

# Explore OWASP ZAP penetration test

2 minutes

ZAP is a free penetration testing tool for beginners to professionals. ZAP includes an API and a weekly docker container image to integrate into your deployment process.

Refer to the [OSWA ZAP VSTS Extension](#) repo for details on setting up the integration. Here we're going to explain the benefits of including it in your process.

The application CI/CD pipeline should run within a few minutes, so you don't want to include any long-running processes.

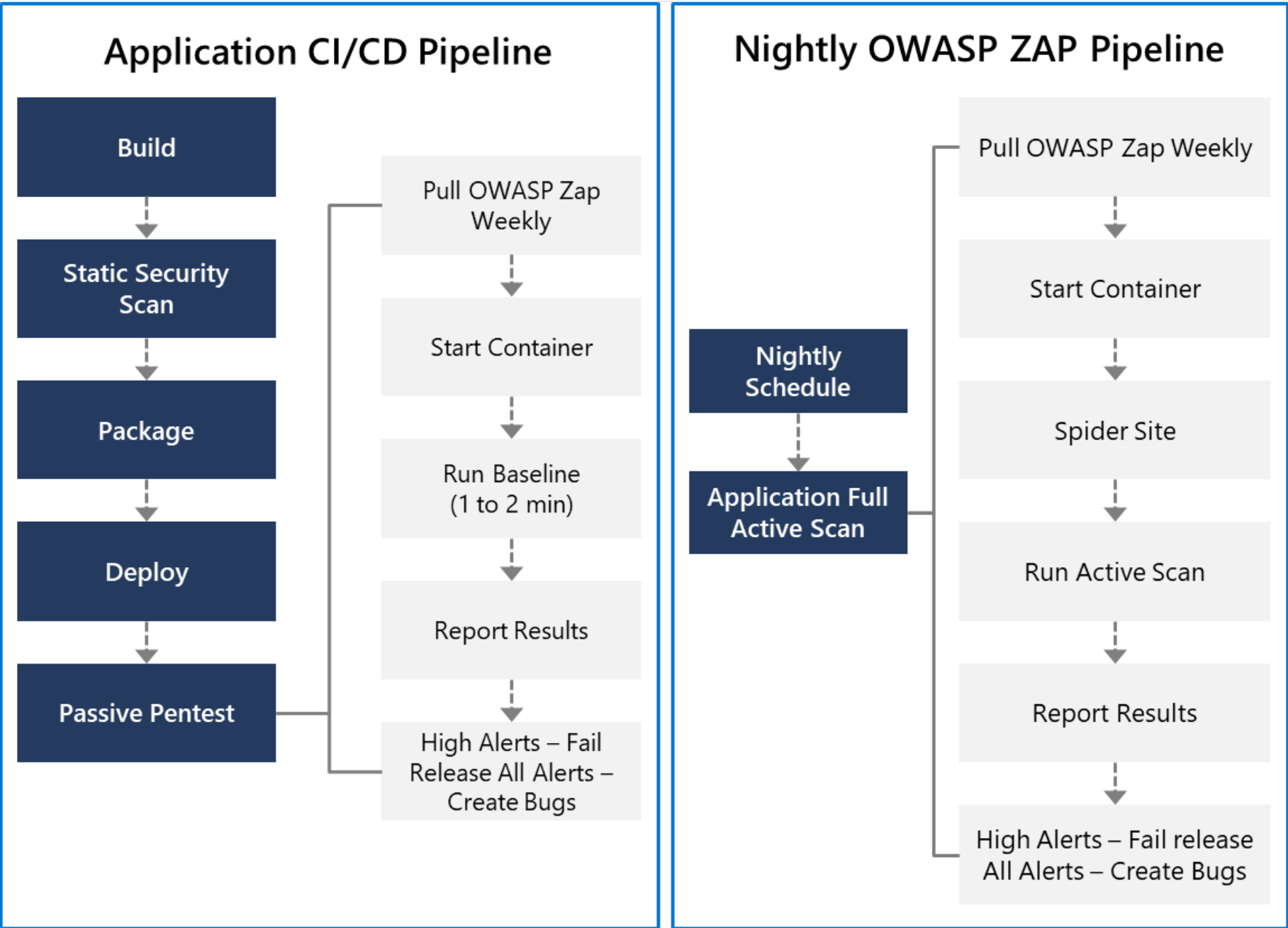
The baseline scan is designed to identify vulnerabilities within a couple of minutes, making it a good option for the application CI/CD pipeline.

The Nightly OWASP ZAP can spider the website and run the full-Active Scan to evaluate the most combinations of possible vulnerabilities.

OWASP ZAP can be installed on any machine in your network, but we like to use the OWASP Zap/Weekly docker container within Azure Container Services.

It allows for the latest updates to the image. It will enable the spin-up of multiple image instances so several applications within an enterprise can be scanned simultaneously.

The following figure outlines the steps for the Application CI/CD pipeline and the longer-running Nightly OWASP ZAP pipeline.



Next unit: Explore OWASP ZAP results and bugs

Continue >