УДК 004.056.5

Ю.С. Корякина, jk169@list.ru
Институт машиноведения автоматики и геомеханики НАН КР
Институт информационных технологий КГТУ им. И.Раззакова И.Раззаков
Ш.Т. Айтбаев, sher.aitbaev@gmail.com
Институт информационных технологий КГТУ им. И.Раззакова И.Раззаков
И.В. Зимин, igorzimin777@mail.ru
Академия цифровых инноваций

АНАЛИТИЧЕСКИЙ ОБЗОР МЕТОДОВ РЕАЛИЗАЦИИ ПОДСИСТЕМ СБОРА, ОБРАБОТКИ, ХРАНЕНИЯ и ВИЗУАЛИЗАЦИИ ДАННЫХ ДЛЯ SOC (SECURITY OPERATIONS CENTER)

Современные корпоративные информационные системы ежедневно подвергаются множеству угроз, требующих не только своевременного обнаружения, но и эффективного анализа и визуализации данных безопасности. В данной работе проведён аналитический обзор методов реализации подсистемы сбора, обработки, хранения и визуализации данных в рамках центров мониторинга безопасности (SOC). Особое внимание уделено анализу архитектурных и функциональных особенностей решения Wazuh, объединяющего возможности SIEM, HIDS, лог-менеджмента и визуального представления информации. Рассмотрены существующие подходы на базе SIEM-систем (Splunk, QRadar, ArcSight), лог-менеджеров (ELK, Graylog), XDR-решений (Cortex XDR, Microsoft Defender) и IDS/IPS-систем (Suricata, Snort), а также проведено их сравнение с решением Wazuh. Описаны ключевые компоненты Wazuh: агент, сервер, индексер и дашборд, а также их взаимодействие при реализации подсистемы. На основе проведённого анализа сформулированы рекомендации по построению универсальной, экономически эффективной и масштабируемой подсистемы для централизованного мониторинга и анализа событий информационной безопасности.

Ключевые слова: SOC, сбор данных, обработка данных, хранение данных, визуализация, SIEM, машинное обучение, кибербезопасность, HIDS, XDR, агент, сервер, индексер, дашборд.

Введение

В условиях стремительного развития цифровых технологий и постоянного роста киберугроз обеспечение эффективной работы центров мониторинга информационной безопасности (SOC) становится критически важной задачей для современных организаций. Возрастающий объём событий безопасности, разнообразие источников данных и необходимость оперативного реагирования требуют внедрения интегрированных и автоматизированных решений, способных обеспечить комплексный контроль и анализ информации в режиме, близком к реальному времени. Объектом исследования в данной работе являются методы и технологии обеспечения информационной безопасности в рамках SOC. Предмет исследования — подсистема сбора, обработки, хранения и визуализации данных, играющая ключевую роль в организации эффективного мониторинга и реагирования на инциденты. В рамках исследования оценивается вклад предложенной подсистемы в повышение эффективности SOC, снижение нагрузки на персонал, сокращение времени реагирования и улучшение прозрачности процессов информационной безопасности.

В условиях постоянного роста объёмов данных и усложнения ИТ-инфраструктур организации сталкиваются с новыми вызовами в обеспечении информационной безопасности. Для эффективного выявления, анализа и реагирования на инциденты критически важна централизованная подсистема сбора, обработки, хранения и визуализации данных. Однако на практике традиционные подходы к работе с данными оказываются недостаточно эффективными. Это приводит к ряду серьёзных проблем, среди которых можно выделить следующие: 1) разрозненность данных и отсутствие единого источника информации; 2) высокий объём данных и сложность их обработки; 3) недостаток видимости и мониторинга; 4) длительное время реакции на инциденты; 5)проблемы соответствия требованиям регуляторов (Compliance); 6) высокая стоимость коммерческих решений; 7) проблемы масштабируемости. Эти проблемы необходимо решить самым оптимальным методом, так как при таких условиях ухудшается эффективность и увеличивается перегруженность самого SOC и персонала[1].

Разрозненность данных и отсутствие единого источника информации. Во многих организациях данные о событиях безопасности поступают из различных источников: сетевых устройств, серверов, приложений, систем контроля доступа и других компонентов инфраструктуры. Эти данные часто хранятся в отдельных системах и форматах, что затрудняет их корреляцию и последующий анализ. Отсутствие единого централизованного хранилища информации снижает эффективность расследований и увеличивает вероятность пропуска критических инцидентов.

