

wazuh.

как DevSecOps платформа

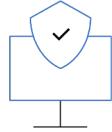
и немного Yandex Cloud



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, company transformation, внедрение DevOps и R&D.

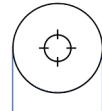
W.



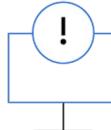
Prevention



Security
analytics



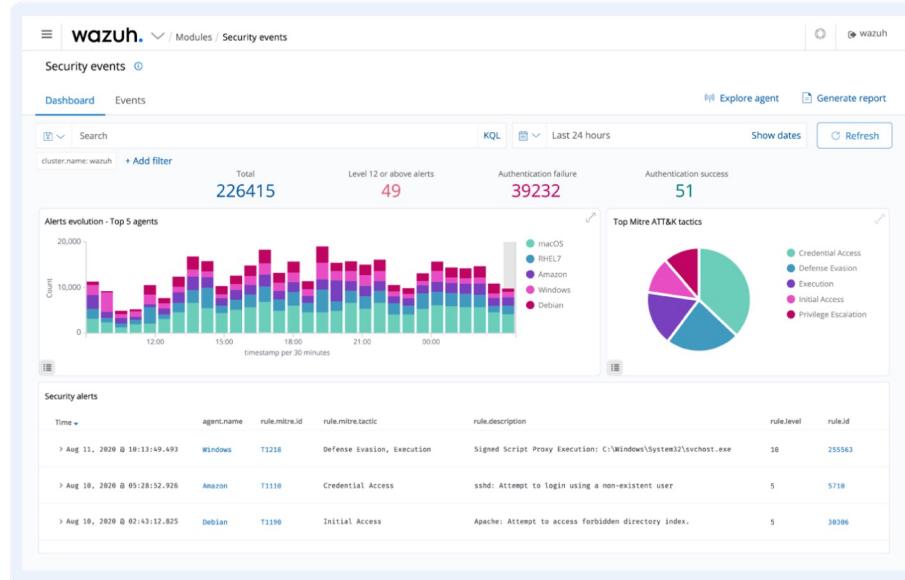
Detection
& response



Threat
Intelligence

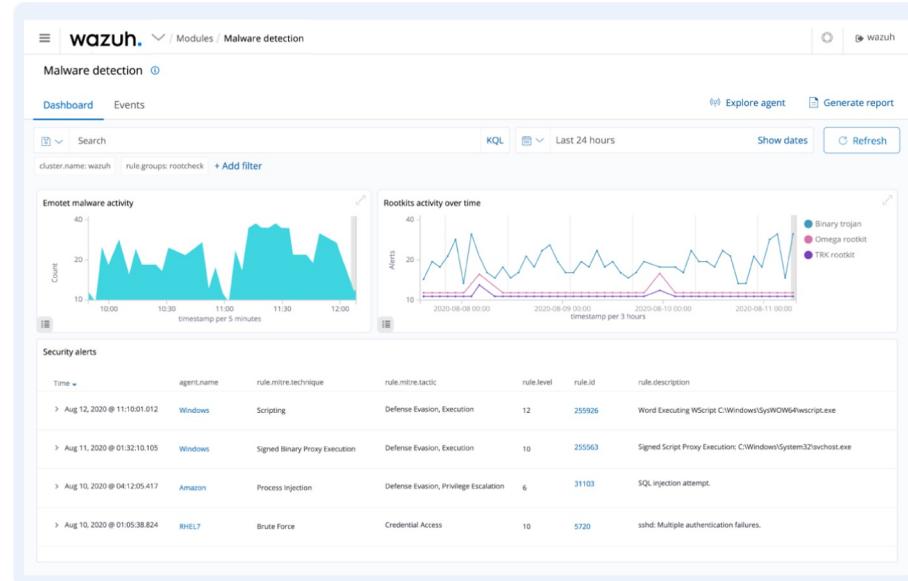
Wazuh – платформа с открытым исходным кодом предназначенная для обнаружения угроз, мониторинга, реагирования на инциденты и соблюдения нормативных требований.

