Capabilities

This section explain more in detail how each capability works, how can be configured, frequently asked questions and some examples that allow a better understanding of all the features. If you find a problem, error or if you want to ask related questions please let us know on our mailing list.

The capabilities are:

- Log data collection
  - How it works
  - Configuration
  - FAQ

- File integrity monitoring
  - How it works
  - Configuration
  - FAQ

- Anomaly and malware detection
  - How it works
  - Configuration
  - FAQ

- Monitoring security policies
  - Rootcheck
  - OpenSCAP

- Monitoring system calls
  - How it works
  - Configuration

- Command monitoring
  - How it works
  - Configuration
  - FAQ

- Active response
  - How it works
  - Configuration
  - FAQ

- Agentless monitoring
  - How it works
  - Configuration
  - FAQ

- Anti-flooding mechanism
  - Why it is an anti-flooding mechanism needed?
  - How it works: Leaky bucket
  - Use case: Leaky bucket
  - Anti-flooding in agent modules

- Agent labels
  - How it works
  - Use case