Высокий объём данных и сложность их обработки. Современные ИТ-системы генерируют огромные объёмы логов и телеметрии, которые необходимо обрабатывать в реальном времени. Ручной анализ становится практически невозможным, а традиционные инструменты не справляются с объёмами и скоростью поступающих данных. Это приводит к перегрузке систем, потере данных и замедлению реакции на потенциальные угрозы[2].

Недостаток видимости и мониторинга безопасности. Без полной картины происходящего в ИТ-среде специалисты по безопасности не могут своевременно обнаруживать аномалии и угрозы. Отсутствие сквозной видимости оставляет слепые зоны, которые могут использовать злоумышленники. Это особенно критично при попытках раннего выявления атак, таких как lateral movement или внутренние угрозы.

*Длительное время реакции на инциденты***.** В условиях фрагментированной информации и отсутствия автоматизации обработка инцидентов требует значительных временных и человеческих ресурсов. Специалисты тратят много времени на поиск, агрегацию и анализ данных из разных источников, что увеличивает среднее время обнаружения (MTTD) и реагирования (MTTR) на инциденты.

*Проблемы соответствия требованиям регуляторов (Compliance***).** Регуляторные стандарты (такие как GDPR, PCI DSS, ISO 27001 и др.) требуют наличия полной и достоверной информации о событиях безопасности, их хранении, анализе и отчётности. При отсутствии централизованной системы эти требования трудно выполнить, что может привести к штрафам, юридическим последствиям и потере доверия со стороны клиентов и партнёров.

Высокая стоимость коммерческих решений. Многие существующие на рынке платформы для управления событиями и инцидентами безопасности являются дорогостоящими и требуют серьёзных затрат на лицензии, инфраструктуру и техническую

поддержку. Для малого и среднего бизнеса это становится барьером для внедрения полноценного решения, соответствующего требованиям безопасности.

Проблемы масштабируемости. По мере роста организации и усложнения её инфраструктуры система мониторинга и хранения данных должна масштабироваться вместе с ней. Однако многие решения не обладают достаточной гибкостью и требуют значительных усилий при расширении. Это может привести к снижению производительности, увеличению времени обработки данных и ухудшению общей эффективности работы системы безопасности[2].

Принято считать, что для решения таких ключевых проблем, как разрозненность данных, высокая нагрузка на сотрудников, недостаточная видимость инцидентов и высокая стоимость решений, организации прибегают к следующим методам, направленным на повышение эффективности работы систем мониторинга и анализа информационной безопасности: 1) найм дополнительных сотрудников; 2) привлечение MSSP (Managed Security Service Provider); 3) Жесткие политики безопасности и обучение сотрудников; 4) использование EDR (Endpoint detection and response); 5) Применение AI/ML; 6) внедрение подсистемы сбора, обработки, хранения и визуализации данных[3].

Найм дополнительных сотрудников. Один из традиционных способов решения проблем с нагрузкой на систему мониторинга — расширение команды. Привлечение новых специалистов позволяет перераспределить текущие задачи, усилить мониторинг, повысить уровень анализа инцидентов и снизить риск пропуска критичных событий. Однако такой подход требует значительных затрат на подбор и обучение персонала, инфраструктурную поддержку и адаптацию процессов. Более того, при росте объёма данных, найм сотрудников лишь частично решает проблему масштабируемости и может не успевать за скоростью роста угроз.

Привлечение MSSP (Managed Security Service Provider). Передача функций мониторинга и реагирования внешнему сервисному провайдеру позволяет организациям сосредоточиться на основном бизнесе, не отвлекая ресурсы на внутреннюю поддержку инфраструктуры ИБ. MSSP обладают необходимыми инструментами, опытом и методологиями для централизованного мониторинга, корреляции событий и реагирования на инциденты. Однако данный подход связан с потерей контроля над данными, рисками в области конфиденциальности, а также ограниченной гибкостью в кастомизации аналитики и визуализации под бизнес-цели конкретной компании.

