МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ

АЗЕРБАЙДЖАНСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИСТЕТ

Кафедра “Радиотехника и телекоммуникация”

На правах рукописи

САДЫГ-ЗАДЕ НАДИР АДИЛЬ

ОМАРОВ РУСЛАН АБДУЛЛА

Специальность: 060627 – “Инженерия электроники, телекоммуникации и радиотехники”

Специализация: “Информационная безопасность телекоммуникационных систем”

Тема: Исследование и проектирование SIEM систем

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Научный руководитель: к.т.н. доц. Г. А. Алиев

БАКУ-2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информация - ключевой актив в современном бизнесе. Использование интернет-технологий позволяет эффективно развивать и увеличивать прибыльность компании, но также открывает широкие возможности для деятельности злоумышленников. В результате информационные системы и сети становятся высоко уязвимыми.

Современные кибер-угрозы представляют собой значительно большую и серьезную угрозу, чем мы можем себе представить. За последние пять лет мировые компании столкнулись с масштабными кибератаками, такими как BlackEnergy, TeleBots, CryptoLocker, GreyEnergy, Industroyer, Petya и NotPetya, BadRabbit, Buhtrap, WannaCry, TeslaCrypt, Nyetya. Целию атаки включают предприятия критической инфраструктуры, энергетический сектор, финансовые организации, транспортные и логистические компании, медицинские и фармацевтические фирмы, а также разработчиков программного обеспечения. Это показывает, что ни одно предприятие не может быть полностью защищено от возможных материальных и финансовых потерь. Для обеспечения безопасности предприятий от таких атак необходимо объективно оценить надежность информационной системы и провести соответствующую проверку.

Аудит информационной безопасности является основным инструментом для контроля уровня защиты информационных активов. Он позволяет руководству и владельцам оценить реальное состояние информационной безопасности, выявить уязвимые места и направления, а также получить представление о необходимых мерах для повышения уровня защищенности. При профессиональном выполнении аудита результаты обеспечивают возможность построения комплексной и эффективной системы защиты, способной эффективно справляться с поставленными задачами. Используя результаты аудита информационной безопасности, построение комплексной системы защиты информации (КСЗИ) позволяет обеспечить постоянный контроль над системой, отслеживать все события и модификации данных, а также

своевременно реагировать на них. Одним из ключевых элементов эффективного аудита безопасности являются системные журналы. Однако, большой объем данных из этих журналов может создать проблему информационного перегруза, когда специалисты по кибербезопасности получают огромное количество сообщений и предупреждений. Поэтому перед ними стоит сложная задача, оптимизации процесса анализа журналов и записей.

Для решения этой проблемы в последние годы стали широко использоваться системы Security Information and Event Management (SIEM). Они позволяют собирать, агрегировать и анализировать данные из различных источников, включая системные журналы, с целью обнаружения аномальных событий и угроз информационной безопасности. SIEM-системы значительно упрощают процесс мониторинга и анализа журналов, повышая эффективность и оперативность реагирования на потенциальные угрозы.

SIEM (Security Information and Event Management) обеспечивает анализ событий, происходящих в информационной системе, в реальном времени. Такой анализ необходим для выявления опасных или непривычных для системы событий безопасности и принятия соответствующих мер.

На сегодняшний день существует множество разнообразных SIEM решений, предлагаемых различными разработчиками. Они отличаются своим функционалом, возможными интеграциями и методами анализа данных. Каждое SIEM-решение имеет свои особенности и преимущества, и выбор конкретного решения зависит от требований и потребностей организации.

Разработчики SIEM-систем стремятся предоставить комплексные решения, включающие сбор, агрегацию, нормализацию и анализ данных из различных источников, включая журналы событий, устройства безопасности, сетевые устройства и другие. Они также предоставляют функционал для обнаружения аномалий, корреляции событий, создания отчетов и предупреждений, а также интеграции с другими системами безопасности.

При выборе SIEM-решения организации должны учитывать свои специфические потребности, бюджетные ограничения и возможности

интеграции с уже используемыми системами. Это позволит эффективно использовать SIEM для обеспечения безопасности информационной системы и своевременного реагирования на потенциальные угрозы.

Во введении аргументирована значимость обследованной проблемы, сформулирована миссии, а также вопросы деятельность, повергнуты ключевые способы изучений, фактическая важность изучения, а также показаны области использования итогов изучений, а, кроме того, состав, а также размер диссертационной деятельность.

В первой главе были рассмотрены угрозы и риски компьютерных сетей, способы проникновения вредоносного ПО.

Во второй главе рассматриваются разные продукты SIEM систем, их обзор, а также сравнительный анализ.

В третьей главе произведено развертывание программного обеспечения, произведено вычисление Attack Potential и Dynamic Attack Potential.

ГЛАВА I. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1. Обзор угроз и рисков компьютерных сетей малого предприятия

В современном мире информация - ключевой актив предприятий, важный для развития общества. Глобальное распространение компьютеров и устройств в различных сферах управления и производства сопровождается появлением новых угроз для предприятий, общества и государства.

С ростом сложности и изменением методов автоматизации процессов работы с информацией увеличивается зависимость предпринимательства от безопасности используемых информационных технологий.

Источники опасности для сохранности информации компании могут включать:

1. Незаконная деятельность экономических структур, связанная с использованием, распространением и формированием информации.

2. Нарушение правил обработки, сбора и передачи информации, установленных для компании.

3. Преднамеренные и непреднамеренные действия пользователей информационных систем, которые могут привести к утечке или повреждению информации.

4. Ошибки на этапе проектирования информационных систем, которые могут привести к уязвимостям и неправильной защите информации.

5. Несоответствие технических средств или сбои программного обеспечения в информационных системах, что может привести к потере или недоступности информации.

Эти и другие факторы могут создавать угрозы для информационной безопасности компании и требуют принятия соответствующих мер для защиты информации от возможных угроз и рисков.

Специалисты по кибербезопасности активно исследуют широкий спектр угроз безопасности информационных систем, которые могут быть классифицированы по нескольким признакам (рисунок 1.1).

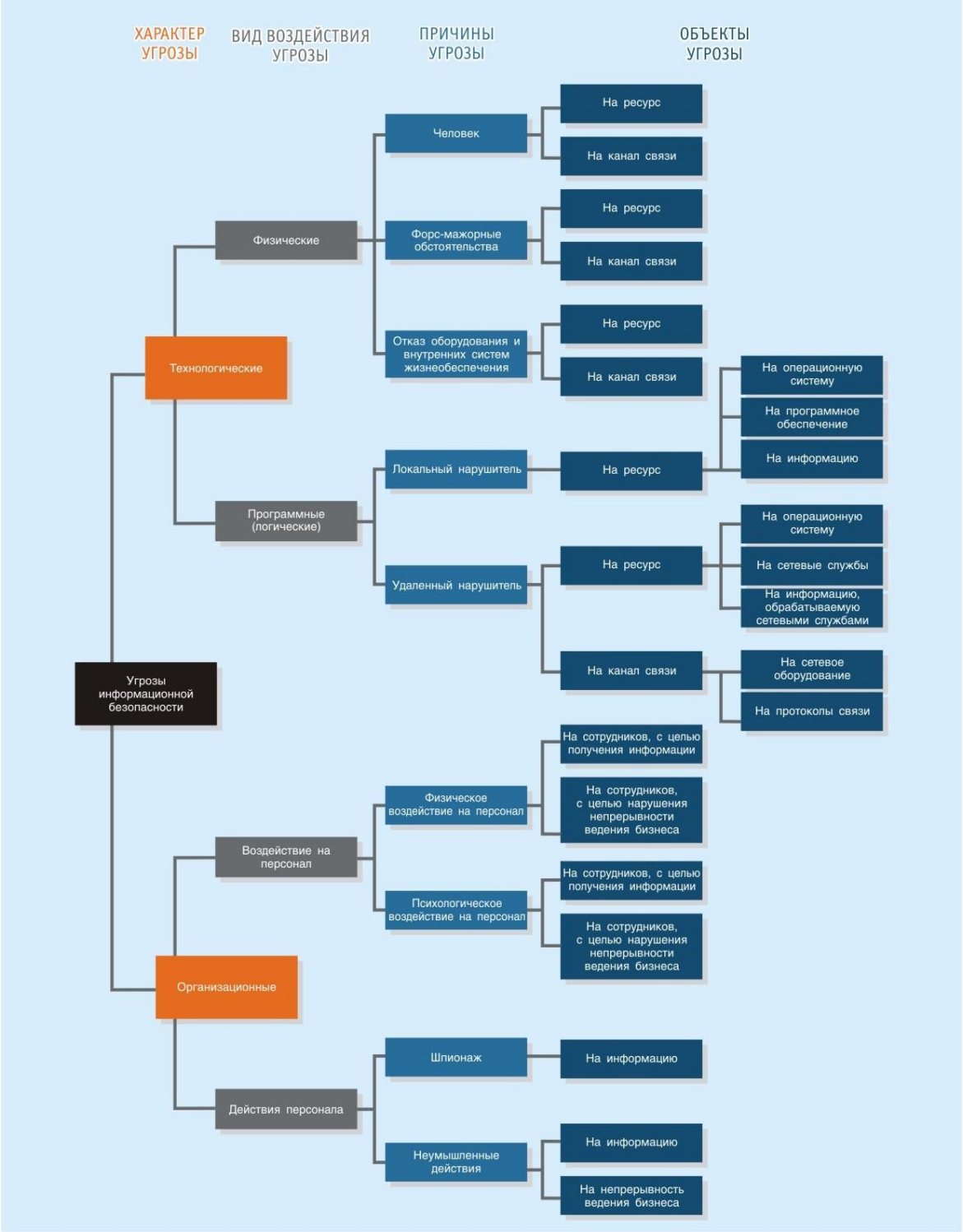

Рис. 1.1- Классификация угроз информационной безопасности

Каждая из этих угроз может иметь фатальные последствия для предприятия. Утечка важной информации или персональных данных сотрудников или

клиентов может привести к значительным потерям и даже угрожать самому существованию бизнеса [1].

1.2. Анализ современного вредоносного ПО

Программное обеспечение — это совокупность программ, разработанных для решения различных задач на компьютере. Каждая программа представляет собой упорядоченный набор команд, которые выполняются для достижения определенных целей. Программное и аппаратное обеспечение работают в тесном взаимодействии. Однако, не всегда программное обеспечение работает в пользу предприятия. Очень часто встречается вредоносное программное обеспечение, которое может нанести вред компьютерной системе и информации, вызвать потери данных, нарушить работу системы или украсть конфиденциальную информацию.

Термин "вредоносное программное обеспечение" или "злонамеренное программное обеспечение" относится к набору команд, который незаконно вводится в компьютерную систему и преднамеренно наносит вред. Такое программное обеспечение может иметь различные цели, включая нарушение безопасности, повреждение информационных ресурсов и даже физическое повреждение компьютерного оборудования. Его целью может быть кража конфиденциальной информации, распространение вирусов или шифрование данных с требованием выкупа (рансомвар). Вредоносное программное обеспечение представляет серьезную угрозу для безопасности и требует активных мер защиты и превентивных мер, таких как использование антивирусных программ и обновление программного обеспечения [2].

Угрожающие программы могут быть классифицированы на основе различных характеристик. Рассмотрим некоторые из основных типов угрожающих программ (Рисунок 1.2).

