ISSA
Information Systems Security Association
Middle Tennessee
INFOSEC
NASHVILLE

INFOSEC NASHVILLE 2024

Cybersecurity Crossroads: Securing the Intersection of Innovation and Tradition

September 12th, 2024

Wazuh, Wazoo, Whatever.

Learning how to design and build XDR with Open Source Tools

Share your thoughts/ photos on LinkedIn!

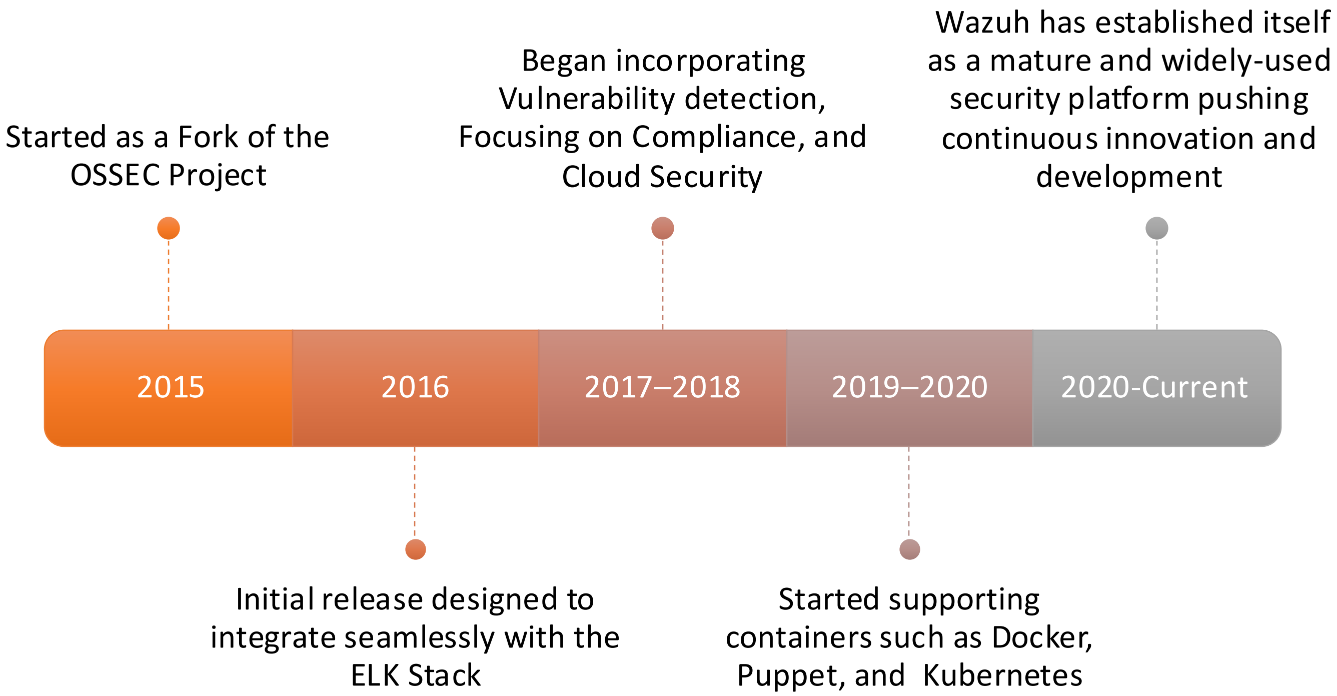
#InfoSec2024

Kyle Goode
System Security Engineer – Acadia Healthcare

Why Wazuh?

- Open Source
- Compliance Focused(GDPR, HIPPA,PCI)
- Affordable Cloud Coverage
- Extremely Customizable
- Ridiculously scalable
- Active Community and Paid Support options
- Active Response
- Extensive Integration Options
- Super Lightweight
- User Friendly

The History of Wazuh



2015

Started as a Fork of the OSSEC Project

2016

Initial release designed to integrate seamlessly with the ELK Stack

2017–2018

Began incorporating Vulnerability detection, Focusing on Compliance, and Cloud Security

2019–2020

Started supporting containers such as Docker, Puppet, and Kubernetes

2020-Current

Wazuh has established itself as a mature and widely-used security platform pushing continuous innovation and development

Who Uses Wazuh?

