Ionx Verisys® Console and Agents

File Integrity Monitoring System

Overview

http://www.ionx.co.uk

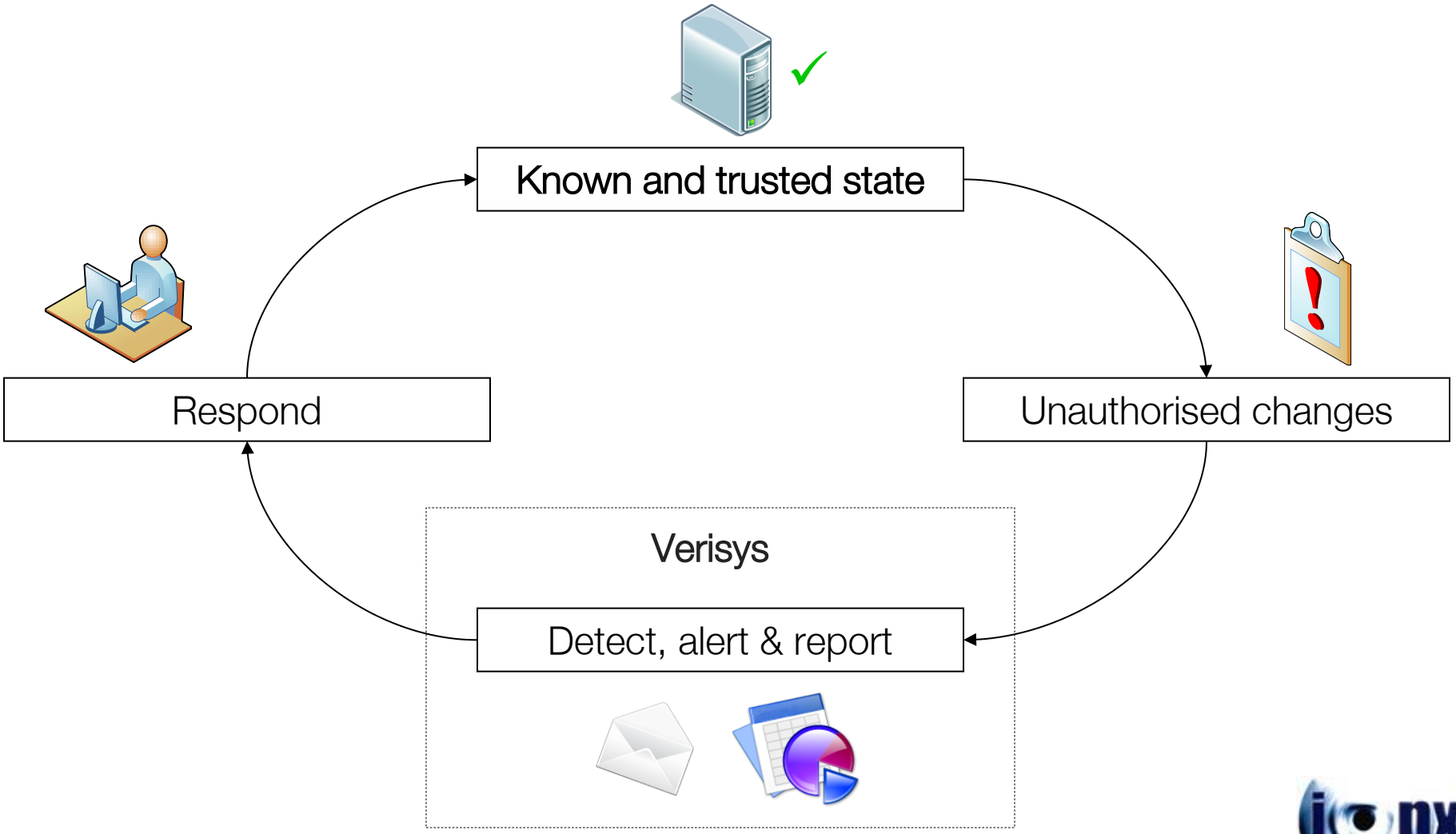
What is Verisys?