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

The screenshot shows the Wazuh Log data analysis interface. At the top, there's a navigation bar with 'wazuh' and 'Log data analysis'. Below it is a dashboard with several sections:

- Attack tactics by agent:** A bar chart showing the count of various attack tactics across different agents. The tactics include Credential Access, Defense Evasion, Execution, Lateral Movement, and Persistence.
- Exploit Public-Facing Application:** A section showing details for an exploit with ID 11190. It includes sections for Technique details, Platform (AWS, Azure, GCP, Linux, Windows, macOS), and Data sources (AWS activity logs, AWS CloudTrail logs, Stackdriver logs, Packet capture, Web logs, Web application firewall logs, Application logs).
- Recent events:** A table listing recent log entries. One entry is highlighted: "2020-08-19 07:45:04 11190 Initial Access 5 30306 Apache: Attempt to access forbidden directory index."
- Information:** A table showing file-level information for rule 30306, including ID 30306, Level 5, File 0250-apache_rules.xml, and File ruleset/rules.
- Details:** A table showing details for rule 30301, specifically for if_sid 30101, which is a Match for "Directory index forbidden by rule".
- Compliance:** A table showing compliance details for PCI DSS 6.5.8, 10.2.4, GDPR IV_35.7.d, HIPAA 164.312.b, and NIST-800-53 SA.11, AU.14, AC.7.
- Related rules:** A table showing related rules, including rule 30104 for "Apache: segmentation fault" with a description of "service_availability, apache, web", groups "PCI", compliance "PCI-HIPAA-GDPR-NIST-800-53-TSC", level 12, and file 0250-apache_rules.xml.

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 множестве других мер по обеспечению безопасности

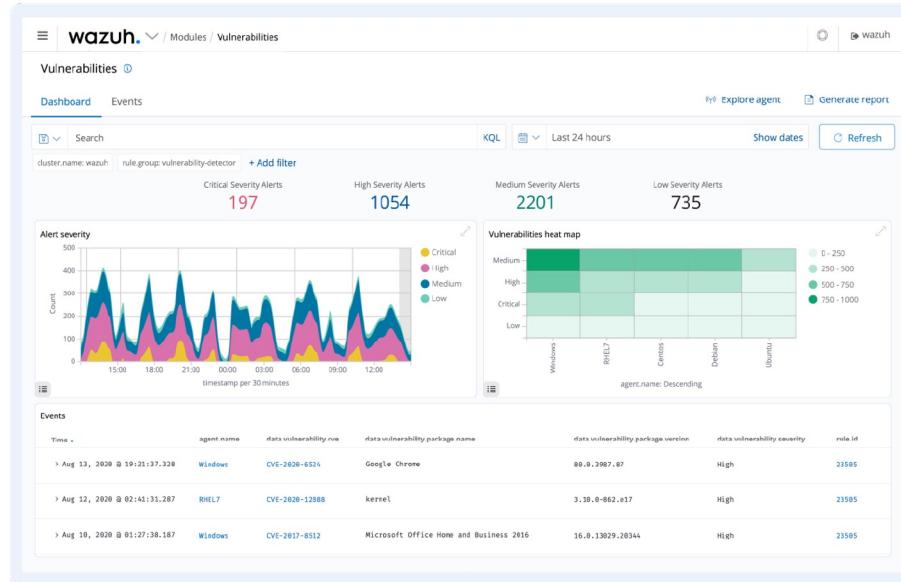
Файловый мониторинг

The screenshot shows the Wazuh Integrity monitoring interface. At the top, there's a navigation bar with 'wazuh.' and 'Modules / Integrity monitoring'. Below it, a search bar and filter options ('Search', 'KQL', 'Last 24 hours', 'Show dates', 'Refresh') are visible. A main chart titled 'Alerts by action over time' displays three stacked areas: 'modified' (red), 'added' (green), and 'deleted' (blue). The x-axis shows dates from 2020-08-06 to 2020-08-12. On the left, a sidebar for the file '/tmp/install_rootkit.sh' provides detailed information: Last analysis (2020-07-30 02:33:29), User ID (0), Group ID (root), Permissions (rw-r--r--), and MD5 (f0e0d923...). On the right, a 'Recent events' table lists file system activity:

Action	Description	Level	Rule ID
deleted	File /root/.bash_history deleted.	10	5551
modified	File /root/.ssh/authorized_keys modified.	8	5758
added	File /usr/bin/vi added.	5	5716
modified	File /etc/hosts modified.	8	5758
added	File /usr/bin/vi added.	5	5716

- 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 информации с CVE (Common Vulnerabilities and Exposures).
- Автоматическая оценка уязвимости слабых мест в критически важных системах с последующим применением мер по исправлению.