Жесткие политики безопасности и обучение сотрудников. Разработка и внедрение политик информационной безопасности, наряду с регулярным обучением сотрудников, помогают предотвратить часть инцидентов на ранних стадиях. Пользователи, осведомленные о правилах обращения с данными и признаках фишинга, снижают вероятность успешных атак. Однако этот метод не решает технические проблемы обработки больших объемов логов и не предоставляет необходимой видимости в инфраструктуре. Он может служить лишь дополнительным элементом в системе защиты, но не заменяет аналитические и визуализационные механизмы.

Использование EDR (Endpoint Detection and Response). EDR-системы обеспечивают сбор, анализ и реагирование на инциденты на уровне конечных точек, предоставляя ценные данные для расследований. Интеграция с другими источниками может повысить уровень видимости, однако зачастую такие системы работают изолированно и не обеспечивают полноценной агрегации и визуализации событий на уровне всей инфраструктуры. Кроме

того, для полноценной работы EDR требуется связка с централизованными платформами хранения и корреляции данных, иначе возникает риск фрагментации информации[4].

AI/ML – алгоритмы предиктивного анализа угроз. Применение машинного обучения и поведенческого анализа (например, UEBA) даёт возможность обнаруживать аномалии и скрытые угрозы, которые сложно выявить с помощью обычных правил. Такие технологии улучшают качество аналитики и позволяют снизить уровень ложных срабатываний. Однако они требуют больших массивов исторических данных и технически сложной интеграции с источниками событий. Без надлежащей платформы для хранения, корреляции и визуализации таких данных эффективность AI/ML-систем резко снижается.

Внедрение подсистемы сбора, обработки, хранения и визуализации данных. Наиболее эффективным способом решения описанных ранее проблем является внедрение централизованной подсистемы, обеспечивающей полный цикл работы с данными: от их сбора и агрегации — до анализа и визуализации. Такая система объединяет логи и телеметрию из разрозненных источников (SIEM, EDR, сетевые устройства, облачные решения), обрабатывает и нормализует их, а затем предоставляет аналитикам удобные панели мониторинга и отчётности. Это не только ускоряет обнаружение инцидентов, но и позволяет выявлять взаимосвязи между событиями, строить гипотезы и подтверждать атаки с опорой на достоверную и полную информацию[5].

Кроме того, такие системы существенно облегчают выполнение требований регуляторов за счёт автоматизированного формирования аудиторской отчетности, журналов учёта событий и хранения данных в соответствии со стандартами. Инструменты визуализации помогают команде безопасности быстро ориентироваться в инцидентах и оценивать критичность происходящего в режиме реального времени. При правильной архитектуре такие платформы масштабируются вместе с бизнесом и легко интегрируются с другими средствами защиты, включая SIEM, SOAR, XDR и AI/ML-системы.

Несмотря на то, что реализация такой системы требует ресурсов на этапе внедрения и настройки, её преимущества делают её стратегически важным элементом современной архитектуры информационной безопасности. Централизация, прозрачность, масштабируемость и соответствие требованиям делают этот подход наиболее предпочтительным для организаций, стремящихся повысить зрелость своей системы защиты[6]. В таблице 1 представлено сравнение методов для решения ключевых проблем.

Таблица 1 - Сравнение методов для решения ключевых проблем

Метод	Разрозненность данных	Высокий объем данных	Недостаток мониторинга	Долгое время реакции	Соответствие требованиям	Стоимость	Масштабируемость
Найм дополнительных аналитиков	Нет	Частично	Частично	Да	Частично	Дорого	Ограничено
MSSP (аутсорсинг SOC)	Частично	Да	Да	Да	нет	Дорого	Да

Политики безопасности и обучение	Нет	Частично	Частично	Частично	Не решает	Дёшево	Ограничено
EDR (защита конечных точек)	Нет	Частично	Да	Да	Нет	Дорого	Да
AI/ML для анализа угроз	Нет	Да	Частично	Да	Нет	Дорого	Да
Внедрение подсистемы сбора, обработки, хранения и визуализации данных (например, Wazuh)	Да	Да	Да	Да	Да	Оптимально	Гибко

При сравнении всех перечисленных методов оптимальным решением в условиях высокой нагрузки, роста объема данных и сложности соблюдения требований регуляторов является внедрение подсистемы сбора, обработки, хранения и визуализации данных. Это подтверждается как практическим опытом, так и аналитическим сравнением методов.