Walgreens

THE HOME DEPOT

CISCO

salesforce

NASA

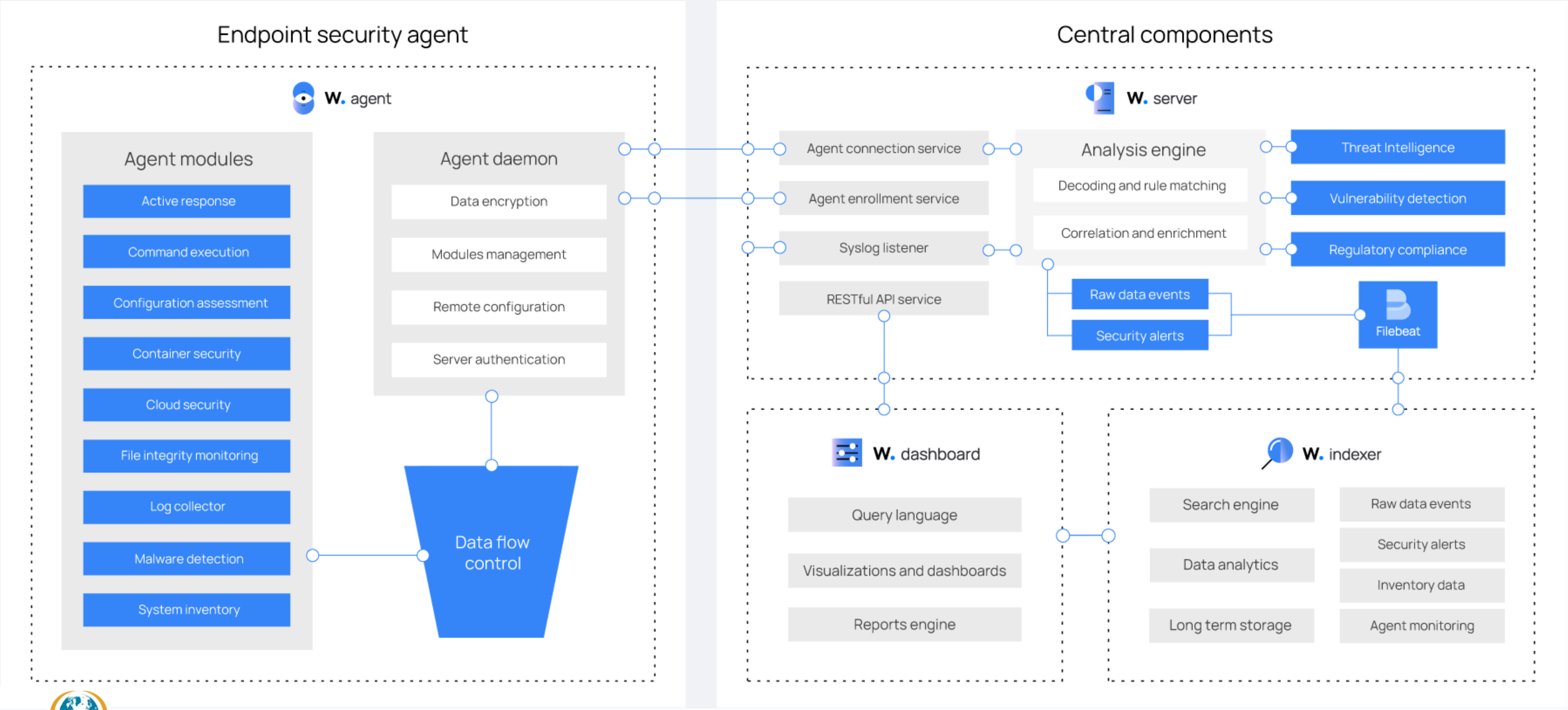
INTUIT

Endpoint and Cloud **Workload Protection**

How does it work?

- Wazuh Indexer
- Wazuh Dashboard
- Wazuh Server
- Wazuh agent

Components and data flow



How Can I Build it?

- Physical Install on Linux Servers
- Prebuilt Virtual Box VM
- Containers(Docker, Puppet, Kubernetes)
- Cloud(Saas Provided, AWS AMI, Cloud Provider of your choice)

What Can It Monitor?

- Operating Systems(EDR)
- Network Devices(NDR)
- Identity Monitioring(IDR)
- Web Servers
- Application Servers
- Web Applications
- Databases
- Cloud Environments
- Containers

What Agents Can Run on IT?

Linux(Debian/Ubuntu,RHEL,SLES, Rocky,Alpine,Fedora,Amazon)

Macos

Windows + Windows Servers

Unix(FreeBSD, Solaris, HP-UX, AIX)

Full Arm,arm64, x86_64 support

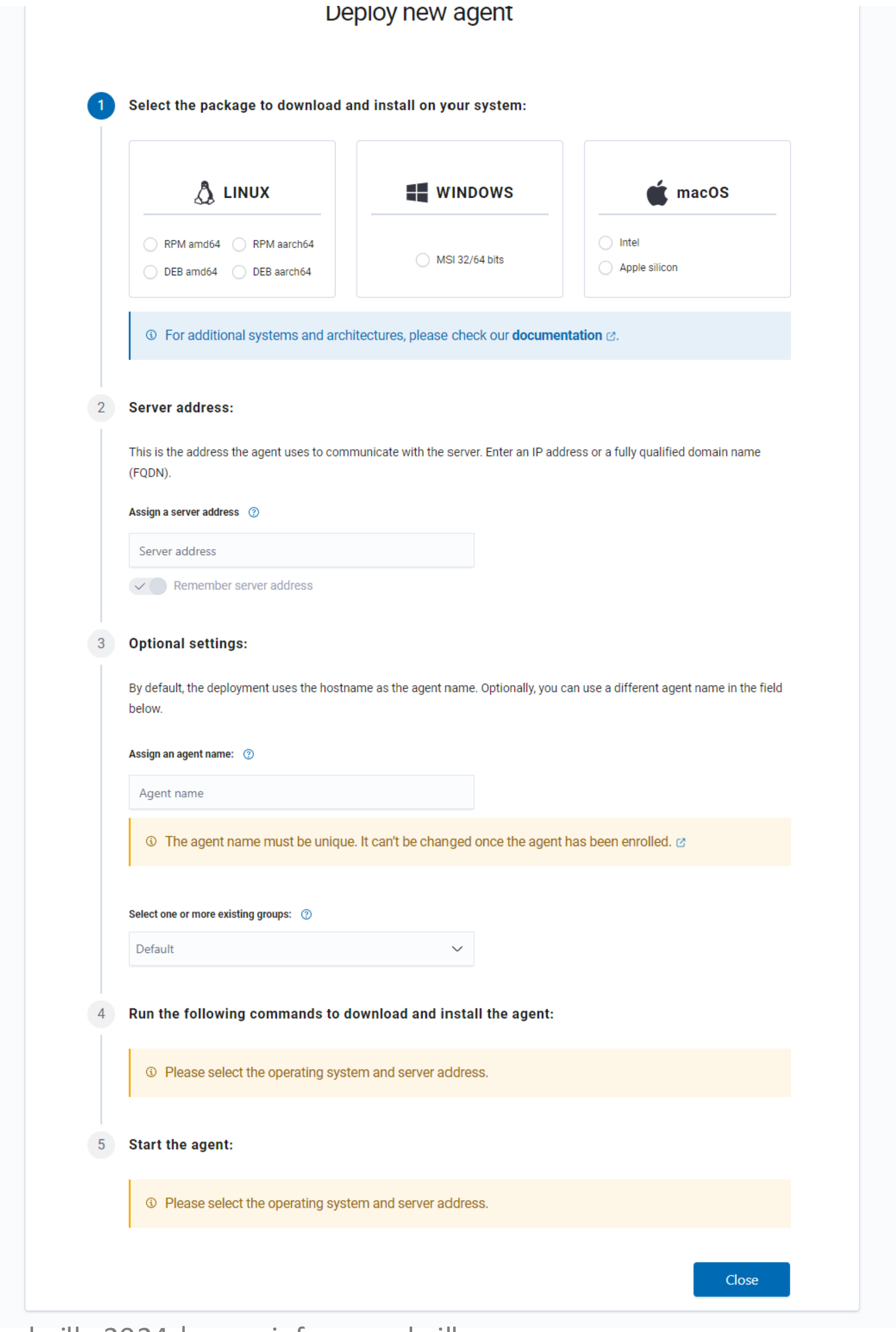
How Do I Enroll Agents?