- File integrity monitoring software
  - Detects unauthorised changes to files and Windows registry objects
  - Allows you to maintain integrity of data, ensuring your systems are in a known and trusted state
  - Sends alerts when discrepancies are detected, allowing a rapid response
  - Includes reporting tools
  - Agents available for Windows and Linux systems

Main Usage Scenarios

- Enhance security
  - Good business practice as part of a comprehensive data security policy
  - Detect unauthorised changes
  - Allow rapid response
- PCI DSS (Payment Card Industry Data Security Standard) Compliance
  - Use of file integrity monitoring software is mandated by the PCI DSS to satisfy requirement 10.5.5 and 11.5
- SOX (Sarbanes-Oxley) Compliance
  - Must be able to demonstrate that your systems remain in a known and trusted state
- Change auditing
  - Provide an audit trail of what was changed, and when
  - Detect changes made outside of formal change/maintenance windows

How it Works


Known and trusted state
Unauthorised changes
Respond
Verisys
Detect, alert & report

How it Works

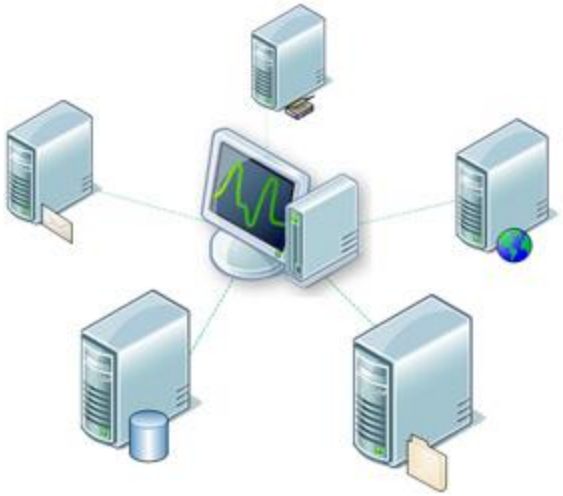
- Takes baseline snapshot of current system state
- Periodically compares current system state to stored baseline and detects any changes
- Checks a number of properties, as well as performing a complex cryptographic hashing algorithm on the actual data
  - Object name
  - Creation time
  - Last modified time
  - Last accessed time
  - Index node
  - Size
  - Flags
  - CRC-32
  - SHA-256 hash
  - Symlink target
  - Owner
  - Primary group
  - Access permissions
  - Audit rules
  - Extended attributes
- If files are altered in any way, Verisys will detect it

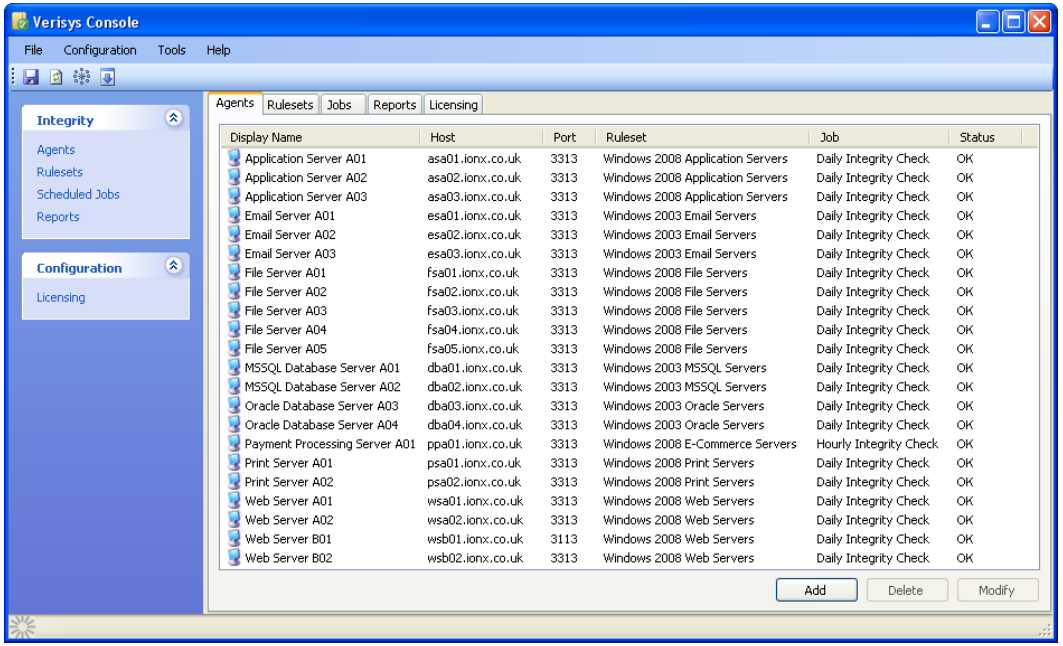
Key Features

- Detects unauthorised changes
- Meets PCI DSS requirements 10.5.5 & 11.5
- Centralised administration
- Schedule automated integrity checks
- Wide range of alerting options
- Comprehensive reporting tools
- Templates for common system configurations

Centralised Administration

- Manage many file integrity monitoring Agents from a single, central location
- Simplifies management of large or distributed deployments
- Easy to use GUI





Automated Alerting

- Send email
- Windows event log
- Syslog
- Save discrepancy report
- Execute any command