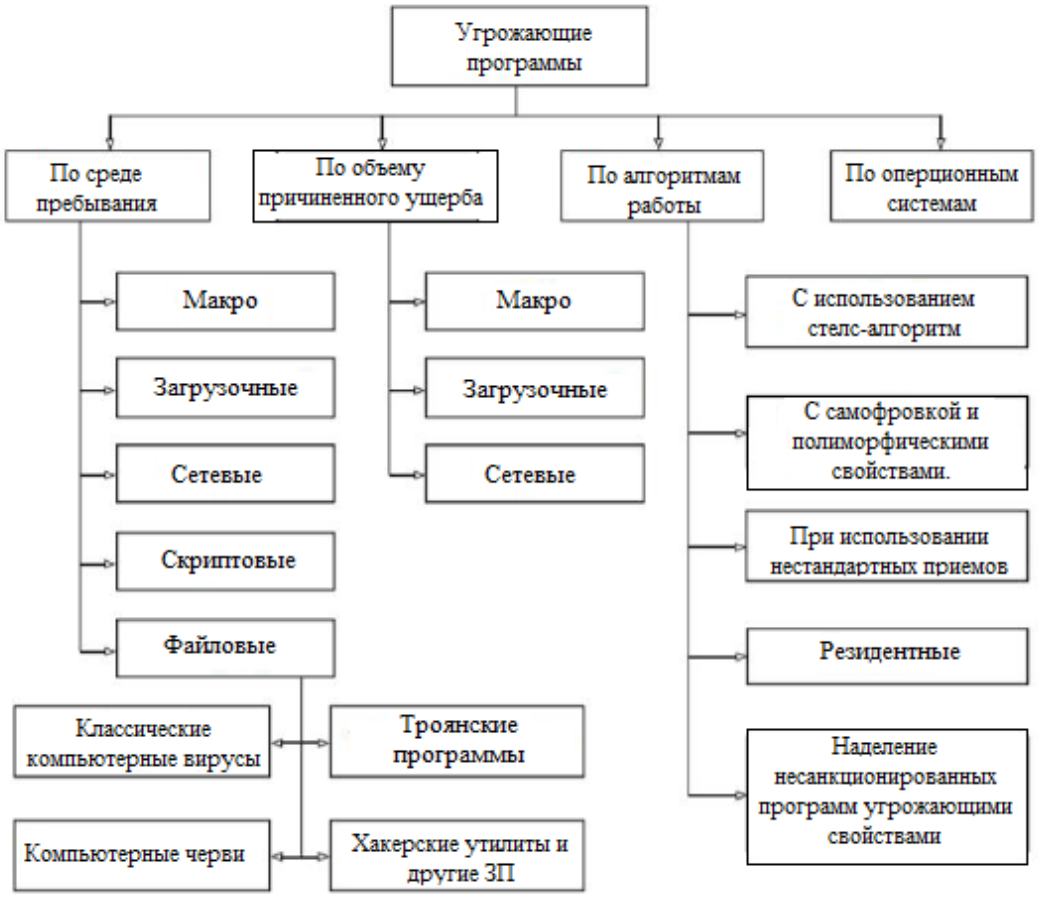

Рис. 1.2 – Классификация угрожающих программ

Вредоносное программное обеспечение включает:

1) уязвимости (программные уязвимости, позволяющие злоумышленникам получить доступ к системе с использованием необычных методов);

2) логические бомбы (код, внедряемый в обычную программу, который при выполнении определенных условий осуществляет незаконные действия; условия могут быть связаны с модификацией или отсутствием определенных файлов, конкретным днем недели или датой, а также запуском приложения от определенного пользователя).

3) Троянский конь (программы, которые маскируются под другие полезные приложения и выполняют нежелательные или вредоносные функции);

4) Вредоносные вирусы (код, который способен заражать другие программы, изменяя их и позволяя им также самостоятельно заражать другие программы);

5) Черви (программы, которые распространяются через сеть без создания своих собственных копий на носителях, активизируясь при наступлении определенных условий);

6) Зомби-программы (программы, скрытно подключающиеся к компьютерам в сети и использующие их для запуска атак, что затрудняет прослеживание пути к разработчику зомби-программы);

7) Программы-воры паролей (программы, разработанные для незаконного получения и кражи паролей пользователей).

Действительно, вредоносное программное обеспечение может существовать на устройствах компьютерной сети незаметно для их владельцев. Это одна из характеристик вредоносного ПО – оно может быть скрытым и выполнять свои функции без ведома пользователя. Злоумышленники могут использовать различные методы, чтобы обойти защиту и установить вредоносное ПО на компьютеры или другие устройства в сети. Поэтому важно принимать меры по защите и регулярно проверять системы на наличие вредоносного ПО, чтобы обеспечить безопасность информации и предотвратить потенциальные угрозы.

1.3. Анализ методов проникновения в компьютерные сети

В современных предприятиях все больше сотрудников нуждаются в персональных компьютерах и доступе к интернету. В связи с этим актуальным становится отслеживание действий каждого пользователя. Время от времени возникают ситуации, когда в системе выполняются незаконные действия, но пользователь даже не подозревает о них. В таких случаях мы можем говорить о проникновении в сеть. Выделяют 3 группы проникновений в сеть предприятия по способу их совершения:

1) Методы физического доступа. К этой группе относятся преступления, при которых информация подвергается модификации, уничтожению или блокировке. Могут быть повреждены или выведены из строя целые устройства. Физический доступ к информации может быть осуществлен сотрудниками или

лицами, работающими с ней, а также незаконными посягательствами на помещения, где происходит обработка информации. В настоящее время такой метод становится менее распространенным из-за усиления безопасности помещений и возможности отслеживания действий каждого пользователя.

2) Методы удаленного доступа. В эту категорию входят действия, связанные с подключением к сети или каналу связи законного пользователя системы и перехватом информации. Это может включать перехват трафика, подбор паролей, взлом через сеть и другие методы удаленного доступа.

3) Сочетание методов. В данной категории сочетаются элементы первого и второго типов. Это включает подмену данных, скрытое внедрение команд в чужую систему для выполнения нежелательных действий (троянский конь), использование логических ошибок в программном обеспечении для выявления уязвимостей и другие подобные методы. Такие смешанные способы проникновения в сеть могут быть использованы злоумышленниками для достижения своих целей.

Злоумышленники могут действительно использовать специальное оборудование для осуществления своих атак. Например, для непосредственного доступа могут быть использованы лазерные диски, накопители данных, электронные ключи и личные коды идентификации в системе. Для удаленного доступа могут быть задействованы средства связи, такие как спутниковая связь или телефонная связь, а также модемы.

Это подчеркивает, что опасность может исходить как от внутренних сотрудников предприятия, так и от внешних злоумышленников. Поэтому важно принимать соответствующие меры по обеспечению безопасности информационных систем и контролировать действия пользователей, чтобы минимизировать риски и защитить компанию от возможных угроз [2].

ГЛАВА II. ОБЗОР SIEM СИСТЕМ

2.1. SIEM система и принцип ее работы

Security Information and Event Management (SIEM) — это система, которая предназначена для сбора, анализа и классификации информации о событиях, связанных с безопасностью, происходящих в информационных системах. SIEM позволяет собирать данные из различных источников, таких как журналы событий, системы мониторинга, сенсоры безопасности и другие источники, и проводить их централизованную обработку.

Первоначально SIEM состояло из двух направлений:

- Первое поколение системы Security Information Management (SIM) было основано на традиционных методах сбора и управления журналами. Она обеспечивала долгосрочное хранение, анализ и отчеты по данным журналов, а также объединение журналов с информацией о возможных угрозах.
- Security Event Management (SEM) - второе поколение, касающееся событий безопасности - агрегирование, корреляция и сообщения о событиях из систем безопасности, таких как антивирус, брандмауэры и системы обнаружения вторжений (IDS), а также события, о которых сообщается непосредственно путем аутентификации , SNMP-ловушки серверы, базы данных и прочее.

В 2005 году произошло объединение и появилось общее понятие Security Information and Event Management [4].

Данные для SIEM поступают из различных источников, включая:

1) Журналы событий: Операционная система и посторонние приложения могут регистрировать события и записывать их в журналы, которые затем передаются в систему SIEM.

2) Сетевое оборудование: Маршрутизаторы, прокси-серверы, шлюзы и другое сетевое оборудование могут генерировать логи о сетевой активности, которые могут быть использованы для обнаружения и анализа потенциальных угроз.

3) Межсетевые экраны (firewall): Логи работы межсетевых экранов содержат информацию о входящем и исходящем сетевом трафике, позволяя выявлять подозрительную активность или несанкционированный доступ.

4) Сканеры уязвимостей: Специальное программное обеспечение для сканирования уязвимостей может обнаруживать потенциальные уязвимости в инфраструктуре и регистрировать соответствующие события.

5) CRM-системы: CRM-системы хранят информацию о клиентах и могут регистрировать события, связанные с обслуживанием клиентов, такие как запросы на поддержку или проблемы с обслуживанием.

6) Рабочие станции пользователей: Логи событий с рабочих станций пользователей могут содержать информацию о действиях пользователей, включая необычную активность или попытки несанкционированного доступа.

7) Антивирусное программное обеспечение: Антивирусные программы могут регистрировать события, связанные с обнаружением и блокировкой вредоносного программного обеспечения.

8) Другие ресурсы: существуют и другие ресурсы, способные регистрировать события и передавать их в SIEM через агентов или встроенные средства. Это может включать системы мониторинга доступа, системы регистрации времени, системы управления конфигурацией и другие.

Интеграция данных из этих различных источников позволяет системе SIEM получать всестороннюю информацию о безопасности и производить анализ и обнаружение потенциальных угроз и нарушений безопасности.

SIEM системы были введены около 2000 года. В первые годы своего существования (с 2000 по 2005 год) эти системы предоставляли базовую функциональность по агрегации журналов из различных типов систем и основные методы корреляции событий. Они сосредоточивались на обнаружении известных угроз и атак.

На начальном этапе развития SIEM системы в основном собирали и анализировали данные из логов и журналов событий, сгенерированных

операционными системами, приложениями и сетевым оборудованием. Они позволяли системному администратору или специалисту по информационной безопасности просматривать и анализировать эти данные для обнаружения аномалий и потенциальных угроз.

Однако на этом раннем этапе SIEM системы имели ограниченые возможности обнаружения атак. Они полагались преимущественно на заранее известные атаки и угрозы, которые были предварительно записаны в базу данных системы. Если событие соответствовало определенному шаблону атаки, система могла сработать и предупредить об этой атаке.

Таким образом, системы SIEM на этом начальном этапе сосредоточились на агрегации журналов и базовой корреляции событий, а также на обнаружении заранее известных атак и угроз. Они представляли собой важный шаг в области информационной безопасности, но с течением времени развивались и улучшались для более эффективного обнаружения и реагирования на угрозы.

Следовательно, они были совершенно не в состоянии столкнуться с атаками нулевых дней на системы предприятий. Другие ограничения систем в течение этого периода включали:

- На самом раннем этапе развития систем SIEM, акцент делался на IP-адресах, а не на отдельных пользователях. IP-адреса использовались в качестве идентификаторов устройств, генерирующих логи и события. Однако, с динамическим распределением IP-адресов и стремительным ростом числа мобильных устройств, идентификация конкретного устройства по его IP-адресу стала проблематичной, поскольку один и тот же IP-адрес мог быть связан с несколькими устройствами в течение дня.
- У традиционных систем SIEM использовались методы, основанные на правилах, для установления связей между различными событиями безопасности. Это означало, что система оперировала с большим количеством правил, которые нужно было постоянно обновлять в режиме реального времени.

Однако, такой подход требовал значительных ресурсов и времени, и мог приводить к неэффективному использованию системы.

Принцип работы системы SIEM можно объяснить следующими пунктами:

1. Сбор данных. Большинство современных SIEM-решений осуществляют сбор данных из информационной системы предприятия при помощи агентов, которые устанавливаются на различных устройствах, включая конечные точки, серверы и сетевое оборудование. Кроме того, они также интегрируются с другими решениями безопасности, такими как брандмауэры или другие устройства защиты сети. Современные SIEM-решения также поддерживают сбор данных из облачных приложений, корпоративных программ и инфраструктуры, чтобы обеспечить полную видимость и анализ безопасности во всей организации.

2. Расширение данных. Процесс расширения данных добавляет контекст к событиям. SIEM-решения должны обогащать входящие данные путем идентификации, определения активов, добавления геолокационной информации и информации об угрозах, чтобы обеспечить более детальное расследование. Расширение данных заполняет пробелы в информации, необходимой для SIEM, позволяя объединять связанные события и обнаруживать потенциальные угрозы. Это помогает обеспечить более полное представление о событиях и более эффективно выявлять потенциальные угрозы.

3. Хранение данных. После расширения, данные безопасности сохраняются в базе данных. Это позволяет проводить поиск и обращаться к данным во время расследования. Обычно хранятся только данные с расширенной информацией, однако иногда сохраняются все данные, в зависимости от требований предприятия. Современные SIEM-решения используют архитектуру больших данных с открытым исходным кодом, чтобы воспользоваться их неограниченной масштабируемостью и возможностью хранить исторические данные. Это обеспечивает легкий доступ и поиск по данным, что является важным аспектом расследования.

4. Использование корреляции и аналитики. Решения SIEM применяют различные методы для извлечения полезной информации из данных и обнаружения аномалий. Методы аналитики могут отличаться в зависимости от поставщика решения. Первые поколения SIEM основывались на простой корреляции и срабатывании на основе подписей. Однако они имели недостатки, такие как высокая вероятность ошибок и генерация большого количества ложных срабатываний, а также способность обнаруживать только известные угрозы. Более современные SIEM-решения используют передовые методы аналитики, включая алгоритмы машинного обучения, чтобы обнаруживать как известные, так и неизвестные угрозы. Это позволяет более точно и эффективно выявлять потенциальные угрозы и предупреждать о них.