Agent Configuratior

Manger API

Agent Configuratior

- Simple Plug and play
- Step by Step Instructions
- Templates for all agent types



Deploy new agent

1 Select the package to download and install on your system:

LINUX
○ RPM amd64 ○ RPM aarch64
○ DEB amd64 ○ DEB aarch64

WINDOWS
○ MSI 32/64 bits

macOS
○ Intel
○ Apple silicon

ⓘ For additional systems and architectures, please check our **documentation**.

2 Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

Server address

Remember server address

3 Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

Agent name

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default

4 Run the following commands to download and install the agent:

ⓘ Please select the operating system and server address.

5 Start the agent:

ⓘ Please select the operating system and server address.

Wazuh API

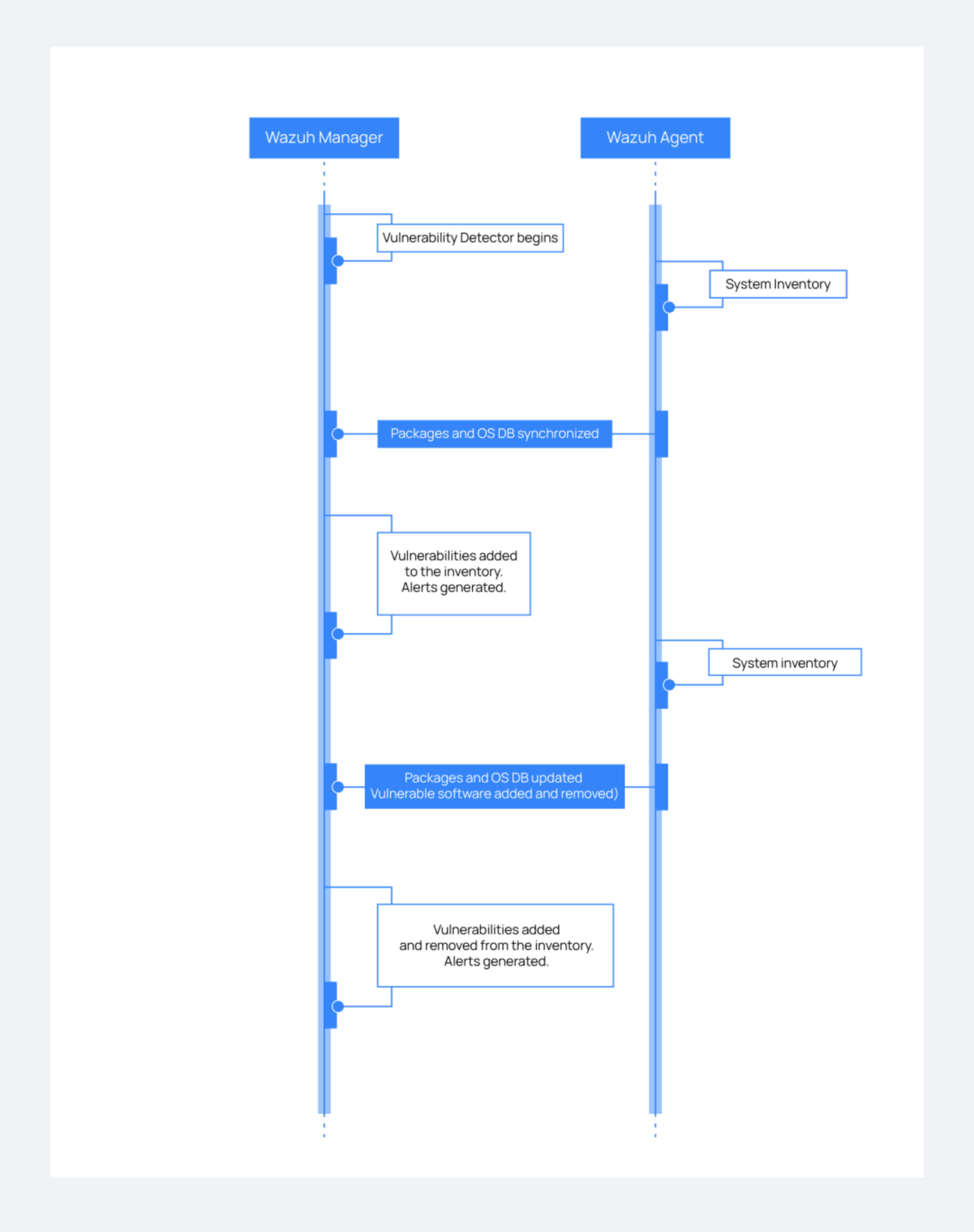
REST BASED

BUILT FOR LARGE SCALE DEPLOYMENTS

WELL DOCUMENTED

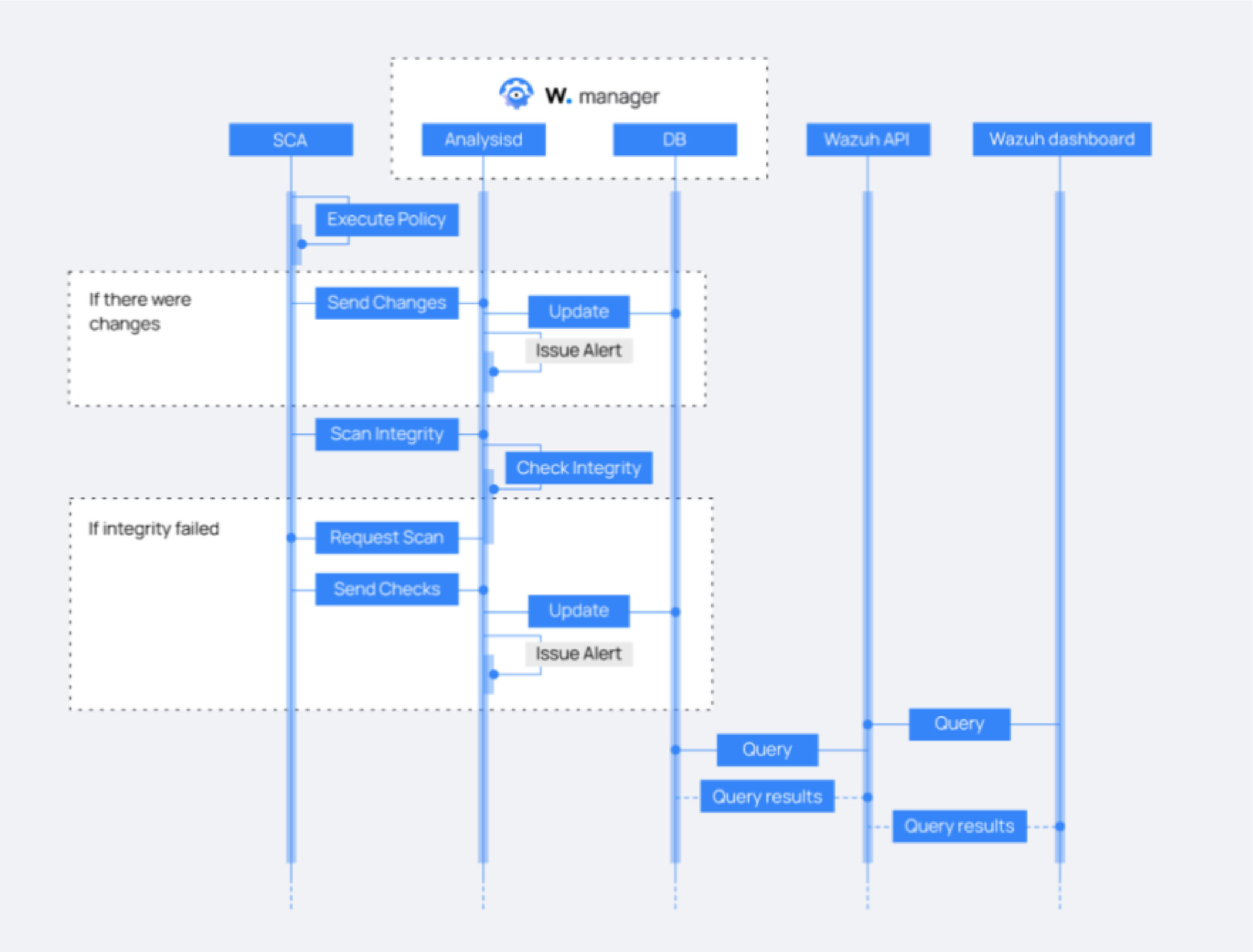
Vulnerability detection

- NVD
- Canonical
- Red Hat
- Debian
- Microsoft
- ALAS
- AlmaLinux
- SUSE
- ARCH