В отличие от точечных решений, таких как MSSP или EDR, данная подсистема обеспечивает централизацию данных, их нормализацию, удобную визуализацию и гибкую масштабируемость, что критично для зрелых SOC. По результатам сравнительного анализа, представленного в таблице 1, только данный подход полностью покрывает все ключевые проблемы: от разрозненности данных до соответствия требованиям регуляторов и адаптации к росту инфраструктуры.

Эффективность такого подхода особенно ярко проявляется в критических аспектах:

- Полная видимость событий безопасности в реальном времени.
- Снижение времени реакции за счет быстрой корреляции и фильтрации данных.
- Централизованная аналитика, обеспечивающая доказательную базу при расследованиях.
- Готовность к аудиту и формирование отчетности для регуляторов без дополнительных затрат.

Кроме того, реализация этой подсистемы возможна как на базе коммерческих решений, так и с использованием open-source инструментов, что делает её доступной и экономически оправданной даже для компаний со средним уровнем зрелости ИБ.

Таким образом, подсистема сбора, обработки, хранения и визуализации данных является не только техническим, но и стратегическим элементом архитектуры кибербезопасности, обеспечивающим фундамент для дальнейшей автоматизации, интеграции с AI/ML и построения комплексной защиты[7].

Описание подсистемы. Основные функции:

Сбор данных - обеспечивает централизованный сбор логов, событий безопасности и телеметрии из различных источников, таких как серверы, рабочие станции, сетевые устройства, приложения и облачные сервисы.

Методы сбора:

- Агентский сбор (Wazuh, OSSEC) — устанавливается агент на конечные узлы для мониторинга событий.
- Безагентский сбор (Syslog, API) — данные передаются по сети без установки дополнительного ПО.
- Сетевой мониторинг (Zeek, Suricata) — анализ трафика на предмет аномалий и вторжений.
- Журналирование событий (SIEM, ELK Stack) — логирование активности пользователей, процессов и систем.

Обработка данных - фильтрует, нормализует и анализирует собранные данные для выявления аномалий, атак и угроз.

Методы обработки:

- Нормализация данных (Elasticsearch, Logstash) — приведение логов к единому формату.
- Корреляция событий (SIEM, Wazuh) — объединение разрозненных событий в единую картину атаки.
- Анализ на основе сигнатур (Suricata, Snort) — поиск известных шаблонов атак.
- Поведенческий анализ (ML, UEBA) — выявление аномального поведения пользователей и систем.

Хранение данных - обеспечивает долговременное хранение логов и событий для расследования инцидентов, соответствия регуляторным требованиям и трендовому анализу.

Методы хранения:

- Реляционные базы данных (MySQL, PostgreSQL) — для структурированной информации.
- NoSQL базы (Elasticsearch, MongoDB) — для хранения логов и событий в реальном времени.
- Облачные хранилища (Amazon S3, Google Cloud Storage) — для долгосрочного хранения архивов.
- Локальное хранилище (NAS, SAN) — для высокой скорости доступа и безопасности данных.

Визуализация данных - предоставляет SOC-аналитикам удобные инструменты для мониторинга, анализа и реагирования на инциденты.

Методы визуализации:

- Дашборды и графики (Kibana, Grafana) — наглядное представление данных.
- Интерактивные отчеты (Power BI, Tableau) — анализ тенденций и угроз.
- Автоматизированные оповещения (Wazuh, Splunk) — уведомления о критических событиях.
- Форензика и анализ инцидентов (TheHive, MISP) — расследование атак на основе логов.

Были выделены следующие методы реализации подсистемы сбора, обработки, хранения и визуализации данных для SOC:

- SIEM-системы (Splunk, ArcSight, QRadar)

- Wazuh
- Лог-менеджеры (ELK, Graylog)
- IDS/IPS (Suricata, Snort)
- XDR (Cortex XDR, Microsoft Defender)

SIEM-системы являются ядром многих SOC. Они собирают и централизуют логи из множества источников (серверы, сетевое оборудование, приложения), анализируют события в реальном времени, применяют правила корреляции, выявляют угрозы и создают отчеты. SIEM может интегрироваться с SOAR, XDR, Threat Intelligence и другими компонентами безопасности[8].

Wazuh — это бесплатная open-source платформа, объединяющая функции SIEM, HIDS (системы обнаружения вторжений на хосте), лог-анализа, аудита, FIM (мониторинга целостности файлов), обнаружения уязвимостей и визуализации.