5. Анализ угроз. На базовом уровне SIEM должна обеспечивать интеграцию с решениями организации по безопасности и автоматизации реагирования (SOAR - Security Orchestration, Automation, and Response), чтобы помочь аналитикам в процессе расследования и принятия мер по устранению потенциальных угроз. Решение SOAR предоставляет аналитикам рабочее пространство для сбора информации, отслеживания шагов, предпринятых в ходе расследования, и сохранения информации о том, как угроза была устранена. Это позволяет аналитикам эффективно управлять процессом расследования и реагирования на угрозы, повышая эффективность и скорость реакции на инциденты безопасности.

6. Предоставление статистики данных и отчетности. SIEM обеспечивает быстрый доступ к данным, позволяя аналитикам проводить детальный поиск в предупреждениях и идентифицировать участников инцидентов. Данные могут быть визуализированы в виде информационных панелей или экспортированы в стандартные форматы данных. Платформа также предлагает готовые отчеты, которые можно использовать, а также возможность создания настраиваемых отчетов в случае необходимости. Это позволяет представлять информацию о безопасности организации в наглядной форме и

обеспечивает легкость анализа и обобщения данных для принятия решений и отчетности.

2.2. Основные производители SIEM систем на рынке продуктов

В связи с осознанием руководителями предприятий важности тщательного подхода к информационной безопасности, рынок SIEM-систем стремительно развивается, а количество предлагаемых решений продолжает расти. Вот краткий обзор нескольких популярных представителей SIEM-систем на международном рынке.

2.3. IBM QRadar Security Intelligence

Для обеспечения защиты от угроз сетевой безопасности, компания IBM предлагает решение IBM QRadar Security Intelligence Platform. Эта платформа предоставляет общую архитектуру, которая интегрирует информацию о безопасности, управление событиями и журналами, обнаружение аномалий, анализ инцидентов, реагирование на них, управление конфигурациями и устранение уязвимостей.

Архитектура QRadar Security Intelligence Platform позволяет анализировать различные типы данных, включая журналы, сетевые потоки, пакеты, информацию об уязвимостях, а также данные о пользователях и ресурсах. С помощью Sense Analytics осуществляется анализ корреляции в реальном времени для обнаружения серьезных угроз, атак и уязвимостей. Это позволяет IT-отделам определить приоритетные инциденты из большого объема данных. Решение также автоматически реагирует на инциденты и обеспечивает соответствие нормативным требованиям путем сбора данных, их корреляции и составления отчетов. Возможен также анализ рисков, связанных с неправильной конфигурацией устройств и известными уязвимостями.

IBM QRadar Security Intelligence Platform включает в себя несколько модулей, и одним из ключевых компонентов является IBM QRadar SIEM. QRadar SIEM является системой сбора и анализа событий, которая объединяет информацию из различных источников, таких как журналы событий, устройства, конечные точки и приложения в сети. Он обрабатывает и нормализует данные, а затем проводит анализ корреляции для выявления потенциальных угроз безопасности. Благодаря передовому механизму Sense Analytics, QRadar SIEM способен обнаруживать аномалии, выявлять нормальное поведение и распознавать передовые угрозы. Этот модуль программы позволяет объединять связанные события в один инцидент, что облегчает расследование и управление безопасностью.

Кроме того, важно отметить, что в ближайшей перспективе компания IBM планирует применять платформу искусственного интеллекта Watson в области безопасности, объединяя ее с программным обеспечением QRadar и базой данных X-Force. Это способствует повышению уровня аналитических возможностей для выявления характера угроз, а также решает проблему нехватки специалистов в области информационной безопасности.

Инструмент QRadar SIEM включает в себя ряд модулей, которые значительно увеличивают его эффективность. Один из ключевых модулей - QRadar Risk Manager, который связывает информацию о уязвимостях с данными о топологии сети и соединениях. Это решение позволяет обнаружить уязвимости в корпоративной сети и работающих приложениях, оценить риски и минимизировать их. Risk Manager отслеживает конфигурацию маршрутизаторов, коммутаторов, сетевых экранов и систем предотвращения вторжений, находя условия, которые представляют угрозу для безопасности. Более того, он позволяет моделировать сетевые атаки и другие сценарии вторжений, внося изменения в сетевую конфигурацию, что позволяет оценить масштаб потенциальной угрозы.

Еще одним интересным инструментом является модуль QRadar Log Manager. Он предназначен для сбора и обработки данных о событиях в режиме

реального времени, поступающих от маршрутизаторов, брандмауэров, коммутаторов, сетей VPN, систем обнаружения и предотвращения вторжений и других источников. Log Manager значительно упрощает ведение необходимой отчетности и обеспечивает контроль за соблюдением нормативно-правовых требований. Он позволяет анализировать и коррелировать данные с различных источников, обнаруживая потенциально важные события и предупреждая о возможных угрозах в реальном времени. Это позволяет оперативно реагировать на инциденты безопасности и принимать соответствующие меры по защите информации.

IBM QRadar SIEM является одной из самых эффективных систем аналитики безопасности. Важно отметить, что это решение поддерживает работу с более чем 200 продуктами от ведущих производителей и осуществляет сбор, анализ и корреляцию данных из широкого спектра систем, включая сетевые решения, средства безопасности, серверы, хосты, операционные системы и приложения. Кроме того, дополнительным преимуществом этой системы является ее низкая стоимость в базовой конфигурации [7].

2.4. Splunk Enterprise Security

Splunk Enterprise Security (SES) - инструмент для управления безопасностью и событиями, который анализирует разнообразные данные, создаваемые различными технологиями безопасности (сеть, конечные точки, доступ, вредоносное ПО, уязвимости). С помощью Splunk Enterprise Security специалисты по безопасности быстро выявляют внутренние и внешние атаки и предпринимают соответствующие меры. Этот инструмент упрощает операции по защите от угроз, снижает риски и обеспечивает безопасность бизнеса. Splunk Enterprise Security оптимизирует все аспекты безопасности и подходит для организаций разного масштаба и уровня экспертизы.

Этот продукт состоит из нескольких модулей, которые отвечают за проведение расследований и интеграцию с различными внешними сервисами.

Такой подход обеспечивает возможность проводить детальный анализ по множеству параметров и устанавливать связь между разными событиями, которые на первый взгляд не имеют явной взаимосвязи. Splunk Enterprise Security позволяет ассоциировать данные по времени, местоположению, создаваемым запросам, подключениям к различным системам и другим характеристикам.

Splunk User Behavior Analytics (Splunk UBA) использует алгоритмы машинного обучения, аналитику базовых линий поведения пользователей и временных групп, чтобы помочь предприятиям обнаруживать скрытые угрозы и аномальное поведение пользователей, устройств и приложений. Это позволяет организациям выявлять постоянные угрозы повышенной сложности, заражение вредоносными программами и внутренние угрозы. Splunk UBA оптимизирует рабочие процессы аналитиков и разработчиков процедур безопасности, требуя минимального уровня администрирования, и легко интегрируется с существующей инфраструктурой для обнаружения скрытых угроз.

Splunk Enterprise Security также обладает возможностью работать с большими объемами данных, которые могут быть обработаны как в режиме реального времени, так и в режиме исторического поиска. Он поддерживает множество источников данных. Splunk Enterprise Security способен индексировать сотни терабайтов данных ежедневно, что делает его применимым даже в крупных корпоративных сетях. С помощью специального инструмента MapReduce система может быстро масштабироваться и равномерно распределять нагрузку, что обеспечивает стабильную производительность. Пользователям также доступны конфигурации для кластеризации и аварийного обновления [8].

2.5. McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) является частью семейства систем управления информацией и событиями безопасности от компании McAfee. Это решение отличается высокой производительностью и предоставляет

специалистам по безопасности информацию в режиме реального времени, необходимую для принятия соответствующих мер. Благодаря своей быстродействию и масштабируемости, McAfee ESM позволяет обнаруживать, анализировать и нейтрализовывать скрытые угрозы. Встроенная структура обеспечения нормативно-правового соответствия упрощает контроль за соблюдением требований. Решение от компании McAfee интегрируется как с физическими и виртуальными устройствами, так и с программным обеспечением. Оно состоит из нескольких модулей, которые могут быть использованы как вместе, так и по отдельности. McAfee Enterprise Security Manager обеспечивает постоянный мониторинг корпоративной ИТ инфраструктуры, собирает информацию о возможных угрозах и рисках, позволяет приоритезировать угрозы и осуществлять быстрое расследование. Система автоматически анализирует информацию, определяет базовый уровень активности и генерирует предупреждения для администратора при превышении установленных границ. Она также учитывает контекст сообщений, расширяя возможности обнаружения угроз и уменьшая количество ложных срабатываний. McAfee ESM обладает превосходной интеграцией с продуктами сторонних производителей, не требуя использования API. Это позволяет ему совместимо работать с множеством популярных решений в области безопасности. Кроме того, он поддерживает платформу McAfee Global Threat Intelligence, которая расширяет функциональность SIEM. С помощью этой платформы ESM получает постоянно обновляемую информацию об угрозах со всего мира. На практике это дает, например, возможность выявлять события, связанные с подозрительными IP-адресами.

- *McAfee Event Receiver* – сбор и нормализация сырых событий (обязательный);

- *McAfee Enterprise Log Manager* – хранение сырых событий (рекомендуемый);

- *McAfee Enterprise Log Search* – поиск по сырым событиям (опциональный);

- *McAfee Advanced Correlation Engine* (McAfee ACE) – дополнительные возможности по корреляции событий (рекомендуемый);

- *McAfee Application Data Monitor* – мониторинг данных 7-го уровня OSI для выявления угроз на уровне приложений (опциональный).

McAfee ESM обладает инфраструктурой корреляции, которая позволяет анализировать каждое событие в контексте, включая информацию о том, кто, что, где, когда и почему вызвало данное событие. Это помогает понять влияние событий на бизнес-риски. Средства корреляции обеспечивают точную автоматическую приоритизацию угроз безопасности и нарушений соответствия требованиям, представляя события в соответствующем бизнес-контексте.

Для обеспечения эффективного обнаружения инцидентов, быстрой реакции и минимизации ложных срабатываний, настройка такой системы должна быть выполнена с учетом существующих бизнес-процессов и ИТ-инфраструктуры в компании. Это позволит системе работать в гармонии с организацией, адаптироваться к ее потребностям и обеспечивать максимальную эффективность [9].

2.6. AlienVault OSSIM

AlienVault OSSIM — это многофункциональная система управления информацией и событиями безопасности с открытым исходным кодом (SIEM), которая включает сбор событий, нормализацию и корреляцию. AlienVault OSSIM был запущен инженерами из-за отсутствия доступных продуктов с открытым исходным кодом и для решения проблемы, с которой сталкиваются многие специалисты по безопасности, а именно, что SIEM, независимо от того, является ли он открытым исходным кодом или коммерческим, бесполезен, если он не обеспечивает видимость безопасности.

Как система SIEM, OSSIM предназначена для того, чтобы дать аналитикам безопасности и администраторам более полное представление обо всех связанных с безопасностью аспектах их системы за счет объединения

управления журналами, которое может быть расширено с помощью подключаемых модулей, управления активами и обнаружения информации из специализированной системы информационной безопасности. системы контроля и обнаружения. Затем эта информация сопоставляется, чтобы создать контексты для информации, невидимой только из одной части. Предусмотрены представления сигналов тревоги и доступности, а также возможности создания отчетов для расширения возможностей инструмента и его полезности для инженеров по безопасности и системных инженеров.

OSSIM включает следующие программные компоненты:

- *PRADS*, используемый для идентификации хостов и служб путем пассивного мониторинга сетевого трафика.

- *Snort*, используемый в качестве системы обнаружения вторжений (IDS), а также используемый для взаимной корреляции с OpenVAS.

Suricata, используемая в качестве системы обнаружения вторжений (IDS), начиная с версии 4.2, это IDS, используемая в конфигурации по умолчанию.

- *Tcptrack*, используемый для информации о данных сеанса, которая может предоставить полезную информацию для корреляции атак.

Munin за анализ трафика и наблюдение за услугами.

- *NFSen/NFDump*, используемый для сбора и анализа информации NetFlow.

- *FProbe*, используемый для генерации данных NetFlow из захваченного трафика.

- *Nagios* используется для мониторинга хостов и указанных портов на предмет доступности активов, а также для полного мониторинга локальной системы.

- *OpenVas* используется для оценки уязвимости и связан с активами.

OSSIM также включает инструменты собственной разработки, наиболее важным из которых является универсальный механизм корреляции с поддержкой логических директив и интеграцией журналов с плагинами [10].

2.7. Сравнительный анализ современных SIEM систем

Сравнительный анализ приведенных выше систем представлен в Таблице 2.1.

