Security Tools for the DevOps Pipeline-Draft

# Contents

Introduction 1

Security Development Tools 1

Pre-commit Version Control Security Tools 1

Continuous Integration Security Tools 2

Continuous Delivery Security Tools 2

Operation Security tools 3

## Introduction

These are some of the available Open Source security tools for the DevOps pipeline. I have only included the tools that are going to be relevant to the project. I have included both Python and Java for an example. <https://mattboegner.com/secure_cicd_pipeline_2/> This is an interesting article on securing the DevOps pipeline if anybody is interested in reading it.

## Security Development Tools

Mittn: For Python development, allows the developer to create checks based on use cases. Developers can also code check to catch mistakes that they previously made. A security testing tool for CI. <https://github.com/F-Secure/mittn>

BDD-Security: For Java development, works the same way as Mittn. A testing framework used for functional security, infrastructure security and application security testing.

Jasmine: JavaScript

QUnit: JavaScript

### Static and Dynamic code Analysis

SonarQube

OWASP Zap & OWASP Zapper (Jenkins plugin): Allow automating attack proxy to test for possible attacks

## Pre-commit Version control Security

Git-hound: A free security tool to provide automated checks to ensure that no sensitive data is committed into code.

OWASP Threat Dragon: Building security into the design of the application. A threat modeling web application, including system diagramming .

SonarLint: An IDE extension (IntelliJ, Eclipse, Visual Studio). Helps to detect and fix quality issues as the code is written. Bug detection issues are detected and reported, pinpointing the problem, and gives corrective recommendations.

Puma Scan: An IDE extension (Visual Studio) that provides real time continuous source code analysis for C#, .NET. Vulnerabilities are displayed immediately inside the development environment.

## Continuous Integration Security

ESLint: A static code analysis tool. Debugging is done by examining the port without executing the port. A linter tool for identifying and reporting on patterns in JavaScript. Helps to maintain code quality with ease.

Mocha: A JavaScript test framework running on NodeJS and in the browser making asynchronous testing simple and easy. Runs serially allowing for flexible and accurate reporting while mapping uncaught exceptions to the correct test cases.

OWASP Dependency Check: A utility that identifies project dependencies and checks if there are any known publicly disclosed vulnerabilities . A security audit tool with plugins for build-tools, Maven, Jenkins, gradle and Ant-task. It automatically updates itself.

Docker Bench: A script that checks for dozens of common best practices around deploying docker containers in production. Currently supports multiple versions of docker and docker-bench will determine the test set to run based on the docker version on the host machine. It scans the docker environments, start the host level and inspect all the aspects of the host, the docker daemon and its configuration.

### Continuous Delivery Security. (Before, during and after Deployment)

SSLLabs-scan: A command-line scanning tool that doubles as the reference API client of SSL Labs. Security smoke tests. Scans web PKIs. Designed for automated or bulk testing. SSL Labs API exposes the complete SSL/ TLS server testing functionality in a programmatic fashion allowing for scheduled and bulk assessments.

OSQuery: Uses basic SQL commands to leverage a relational data-model to describe a device. Safety checks. When attackers leave a malicious process running but delete the original binary on the disk. This query returns any process whose original binary has been deleted, which could be and indicator of a suspicious process. Under Apache license.

Ansible vault: A feature of Ansible that allows keeping sensitive data in encrypted files. These can then be placed in source code.

Samhain: A host-based intrusion detection system. It provides file integrity checking and log file monitoring/analysis as well as rootkit detection, port monitoring, detection of rogue SUID executables and hidden process. Designed to monitor multiple hosts with potentially different operating systems. It provides centralized logging and maintenance and can be used as a standalone application on a single host.

## Operations Security (Continuous security, monitoring, testing, audit and compliance checks)

Chaos Monkey: It injects faults to randomly terminate virtual machine and container instances that run inside a production environment. Exposing engineers to failures more frequently in order to help them build more resilient services.

Open SCAP: An ecosystem which provides multiple tools to assist administrators and auditors with assessment, measurement and enforcement of security baselines. Provides a wide variety of hardening guides and configuration baseline. Enabling you to choose a security policy that best suits the needs of your organisation.

Grafana: A metric analytics and visualization suite for continuous monitoring. Used for time series data for infrastructure and application analytics. It allows to query, visualise, alert and understand the matrices no matter where they are stored. It creates an explore and share dashboard with your schemas.

ElastAlert: A tool for continuous monitoring. A simple framework for alerting on anomalies , inconsistencies, spikes or other patterns of interest from data in Elasticsearch. It works by combining Elasticsearch with two types of components, rule types and alerts. Elasticsearch is periodically queried and the data is passed to the rule type, which determines when a match is found. When a match occurs, it is given to one or more alerts, which take action based on the match. This is configured by a set of rules, each of which defines a query, a rule type and a set of alerts.