Системы лог-менеджмента предназначены для централизованного сбора, фильтрации, хранения и визуализации логов. ELK Stack (Elasticsearch + Logstash + Kibana) и Graylog предоставляют возможность анализа событий и построения дашбордов, но в отличие от SIEM, не имеют продвинутой корреляции и встроенных механизмов реагирования.

Системы обнаружения (IDS) и предотвращения (IPS) вторжений анализируют сетевой трафик для выявления угроз и вредоносной активности. Они используют сигнатуры атак и аномалий, могут действовать как в режиме мониторинга, так и в режиме блокировки.

XDR объединяет в себе данные из EDR, NDR, почтовых и облачных решений для комплексного мониторинга инфраструктуры. Использует машинное обучение, поведенческий анализ и автоматизацию для обнаружения и устранения угроз. Является «следующим поколением SIEM», действующим проактивно[9]. В таблице 2 представлено сравнение методов реализации.

Таблица 2 - Сравнение методов реализации

Проблема SOC	SIEM-системы (Splunk, ArcSight, QRadar)	Wazuh (Open-source SIEM)	Лог-менеджеры (ELK, Graylog)	IDS/IPS (Suricata, Snort)	XDR (Cortex XDR, Microsoft Defender)
Разрозненность данных	Централизованный сбор логов	Централизованный сбор логов	Собирают логи, но без глубокой аналитики	Не собирают логи, только анализируют пакеты	Собирают и анализируют данные, но в рамках вендорской экосистемы
Высокий объем данных и сложность обработки	Хорошая масштабируемость, но дорого	Масштабируемость через Elasticsearch	Ограниченная обработка данных	Не предназначены для работы с большими логами	Используют машинное обучение, но требуют мощных ресурсов
Недостаток видимости и мониторинга	Развитые дашборды и аналитика	Интеграция с Kibana для визуализации	Гибкая визуализация, но требует настройки	тсутствует централизованная визуализаци	Встроенная аналитика, но только в пределах

				я	экосистемы
Долгое время реакции на инциденты	Автоматизированные правила корреляции	Встроенные механизмы обнаружения угроз	Нет механизмов автоматического реагирования	Обнаруживают атаки, но не хранят события	Реагируют на инциденты в реальном времени
Соответствие требованиям регуляторов (Compliance)	Встроенные инструменты соответствия	Политики соответствия (PCI DSS, GDPR и др.)	Не сертифицированы для compliance	Не связаны с регуляторными требованиями	Автоматический аудит и отчеты
Высокая стоимость	Дорогое лицензирование	Бесплатно	Бесплатно, но требует настройки	Бесплатно, но не заменяет SIEM	Высокая стоимость подписки
Проблемы масштабируемости	Ограничена лицензиями, высокие затраты	Гибкая масштабируемость	Хорошая масштабируемость	Не предназначены для хранения больших данных	Масштабируются в облаке, но дорого

Выводы из сравнительного анализа:

- **SIEM-системы (Splunk, ArcSight, QRadar)** — мощные решения, но дорогостоящие, требуют сложного администрирования и масштабируемость зависит от лицензии.
- **Wazuh** — решает практически все проблемы SOC, обеспечивая бесплатную альтернативу коммерческим SIEM-системам, но требует ручной настройки.
- **Лог-менеджеры (ELK, Graylog)** — хороши для хранения и визуализации, но не включают автоматическое обнаружение угроз и compliance.
- **IDS/IPS (Suricata, Snort)** — полезны для выявления сетевых атак, но не могут заменять полноценный SIEM.
- **XDR (Cortex XDR, Microsoft Defender)** — продвинутые решения, но их возможности ограничены экосистемой конкретного вендора и высокой стоимостью.

Таким образом, подводя итог изложенного выше Wazuh — оптимальный вариант для построения SOC, так как объединяет возможности SIEM, лог-менеджеров и compliance-систем при минимальных затратах.

Платформа Wazuh предоставляет функции XDR и SIEM для защиты облачных, контейнерных и серверных рабочих нагрузок. Они включают анализ данных журналов, обнаружение вторжений и вредоносных программ, мониторинг целостности файлов, оценку

конфигурации, обнаружение уязвимостей и поддержку соответствия нормативным требованиям.

