**Top DevSecOps Tools for 2023: Open Source Solutions for Enterprises**

**Introduction**

DevSecOps, short for Development, Security, and Operations, is a practice that integrates security into every phase of the application or software development lifecycle. It focuses on automating security processes and minimizing vulnerabilities to meet the security and compliance objectives of IT and business. By incorporating security early in the development cycle and integrating it with continuous integration, continuous delivery, and continuous deployment (CI/CD) pipelines, DevSecOps helps organizations ensure the security of their applications.

The DevSecOps approach requires the use of various tools and strategies to identify and address security risks. In this article, we will explore some of the best open-source DevSecOps tools available in 2022.

**DevSecOps Tools Categories**

DevSecOps tools can be categorized into several groups based on their functionality. These categories include:

1. *Static Application Security Testing (SAST) Tools*

*2. Dynamic Application Security Testing (DAST) Tools*

*3. Software Composition Analysis (SCA) Tools*

*4. Container Security Tools*

*5. Infrastructure as Code (IaC) Security Tools*

*6. Continuous Integration/Continuous Deployment (CI/CD) Security Tools*

*7. Compliance and Governance Tools*

*8. Security Dashboard and Analytics Tools*



OpenSource tools DevSecOps for different stages

**Top OpenSource tools DevSecOps for 2023**

**Software Composition Analysis (SCA) Tools:**

1. [**OWASP Dependency-Check**](https://owasp.org/www-project-dependency-check/): OWASP Dependency-Check is a software composition analysis tool that identifies known vulnerabilities in project dependencies.
2. [**Retire.js**](https://github.com/retirejs/retire.js/)**:** Retire.js is a scanner that detects vulnerable JavaScript libraries in your web application.
3. [**WhiteSource Bolt**](https://marketplace.visualstudio.com/items?itemName=whitesource.ws-bolt): WhiteSource Bolt is an open-source SCA tool that scans your project dependencies for known vulnerabilities and provides actionable remediation steps.
4. [**Dependency-Track**](https://github.com/DependencyTrack/dependency-track): Dependency-Track is an open-source platform that tracks and monitors your project’s dependencies, providing insights into their known vulnerabilities.
5. [**OSSIndex**](https://github.com/sonatype/ossindex-public): OSSIndex is an open-source vulnerability database and analysis platform that integrates with various development tools to provide real-time security intelligence on project dependencies

**Static Application Security Testing (SAST) Tools:**

1. [**SonarQube**](https://sonarcloud.io/explore/projects): SonarQube is an open-source platform for continuous code quality inspection that includes static code analysis for identifying security vulnerabilities.
2. [**Bandit**](https://github.com/PyCQA/bandit): Bandit is a Python-focused SAST tool that analyzes Python code for common security issues and vulnerabilities.
3. [**SpotBugs**](https://github.com/spotbugs/spotbugs): FindBugs is an open-source static analysis tool for Java applications that detects common coding errors, potential vulnerabilities, and performance issues.
4. [**RIPS**](https://github.com/robocoder/rips-scanner): RIPS is an open-source PHP security analysis tool that helps identify security vulnerabilities and coding flaws in PHP applications.
5. [**PMD**](https://github.com/pmd/pmd): PMD is an open-source source code analyzer for various programming languages, including Java, JavaScript, and XML, which identifies potential bugs, dead code, and security vulnerabilities.

**Dynamic Application Security Testing (DAST) Tools:**

1. [**OWASP ZAP**](https://github.com/zaproxy/zaproxy)**:** OWASP ZAP (Zed Attack Proxy) is an open-source web application security scanner that helps you identify vulnerabilities in web applications.
2. [**Nikto**](https://github.com/sullo/nikto): Nikto is an open-source web server scanner that performs comprehensive tests against web servers to identify potential vulnerabilities.
3. [**Wapiti**](https://github.com/wapiti-scanner/wapiti): Wapiti is an open-source web application vulnerability scanner that audits the security of web applications by performing black-box testing.
4. [**Arachni**](https://github.com/Arachni/arachni): Arachni is an open-source, modular web application security scanner that checks for a wide range of vulnerabilities and provides comprehensive reports.
5. [**Grabber**](https://github.com/amoldp/Grabber-Security-and-Vulnerability-Analysis-): Grabber is an open-source web application scanner that detects security vulnerabilities by crawling and scanning web pages.

