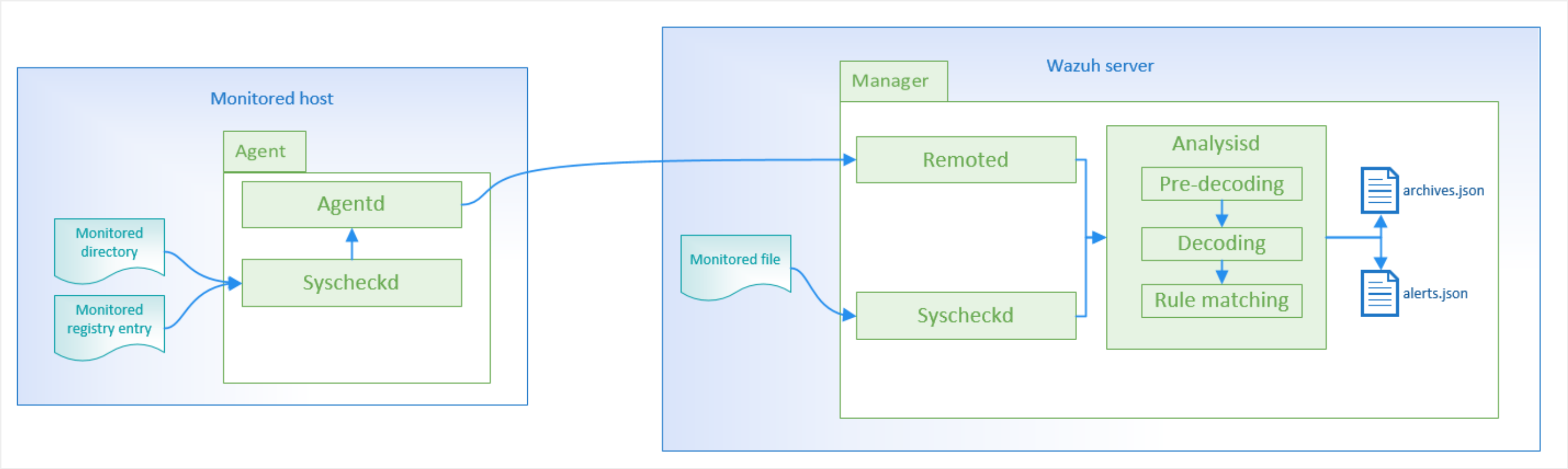
How it works



1. Wazuh agent scans the system and sends the checksums and attributes of the monitored files and Windows registry keys to the Wazuh manager. We can configure:

- **Frequency**: By default, syscheck runs every 6 hours, but this is entirely configurable.
- **Real-time monitoring**: Wazuh supports real-time file integrity monitoring on servers running Windows or Linux. Note that that the real-time option is only configurable for directories, not for single files.

2. Wazuh manager stores the checksums/attributes and looks for modifications by comparing the new values to the old values. It's possible to configure syscheck to report a diff summary of the actual changes made to text files.
3. An alert is generated if changes are detected on monitored files and/or registry keys.

It's possible to handle false positives using configuration options like `ignore`. You can also create rules that profile files that are to be excluded from FIM alerts.

Alert example, generated by **syscheck**:

```
** Alert 1460948255.25442: mail  - ossec,syscheck,pci_dss_11.5,
2016 Apr 17 19:57:35 (ubuntu) 10.0.0.144->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
Integrity checksum changed for: '/test/hello'
Size changed from '12' to '17'
Old md5sum was: 'e59ff97941044f85df5297e1c302d260'
New md5sum is : '7947eba5d9cc58d440fb06912e302949'
Old sha1sum was: '648a6a6ffffdaa0badb23b8baf90b6168dd16b3a'
New sha1sum is : '379b74ac9b2d2b09ff6ad7fa876c79f914a755e1'
```