Оценка конфигурации системы

The screenshot shows the Wazuh security configuration assessment interface. At the top, it displays the score: Pass (30), Fail (33), Not applicable (1), Score (47%), and the date (2020-08-19 07:26:17). Below this, there are two tabs: 'Inventory' and 'Events'. The 'Inventory' tab is selected, showing a table of findings:

ID	Title	Target	Result
5540	Ensure FTP server is not enabled	Command: systemctl is-enabled vsftpd	Passed
5541	Ensure HTTP server is not enabled	Command: systemctl is-enabled httpd	Failed
5542	Ensure IMAP and POP3 server is not enabled	Command: systemctl is-enabled dovecot	Passed

On the right side, there is a detailed view for the failed finding (5541):

- Rationale:** FTP does not protect the confidentiality of data or authentication credentials. It is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the service be disabled to reduce the potential attack surface.
- Remediation:** Run the following command to disable vsftpd: # systemctl disable vsftpd.
- Description:** The File Transfer Protocol(FTP) provides networked computers with the ability to transfer files.
- Check (Condition: none):** systemctl is-enabled vsftpd -> r=enabled
- Compliance:** CIS: 2.2.9 | PCI DSS: 2.2.2 | NIST 800-53: CM.1 | CIS CSC: 9.1

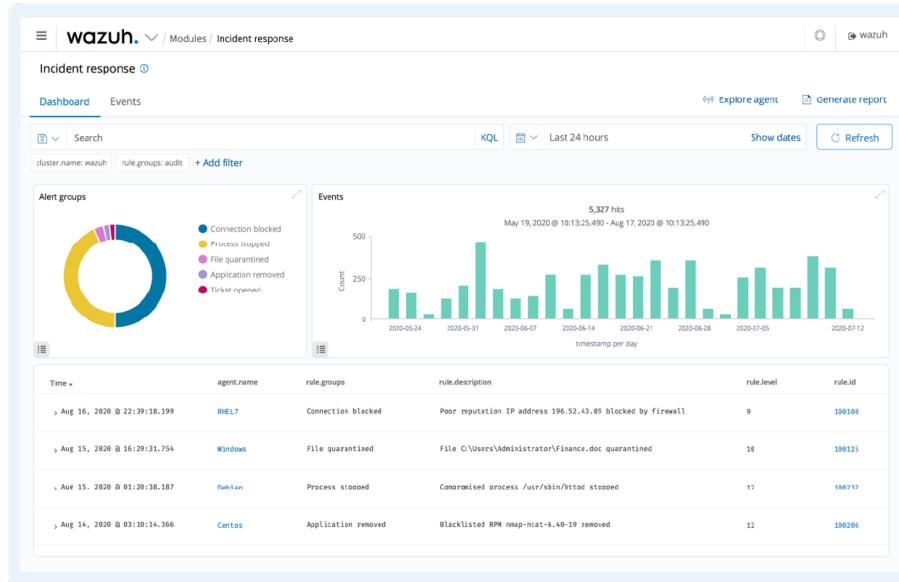
Below the table, there is a section titled 'Hardening results' with a donut chart showing the status of findings: green (pass), orange (fail), and red (not applicable).

At the bottom, there is a table titled 'Alerts' showing recent alerts:

Time	data.sca.check.title	data.sca.check.file	data.sca.policy
Jul 28, 2020 23:05:57,080	Ensure root is the only UID 0 account	/etc/passwd	CIS Benchmark for RHEL7
Jul 19, 2020 16:00:04,106	Ensure SSH root login is disabled	/etc/ssh/sshd_config	CIS Benchmark for RHEL7
Jul 18, 2020 11:51:42,824	Ensure ntp is configured	/etc/ntp.conf	CIS Benchmark for RHEL7

