Infopercept

INVINSENSE | OODA

Setting the Context

To survive the ever-increasing cyber threats, businesses need to be able to detect and respond to security incidents in a timely and responsive manner. Businesses suffer huge financial and reputation loss due to the inability to do so.

The question is how one can do that in a strategic manner and implement that in a tactical manner within an organization. The answer to that question is to put in an integrated platform that considers Strategy, Services and Solutions all under one approach. Then, what are the key considerations when implementing such an approach.

An Integrated platform shall need to address the following key considerations through the end-to-end cycle:

At Infopercept, we address this requirement through **OODA** (Observe; Orient; Decide and Act) Strategy.

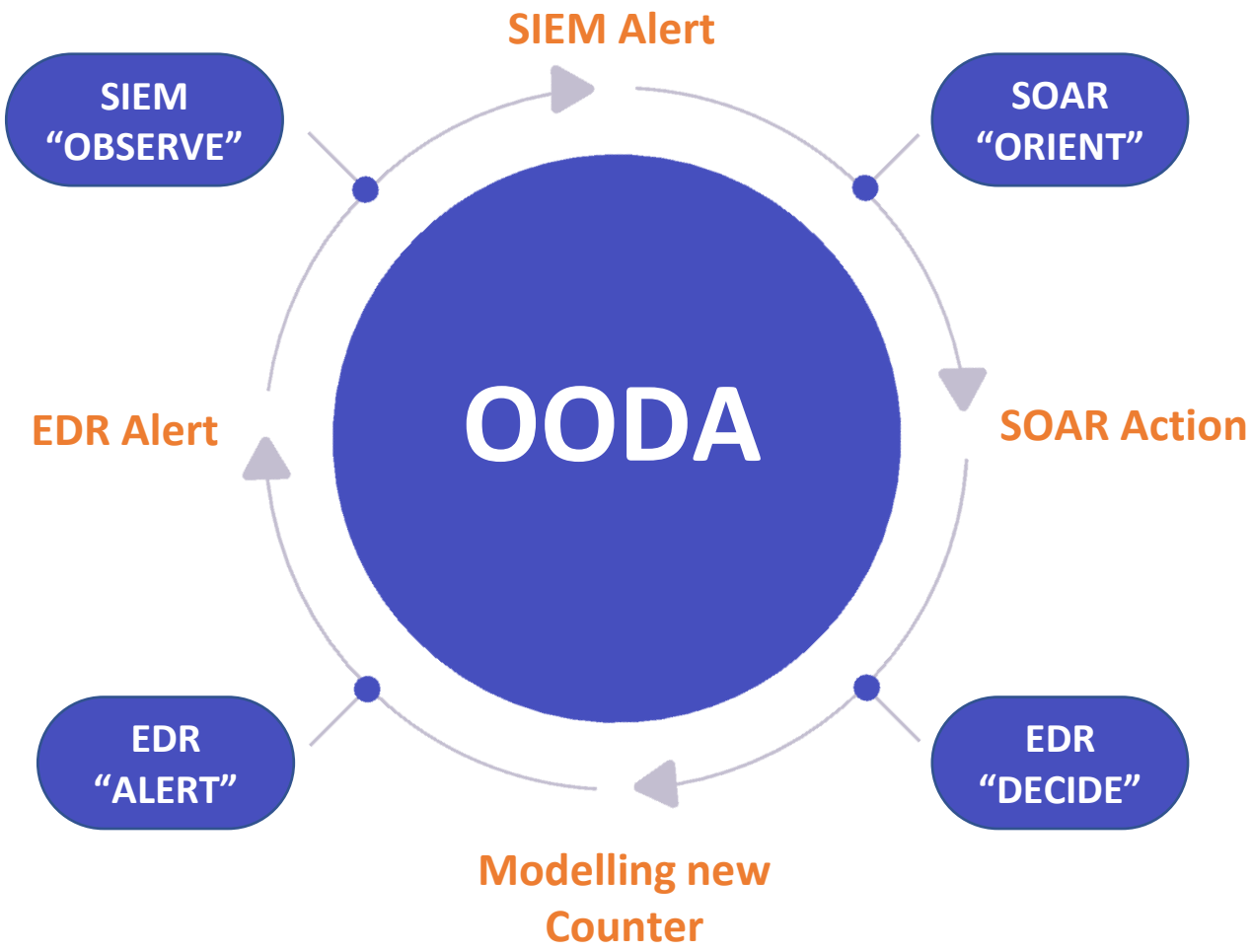
Introducing Invinsense OODA

Why Invinsense OODA? It brings together broadly 3 areas of Security Incident and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Endpoint Detection and Response (EDR) under one approach to achieve the end-objective of detecting and responding to security incidents on a real-time basis.