Архитектура Wazuh включает три ключевых компонента, которые взаимодействуют между собой для обеспечения централизованного сбора, обработки, хранения и визуализации данных безопасности в SOC.

1. Wazuh Server (Сервер)

Основная функция:

- Управляет агентами (Wazuh Agents)
- Обрабатывает собранные события безопасности
- Выполняет анализ логов, корреляцию событий и обнаружение угроз
- Интегрируется с Threat Intelligence (MISP, OTX, VirusTotal)

Связь:

- Получает данные от Wazuh Agents
- Передает обработанные данные в Wazuh Indexer
- Поддерживает связь с Wazuh Dashboard для настройки правил безопасности

2. Wazuh Indexer (Индексатор данных, аналог Elasticsearch)

Основная функция:

- Является хранилищем данных (индексирует и хранит события безопасности)
- Обеспечивает быстрый поиск и анализ данных
- Оптимизирован специально для работы с Wazuh (заменил Elasticsearch в новых версиях)

Связь:

- Получает обработанные данные от Wazuh Server
- Предоставляет хранимую информацию Wazuh Dashboard

3. Wazuh Dashboard (Панель мониторинга, UI-интерфейс)

Основная функция:

- Визуализирует данные из Wazuh Indexer
- Позволяет анализировать угрозы через дашборды и отчеты
- Позволяет управлять настройками Wazuh (конфигурация правил, агентов и политик безопасности)

Связь:

- Получает данные от Wazuh Indexer
- Позволяет управлять настройками Wazuh Server

Как взаимодействуют компоненты Wazuh?

1. Wazuh Server анализирует логи и отправляет их в Wazuh Indexer
2. Wazuh Indexer хранит и индексирует данные
3. Wazuh Dashboard визуализирует события и предоставляет интерфейс для анализа[10]

На рисунке 1 представлена центральные компоненты архитектуры Wazuh.

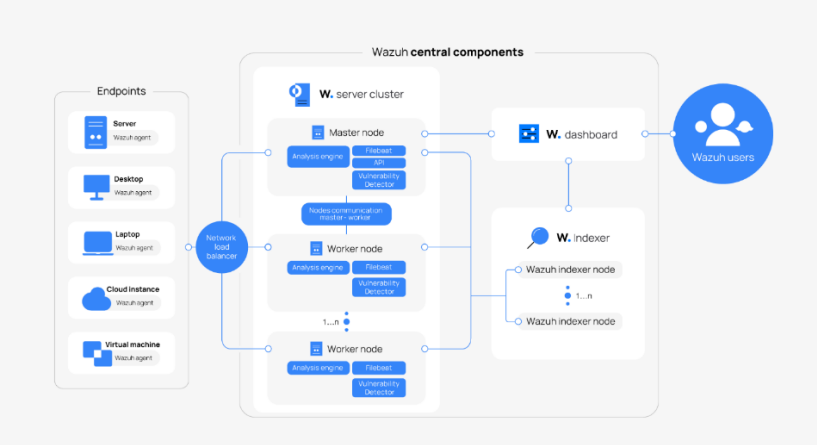

Рисунок 1 - Центральные компоненты Wazuh

Решение Wazuh основано на агенте Wazuh, который развертывается на контролируемых конечных точках, и на трех центральных компонентах: сервере Wazuh, индексаторе Wazuh и панели мониторинга Wazuh.

Индексатор Wazuh — это высокомасштабируемый полнотекстовый поисковый и аналитический движок. Этот центральный компонент индексирует и хранит оповещения, сгенерированные сервером Wazuh.

Сервер Wazuh анализирует данные, полученные от агентов. Он обрабатывает их с помощью декодеров и правил, используя разведку угроз для поиска известных индикаторов компрометации (IOC). Один сервер может анализировать данные от сотен или тысяч агентов и масштабироваться горизонтально при настройке в качестве кластера. Этот центральный компонент также используется для управления агентами, настраивая и обновляя их удаленно при необходимости.

Панель управления Wazuh — это веб-интерфейс пользователя для визуализации и анализа данных. Она включает готовые панели управления для поиска угроз, соответствия нормативным требованиям (например, PCI DSS, GDPR, CIS, HIPAA, NIST 800-53), обнаруженных уязвимых приложений, данных мониторинга целостности файлов, результатов оценки конфигурации, событий мониторинга облачной инфраструктуры и других. Она также используется для управления конфигурацией Wazuh и для мониторинга ее состояния.