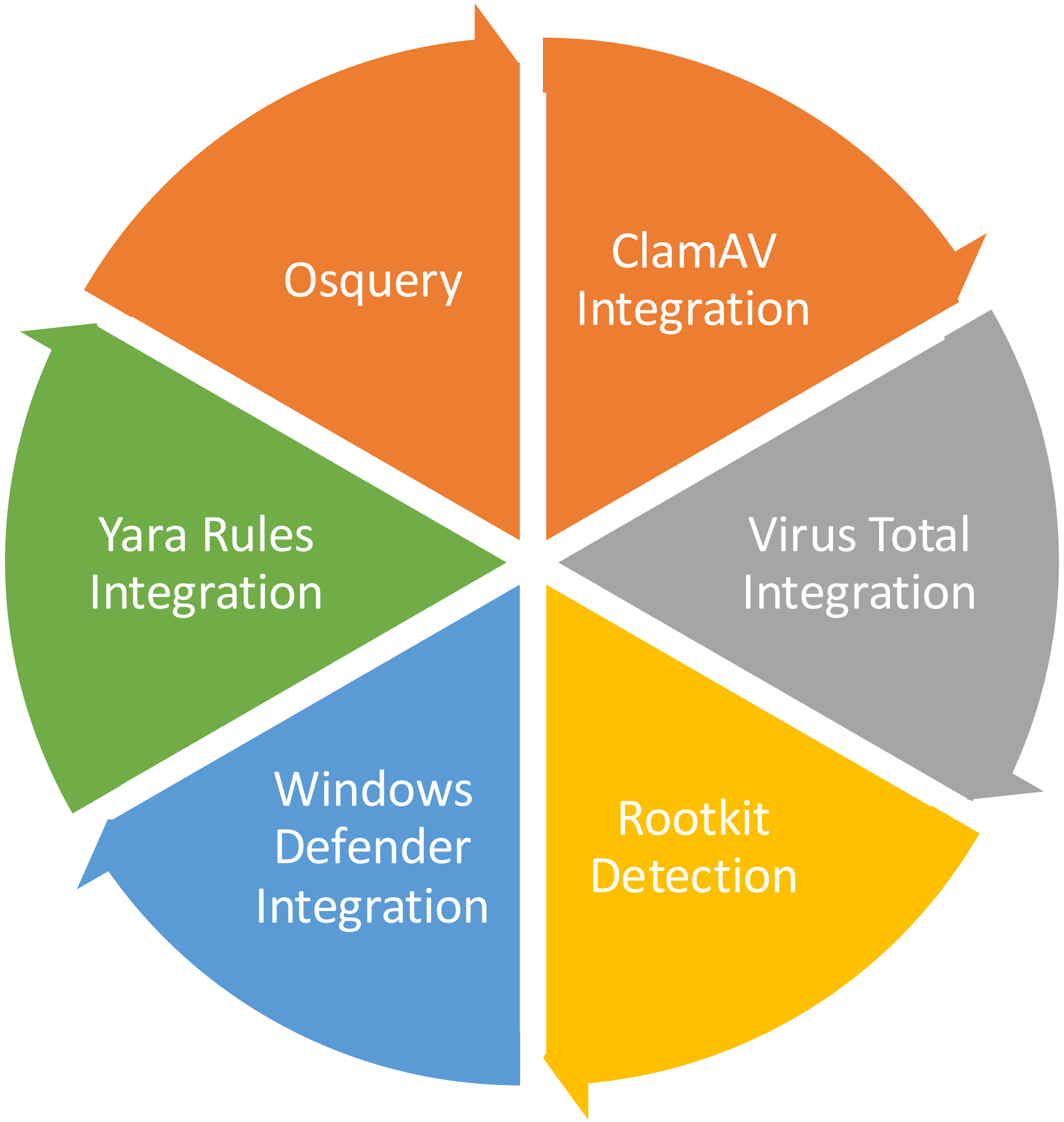

Wazuh Manager
Wazuh Agent
Vulnerability Detector begins
System Inventory
Packages and OS DB synchronized
Vulnerabilities added to the inventory. Alerts generated.
System inventory
Packages and OS DB updated Vulnerable software added and removed)
Vulnerabilities added and removed from the inventory. Alerts generated.