The strategy and implementation that combat threats with synchronization and optimization of your security solutions to not only take actions but also make your systems adapt to be ready for any such attack in future.

- **Observe** - SIEM
- **Orient** - SOAR
- **Decide** - Security Solutions in the landscape and EDR
- **Act** - Security Solution in the landscape and EDR

OODA Approach is a 4-Pronged Strategy

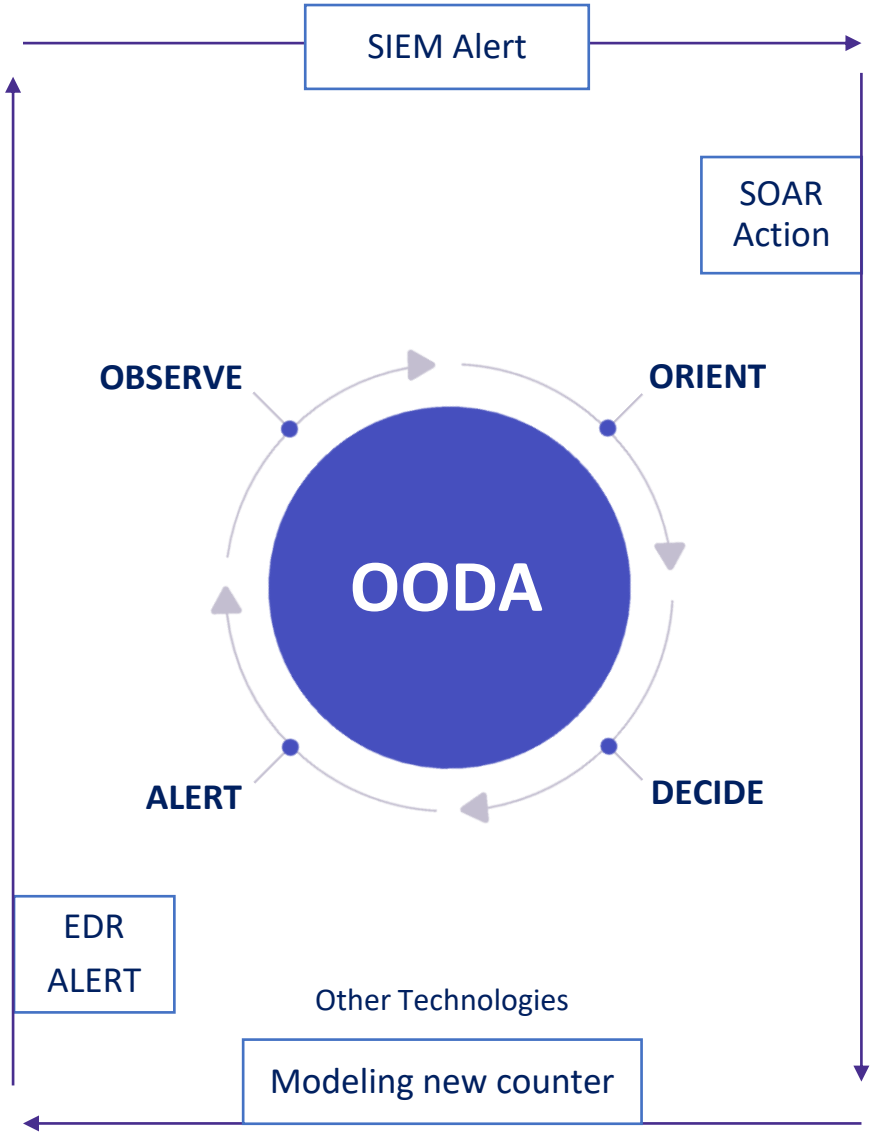


INYINSENSE

OODA Approach is a 4-Pronged Strategy

SIEM "OBSERVE"	
Analysis	Dashboards
	Alerts
	Reports
	Link Analysis Visualization
Correlation Engine	Cross-Log Source correlation
	User Behavior Analytics
	Vulnerability Management
	Cyber Threat Intelligence
	Network Model/Hierarchy

