

# Anomaly and malware detection

Anomaly detection refers to the action of finding patterns in the system that do not match the expected behavior. Once malware (e.g., a rootkit) is installed on a system, it modifies the system to be hidden from the user. Although malware uses a variety of techniques for this purpose, Wazuh uses a broad spectrum approach to finding anomalous patterns that indicate possible intruders.

The main component responsible for this task is *rootcheck*. *Syscheck* also plays an important role.

## Contents

- [How it works](#)
  - [File integrity monitoring](#)
  - [Check running processes](#)
  - [Check hidden ports](#)
  - [Check unusual files and permissions](#)
  - [Check hidden files using system calls](#)
  - [Scan the \*/dev\* directory](#)
  - [Scan network interfaces](#)
  - [Rootkit checks](#)
- [Configuration](#)
  - [Basic example](#)
  - [Ignoring false positives](#)
- [FAQ](#)
  - [How often does rootcheck run?](#)
  - [How does rootcheck know the rootkit files to look for?](#)
  - [Does rootcheck inspect running processes?](#)
  - [What about hidden files?](#)

