**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Информационная безопасность автоматизированных систем на транспорте»

**ОТЧЕТ**

по производственной практике

«НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА»

на тему: «Анализ SIEM-системы Wazuh как объекта ИБ»

Форма обучения – очная

|  |  |  |
| --- | --- | --- |
| **Выполнил обучающийся**  Курс 5  Группа КИБ-012 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Груздев Г.Е. |
|  |  |  |
| **Руководитель** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Корниенко С.В. |

Санкт-Петербург

2025

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральноегосударственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Информационная безопасность автоматизированных систем на транспорте»

**Задание на выполнение практического задания**

по производственной практике

«НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА»

Груздев Георгий Евгеньевич

Тема: «Анализ SIEM-системы Wazuh как объекта ИБ»

Срок сдачи обучающимся законченного проекта:

Исходные данные для выполнения проекта:

Содержание пояснительной записки:

Перечень графического материала: \_\_ табл., \_1\_\_ рис.

Дата выдачи задания:

Руководитель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Корниенко С.В.

Задание принял к исполнению: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Груздев Г.Е.

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Информационная безопасность автоматизированных систем на транспорте»

**Календарный план выполнения и защиты выполнение практического задания**

по производственной практике

«НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА»

Груздев Георгий Евгеньевич

Тема: «Анализ SIEM-системы Wazuh как объекта ИБ»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование этапов** | **Планируемая дата** | **Фактическая дата** | **Подпись руководителя** | **Примечание** |
| 1 | Выдача практического задания |  |  |  |  |
| 2 | Сдача отчета на первую проверку |  |  |  |  |
| 3 | Сдача отчета на повторные проверки при необходимости |  |  |  |  |
| 4 | Допуск к защите отчета |  |  |  |  |
| 5 | Защита отчета |  |  |  |  |

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (подпись)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Информационная безопасность автоматизированных систем на транспорте»

**Оценочный лист на выполнение практического задания**

по производственной практике

«НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА»

Тема: «Анализ SIEM-системы Wazuh как объекта ИБ»

| **№**  **п/п** | **Материалы необходимые для оценки знаний, умений**  **и навыков** | **Показатель**  **оценивания** | | **Критерии**  **оценивания** | **Шкала оценивания** | | **Полученные баллы** | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Отчет по заданию | Соответствие структуры отчета установленной структуре | | Соответствует | 10 | |  | | | |
| Не соответствует | 0 | |  | | | |
| Соответствие содержания отчета выданному заданию | | Соответствует | 20 | |  | | | |
| Не соответствует | 0 | |  | | | |
| Оформление списка использованных источников в соответствии с ГОСТ 7.1-2003 | | Соответствует | 10 | |  | | | |
| Не соответствует | 0 | |  | | | |
| Итого максимальное количество баллов по п. 1 | | | | | **40** | |  | | | |
| 2 | Организация практики | Сроки прохождения практики | | Практика пройдена в указанные сроки | 30 | |  | | | |
| Сроки не соблюдены | 0 | |  | | | |
| Итого максимальное количество баллов по п. 2 | | | | | **30** | |  | | | |
| **ИТОГО максимальное количество баллов** | | | | | **70** | |  | | | |
| **Защита отчета по практике** | | | * получены полные ответы на вопросы – 23-30 баллов; * получены достаточно полные ответы на вопросы – 17-22 баллов; * получены неполные ответы на вопросы или часть вопросов – 10-16 баллов; * не получены ответы на вопросы или вопросы не раскрыты – 0 баллов. | | | **30** | |  |  |  |
| **Итоговая оценка** | | | «Отлично» - 86-100 баллов  «Хорошо» - 75-85 баллов  «Удовлетворительно» - 60-74 баллов  «Неудовлетворительно» - менее 59 баллов (вкл.) | | | | | | |  |

Руководитель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Корниенко С.В.

(подпись)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

# **АНАЛИЗ SIEM-СИСТЕМЫ WAZUH КАК ОБЪЕКТА ИБ**

## **1.1 Общее описание SIEM-систем**

SIEM (Security Information and Event Management) – это система управления событиями информационной безопасности, которая объединяет функции мониторинга, анализа и корреляции данных из различных источников. Основной задачей SIEM является обнаружение угроз, расследование инцидентов и автоматизация реагирования на инциденты информационной безопасности (ИБ).

