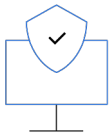
wazuh.

как DevSecOps платформа

и немного Yandex Cloud

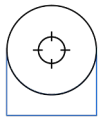
Technical lead, более 12 лет работает с частными и общедоступными облачными средами, инструментами HashiCorp, CI/CD, DevOps и DevSecOps.

Эксперт в таких областях, как частные и общедоступные облачные среды, инструменты HashiCorp, SRE management, ccompany transformation, внедрение DevOps и R&D.

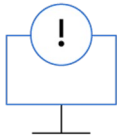


Prevention

Security analytics



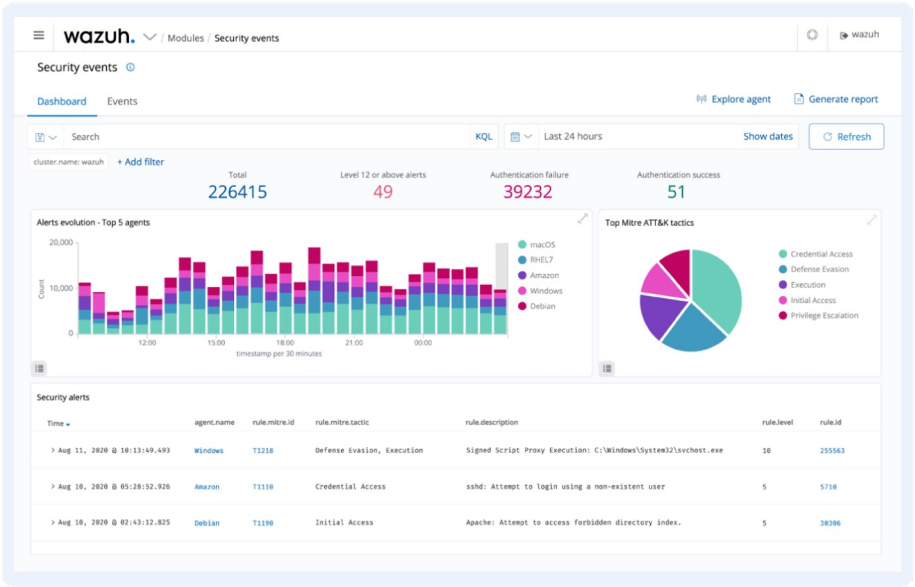
Detection & response



Threat Intelligence

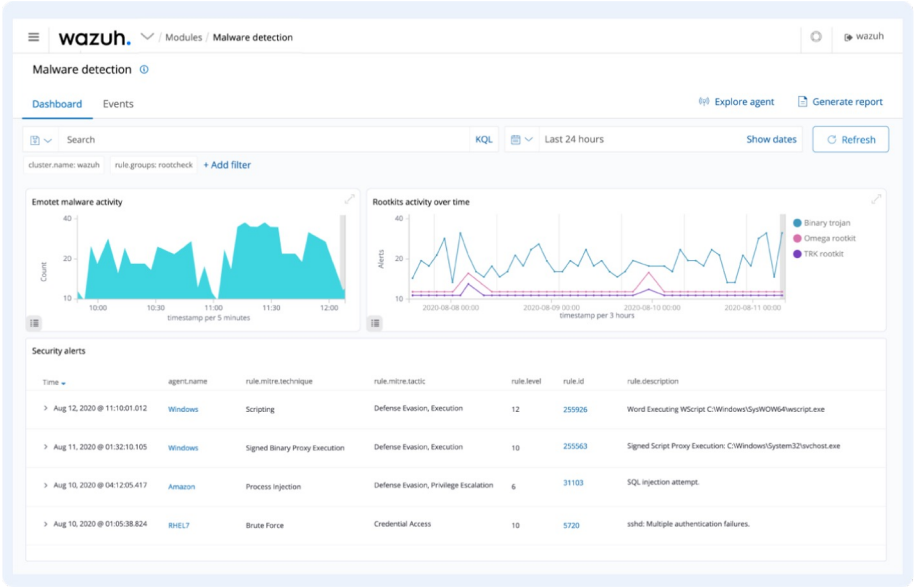
Wazuh – платформа с открытым исходным кодом предназначенная для обнаружения угроз, мониторинга, реагирования на инциденты и соблюдения нормативных требований.