Таблица 2.1 – Сравнительный анализ SIEM систем

Критерий оценки	McAfee ESM	IBM Radar	Splunk	AlienVault
Целевой сегмент	Государственный сектор, крупный и средний бизнес	Банковский, государственный секторы, крупный и средний бизнес	Все сегменты во всех отраслях, от бесплатных версий до самых больших инсталляций	Малый и средний бизнес
Языки интерфейса	Английский	Русский, английский	Русский, английский	Английский
Пути эксплуатации инцидентов	Эскалация вручную или при формировании автоматического оповещения	Вручную	Автоматическ и настраиваемая эскалация на SOAR и другие средства реагирования через механизм модульных уведомлений	Вручную

			Alerts. Ручная эскалация через Workflow Actions в карточке инцидента	
Принятие решений в рамках процесса обработки инцидентов	Ручное и автоматическое	Ручное и автоматическое	Ручное	Ручное
Наличие установленных графических панелей (Dashboards)	Более 100 (сочетано с отчетами)	Дополнительно с AppExchange может быть установлено приложение визуализации IBM QRadar Pulse	57	Более 50
Наличие установленных отчетов	Более 110	Более 110, а также Content Extention Pack из IBM X-Force App Exchange	462	Более 100

Операционная система в основе решения	Customized Mcafee linux	Red Hat Enterprise Linux	Linux с ядром 2.6+, Windows Server 2008 R2 и выше	Microsoft Windows (Server)
Наличие сформированных образов для платформ виртуализации	VMware, KVM, AWS	VMware, AWS	VMWare, AZURE, AWS, Docker Hub	VMware,
Настройка собственной модели для определения критичности уязвимости	Можно влиять на параметры критичности, используя метки Assets. Влияние на параметр риска возможно из риск-корреляции на базе правил	Нет	Да	Да
Возможность формирования отчетов в виде документов, форматы экспорта отчетов	PDF, HTML, CSV	PDF, HTML, RTF, XML, XLS	Raw, PDF, CSV, XML, JSON	PDF, HTML, RTF, XML

Итак, просмотрев сравнительный анализ, мы можем заключить, что система каждого производителя имеет свои особенности и преимущества.

ГЛАВА III. ПРАКТИЧЕСКАЯ ЧАСТЬ

3.1. Выбор методов решения задачи

В свете необходимости создания безопасной информационной среды на предприятии, специалистам информационной системы становится важным реализовать систему мониторинга, способную обработать множество источников информации и предоставить надежную оценку уровня защищенности системы.

В качестве примера такой системы, была выбрана AlienVault OSSIM, благодаря ее бесплатному распространению и широкому спектру функциональности, позволяющему построить надежную систему мониторинга.
AlienVault OSSIM (Open Source Security Information and Event Management) является бесплатной версией AlienVault, ведущей коммерческой системы SIEM. OSSIM представляет собой фреймворк с открытым исходным кодом, включающий Snort для обнаружения вторжений, Nagios для мониторинга сетей и узлов, а также OSSEC и OpenVAS для обнаружения уязвимостей.
Система основана на стеке ElasticStack, включающем Elasticsearch, Logstash и Kibana, и поддерживает как сбор данных с помощью агентов, так и прием системных журналов. Это делает ее эффективной для мониторинга устройств, которые генерируют журналы, но не поддерживают установку агента, таких как сетевые устройства, принтеры и периферийные устройства (6).

Также есть удобный EventLog Analyzer. С использованием этого инструмента вы можете автоматизировать управление терабайтами журналов, генерируемых устройствами, путем сбора, анализа, поиска, отчетности и архивирования из одной централизованной консоли. Это программное обеспечение помогает контролировать целостность файлов, проводить анализ журналов, отслеживать привилегированных пользователей и отвечать требованиям различных регуляторных органов. Для этого используется анализ журналов, что позволяет мгновенно генерировать разнообразные отчеты.

3.2. Развертывание AlienVault OSSIM

Установка системы происходит с использованием предварительно подготовленного образа, который включает в себя операционную систему Debian и все необходимые компоненты, и модули.

3.2.1. Развертывание и отладка серверной части

Сначала была загружена последняя версия дистрибутива OSSIM и установлен VirtualBox на свой персональный компьютер. Виртуальная машина, созданная во время работы, будет выполнять роль виртуального сервера.

Создаем виртуальную машину с представленными параметрами (Рисунок 3.1 и Рисунок 3.2)

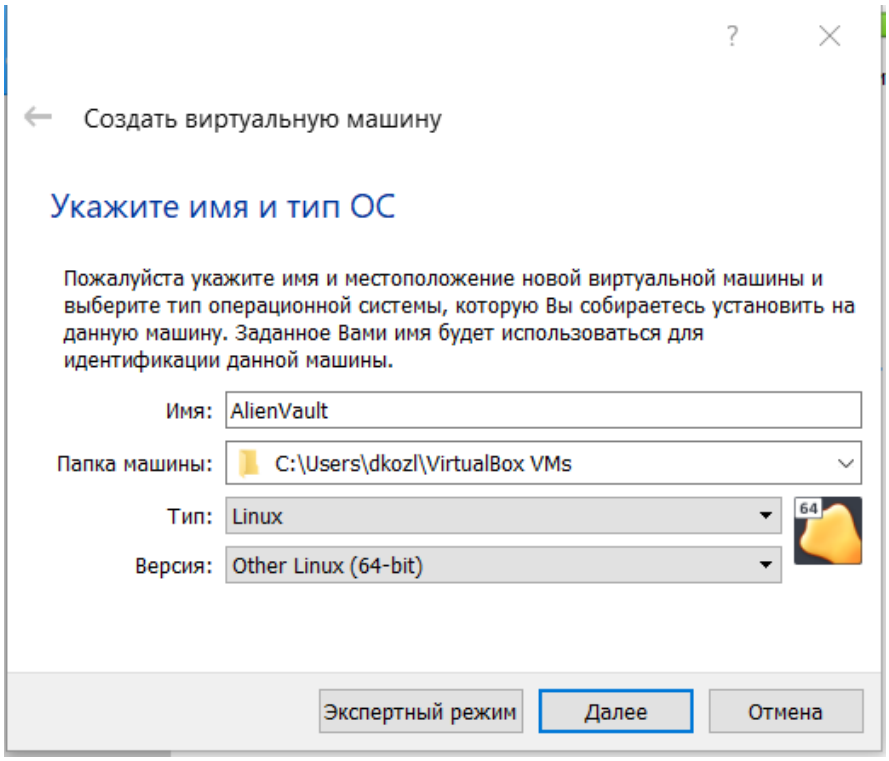

Рис. 3.1 – Название и тип операционной системы

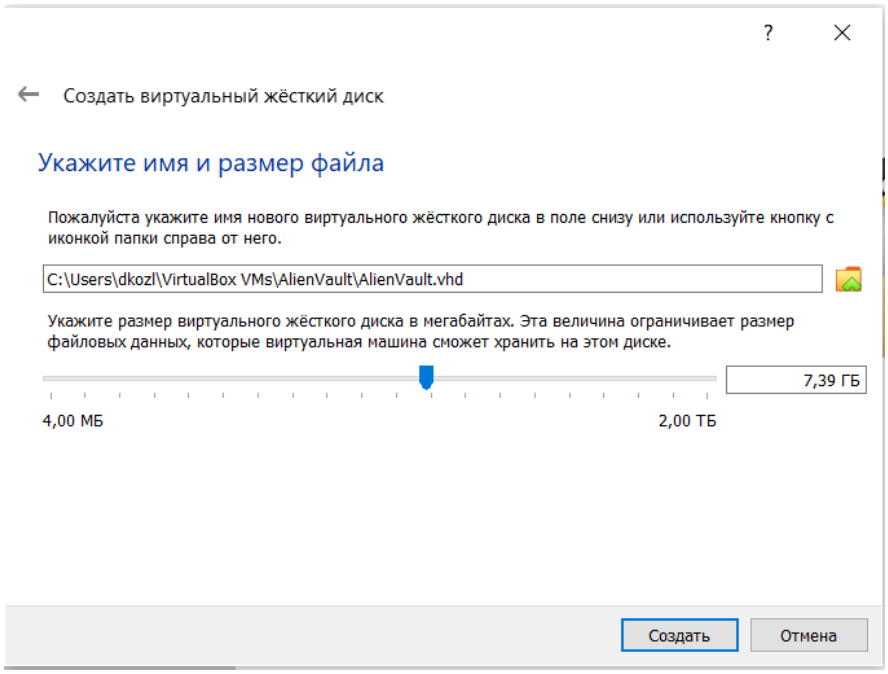

Рис. 3.2 – Название файла будущей ВМ и размер виртуального диска

После успешного создания и запуска ВМ нужно выбрать загрузочный диск (мне пришлось встроить образ диска с помощью программы DAEMON Tools Lite, поэтому это диск E:) (рисунок 3.3).

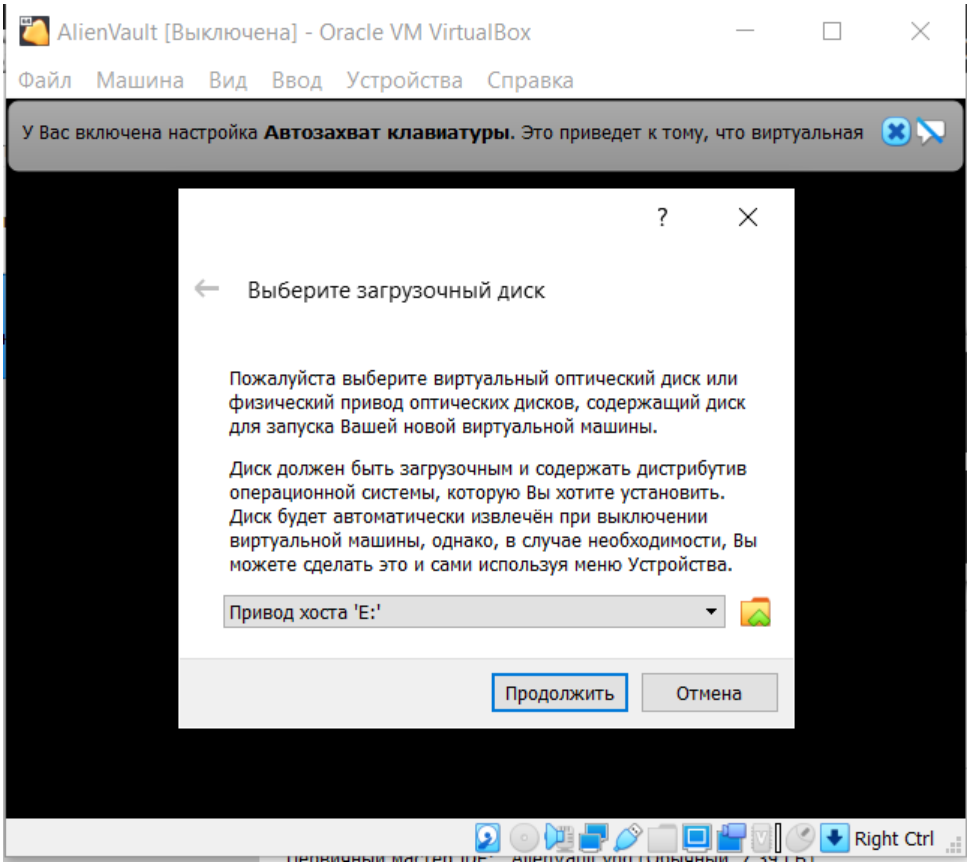

Рис. 3.3 – Выбор погрузочного диска

Далее выбираем первый вариант установки, который не отличается от установки Debian (Рисунок 3.4).