Основные функции SIEM:

* централизованный сбор и агрегация логов с различных систем;
* корреляция событий для выявления потенциальных угроз;
* генерация отчетов и оповещение о возможных инцидентах;
* анализ поведения пользователей (UEBA – User and Entity Behavior Analytics).

События информационной безопасности (СИБ) – это записи (логи), фиксирующие активность в информационной системе, которая может иметь значение с точки зрения безопасности.

К СИБ можно отнести:

* попытки входа в систему (успешные и неуспешные);
* изменения в конфигурациях системы;
* попытки несанкционированного доступа к данным;
* аномальные сетевые соединения и передача данных.

Анализ СИБ помогает выявлять подозрительные активности и предотвращать возможные кибератаки.

## **1.2 Архитектура SIEM-системы Wazuh**

На рисунке 1 представлена Архитектура SIEM-системы Wazuh:

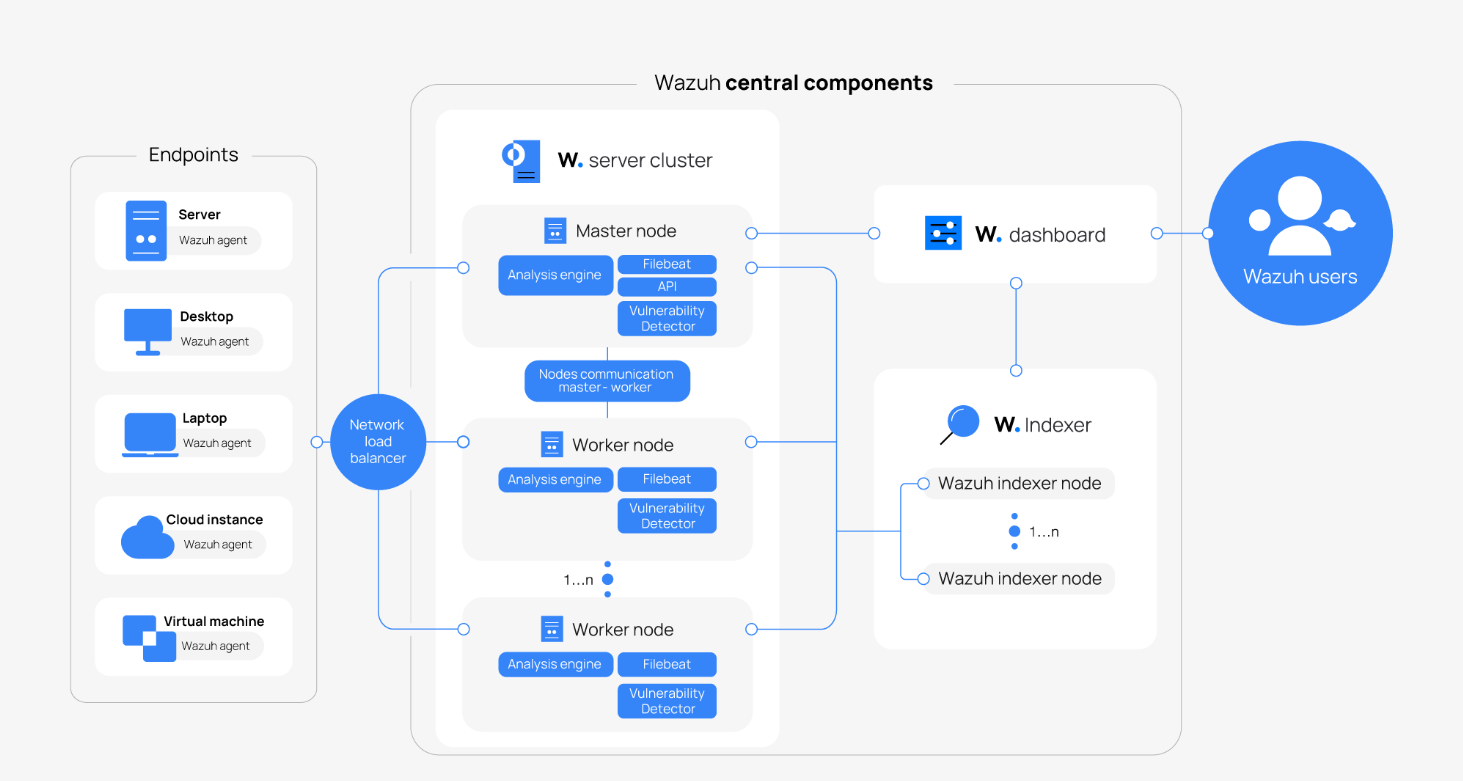


Рисунок 1 – Архитектура SIEM-системы Wazuh

Wazuh состоит из следующих компонентов:

* Wazuh indexer (индексер) – индексирует данные и хранит их в базе данных;
* Wazuh server (сервер) – анализирует данные, обрабатывает события и отправляет их на другие компоненты;
* Wazuh dashboard (панель мониторинга) – предоставляет графический интерфейс для просмотра и анализа данных;
* Wazuh agent (агент) – собирает данные с локальных устройств и отправляет их на сервер.

Архитектура Wazuh основана на агентах, пересылающих данные с различных технических устройств на центральный сервер. Для сбора СИБ с устройств, на которые невозможно установить агента, применяется безагентный сбор, отправляющий данные через системный журнал, SSH или API. Центральный сервер расшифровывает и анализирует пришедшие к нему данные, передавая их в индексатор Wazuh. Кластер индексаторов Wazuh состоит из одного или нескольких узлов для чтения и записи индексов.

**1.2.1 Связь между агентом и сервером**

Агент непрерывно отправляет события на сервер для анализа и обнаружения угроз. Для начала отправки логов агент устанавливает соединение со специальной службой сервера, которая по умолчанию прослушивает 1514 порт (это значение настраивается). При получении данных с агентов, сервер декодирует и события на срабатывание правил. Проверкой событий занимается модуль обнаружения уязвимостей, который регулярно