Аналитика безопасности



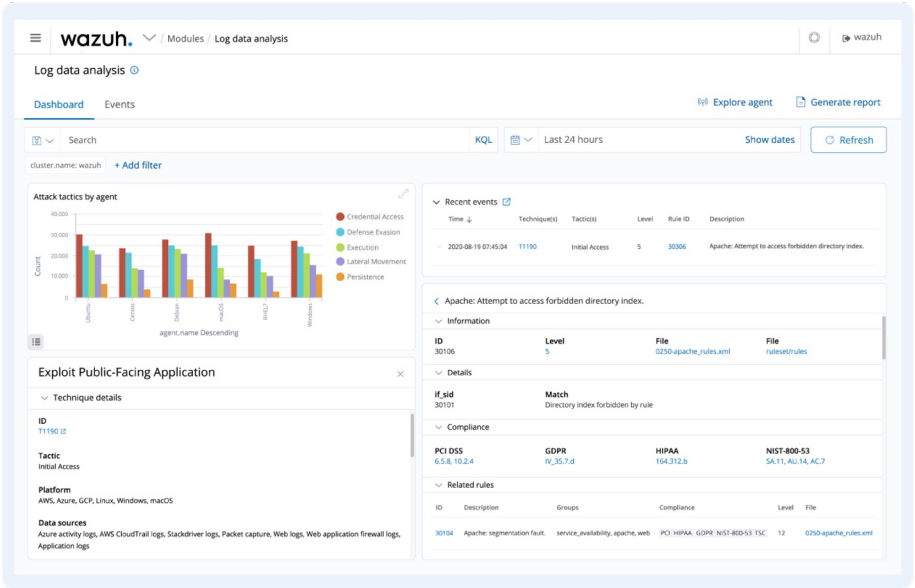
Wazuh используется для сбора, агрегирования и анализа данных безопасности, помогая организациям обнаруживать вторжения, угрозы и аномалии.

Система обнаружения вторжений



- Сканирует систему в поисках вредоносных программ, руткитов и подозрительных аномалий.
- Обнаруживает скрытые файлы, процессы или незарегистрированные сетевые listeners, а также аномалии в системных вызовах.

Анализатор журналов

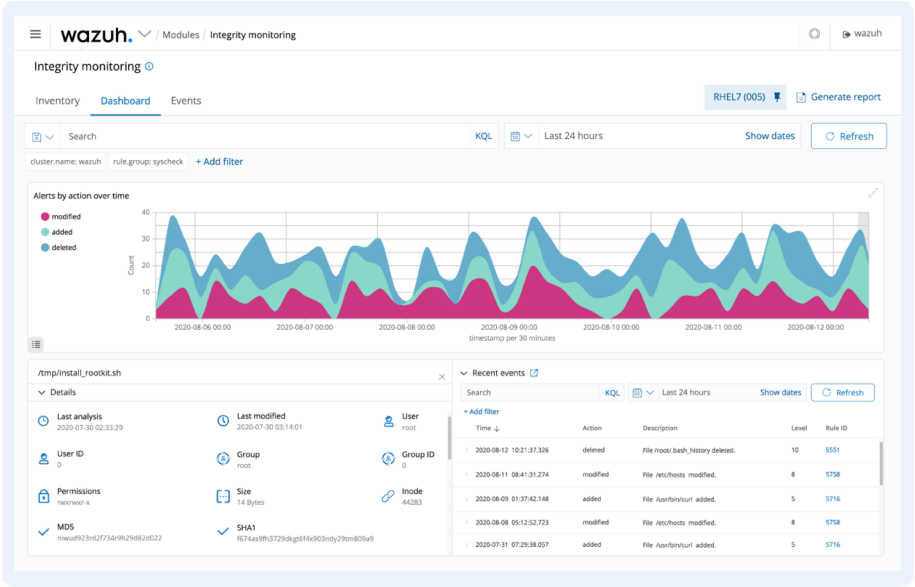


Агенты Wazuh отслеживают журналы ОС и приложений, и отсылает данные для анализа.

Правила Wazuh - это данные:

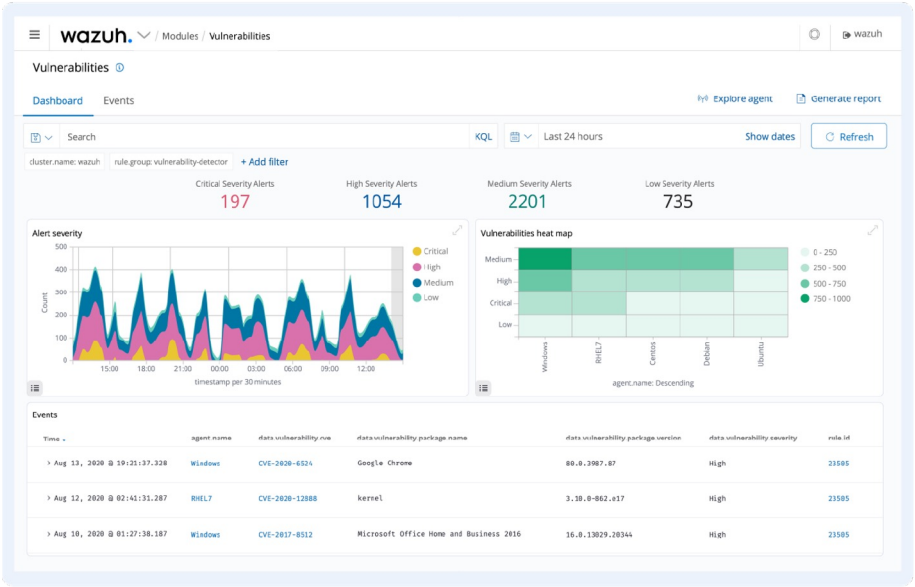
- об ошибках приложений или систем,
- о некорректных конфигурациях,
- о попытках и/или успешных вредоносных действиях,
- об нарушениях политик и множество других мер по обеспечению безопасности

Файловый мониторинг



- Отслеживание файловой системы в реальном времени.
- Выявление изменений атрибутов файлов.
- Создание первоначальной сигнатуры файлов.
- Мониторинг целостности файлов.