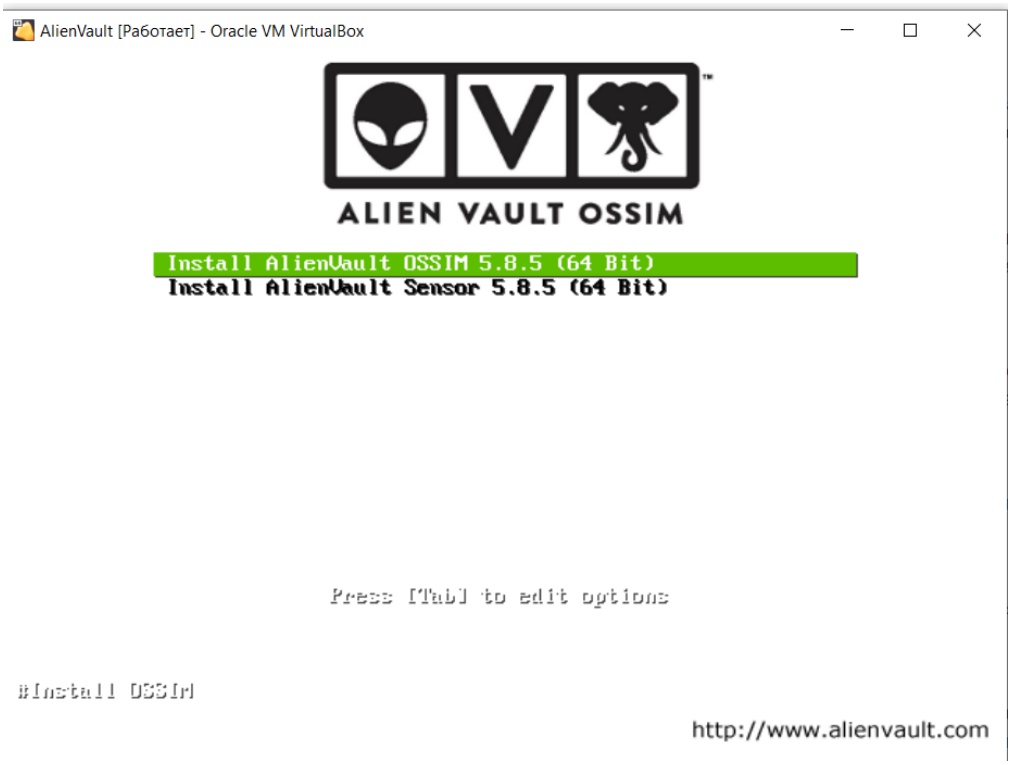

Рис. 3.4 - Выбор варианта установки

Выбираем язык и ждем полной загрузки. Начинаем конфигурацию сети. Вводим IP, который будет использоваться для входа через браузер. В моем случае это 192.168.1.150 (Рисунок 3.5)

Рис. 3.5 – Определение IP для SIEM системы

После этого также прописываем маску подсети – 255.255.255.0. После этих действий конфигурация ВМ завершена. Нам остается только авторизироваться и попытаться через браузер попасть на наш виртуальный сервер (Рисунок 3.6 и Рисунок 3.7).

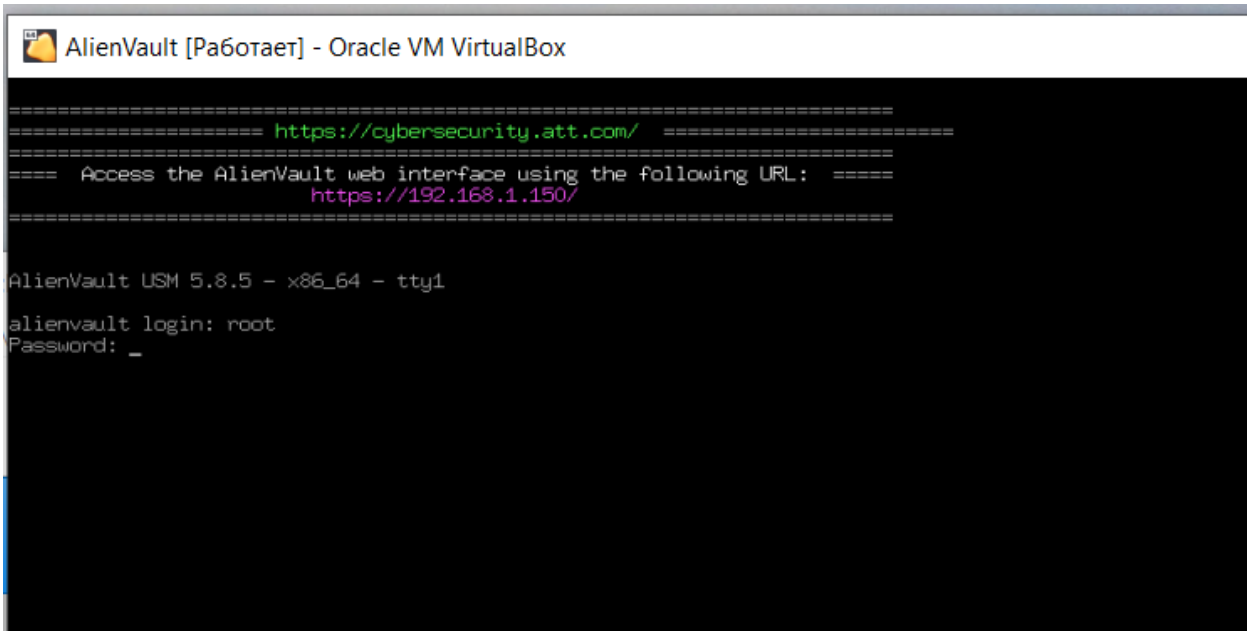

Рис. 3.6 – Авторизация в системе через консоль

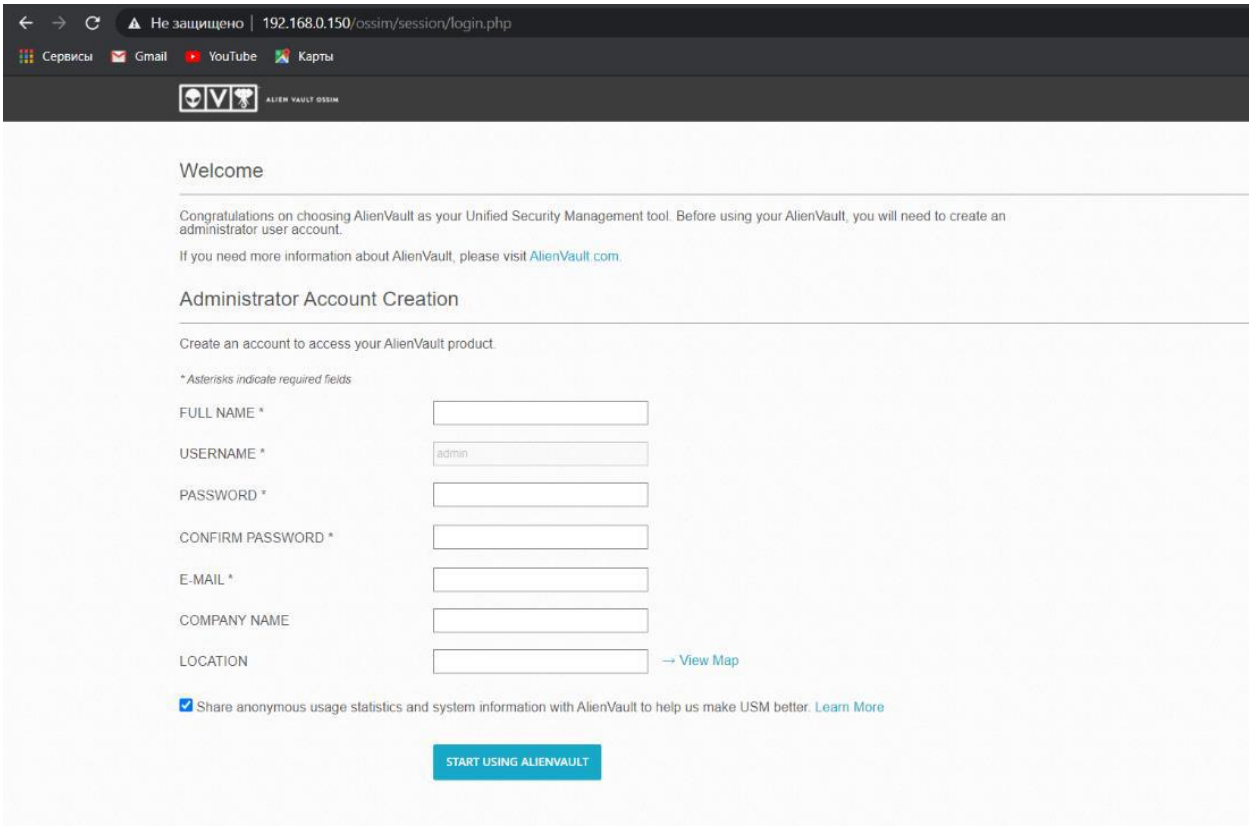

Рис. 3.7 – Настройка админ-пользователя через веб-страницу

3.2.2. Развертывание клиентской части

Чтобы увидеть, как работает наша система, мы продолжаем настройки через веб интерфейс и добавляем мой локальный ноутбук к конфигурации. Для этого сканируем сеть 192.168.0.0/16, в которой находится наша система и ноутбук (Рисунок 3.8).

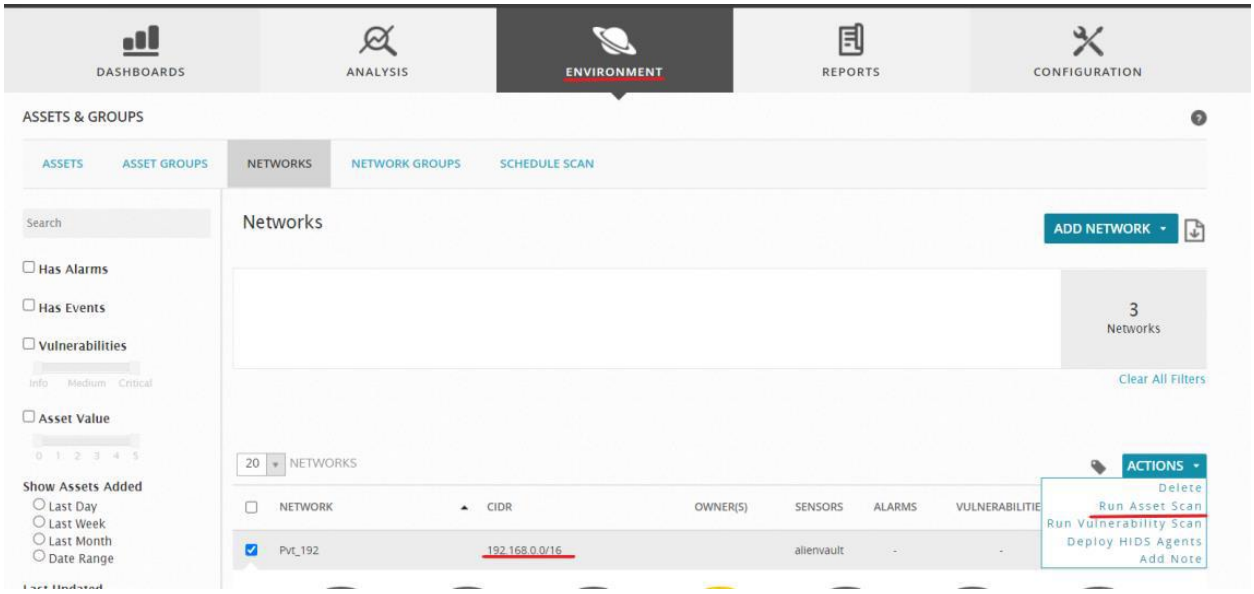

Рис. 3.8 – Сканирование локальной сети

Получаем список устройств, находящихся в одной сети (рисунок 3.9).

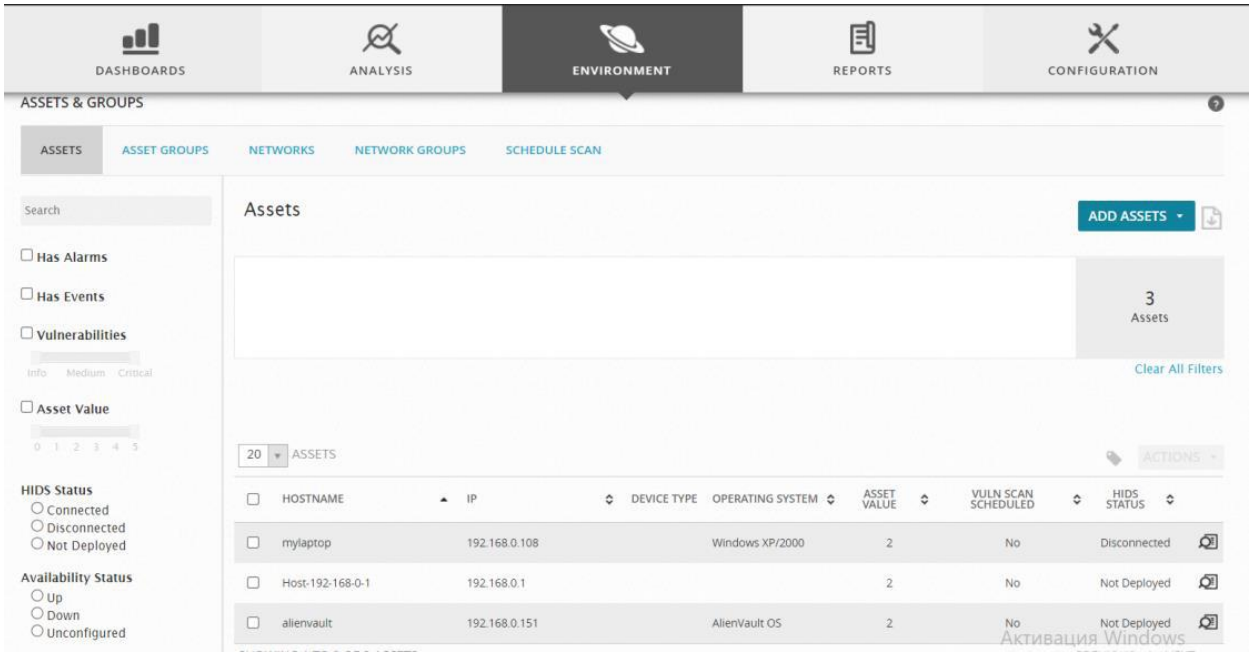

Рис. 3.9 – Список локальных устройств

Как мы видим, наша система уже начала собирать информацию о нужном хосте (Рисунок 3.10).

