Ruleset

This documentation explains how to install, update, and contribute to Wazuh Ruleset. These rules are used by the system to detect attacks, intrusions, software misuse, configuration problems, application errors, malware, rootkits, system anomalies or security policy violations. OSSEC provides an out-of-the-box set of rules that we update and augment, in order to increase Wazuh detection capabilities.

Contents