обновляет список уязвимостей и генерирует оповещения в случае обнаружения подозрительной активности. При срабатывании правила, сервер дополняет событие информацией (идентификатор правила (rule ID), название правила (rule name) и т. д.) Все события записываются в файл /var/ossec/logs/archives.json. События, для которых сработали правила, записываются в /var/ossec/logs/alerts.json.

**1.2.2 Связь между сервером и индексатором**

Сервер использует Filebeat для передачи данных в индексатор, безопасность передачи обеспечивается с помощью шифрования TLS. Filebeat отслеживает данные, которые даёт сервер, и пересылает их индексатору, который прослушивает порт 9200/TCP. После индексации данные можно просмотреть и проанализировать с помощью панели мониторинга Wazuh.

**1.2.3 Хранение архивных данных**

Оповещения и события хранятся в файлах на сервере и отправляются в индексатор. Файлы ежедневно сжимаются и подписываются с использованием контрольных сумм MD5, SHA1 и SHA256. Рекомендуется ротация и резервное копирование архивных файлов в зависимости от емкости хранилища.

## **1.3 Определение защищаемых информационных ресурсов**

1. Защищаемой информацией в подсистеме управления, мониторинга и реагирования на компьютерные инциденты Wazuh являются:

* персональные данные пользователей системы: включает в себя личные данные сотрудников, поддерживающих и обслуживающих Wazuh.

1. Системные сообщения и логи:

* информация, представляющая служебные сообщения и данные, передаваемые между компонентами системы.

1. Данные от датчиков и мониторов:

* сведения, получаемые от различных датчиков, используемых в рамках Wazuh для мониторинга и контроля различных параметров.

1. Рабочие отчеты и аналитика:

* информация, создаваемая системой в процессе работы, включая отчеты, аналитическую информацию и другие документы, связанные с оперативной деятельностью.

1. Данные о пользователях системы:

* включают в себя информацию о пользователях Wazuh, их ролях и уровнях доступа.

Защищаемой информационной инфраструктурой в Wazuh являются:

1. Рабочие места и станции операторов:

Компьютерные рабочие места операторов и других пользователей системы.

1. Каналы связи и сетевое оборудование:

Инфраструктура сетевого взаимодействия, включая коммуникационные каналы и сетевое оборудование.