**Container Security Tools:**

1. [**Clair**](https://github.com/quay/clair): Clair is an open-source container vulnerability scanner that analyzes container images and provides reports on known vulnerabilities.
2. [**Trivy**](https://github.com/aquasecurity/trivy): Trivy is an open-source vulnerability scanner for containers and other artifacts, such as operating system packages and application dependencies. It scans container images and provides detailed reports on any vulnerabilities detected, including their severity and remediation steps.
3. [**Anchore Engine**](https://github.com/anchore/anchore-engine): Anchore Engine is an open-source tool for analyzing container images for vulnerabilities, policy violations, and best practices.
4. [**Sysdig Falco**](https://github.com/falcosecurity/falco): Sysdig Falco is an open-source behavioral activity monitoring tool designed specifically for containers and Kubernetes. It detects and alerts on anomalous behavior and potential security threats in real-time. Falco uses rules and policies to define expected container behavior and raises alerts when deviations occur.

**Infrastructure Security Tools:**

1. [**OpenSCAP**](https://www.open-scap.org/features/vulnerability-assessment/): OpenSCAP is an open-source framework for compliance checking and vulnerability management, which includes capabilities for assessing and securing infrastructure systems.
2. [**Lynis**](https://github.com/CISOfy/lynis): Lynis is an open-source security auditing tool that assesses the security configuration of Linux and Unix-based systems.
3. [**Dagda**](https://github.com/eliasgranderubio/dagda): Dagda is an open-source container security analysis tool that performs static analysis of container images to detect security issues and vulnerabilities.
4. [**ScoutSuite**](https://github.com/nccgroup/ScoutSuite): ScoutSuite is an open-source multi-cloud security auditing tool that assesses the security posture of containerized infrastructure in public cloud environments.

**Compliance Tools:**

1. [**OpenSCAP**](https://www.open-scap.org/resources/documentation/perform-vulnerability-scan-of-rhel-6-machine/): OpenSCAP is a Security Content Automation Protocol (SCAP) framework for compliance checking, vulnerability management, and measurement.
2. [**OpenVAS**](https://openvas.org/): OpenVAS (Open Vulnerability Assessment System) is a full-featured vulnerability scanner that can detect security vulnerabilities in systems and networks.
3. [**Wazuh**](https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/how-it-works.html): Wazuh is an open-source host-based intrusion detection system (HIDS) that helps with compliance monitoring, file integrity monitoring, and log analysis.

**Dashboard Tools:**

1. [**Grafana**](https://grafana.com/oss/): Grafana is an open-source analytics and monitoring platform that allows you to create customizable dashboards for visualizing various metrics and data sources.
2. [**Kibana**](https://github.com/elastic/kibana): Kibana is an open-source data visualization dashboard for Elasticsearch, used for exploring, analyzing, and visualizing data stored in Elasticsearch indices.
3. [**Metabase**](https://www.metabase.com/start/oss/): Metabase is an easy-to-use open-source business intelligence and analytics tool that allows you to create dashboards and visualize data from various sources.

**Vulnerability Tracking Tools:**

1. [**OWASP DefectDojo**](https://owasp.org/www-project-defectdojo/): DefectDojo is an open-source vulnerability management tool that helps you track and manage vulnerabilities in your applications and infrastructure.
2. [**TheHive**](https://github.com/TheHive-Project/TheHive): TheHive is an open-source incident response and case management platform that includes features for tracking and managing vulnerabilities.

In conclusion, open-source tools play a crucial role in the field of cybersecurity, offering a wide range of solutions for different categories such as Software Composition Analysis (SCA), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Container Security, and Infrastructure Security. These tools provide valuable support in identifying vulnerabilities, assessing security risks, and ensuring compliance.

However, it’s important to note that the landscape of open-source tools is dynamic, and the availability and popularity of specific tools may change over time. Open-source projects rely on community feedback and contributions for maintenance and updates, which means that their support can vary based on community involvement.

Ultimately, while open-source tools offer valuable resources and cost-effective solutions for cybersecurity, it is important to approach their selection and usage with a thorough understanding of their limitations and dependencies on community support.