Security Configuration Assessments

CIS Benchmarks™

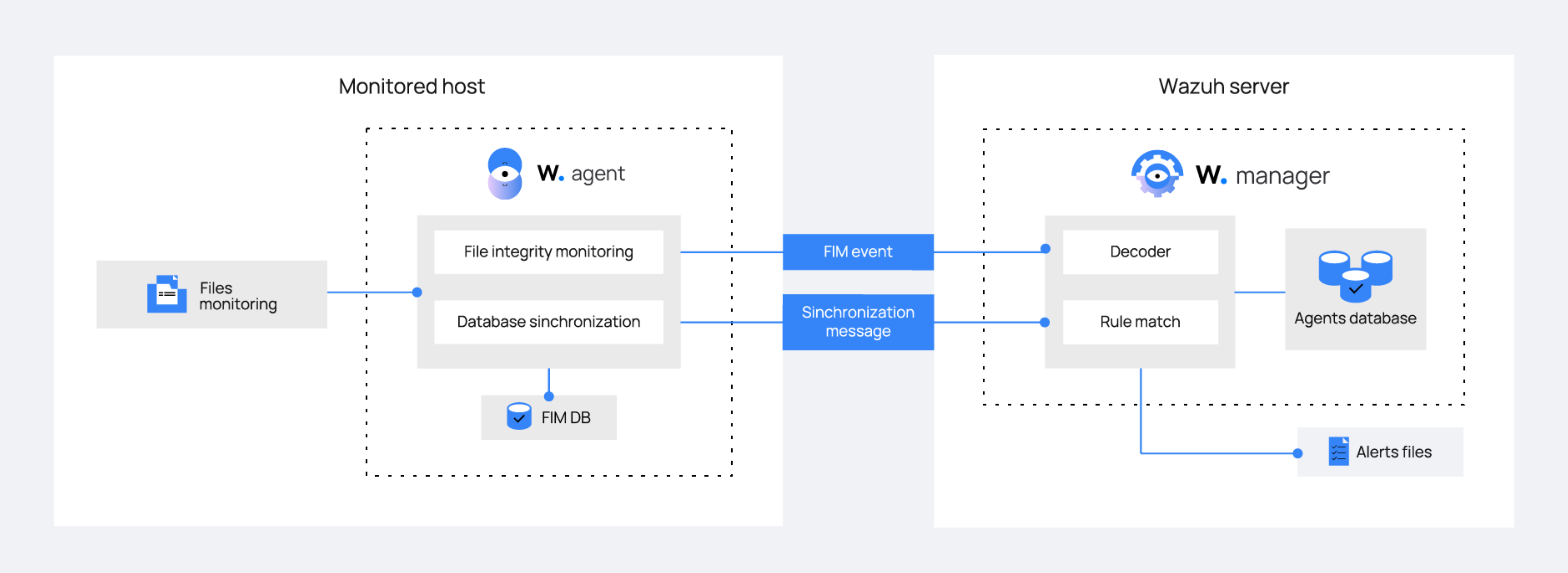


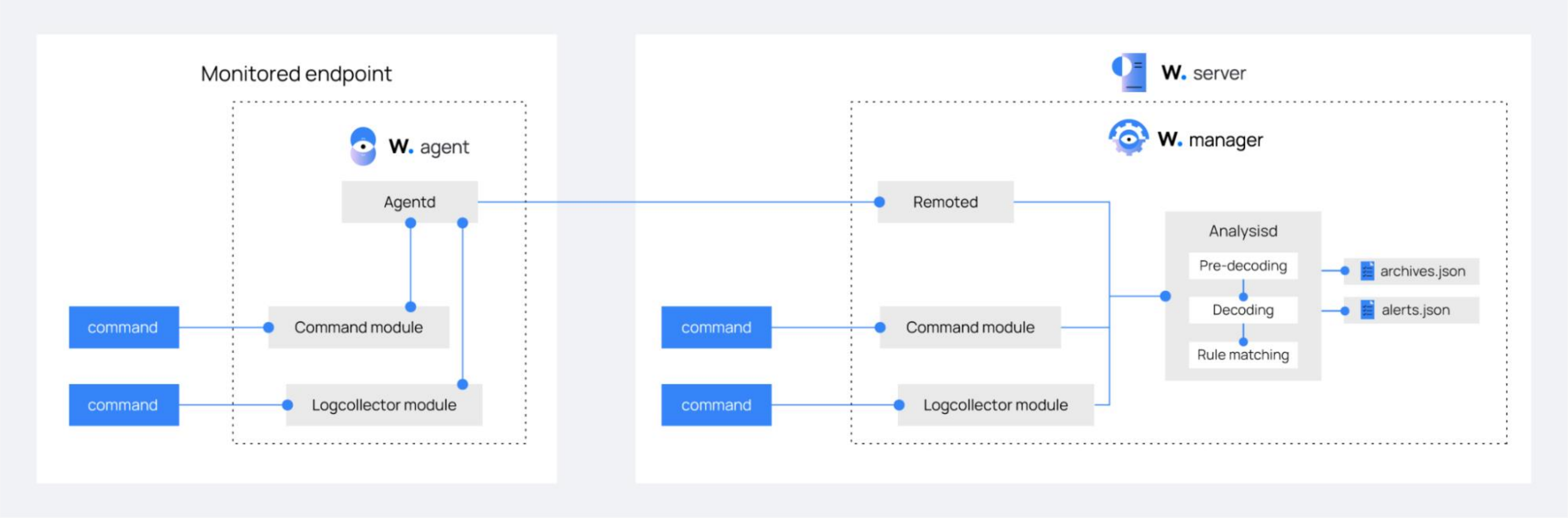
Malware Detection



File Integrity Monitoring

Real time change monitoring





Command Monitoring

Decoders and Rules

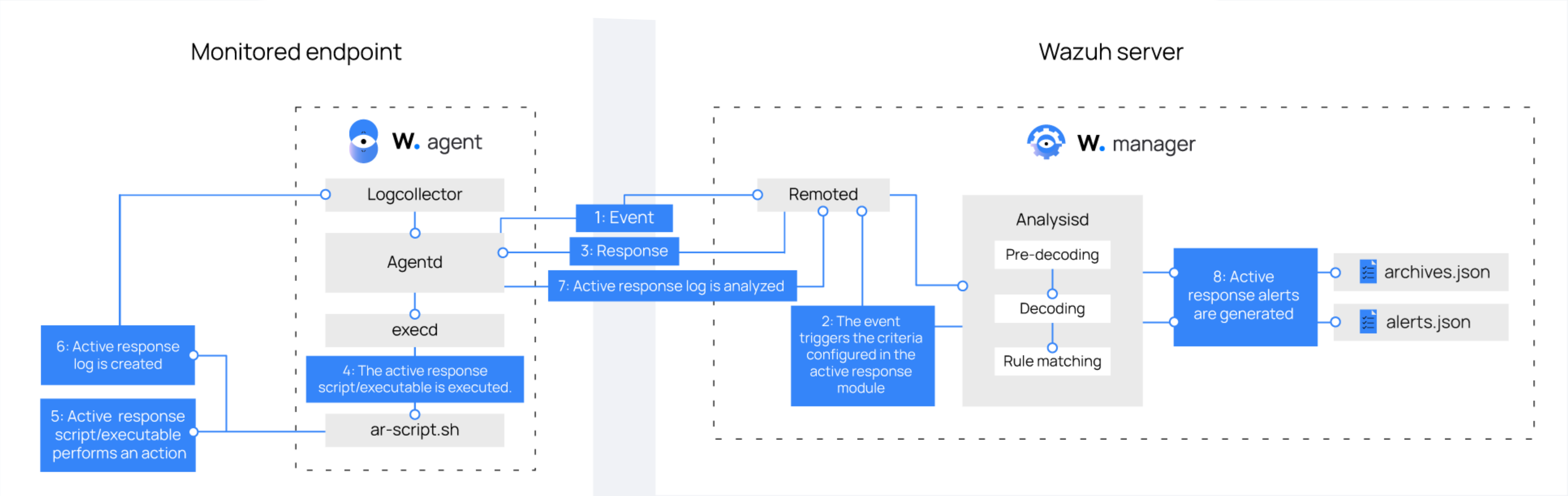
DECODERS = PRETTY LOGS

RULES = ALERTS

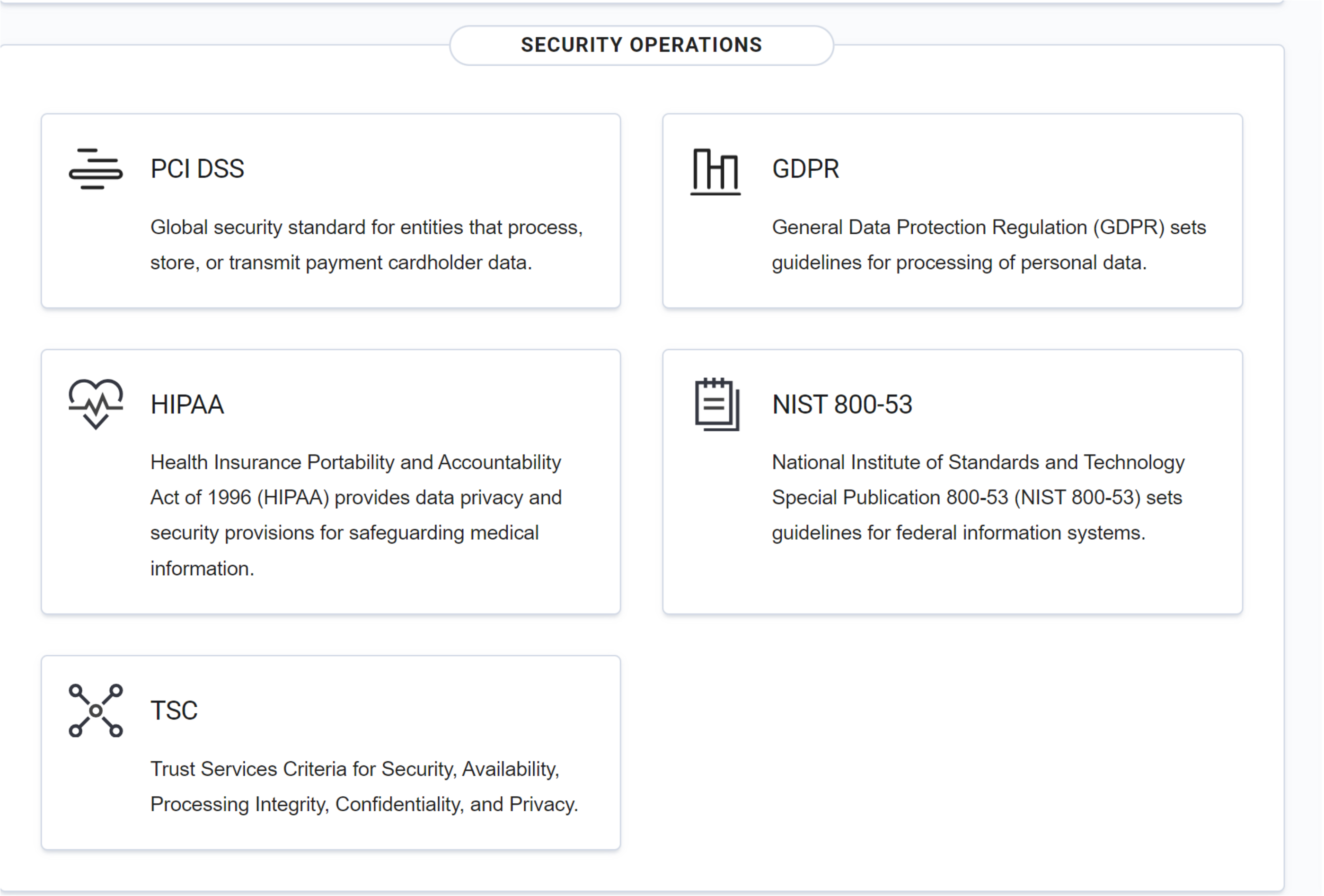
EXTENSIVE SUPPORT FOR POPULAR LOG SOURCES

Active Response

- Automated Threat Mitigation
- Real-Time Response
- Predefined Actions
- Custom scripts


Monitored endpoint
Wazuh server
W. agent
Logcollector
Agentd
execd
ar-script.sh
1: Event
3: Response
7: Active response log is analyzed
4: The active response script/executable is executed.
5: Active response script/executable performs an action
6: Active response log is created
W. manager
Remoted
2: The event triggers the criteria configured in the active response module
Analysisd
Pre-decoding
Decoding
Rule matching
8: Active response alerts are generated
archives.json
alerts.json