1. Программное обеспечение (ПО) на серверах и АРМах:

Все компоненты программного обеспечения, установленные на серверах и рабочих станциях.

1. Сервера (приложений, баз данных):

Сервера, обеспечивающие функционирование приложений и хранение данных в рамках Wazuh.

## **1.4 Определение угроз безопасности информации для Wazuh:**

1. Целостности:

* незащищенный канал технической поддержки;
* получения информации из неавторизованного источника;
* не декларированные возможности программы ПЛК;
* воздействия на канал связи на аппаратном и программном уровнях.

1. Конфиденциальности:

* незащищенный канал технической поддержки;
* отправления информации неавторизованному объекту на аппаратном уровне
* воздействия на канал связи на аппаратном уровне;
* отправка информации неавторизованному источнику.

1. Доступности:

* перегрузка канала связи;
* отказ в обслуживании;
* уничтожение канала связи.

Определим угрозы безопасности информации для Wazuh, как для ИСПДн. В соответствии с базовой моделью угроз безопасности информации при их обработке в ИСПДн:

1. Утечка по техническим каналам: перехват акустической, видовой информации, через ПЭМИН.
2. Угрозы модификации информации:

* нештатные режимы работы: риск изменения нормального функционирования системы путем преднамеренных изменений служебных данных, игнорирования ограничений и модификации самих данных;
* внедрение вредоносных программ: возможность внедрения вредоносных программ, которые могут нарушить работу системы, а также угрожать конфиденциальности и целостности данных;
* комбинированные угрозы: риск возникновения ситуаций, когда несколько угроз объединяются для создания более сложных и опасных сценариев атак.

В соответствии с методикой оценки угроз безопасности информации ФСТЭК актуальные нарушители разделяются на следующие группы нарушителей:

* внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;
* внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

Составим перечень актуальных нарушителей и их возможностей для Wazuh:

1. специальные службы иностранных государств (внутренние, внешние) – обладают высокими возможностями по реализации угроз безопасности (Н4);
2. террористические, экстремистские группировки (внешние) – обладают высокими возможностями по реализации угроз безопасности (Н4);
3. преступные группы (внешние) – средними возможностями по реализации угроз безопасности информации (Н3);
4. отдельные физические лица (хакеры; внешние, внутренние) – базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
5. конкурирующие организации (внешние) – базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
6. разработчики программных, программно-аппаратных средств (внешние) – средними возможностями по реализации угроз безопасности информации (Н3);
7. лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем (внутренние) – базовыми повышенными возможностями по реализации угроз безопасности информации (Н2);
8. поставщики услуг связи, вычислительных услуг (внешние) – базовыми возможностями по реализации угроз безопасности информации (Н1);
9. лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ (внешние) – базовыми возможностями по реализации угроз безопасности информации (Н1);
10. лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.; внутренние) – базовыми возможностями по реализации угроз безопасности информации (Н1);
11. авторизованные пользователи систем и сетей (внутренние) – базовыми возможностями по реализации угроз безопасности информации (Н1);
12. системные администраторы и администраторы безопасности (внутренние) – высокими возможностями по реализации угроз безопасности информации (Н4);
13. бывшие (уволенные) работники (пользователи; внешние) – базовыми возможностями по реализации угроз безопасности информации (Н1).

## **1.5 Проблема с безагентным сбором событий информационной безопасности**

В ходе настройки и тестирования SIEM-системы Wazuh была обнаружена проблема с безагентным сбором событий информационной безопасности по протоколам syslog, HTTP, FTP, NetFlow, SNMP и SQL. Безагентный сбор данных – это метод получения информации о событиях безопасности без установки специализированного программного обеспечения (агентов) на конечных узлах системы. Такой подход снижает нагрузку на систему и упрощает процесс администрирования, но может иметь ограничения в глубине сбора данных. Недостаточная поддержка различных технических устройств системой Wazuh приводит к двум критически важным последствиям:

* нарушение доступности информации, так как логи с определенных устройств невозможно получить;
* нарушение целостности информации, поскольку отсутствие данных от части технических устройств искажает общую картину состояния инфраструктуры.