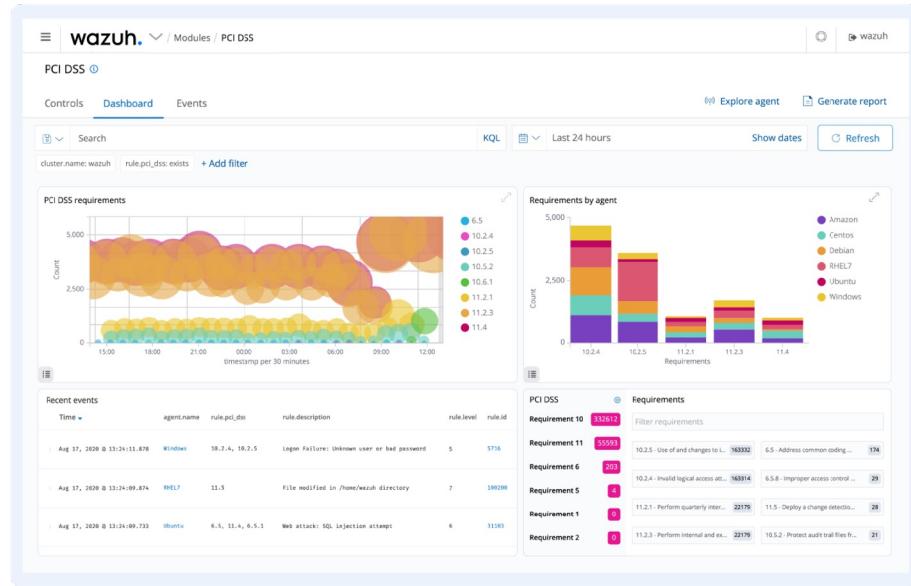
- Отслеживание конфигурацию системы и ПО на предмет соответствия с политиками и стандартами безопасности.
- Периодическое сканирование для обнаружения ПО на предмет известных уязвимостей, отсутствия исправлений или небезопасной конфигурацией.

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.

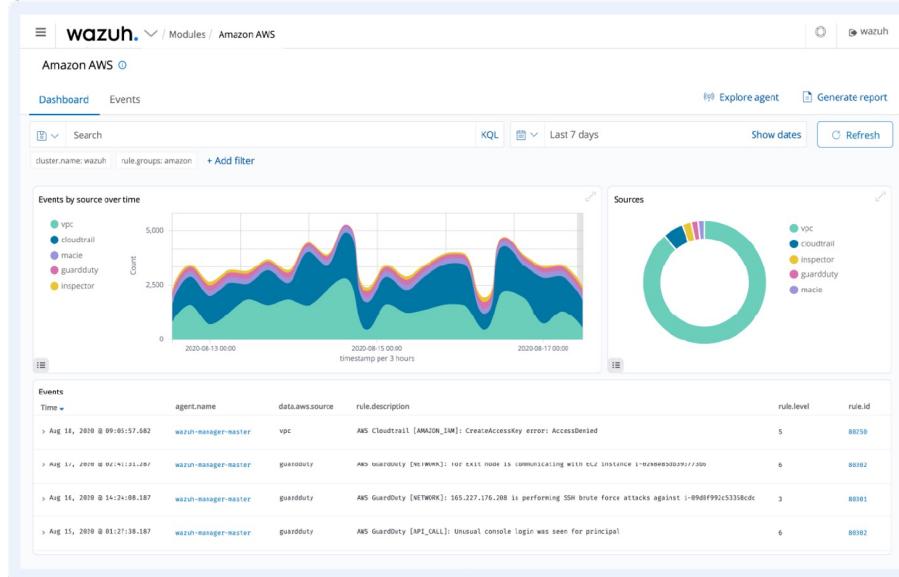
Compliance



Wazuh поддерживает:

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

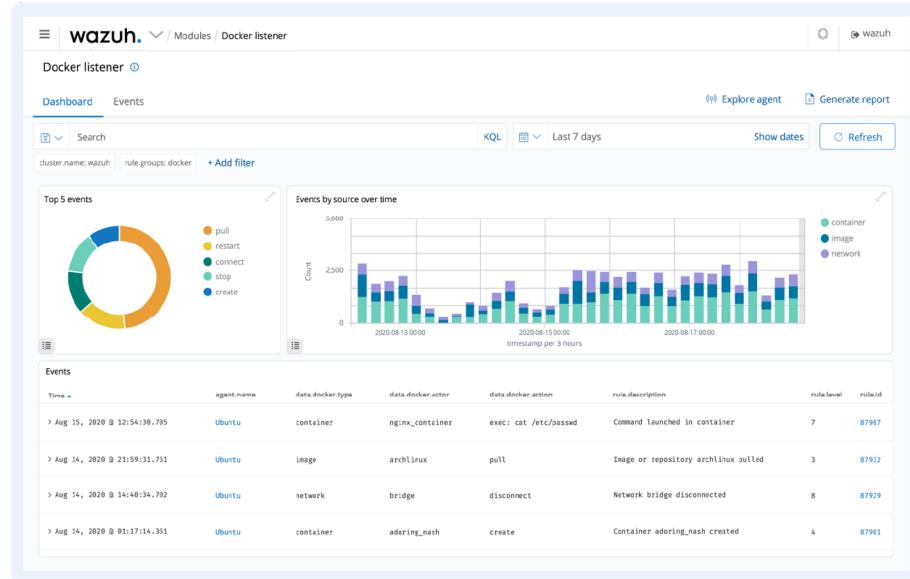
Безопасность и аудит облачных провайдеров



- Мониторинг и аудит облачных провайдеров на уровне API, используя module 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.