Compliance



SECURITY OPERATIONS

PCI DSS

Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

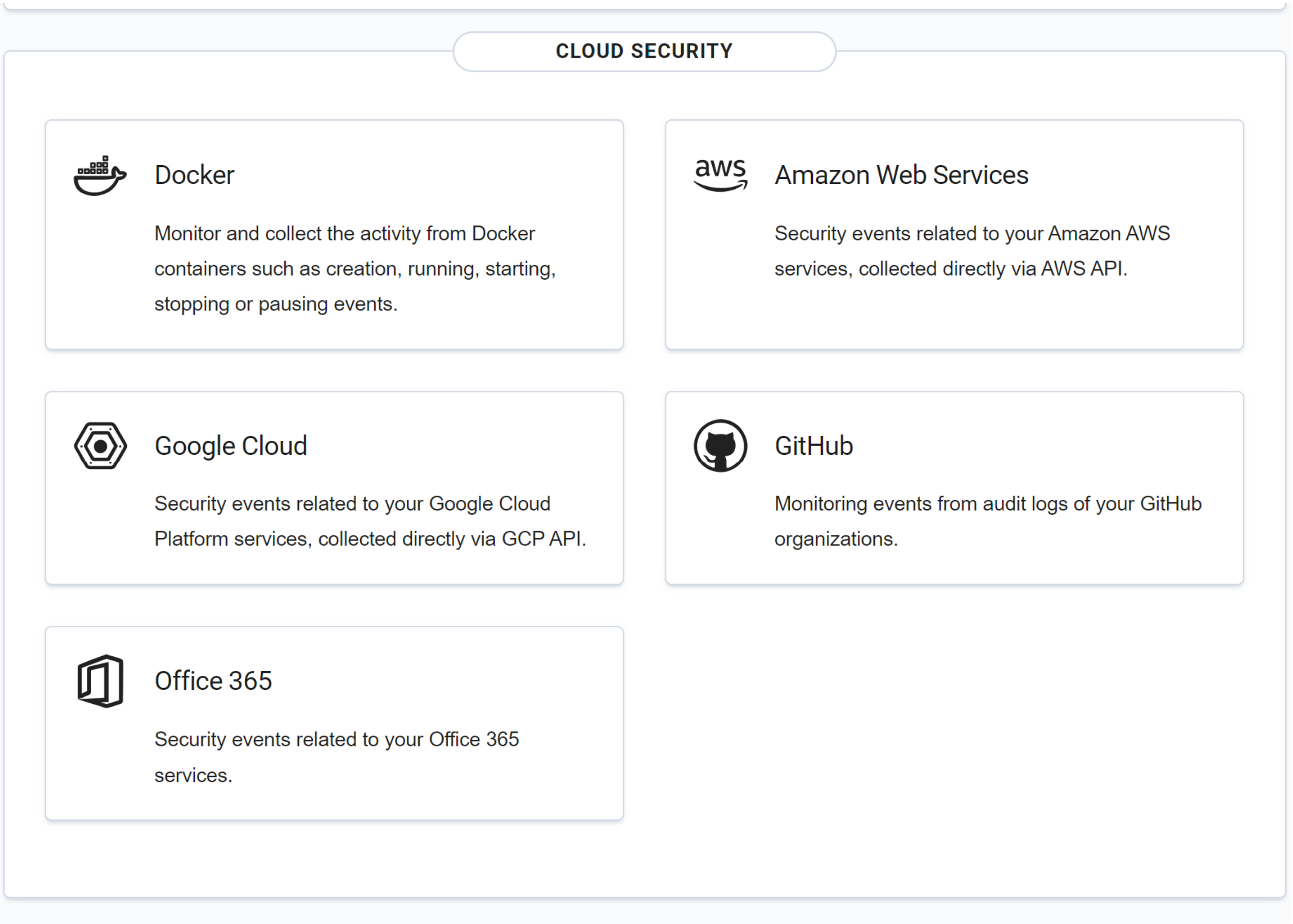
NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

TSC

Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Cloud Security



CLOUD SECURITY

Docker

Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services

Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud

Security events related to your Google Cloud Platform services, collected directly via GCP API.

GitHub

Monitoring events from audit logs of your GitHub organizations.

Office 365

Security events related to your Office 365 services.

Integrations

VIRUSTOTAL

osquery

maltiverse

SURICATA

zeek®

ATT&CK®

SHUFFLE

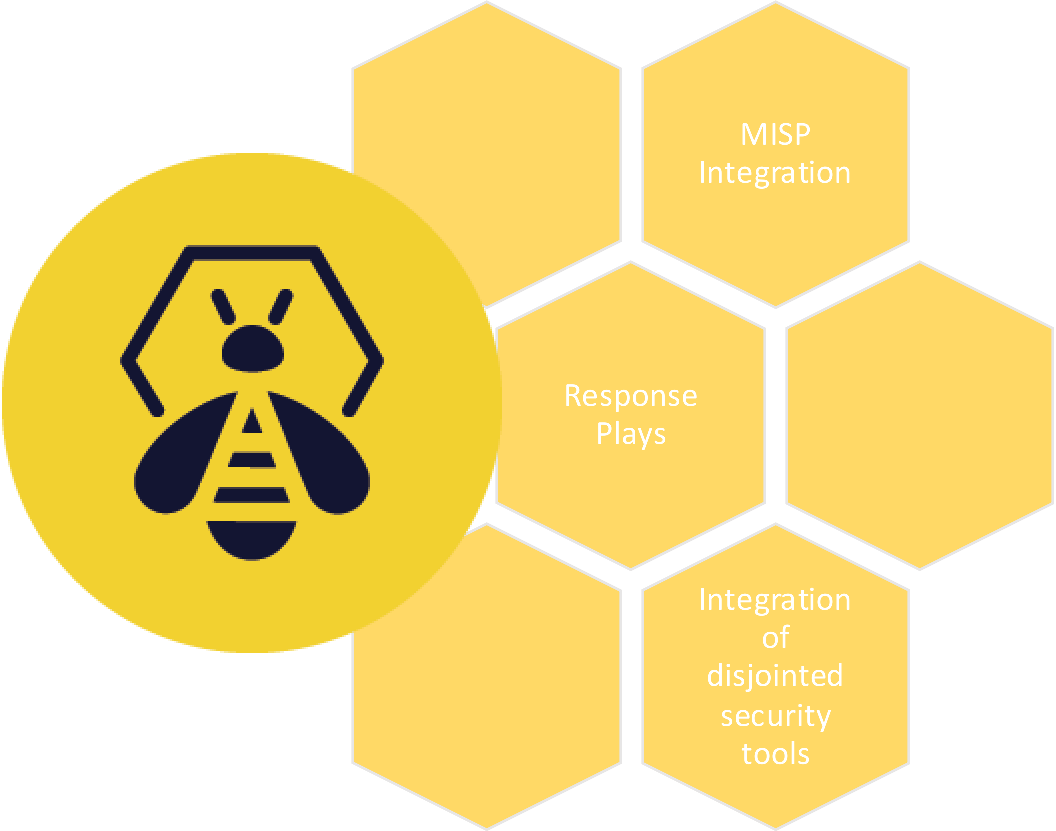
PAGERDUTY

ClamAV

Fleet DM

- Open source mdm and osquery orchestrator
- Osquery defense kit

The Hive/Cortex



MISP Integration

Response Plays

Integration of disjointed security tools

Resources

Wazuh Documentation

Wazuh Blog

OxBEN

Taylor Walton – Socfortress

Thank You

Kyle Goode