Краткая характеристика протоколов:

* Syslog – это стандартный протокол для передачи логов, широко используемый в сетевых устройствах, серверах и приложениях. Поддерживает централизованный сбор событий и их фильтрацию;
* протокол HTTP используется для передачи событий в формате JSON или XML. HTTPS обеспечивает защищенный канал передачи данных;
* протокол FTP (File Transfer Protocol) используется для передачи файлов между клиентом и сервером по сети;
* NetFlow – технология мониторинга сетевого трафика, позволяющая анализировать потоки данных и выявлять подозрительную активность в сети;
* протокол SNMP (Simple Network Management Protocol) используется для мониторинга состояния сетевого оборудования и передачи событий о его работе;
* методы сбора событий через SQL-запросы позволяют анализировать активность в базах данных и фиксировать потенциально опасные операции.

Сам сервер Wazuh может принимать события только по протоколу syslog (указывается в настройках по пути /var/ossec/etc/ossec.conf), что не соответствует нашим требованиям. Поэтому встал вопрос с использованием дополнительного модуля, который бы смог принимать события по всем нужным протоколам, был достаточно прост в настройке и развёртывании, не потреблял много ресурсов, был совместим со всеми техническими устройствами, в том числе и специфичными для российских реалий. Были рассмотрены следующие методы решения данной проблемы:

#### ****1.5.1 Использование Filebeat****

Filebeat – это легковесный агент для передачи лог-файлов в системы анализа данных (например, Opensearch или Logstash). Он часто используется в архитектуре Wazuh для отправки логов с серверов и устройств, работающих без агентов.

**Как используется в Wazuh?** Filebeat устанавливается на отдельный сервер (или на сам сервер Wazuh) и настраивается на чтение логов из файлов или приема данных по различным протоколам. Далее он пересылает эти логи в Wazuh через Logstash или напрямую в Opensearch.

**Недостатки Filebeat:**

* ограниченный функционал – Filebeat только передает данные, не выполняя их нормализацию или обработку;
* не поддерживает сложные преобразования – если требуется изменить формат данных или объединить события, необходимо дополнительное ПО (например, Logstash);
* не всегда удобен для безагентного сбора – Filebeat хорошо работает с файловыми логами, но не интегрируется напрямую с SNMP, NetFlow и SQL-запросами.

#### ****1.5.2 Использование Logstash****

Logstash – это инструмент для сбора, обработки и передачи данных, входящий в ELK-стек. В отличие от Filebeat, Logstash обладает мощными возможностями по обработке событий, включая парсинг, фильтрацию и преобразование данных.

**Как должно работать в Wazuh?** Logstash получает данные от различных источников (Syslog, HTTP, FTP, SQL и т. д.), обрабатывает их с помощью фильтров и передает в Wazuh (Elasticsearch).

**Преимущества Logstash:**

* поддерживает обработку данных из множества источников, включая нестандартные форматы;
* позволяет нормализовать и фильтровать данные перед отправкой;
* гибкая система плагинов для настройки интеграций.

**Недостатки Logstash:**

* сложность настройки – требует детальной конфигурации, что увеличивает время развёртывания;
* ресурсоемкость – потребляет много оперативной памяти и CPU, особенно при обработке большого потока данных;
* ограниченная гибкость конфигурации – некоторые специфические требования трудно реализовать без дополнительных плагинов.

В конечном итоге ни одно из решений не удовлетворяет требований к модулю – решение с разработкой собственного модуля напрашивается само собой.

## **1.6 Вывод**

Ограничения Wazuh и существующих инструментов (Filebeat, Logstash) делают безагентный сбор событий проблематичным, особенно если требуется поддержка **HTTP, FTP, SNMP и SQL**.

Для SIEM-системы **критически важна непрерывность и полнота собираемой информации**. Пропуски в логах или невозможность получать данные от части устройств могут привести к потере ценных сведений о потенциальных угрозах и искажению общей картины состояния инфраструктуры.

Для решения этой проблемы необходимо разработать **собственное программное решение**, которое будет учитывать особенности российской инфраструктуры и отвечать следующим требованиям:

* простая настройка и администрирование;
* минимальное потребление ресурсов;
* поддержка всех необходимых протоколов.

Такое решение позволит решить проблемы с доступностью и целостностью данных, обеспечив эффективный мониторинг безопасности в инфраструктуре организации.