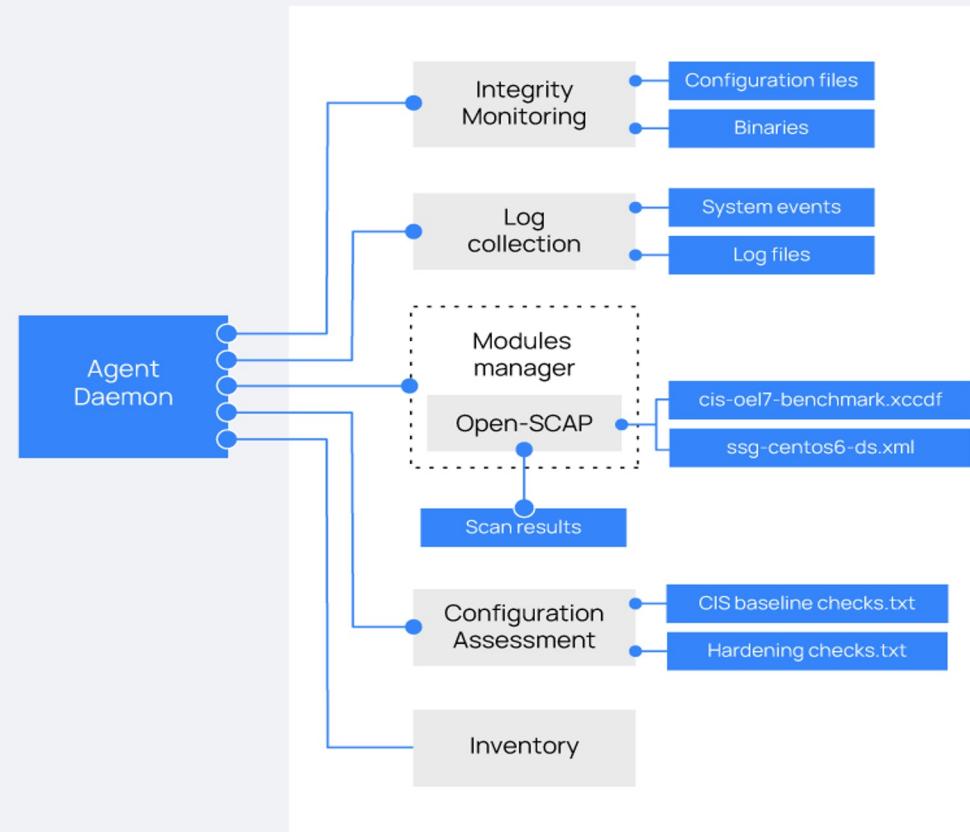
Elastic Stack

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

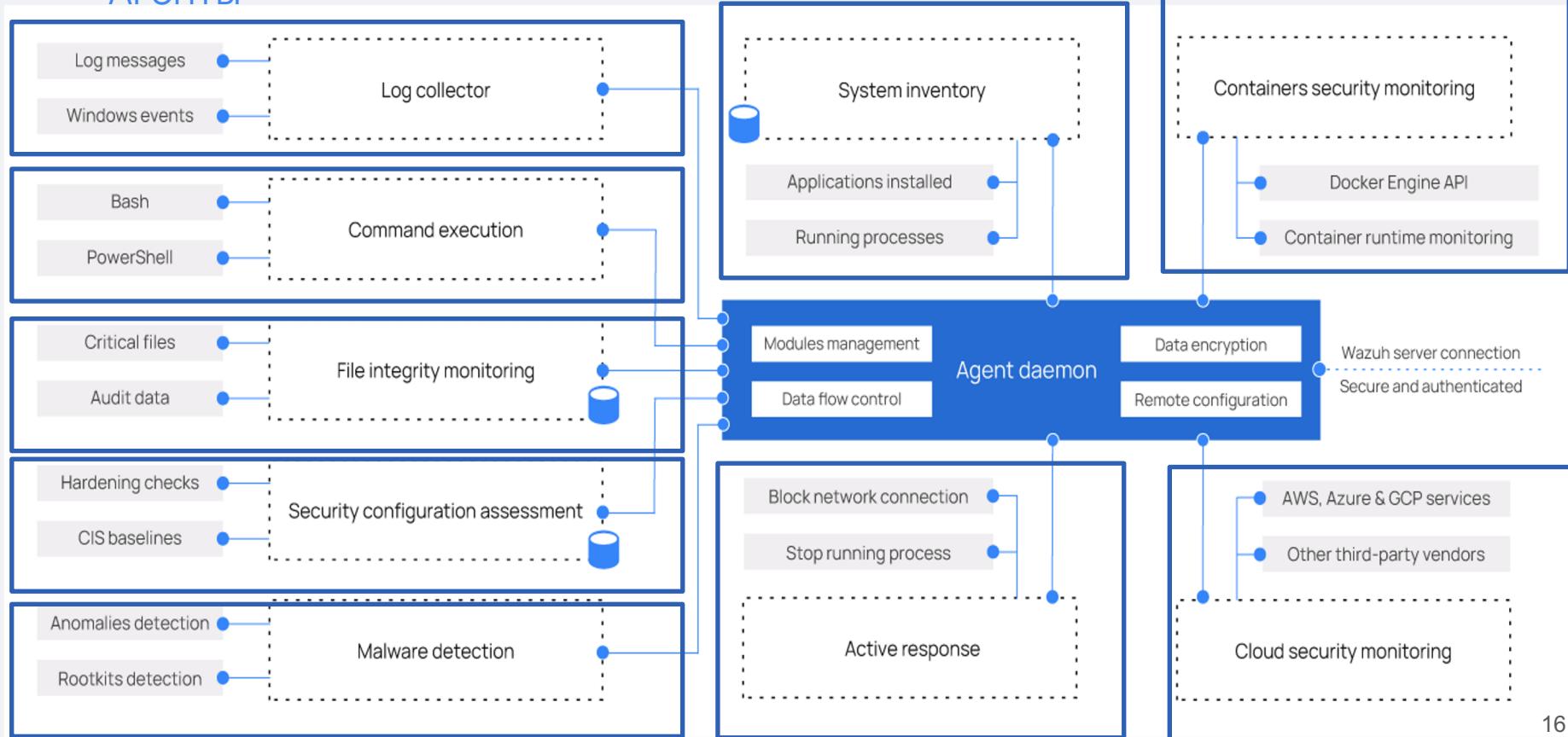
Агенты

Wazuh агент поддерживает различные ОС:

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



Агенты



Модули Агента

Log collector:

- Чтение логов и событий ОС
- Сбор логов приложений с поддержкой в различных форматах (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.