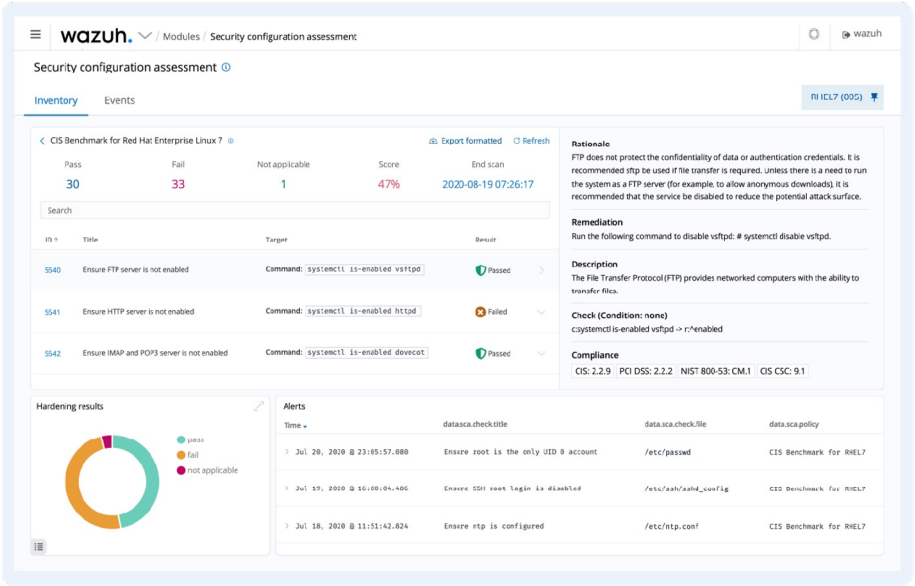
Обнаружение уязвимостей



- Сканирование ПО с отправкой результатов для сопоставления информация с CVE (Common Vulnerabilities and Exposure).

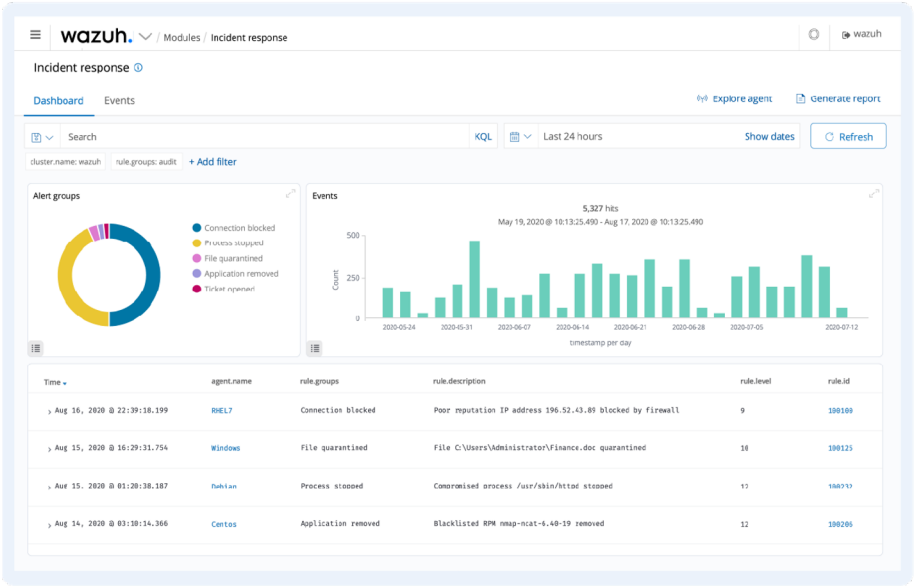
- Автоматическая оценка уязвимости слабых мест в критически важных системах с последующим применением мер по исправлению.