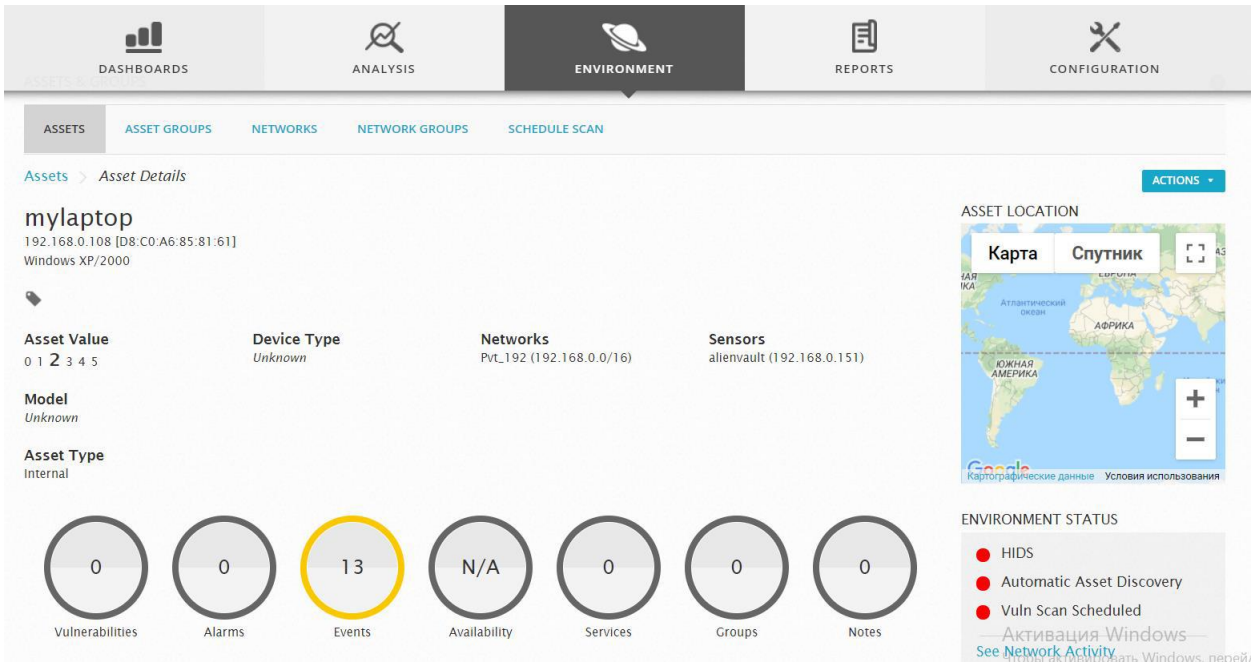

Рис. 3.10 - Информация, собранная при сканировании сети

В дальнейшем мы можем использовать веб-интерфейс для дальнейшего мониторинга и получения требуемой информации.

Dashboards – показывает полное представление обо всех компонентах сервера OSSIM, таких как серьезность угрозы, уязвимости в сетевом узле, состояние развертывания, карты рисков и статистика (Рисунок 3.11).

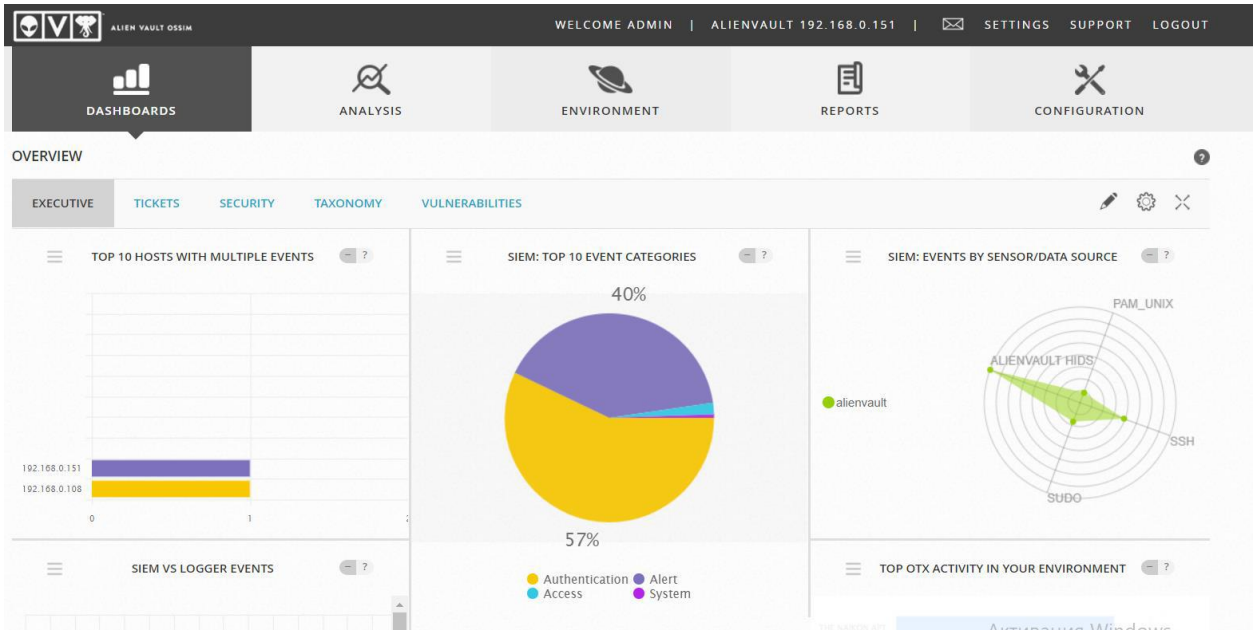

Рис. 3.11 - Вкладка Dashboards

Analysis – является очень важной составляющей любого устройства SIEM. Сервер OSSIM проанализирует хосты на основе их логов. Это меню показывает сигналы тревоги, SIEM (события безопасности), тикеты и необработанные логи (Рисунок 3.12).

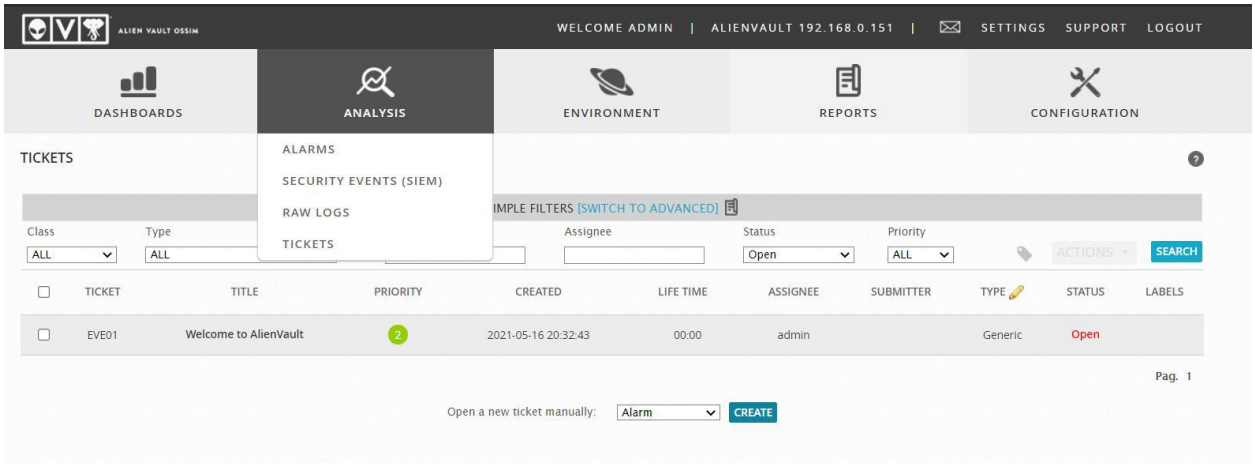

Рис. 3.12 – Вкладка Analysis

Environment – в этом меню сервера OSSIM настройки связаны с устройствами организации. Оно показывает устройства, группу и сеть, уязвимость, сетевой поток и настройку обнаружения (Рисунок 3.13).

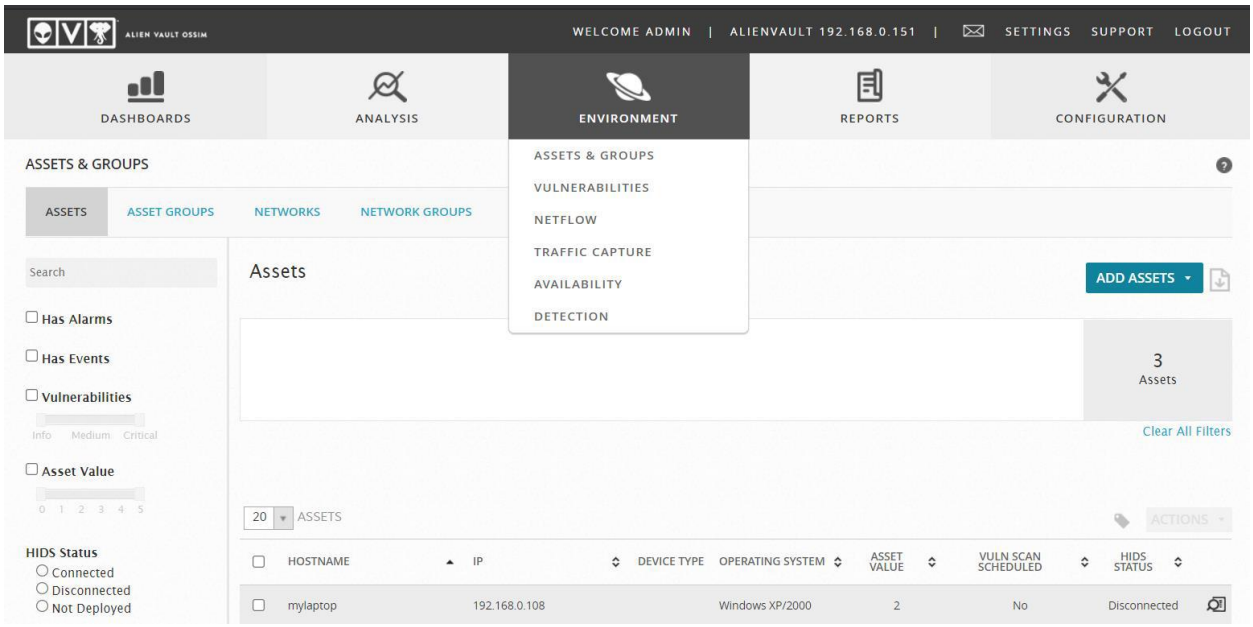

Рис. 3.13 – Вкладка Environment

Reports – отчетность является важным компонентом любого сервера регистрации. Сервер OSSIM также генерирует отчеты, очень полезные для детального исследования любого конкретного хоста (Рисунок 3.14).