Other Technology "ACT"	
Endpoint Detection	File Add/Remove/Modifications
	Registry Add/Remove/Modifications
	DNS & Network Connections
	Shell/CMD Command Execution
	Process & Cross-Process Executions
	User Behavior Analytics
	Binary & Executable Storage
	Cyber Threat Intelligence



SOAR "ORIENT"	
Play Books	Fully Automated Playbooks
	Semi Automated Playbooks
	Manual Playbooks
Types of Automation	Defensive Enrichment Automation
	Defensive Mitigation Automation
	Forensic Escalation Automation
	Forensic Enrichment Automation
	Forensic Analysis Automation

Other Technology "DECIDE"	
Endpoint Detection	Endpoint Isolation
	Executable Quarantine
	Remote Backdoor
	File Upload & Download
	Registry Add/Remove/Modifications
	Process Execution, Termination & Block
	Executable Sandbox Analysis
	Forensic Memory Dumps

Invinsense OODA – Implementation Approach

The main objective of this approach is to set the priorities clear with respect to the tools and technologies to be integrated to deliver the expected outcomes. The complex problem of early detection and response to security incidents is solved by integrating the strategies, solutions and services under the holistic approach of OODA as seen below:

Consult	Implement & Integrate	Develop	Optimization
• SIEM - Touchpoint and Data Sources • SOAR - Automation and Triage • EDR - Endpoint Detection and Response	• Onboarding • Placement • Integration	• Use-case and Corelation development • Automation	• Ongoing Use-case development • Content Development • Optimization

Key Features of Invinsense OODA

SIEM

- Comprehensive SIEM solution
- Enterprise-ready security monitoring solution for threat detection
- Lightweight multi platform agents
- Host-based Intrusion Detection
- Integrity monitoring
- Beyond Compliance & Security
- Deployed on-premises or in hybrid and cloud environments.
- 360º of visibility and protection
- Unlimited monitored systems
- Painless upgrades

SOAR

- Built-in live stream
- Real time information pertaining
- A simple yet powerful template engine
- Multi-tenancy
- Role Based Access Control to define fine grained user profiles
- Automate Responses to Alerts, Incidents, Vulnerabilities
- Customizable interface and modules
- Simultaneously query multiple MISP instances.

EDR

- Log and events data collection
- File and registry keys integrity monitoring
- Inventory of running processes and installed applications
- Monitoring of open ports and network configuration
- Detection of rootkits or malware artifacts
- Configuration assessment and policy monitoring
- Execution of active responses