Оценка конфигурации системы



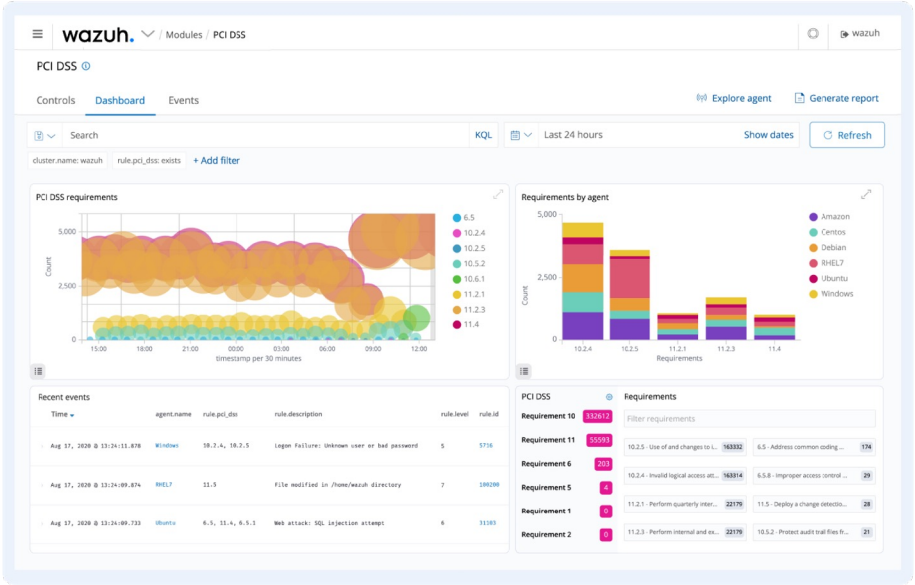
- Отслеживание конфигурацию системы и ПО на предмет соответствия с политиками и стандартами безопасности.
- Периодическое сканирование для обнаружения ПО на предмет известных уязвимостей, отсутствия исправлений или небезопасной конфигурацией.

Реакция на инциденты безопасности



- Использование механизма готовых контрмер для устранения активных угроз, например блокировка доступа к системе на основе набора правил.
- Выявление индикатора компрометации (IOC).
- Выполнение оперативных задач реагирования на инциденты.

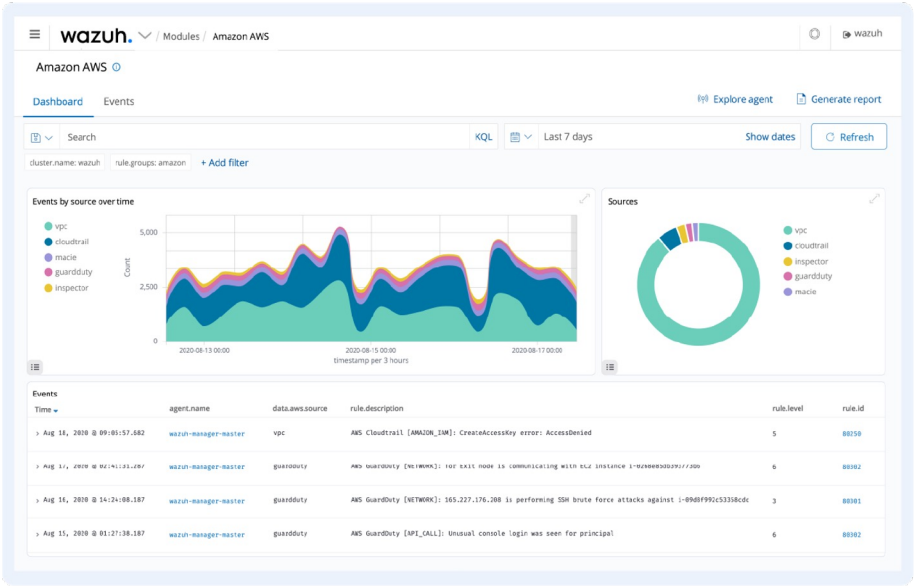
Compliance



Wazuh поддерживает:

- PCI DSS
- GDPR
- NIST 800-53
- GPG13
- TSC SOC2

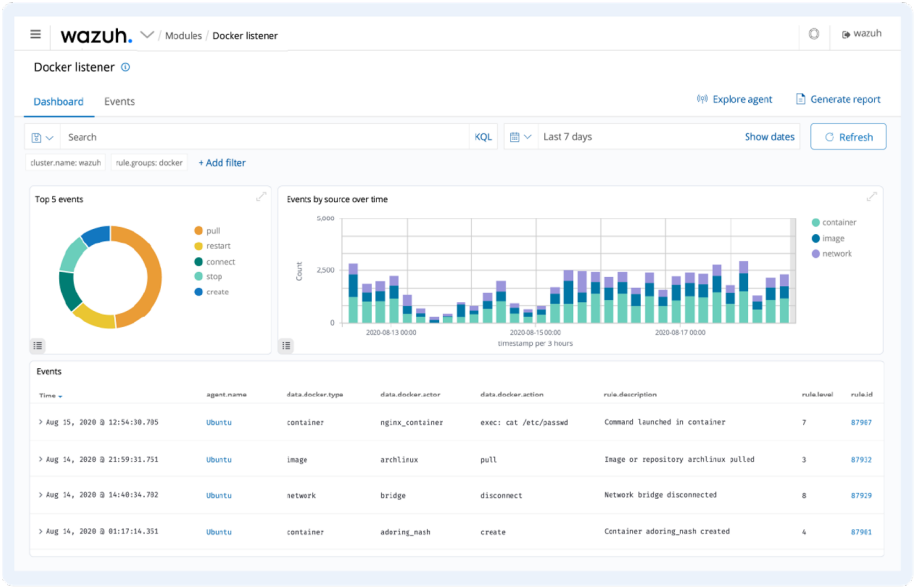
Безопасность и аудит облачных провайдеров