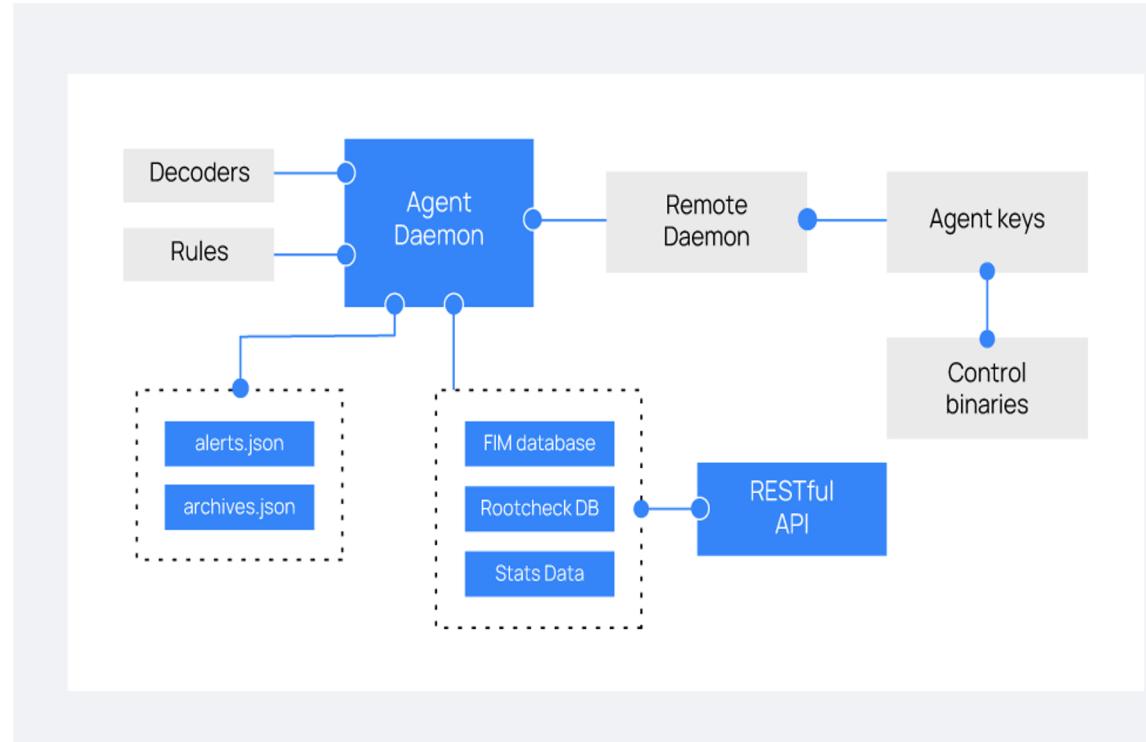


w. agent

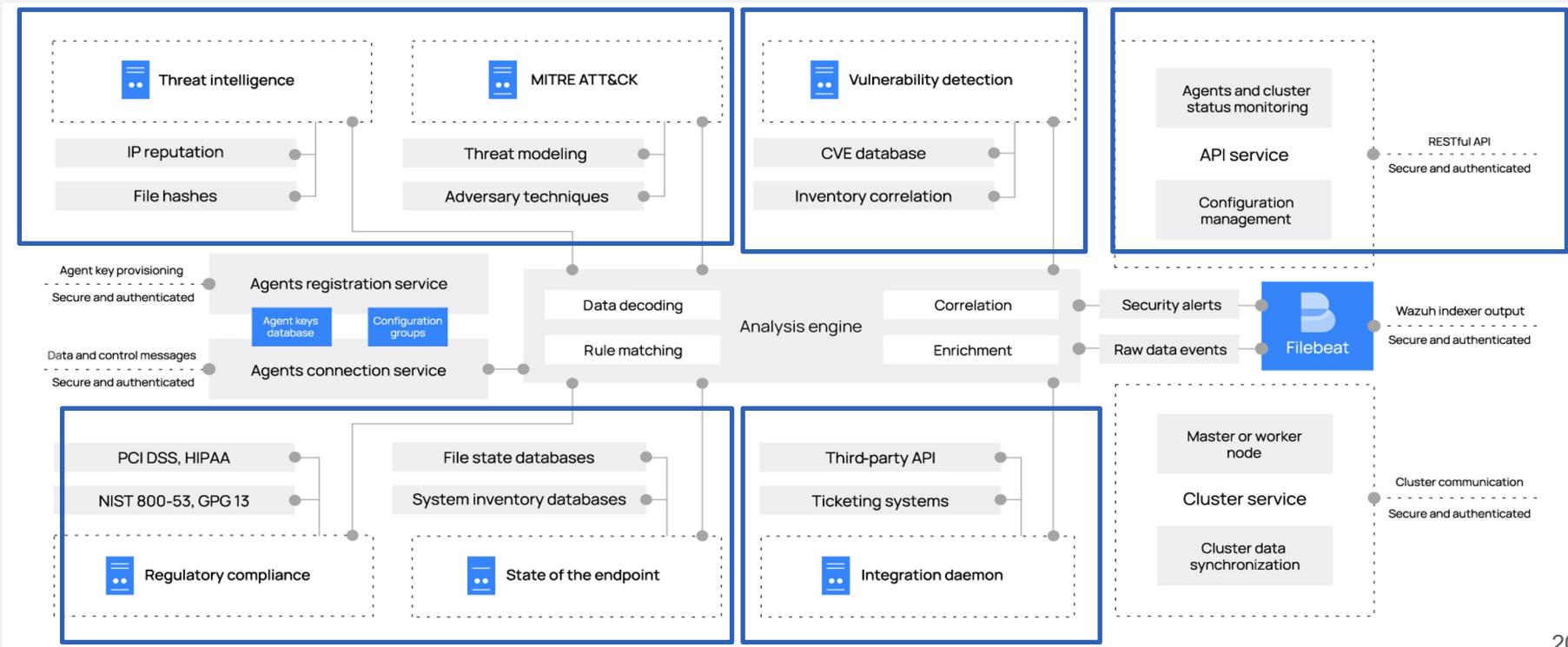
Wazuh сервер

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

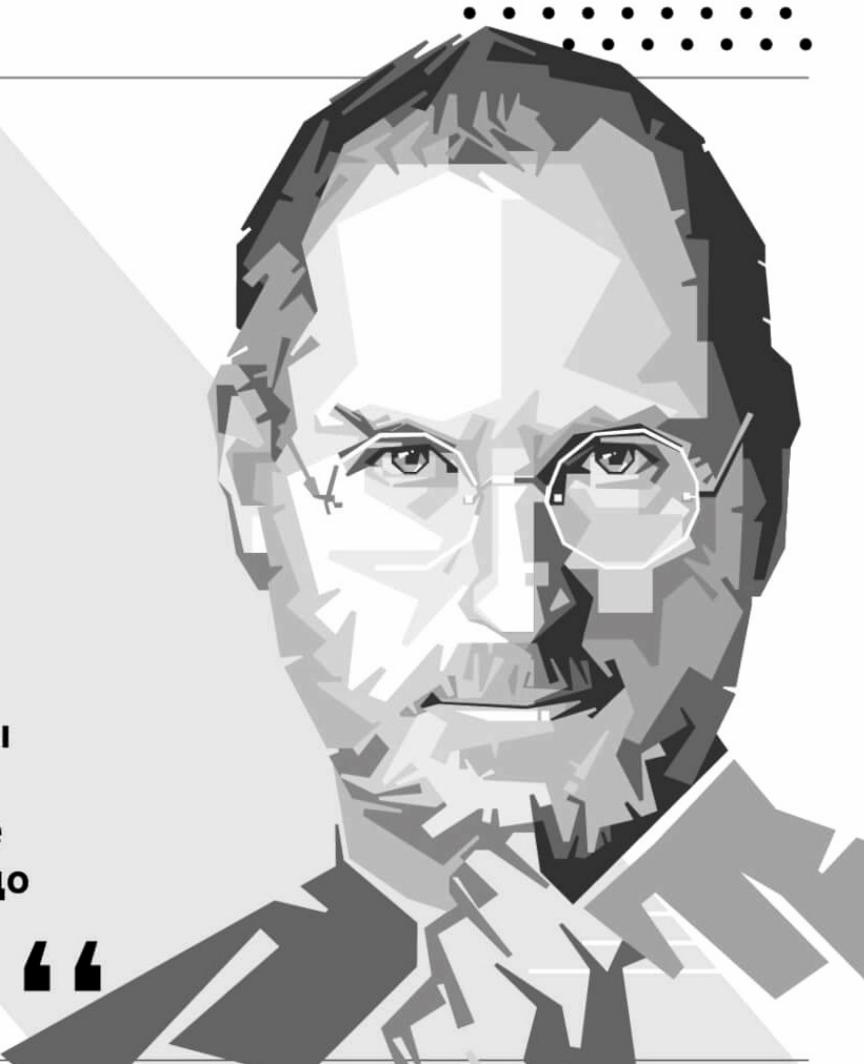
Отдельная благодарность

- Михаилу Дымскому – 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 энтузиазом. В противном случае вам никогда не хватит сил, чтобы довести дело до конца.

“



Вопросы?