WAZUH

SHUFFLE

TheHive

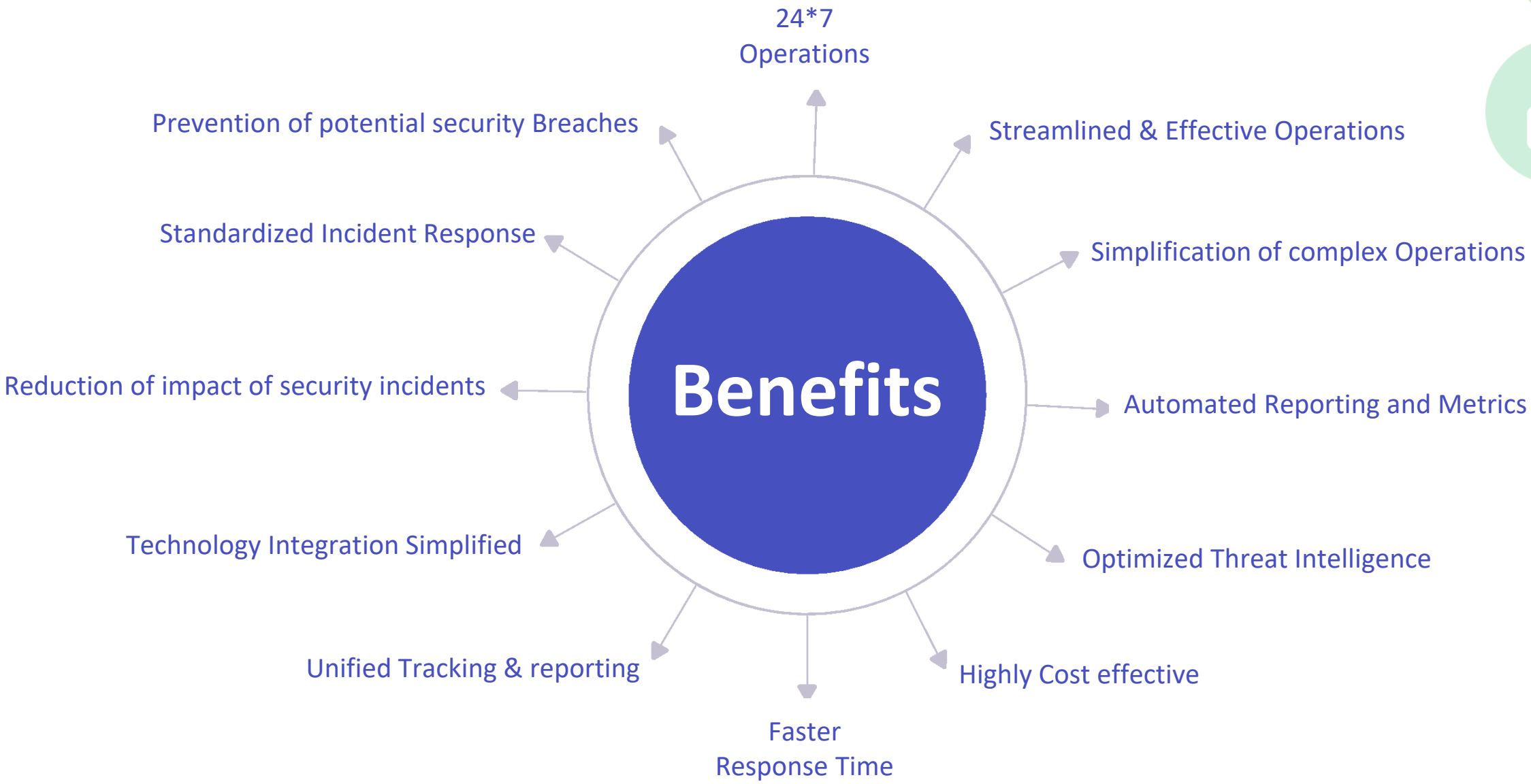
Cortex

MISP Threat Sharing

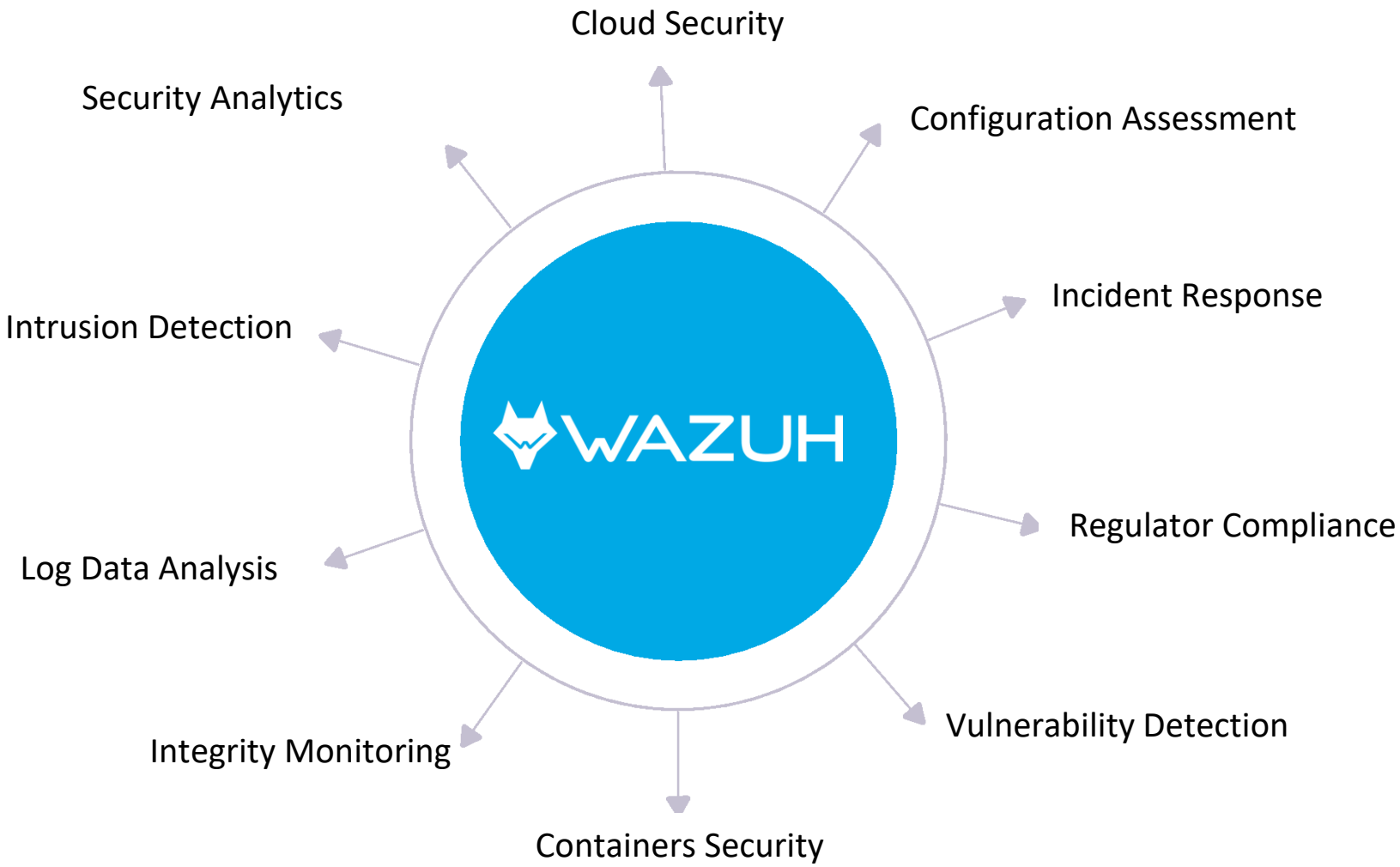
WAZUH EDR

INVINSENSE

Benefits of Invinsense OODA

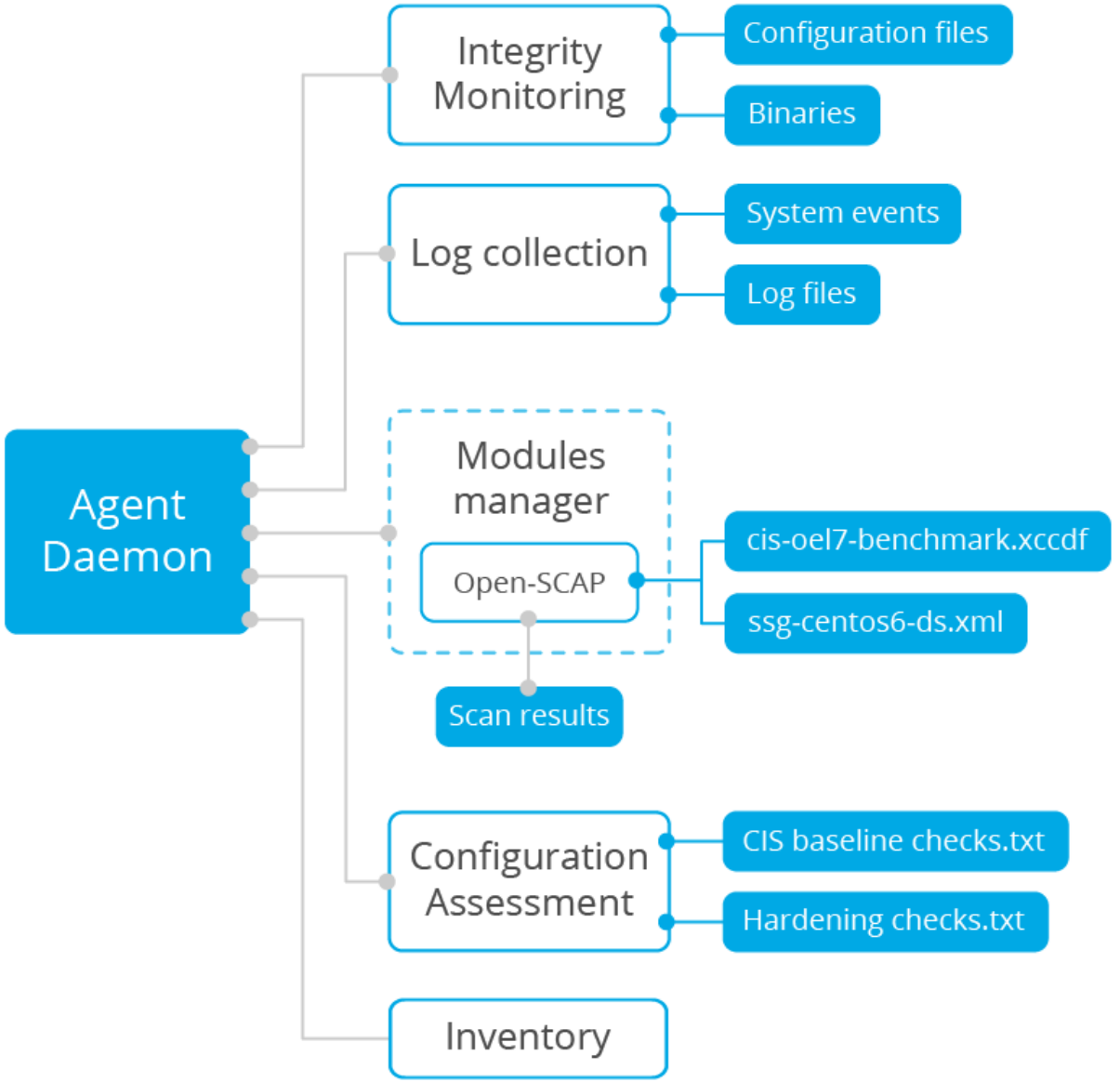


Invinsense OODA – SIEM Use Cases



