation of custom rules to detect specific patterns in code	Detection
gosec	Static analysis tool for Go code aimed at detecting security vulnerabilities.	Security analysis for Go language	Identifies security vulnerabilities in Go code	Security
Bearer	Static analysis tool for detecting security errors in APIs and services.	Detection of security errors in APIs	Ensures API security by detecting security issues and misconfigurations	API

DAST

Tool	Definition	Strength	Advantage	Utility
Zap Proxy	Open source tool for discovering vulnerabilities in web applications.	Dynamic analysis of web applications	Detects vulnerabilities by analyzing application behavior in real-time	Vulnerabilities
Akto	Security testing tool for APIs and web applications.	Security testing for APIs and web applications	Identifies security weaknesses in APIs and web applications	Security
Wapiti	Web vulnerability scanner that performs security tests on web applications.	Web vulnerability analysis	Provides detailed reports on vulnerabilities found in web applications	Web
Skipfish	Security scanner for web applications that detects common vulnerabilities.	Speed and comprehensiveness of scanning	Allows for rapid and thorough analysis of vulnerabilities in web applications	Analysis
Nikto	Vulnerability scanner for web servers, detecting common security issues.	Detection of vulnerabilities in web servers	Identifies security issues in web server configurations	Servers

Continuous deployment security

Tool	Definition	Strength	Advantage	Utility
SecureCodeBox	Open source framework for automating security tests in CI/CD pipelines.	Automation of security tests	Integrates security tests into CI/CD pipelines for early detection of vulnerabilities	Automation
OpenSCAP	Tool for compliance assessment and vulnerability management in IT environments.	Compliance assessment and vulnerability management	Provides compliance reports and security analyses to ensure system compliance	Compliance
ThreatMapper	Tool for mapping and analyzing threats in production environments.	Threat mapping and analysis	Enables visualization and analysis of threats in production environments for better risk management	Mapping

Kubernetes

Tool	Definition	Strength	Advantage	Utility
KubeSec	Tool for assessing the security of Kubernetes configurations using security policies.	Assessment of Kubernetes configurations	Identifies security flaws in Kubernetes configurations	Security
KubiScan	Tool for analyzing the security of Kubernetes deployments and detecting vulnerabilities.	In-depth analysis of Kubernetes deployments	Detects vulnerabilities in Kubernetes deployments for enhanced security	Vulnerabilities
Kubeaudit	Tool for auditing Kubernetes configurations to detect security issues.	Auditing Kubernetes configurations	Provides an audit of configurations to detect security issues	Audit
kube-hunter	Tool for finding vulnerabilities and security flaws in Kubernetes clusters.	Proactive vulnerability searching	Identifies vulnerabilities and flaws in Kubernetes clusters	Discovery
kube-linter	Tool for validating Kubernetes configurations and ensuring adherence to best practices.	Validation of Kubernetes configurations	Ensures Kubernetes configurations follow best practices	Validation
kube-scan	Tool for scanning Kubernetes configurations and	Scanning configurations and	Detects vulnerabilities in Kubernetes	Scanning

	deployments for vulnerabilities.	deployments	configurations and deployments	
trivy-operator	Tool for integrating Trivy with Kubernetes to scan container images for vulnerabilities.	Trivy integration with Kubernetes	Scans container images for vulnerabilities directly within Kubernetes	Scanning

Containers

Tool	Definition	Strength	Advantage	Utility
Harbor	Open source container registry for storing, managing, and distributing container images.	Comprehensive container image management	Provides security, management, and replication features for container images	Management
Clair	Security analysis tool for container images that detects vulnerabilities.	Vulnerability detection in container images	Identifies vulnerabilities in container images to improve security	Security
Falco	Tool for detecting suspicious behaviors in containers and hosts.	Real-time anomaly detection	Monitors containers and hosts for unusual behavior	Monitoring
Trivy	Open source security scanner for container images and configurations.	Comprehensive image and configuration analysis	Identifies vulnerabilities in images and configurations to enhance security	Scanning
Notary	Tool for signing and verifying container images to ensure their integrity and	Image signing and verification	Ensures the integrity and authenticity of container images using	Integrity

	authenticity.		digital signatures	
Cosign	Tool for signing and verifying container images and artifacts with signatures.	Secure signing and verification	Allows signing of container images and verification of their integrity and provenance	Security
Grype	Vulnerability scanner for container images and dependencies.	Vulnerability detection in images and dependencies	Identifies vulnerabilities to improve the security of containers and their dependencies	Scanning

Justification pour les outils Kubernetes

- **kubectl** : Essentiel pour la gestion quotidienne des ressources Kubernetes.
- **Helm** : Simplifie la gestion des applications Kubernetes complexes.
- **Kustomize** : Facilite la personnalisation des configurations sans duplication.
- **K9s** : Offre une interface conviviale pour gérer Kubernetes via le terminal.
- **Kubeless** : Permet d'exécuter des fonctions serverless dans Kubernetes.
- **ArgoCD** : Automatiser le déploiement en utilisant Git comme source de vérité améliore la continuité des opérations.
- **Prometheus** : Collecte et surveille les métriques pour maintenir des performances optimales.
- **Grafana** : Visualisation des métriques aide à comprendre les performances du système.
- **Kiali** : Aide à gérer les services mesh en fournissant des outils de visualisation.
- **Jaeger** : Offre des capacités de traçage pour le débogage et l'optimisation.

Justification pour les outils Docker

- **Docker CLI** : Outil de base pour la gestion des conteneurs.
- **Docker Compose** : Simplifie la gestion des applications multi-conteneurs.
- **Docker Swarm** : Fournit une orchestration intégrée pour les clusters Docker.
- **Docker Registry** : Stocke et distribue les images Docker efficacement.
- **Portainer** : Facilite la gestion des conteneurs via une interface graphique.
- **Docker Hub** : Permet le partage et la recherche d'images Docker.
- **Trivy** : Analyse les images Docker pour des vulnérabilités de sécurité.
- **Hadolint** : Améliore les Dockerfiles en détectant les problèmes de style et de sécurité.
- **Dive** : Optimise les images Docker en examinant les couches.
- **Snyk** : Renforce la sécurité des images Docker en détectant les vulnérabilités.

`https://gitlab.u-cloudsolutions.xyz/summary-internship/2024/wissem-sghaier/devsecops-tools.git`