- Мониторинг и аудит облачных провайдеров на уровне API, используя wodle Wazuh, позволяющего реагировать на опережение.

- Поддержка:
  - Amazon AWS
  - MS Azure
  - Google Cloud
  - Yandex cloud*

Поддержка контейнеров



- Осуществление контроля безопасности и интеграция с Docker контейнерами.
- Обнаружение и анализ угроз, уязвимостей и аномалий.

Основные компоненты

Wazuh Agent

Устанавливается на

- ПК
- Серверы
- Облачные экземпляры
- Виртуальные машины

Wazuh Server

- Обработка и анализ данных с помощью декодеров и правил
- Анализ известных индикаторов компрометации (IOC)
- Сбор данных от сотен или тысяч агентов, с возможностью поддержки кластерного режима.

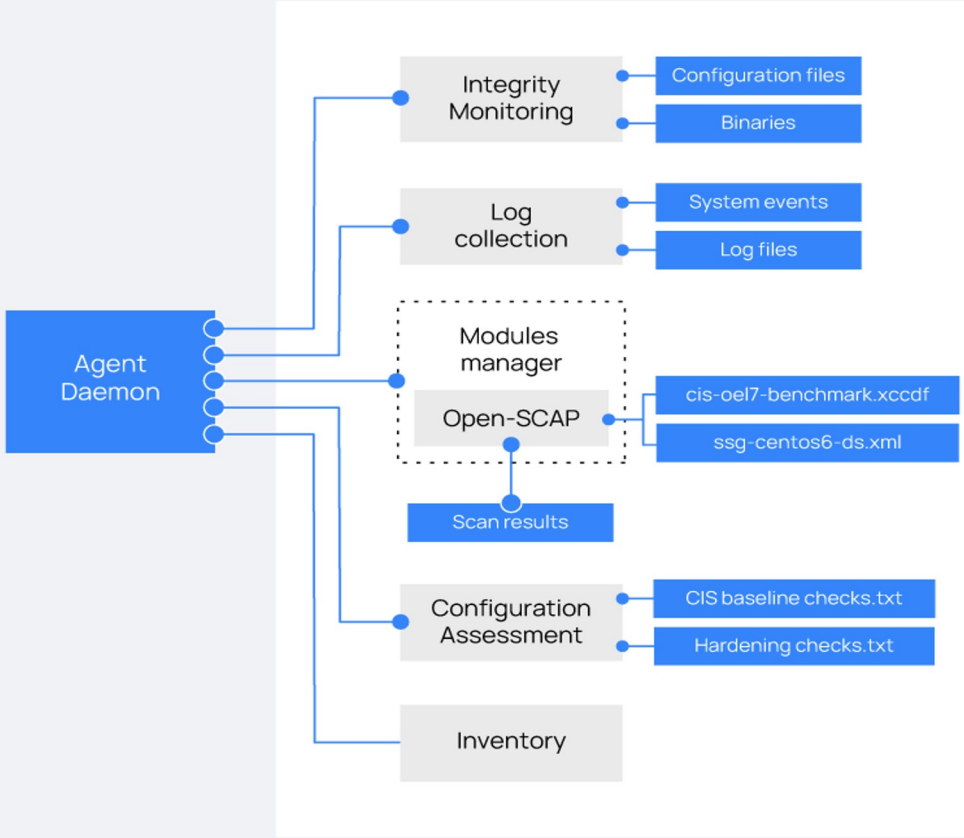
Elastic Stack

- Kibana (визуализация, анализ данных, управление конфигурациями)
- ElasticSearch (полнотекстовый поиск)