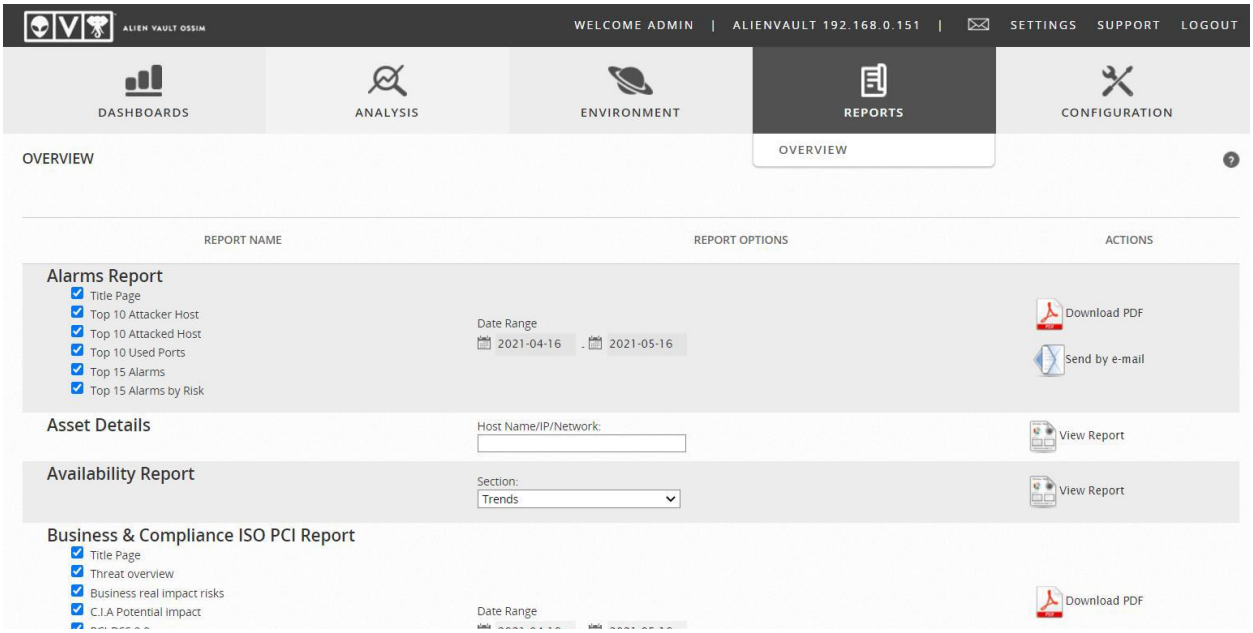

Рис. 3.14 - Вкладка Reports

Configuration – для установки и настройки AlienVault SIEM (OSSIM) пользователь может изменить настройки сервера OSSIM, например, изменить IP адрес интерфейса управления, добавить дополнительный хост для мониторинга и логирования, а также добавить/удалить различные датчики или плагины (Рисунок 3.15).

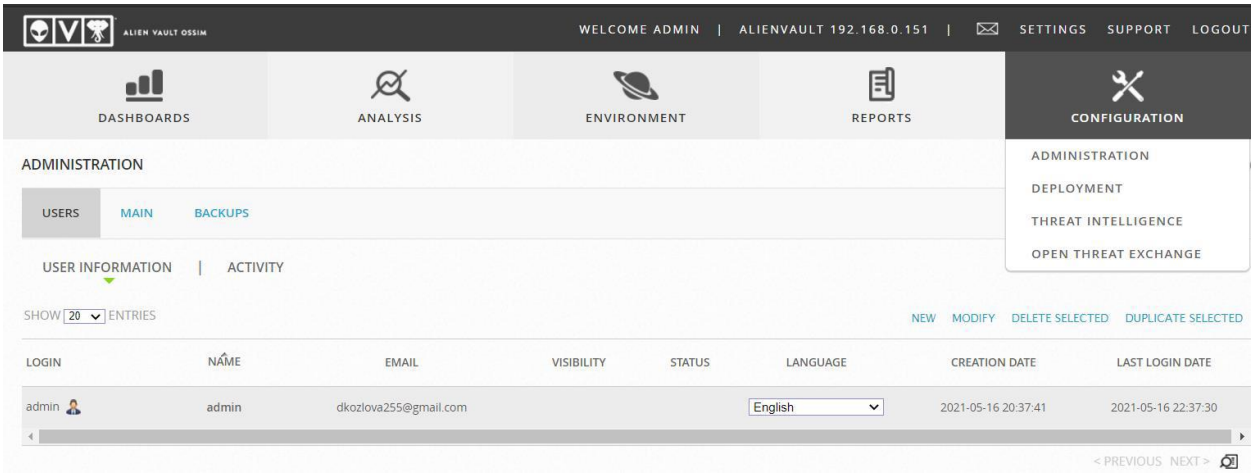

Рис. 3.15 – Вкладка Configuration

3.3. Развертывание модуля EventLog Analyzer для AlienVault SIEM

EventLog Analyzer устанавливается как обычная программа через загрузчик и не требует предварительных настроек.

Поскольку EventLog Analyzer была запущена с рабочей станции, она автоматически начинает мониториться. После авторизации мы видим уже собранную информацию с хостовой машины и вкладку Dashboard (содержит несколько информационных панелей, которые дают вам представление о важных сетевых событиях) (Рисунок 3.16).

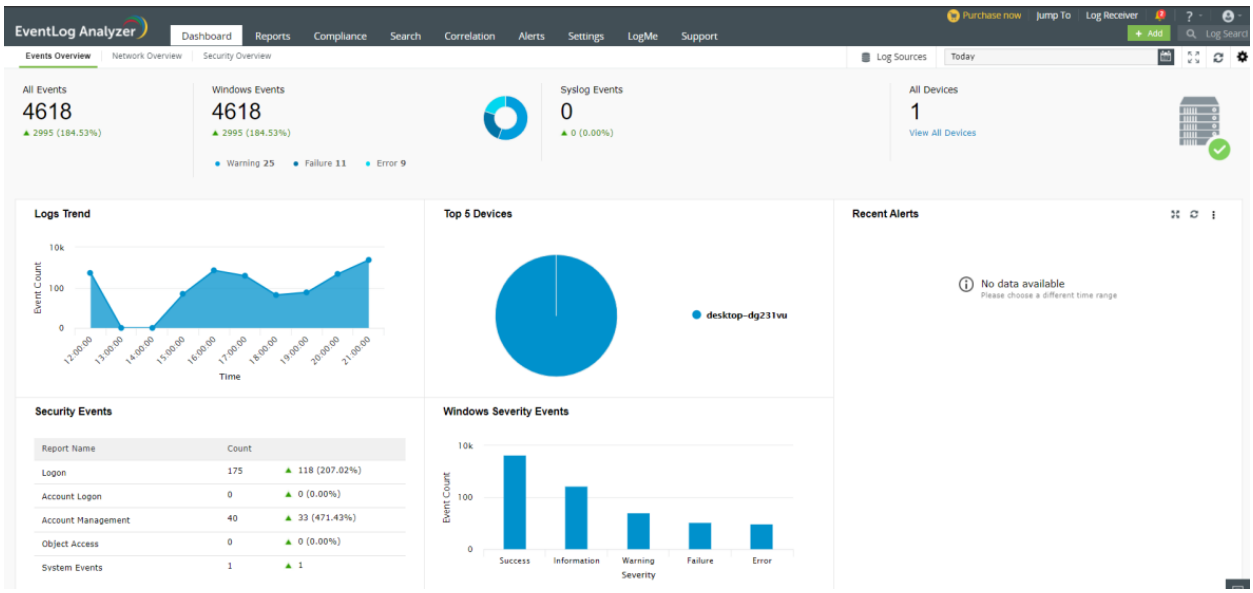

Рис. 3.16 - Начальная страница EventLog Analyzer

Доступ к отчетам можно получить на вкладке "Reports" в пользовательском интерфейсе. Количество событий, показанных в отчетах, можно подробно просмотреть в необработанных журналах. Журналы можно дополнительно фильтровать на основе разных полей журнала. EventLog Analyzer также позволяет планировать автоматическое создание отчетов и их периодическую передачу по электронной почте. Специальные профили отчетов можно экспортировать как файлы XML, а затем импортировать, если это необходимо (Рисунок 3.17).

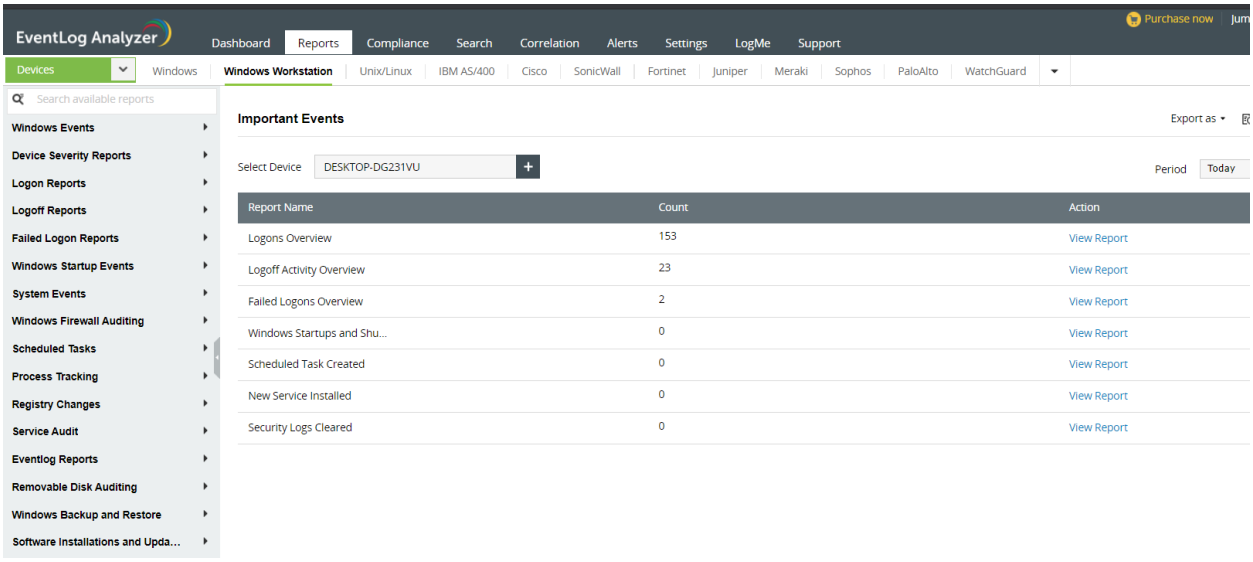

Рис. 3.17 - Вкладка Reports

Также с помощью этой вкладки мы можем просматривать информацию о входах и выходах из системы всех пользователей, смотреть статистику по времени (в какое время было больше входов или выходов), за пользователями (частота авторизаций каждого) и прочее (Рисунок 3.18 и Рисунок 3.19).

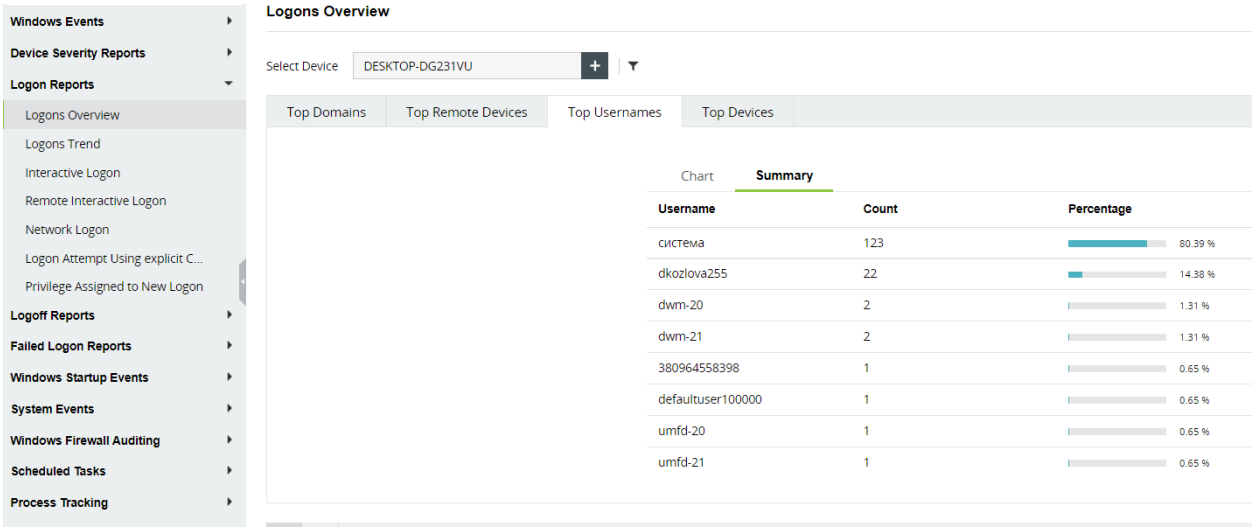

Рис. 3.18 – Статистика авторизаций в системе по пользователям

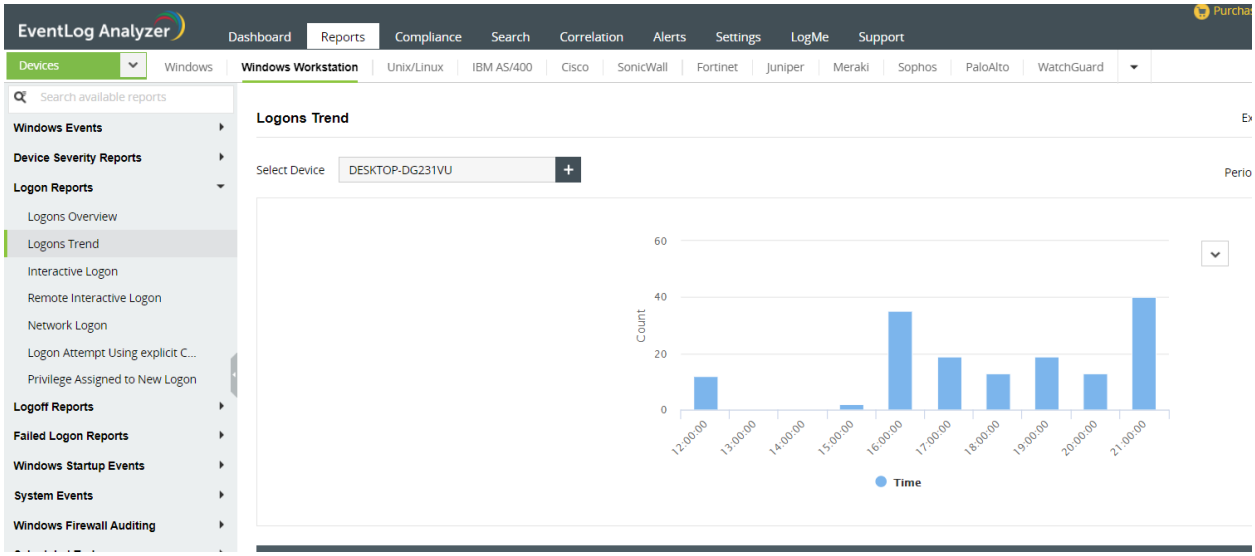

Рис. 3.19 – Статистика авторизаций по времени

Также мы можем просматривать статистику неудачных авторизаций, видеть по какой причине пользователя не было авторизовано (Рисунок 3.20).

