

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

- [Getting started](#)
 - [GitHub repository](#)
 - [Directory layout](#)
- [Update ruleset](#)
 - [Usage examples](#)
 - [Configure weekly updates](#)
- [Custom rules and decoders](#)
 - [Adding new decoders and rules](#)
 - [Changing an existing rule](#)
 - [Changing an existing decoder](#)
- [Dynamic fields](#)
 - [Traditional decoders](#)
 - [Dynamic decoders](#)
- [Ruleset XML syntax](#)
 - [Decoders Syntax](#)
 - [Rules Syntax](#)
 - [Regular Expression Syntax](#)
- [Testing decoders and rules](#)
- [Using CDB lists](#)
 - [Creating a CDB list](#)
 - [Using the CDB list in the rules](#)
- [Contribute to the ruleset](#)