Агенты Wazuh устанавливаются на конечных точках, таких как ноутбуки, настольные компьютеры, серверы, облачные экземпляры или виртуальные машины. Они обеспечивают возможности предотвращения, обнаружения и реагирования на угрозы. Они работают на таких операционных системах, как Linux, Windows, macOS, Solaris, AIX и HP-UX. На рисунке 2 представлена функциональная схема работы Wazuh.

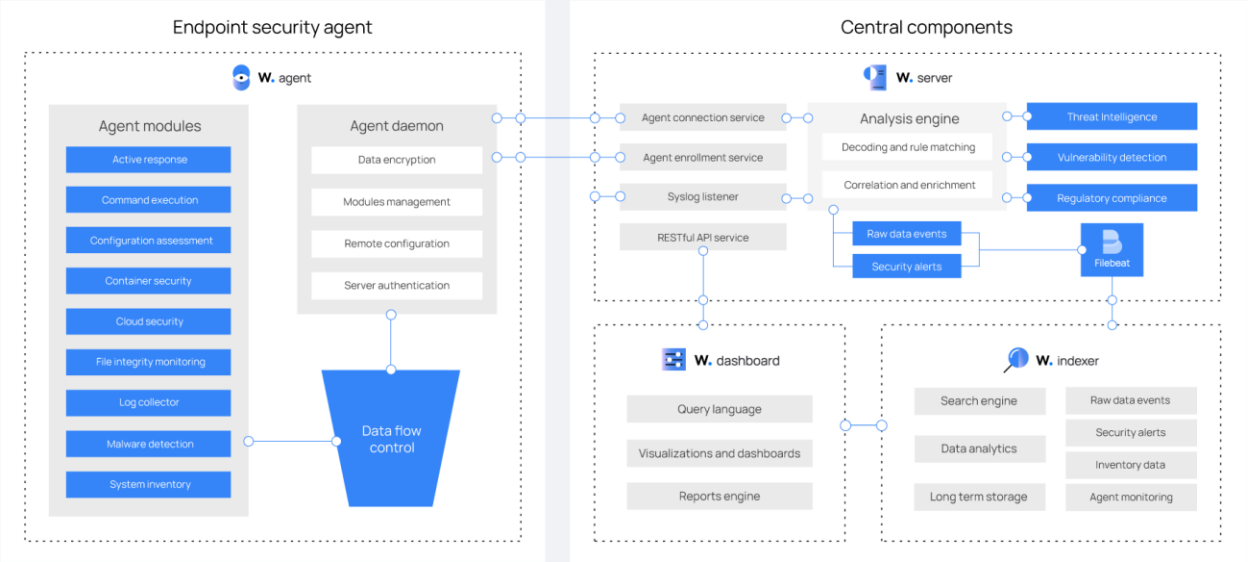

Рисунок 2 - Функциональная схема работы Wazuh

Таким образом, в настоящее время организации всё чаще внедряют **Wazuh** как эффективное и доступное решение для реализации подсистемы сбора, обработки, хранения и визуализации данных в SOC. Это подтверждается реальными примерами успешной интеграции Wazuh в инфраструктуру как частных компаний, так и облачных провайдеров.

Например, облачный провайдер **Nubes** внедрил Wazuh для построения системы мониторинга и реагирования на инциденты в своей платформе NGcloud [11]. До внедрения платформа испытывала трудности с централизованным сбором и визуализацией логов, а также с оперативным реагированием на аномалии [12].

После интеграции Wazuh организация получила централизованный доступ ко всем логам, а дежурные администраторы и первая линия поддержки смогли быстро выявлять и анализировать потенциальные угрозы [13]. Это позволило значительно снизить нагрузку на специалистов по ИБ и повысить общую эффективность мониторинга [13].

Кроме того, благодаря модулю корреляции событий и встроенной визуализации в Wazuh Dashboard, организация сократила время на анализ инцидентов и повысила уровень прозрачности инфраструктуры [14]. Решение показало свою эффективность, при этом не потребовав больших финансовых затрат, что делает Wazuh особенно привлекательным для компаний с ограниченным бюджетом на ИБ.

Заключение.