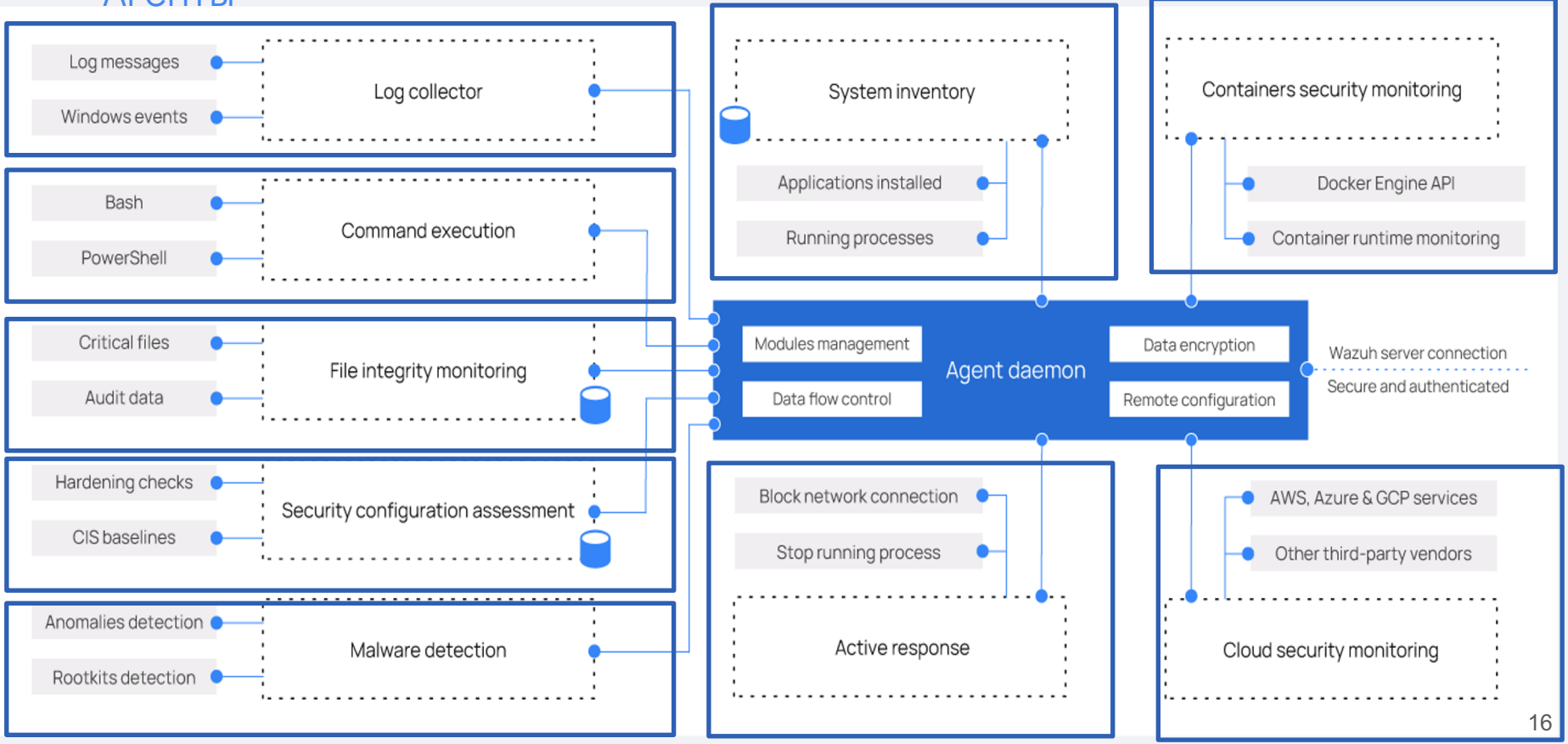
Агенты

Wazuh агент поддерживает различные ОС:

- Linux
- Windows
- macOS
- Solaris
- AIX
- HP-UX
- FreeBSD



Агенты


Log messages
Windows events
Log collector
Bash
PowerShell
Command execution
Critical files
Audit data
File integrity monitoring
Hardening checks
CIS baselines
Security configuration assessment
Anomalies detection
Rootkits detection
Malware detection
System inventory
Applications installed
Running processes
Containers security monitoring
Docker Engine API
Container runtime monitoring
Modules management
Data flow control
Agent daemon
Data encryption
Remote configuration
Wazuh server connection
Secure and authenticated
Block network connection
Stop running process
Active response
AWS, Azure & GCP services
Other third-party vendors
Cloud security monitoring

Модули Агента

Log collector:

- Чтение логов и событий ОС
- Сбор логов приложений с поддержкой в различных форматов(JSON, Docker format и др)

Command Execution:

- Запуск команд по расписанию (мониторинг свободного места на диске)
- Сбор результатов выполнения с последующей отправкой в Wazuh сервер

File Integrity Monitoring (FIM):

- Отслеживание изменения
- Мониторинг изменения атрибутов в режиме реального времени.
- Учет и хранение состояния изменений

Security Configuration Assessment (SCA):

- Отслеживание изменений конфигураций системы.
- Сравнение текущей конфигурации с Center of Internet Security (CIS)

Агенты постоянно поддерживают связь с сервером для отправки данных и событий на основе конфигураций и правил, так же они отправляют данные о своем состоянии.

При установлении связи между агентом и сервером управление конфигурациями агента можно осуществлять централизовано.