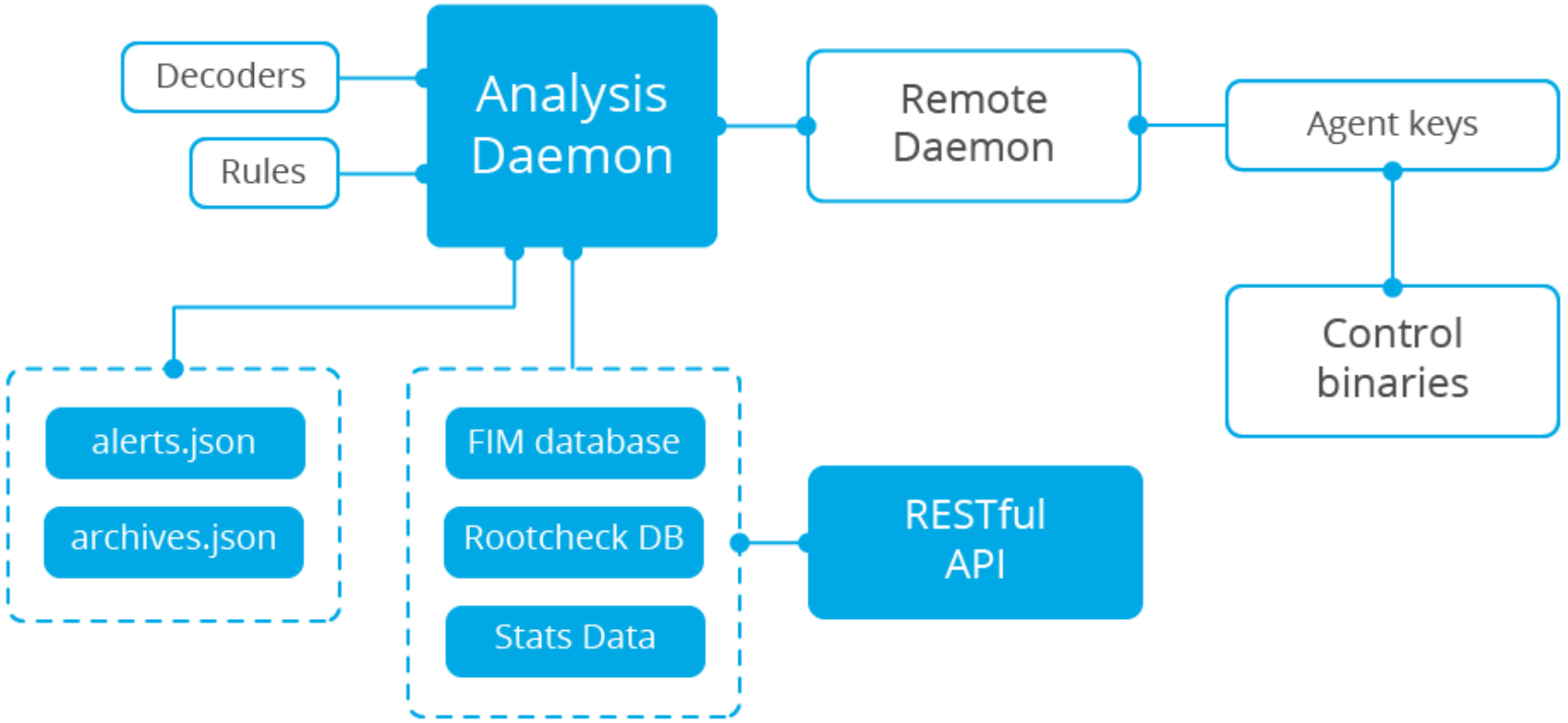
INVINSENSE

Invinsense OODA - SIEM Agent



INVINSENSE

Invinsense OODA - SIEM Server



Invinsense OODA - SOAR

SHUFFLE

- Shuffle helps you understand your risk by knowing what's missing and unifies all your security services in a single view

The Hive

- TheHive is the central Case Management platform

Cortex

- Cortex provides Analyzers & Responders for automation

MISP

- MISP can be used to centrally store & use threat intelligence

Invinsense OODA - EDR

Prevention

- Wazuh endpoint prevents attacks in-line in real time. Consistently ranked for highest efficacy and lowest false-positives.

Dectection

- Patented Behavioral recognizes malicious actions regardless of vector. Wazuh EDR is the endpoint security vendor to detect fileless, zero-day, and nation-grade attacks in real time.