Таким образом следует отметить, что в ходе проведенного анализа были рассмотрены основные проблемы, влияющие на эффективность функционирования центров мониторинга информационной безопасности (SOC): высокая нагрузка на аналитиков, замедленное реагирование на инциденты, а также разрозненность источников и форматов данных. Для устранения этих проблем исследовались различные методы реализации подсистемы сбора, обработки, хранения и визуализации данных, включая SIEM-системы (Splunk, ArcSight, QRadar), лог-менеджеры (ELK, Graylog), IDS/IPS (Suricata, Snort), решения класса XDR (Cortex XDR, Microsoft Defender) и Wazuh.

Результаты сравнительного анализа показали, что Wazuh является наиболее сбалансированным и универсальным решением. Он объединяет функции нескольких классов систем: SIEM, HIDS, лог-менеджмента и визуализации, при этом оставаясь доступным по лицензированию и гибким в развертывании. Подсистема, построенная на базе Wazuh,

позволяет централизованно собирать и нормализовать данные с различных источников, эффективно обрабатывать события, хранить их в масштабируемом хранилище (через Elasticsearch/OpenSearch) и визуализировать через настраиваемые дашборды в Wazuh Dashboard. Это значительно упрощает выявление и расследование инцидентов, снижает нагрузку на специалистов и повышает уровень прозрачности инфраструктуры.

Таким образом, реализация подсистемы сбора, обработки, хранения и визуализации данных на базе Wazuh становится оптимальным решением для построения эффективного SOC. Она обеспечивает высокий уровень автоматизации и интеграции, способствует сокращению времени реагирования и помогает организациям достигать высокого уровня киберустойчивости при минимальных затратах. Благодаря активному сообществу, расширяемой архитектуре и поддержке стандартов безопасности, Wazuh представляет собой стратегически целесообразный выбор для компаний, стремящихся к усилению информационной безопасности и оптимизации процессов внутри SOC.

Литература

1. Gartner. Market Guide for Security Information and Event Management [Электронный ресурс]. – 2024. – Режим доступа: https://www.gartner.com/, свободный.
2. Forrester. The State of Open-Source Security Tools Adoption [Электронный ресурс]. – 2023. – Режим доступа: https://www.forrester.com/, свободный.
3. MITRE ATT&CK Framework [Электронный ресурс]. – Офиц. сайт MITRE ATT&CK. – Режим доступа: https://attack.mitre.org/, свободный.
4. Elastic Stack Documentation. How Wazuh integrates with Elastic Stack [Электронный ресурс]. – Режим доступа: https://www.elastic.co/, свободный.
5. IBM QRadar SIEM Overview [Электронный ресурс]. – Офиц. сайт IBM. – Режим доступа: https://www.ibm.com/qradar, свободный.
6. Splunk SIEM Documentation [Электронный ресурс]. – Режим доступа: https://www.splunk.com/, свободный.
7. Microsoft Sentinel. Cloud-native SIEM capabilities [Электронный ресурс]. – 2024. – Режим доступа: https://www.microsoft.com/sentinel, свободный.
8. ArcSight SIEM by Micro Focus [Электронный ресурс]. – Режим доступа: https://www.microfocus.com/arcsight, свободный.
9. Zeek (Bro) Network Security Monitor. Official Zeek documentation [Электронный ресурс]. – Режим доступа: https://www.zeek.org/, свободный.
10. Wazuh Documentation. Features, integrations, and use cases [Электронный ресурс]. – Режим доступа: https://documentation.wazuh.com/, свободный.
11. Cybersecurity Trends Report. Analysis of SIEM adoption trends [Электронный ресурс]. – 2023. – Режим доступа: https://www.cybersecurity-insiders.com/, свободный.
12. CISO Club. Почему open-source становится доминирующим трендом в кибербезопасности [Электронный ресурс]. – 2024. – Режим доступа: https://cisoclub.ru/, свободный.
13. Как Wazuh помог наладить круглосуточный мониторинг и реагирование на ИБ-события [Электронный ресурс] // Habr. – Режим доступа: https://habr.com/ru/companies/nubes/articles/778990/, свободный.
14. Google Chronicle Security Analytics. Cloud-based SIEM and security tools [Электронный ресурс]. – Режим доступа: https://cloud.google.com/chronicle, свободный.