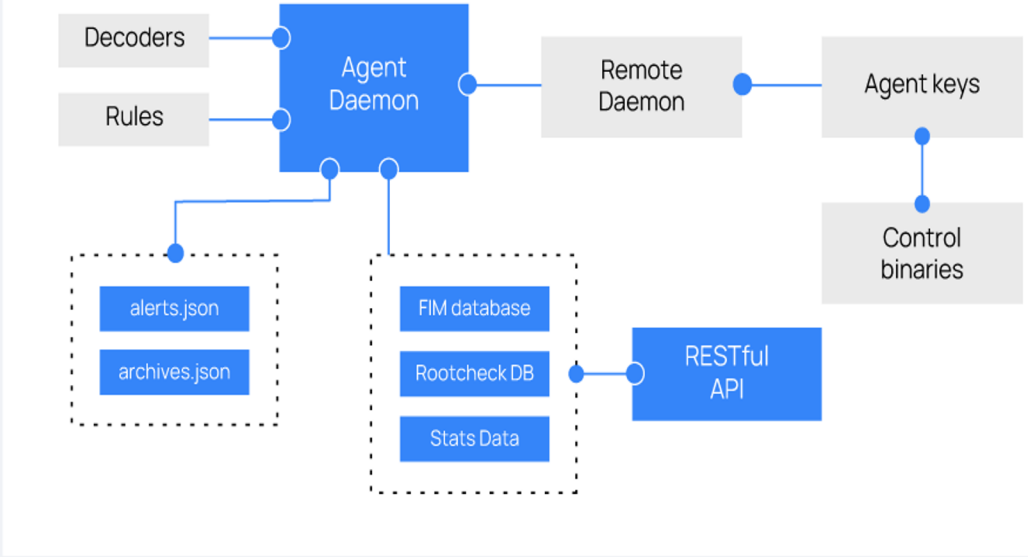
Агент подключается к серверу по защищенному каналу и может использовать как TCP, так и UDP протоколы. Что не маловажно существует встроенный механизм защиты от лавинной очереди событий.

W. agent

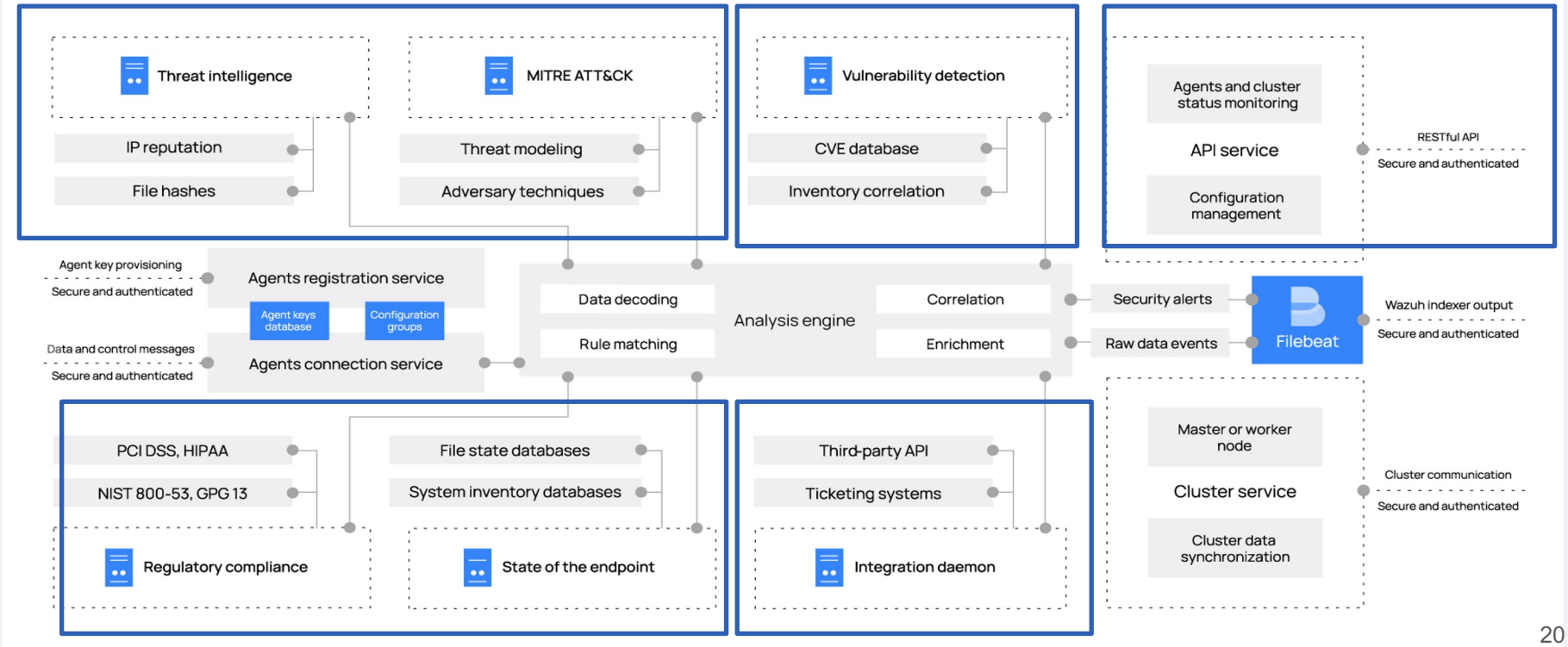
Wazuh сервер

Отвечает за:

- анализ данных
- оповещение при обнаружении угроз или аномалий
- управление конфигурациями агентов и отслеживание состояний
- интеграция с внешними системами (Service Now, Jira или PagerDuty)



Архитектура серверной части



ElasticStack

Filebeat

Легковесный доставщик лог-сообщений. Используется для отправки событий и предупреждений в Elasticsearch.

Elasticsearch/OpenSearch

Масштабируемая система полнотекстового поиска и аналитики с использованием разных индекс для предупреждений, событий и мониторинга.

Kibana/OpenSearch Dashboard

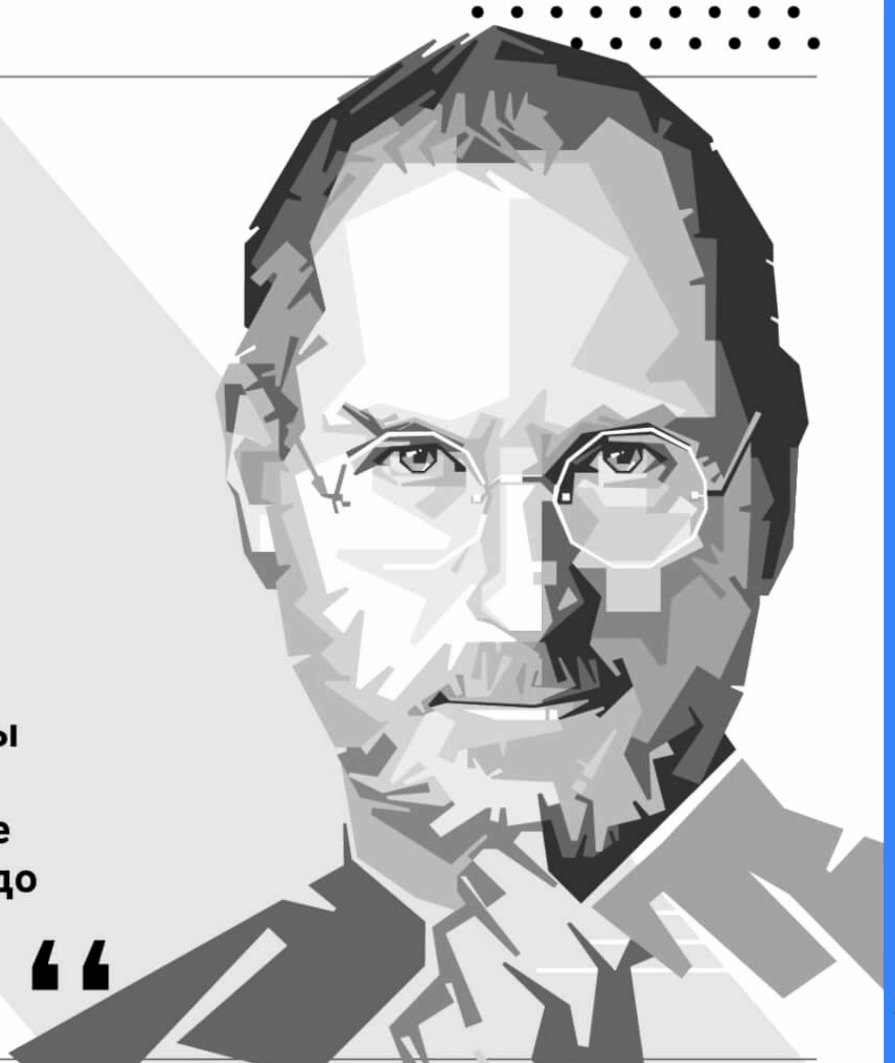
Визуализация данных, но в контексте Wazuh это отдельное Kibana-приложение, которое осуществляет пользовательский доступ к информации о событиях безопасности, о соответствии со стандартами такими как PCI DSS, GDPR, CIS, HIPAA, NIST 800-53, об уязвимостях, файлового мониторинга, и многим другим.

Demo

Отдельная благодарность

- Михаилу Дымскову – Team Lead тех поддержки Yandex Cloud
- Алексею Миртову - Архитектор Yandex Cloud
- Santiago Bassett - Founder of Wazuh
- Agus O'Farrell - Marketing Director Wazuh

МУДРАЯ ЦИТАТА



”Заниматься нужно тем, к чему вы относитесь с энтузиазмом. В противном случае вам никогда не хватит сил, чтобы довести дело до конца.“

Вопросы?