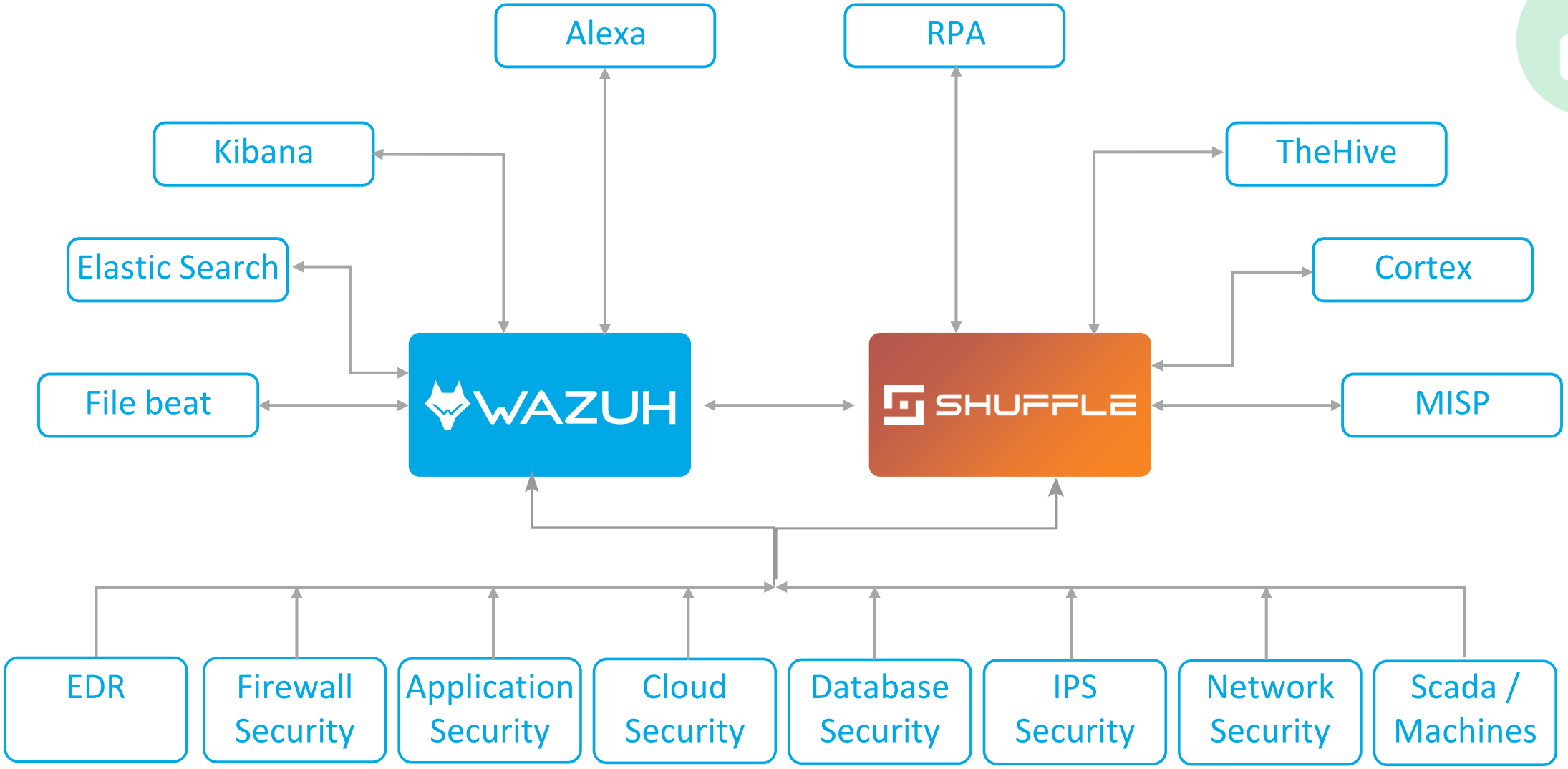
Response

- Wazuh addresses the need for continuous monitoring and response to advanced threats. It is focused on providing the right visibility, with the insights to help security analysts discover, investigate and response to threats and attack campaigns across multiple endpoints.

Threat Hunting

- The industry’s fastest query times and longest data retention. Advanced actions such as full native remote shell, memory dumps, and pre-indexed forensic context. Hunt more, pivot less.

Invinsense OODA - Solution Architecture



INVINSENSE

Invinsense – OODA Case Study of Giant Finance Company

Challenges

- So many alerts going completely uninvestigated, security breaches were going undiscovered for months
- No mechanism to minimize the impact of security management on end-users
- To setup operational processes to cover multiple locations/countries
- Demonstrating a security program's strong and quantifiable return on investment (ROI) can be a challenge for security teams

Solutions

- Threat intelligence significantly reduces the time needed to manually research and triage alerts by supplying TheHive SOAR solutions with automated intelligence in real time
- Wazuh Endpoint Protection Platform Simplified security management with zero impact on end-users
- With Wazuh Integrate log sources including servers, network devices, database and applications; ensure complete coverage across multiple location
- With our integrated approach the organization was able to contextualize its data and develop trackable metrics to demonstrate time/cost savings

Benefit and Business Impact

- Reduced efforts of the security team
- Automated repetitive analyst tasks
- Developed trackable metrics to show cost and time savings
- Achieved the log management and regulated compliance requirements
- Advanced AI for pre-execution protection and fully-automated, policy-driven response
- Provided centralized security incidents for rapid identification and response measure

Infopercept

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Company's / Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

INVINSENSE

Email
sos@infopercept.com

phone
+91 989 885 7117

website
www.infopercept.com