

OpenSCAP

The **OpenSCAP wodle** is an integration of [OpenSCAP](#) with *Wazuh HIDS* that provides the ability to perform configuration and vulnerability scans of an agent. It is primarily used for:

- Verifying **security compliance**: OpenSCAP policies define the requirements that all systems in an organization must meet in order to be in line with applicable *security policies* and/or *security benchmarks*.
- Performing **vulnerability assessments**: OpenSCAP identifies and classifies vulnerabilities in a system.
- Performing **specialized assessments**: OpenSCAP can perform specific custom system checks (i.e., checking for suspicious file names and suspicious file locations.)

- [How it works](#)
 - [Requirements](#)
 - [Default policies](#)
 - [Wodle flow](#)
- [Configuration](#)
 - [Basic usage](#)
 - [Evaluate PCI-DSS compliance on RHEL7](#)
 - [Auditing Security Vulnerabilities of Red Hat Products](#)
 - [Overwriting the timeout](#)
 - [Using profiles](#)
 - [Using CPE dictionary](#)
 - [Using IDs](#)
- [FAQ](#)
 - [Is there a noticeable performance impact when the OpenSCAP wodle is enabled on an agent?](#)
 - [Are evaluations executed in parallel?](#)
 - [How does the interval work?](#)
 - [Are the policies evaluated when OSSEC starts?](#)
 - [Where are the policies?](#)

