Getting started

The default number of rules and decoders is limited. For this reason, we centralize, test and maintain decoders and rules submitted by open source contributors. We also create new rules and rootchecks periodically and add them to this repository so they can be used by the user community. Some examples are the new rules for Netscaler and Puppet.

GitHub repository

In the ruleset repository you will find:

- **New rules, decoders and rootchecks**

  We update and maintain the out-of-the-box rules provided by OSSEC, both to eliminate false positives and to increase accuracy. In addition, we map the rules to PCI-DSS compliance controls, making it easy to identify when an alert is related to a specific compliance requirement.

- **Tools**

  We provide some useful tools for testing.

Resources

- Visit our repository to view the rules in detail at Github Wazuh Ruleset
- Find a complete description of the available rules at Wazuh Ruleset Summary

Rule and Rootcheck example

Log analysis rule for Netscaler with PCI DSS compliance mapping:

```
<rule id="80102" level="10" frequency="6">
    <if_matched_sid>80101</if_matched_sid>
    <same_source_ip />
    <description>Netscaler: Multiple AAA failed to login the user</description>
    <group>authentication_failures,netscaler-aaa,pci_dss_10.2.4,pci_dss_10.2.5,pci_dss_11.4,</group>
</rule>
```

Rootcheck rule for SSH Server with mapping to CIS security benchmark and PCI DSS compliance:

```
[CIS - Debian Linux - 2.3 - SSH Configuration - Empty passwords permitted {CIS: 2.3 Debian Linux} {PCI_DSS:
4.1}] [any] [http://www.ossec.net/wiki/index.php/CIS_DebianLinux]
f:/etc/ssh/sshd_config -> !r:^# && r:^PermitEmptyPasswords\.+yes;
```

Directory layout

The ruleset folder structure is shown below:

```
/var/ossec/
        ├─ etc/
        |   ├─ decoders/
        |   |        └─ local_decoder.xml
        |   └─ rules/
        |          └─ local_rules.xml
        └─ ruleset/
               ├─ decoders/
               └─ rules/
```

Inside the `ruleset/` folder you will find all the common rules and decoders. All files inside this folder **will be overwritten** or modified in the Wazuh update process, so please do not edit files or add custom files in this folder.

If we need to perform some custom changes, we will use the `etc/` folder. You can add here your own decoders/rules files or use the default `local_decoder.xml` and `local_rules.xml` files.