Documentation › User manual › Capabilities › Anomaly and malware detection › Configuration

Configuration

Basic example

To configure the options for syscheck and rootcheck go to ossec.conf. If you want more information about the exact configuration options go to Syscheck section and Rootcheck section. Also see the following sections: frequency, rootkit_files, rootkit_trojans

A basic example to configure the database for rootkits (files and trojans):

```
<rootcheck>
  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
</rootcheck>
```

Ignoring false positives

```
<rule id="100100" level="0">
    <if_group>rootcheck</if_group>
    <match>/dev/.blkid.tab</match>
    <description>Ignore false positive for /dev/.blkid.tab</description>
</rule>
```