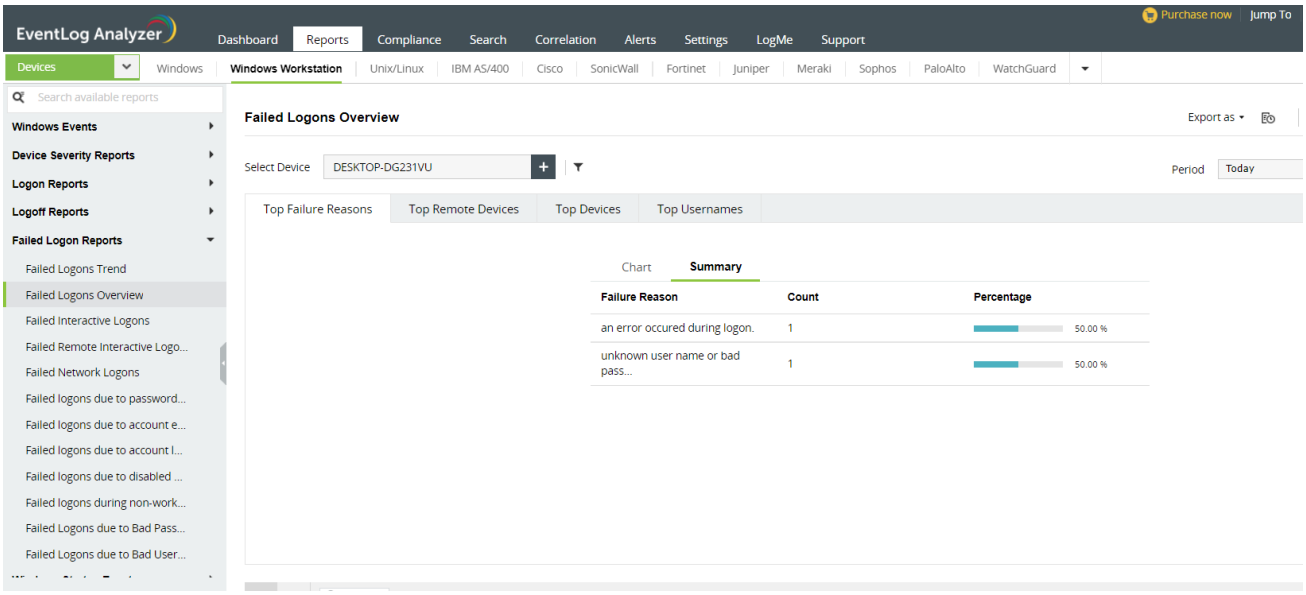

Рис. 3.20 – Статистика неудачных авторизаций

Так же мы можем просматривать статистику по модификации программного обеспечения, просматривать информацию о начале и окончании работы любого сервиса, инициированного любым пользователем, отслеживать изменения времени системы, модификации правил межсетевых экранов и многое другое. Для Linux систем можно настроить мониторинг модификации файлов, авторизаций пользователей через SSH или FTP.

Есть возможность настроить журналы, из которых система будет брать информацию (Рисунок 3.21).

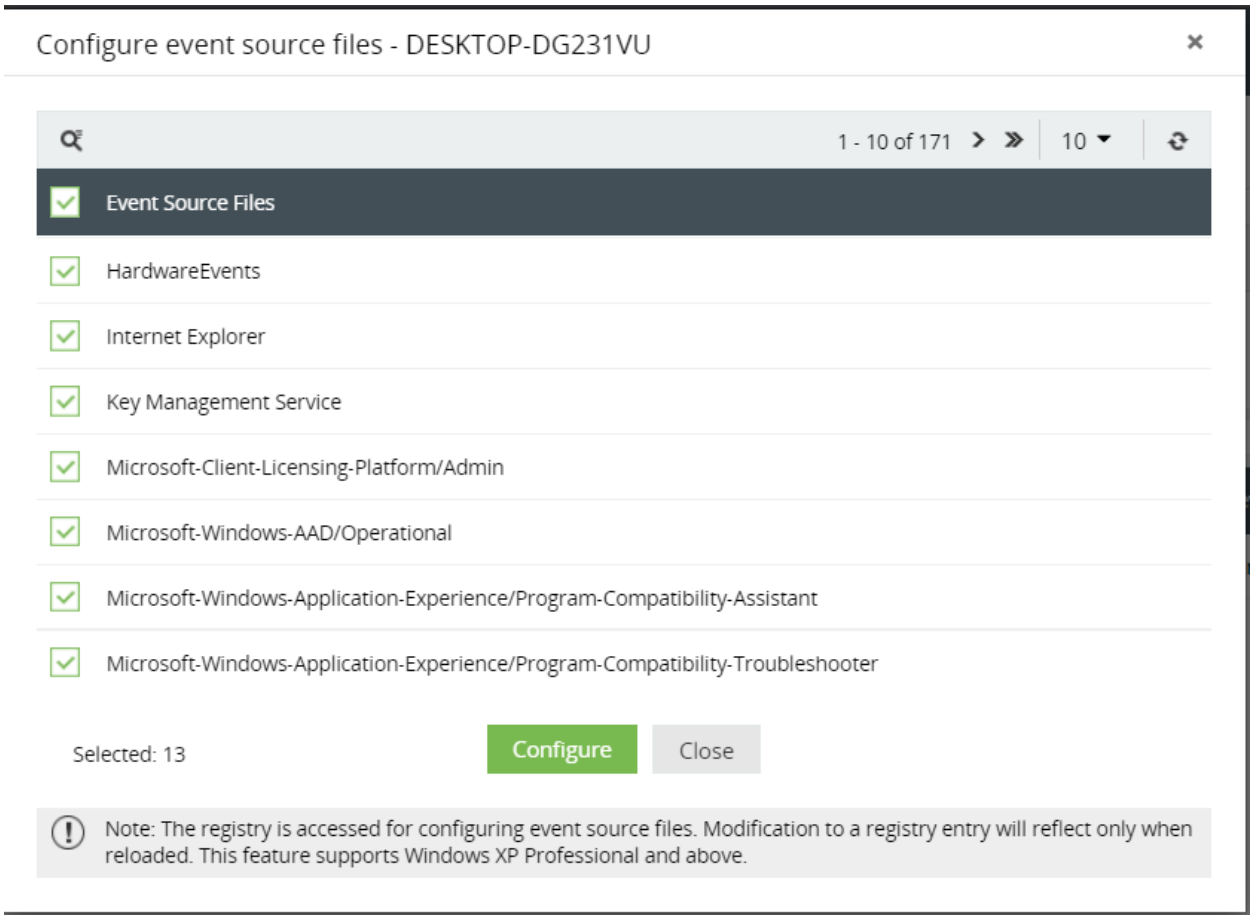

Рис. 3.21 – Конфигурация файлов для информации

С помощью вкладки Alerts мы можем создать собственные сообщения о событии в системе (Рисунок 3.22). Текст сообщения, тип события, устройство настроены, поэтому и полностью адаптированы под каждого администратора.

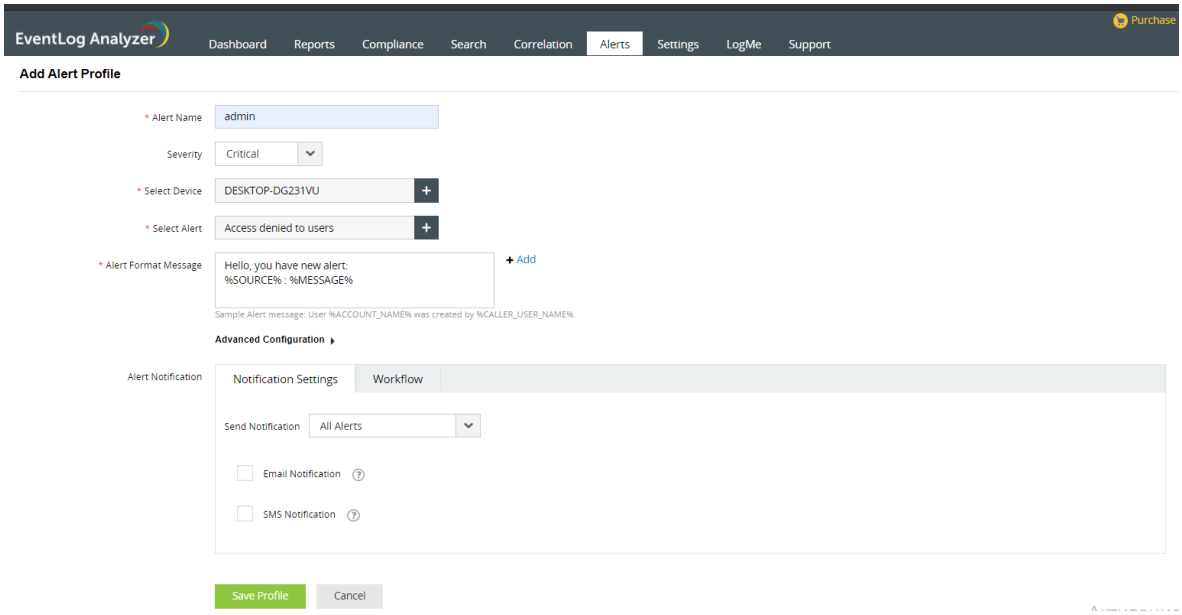

Рис. 3.22 - Настройка собственных сообщений

Также у нас есть возможность создать отчеты по собственным потребностям. Мною был разработан отчет о получении доступа к файлам или удалении их на локальном компьютере (Рисунок 3.23, Рисунок 3.24, Рисунок 3.25 и Рисунок 3.26).

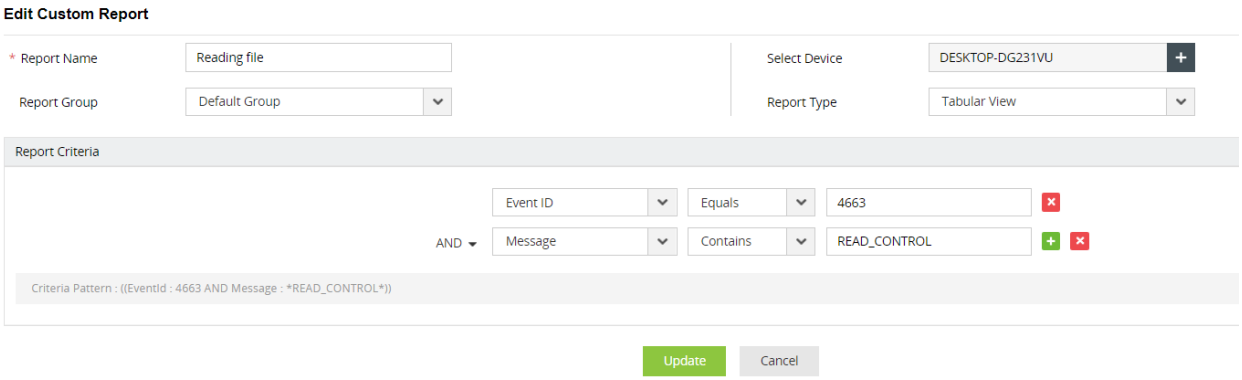

Рис. 3.23 - Настройка отчета “Reading files”

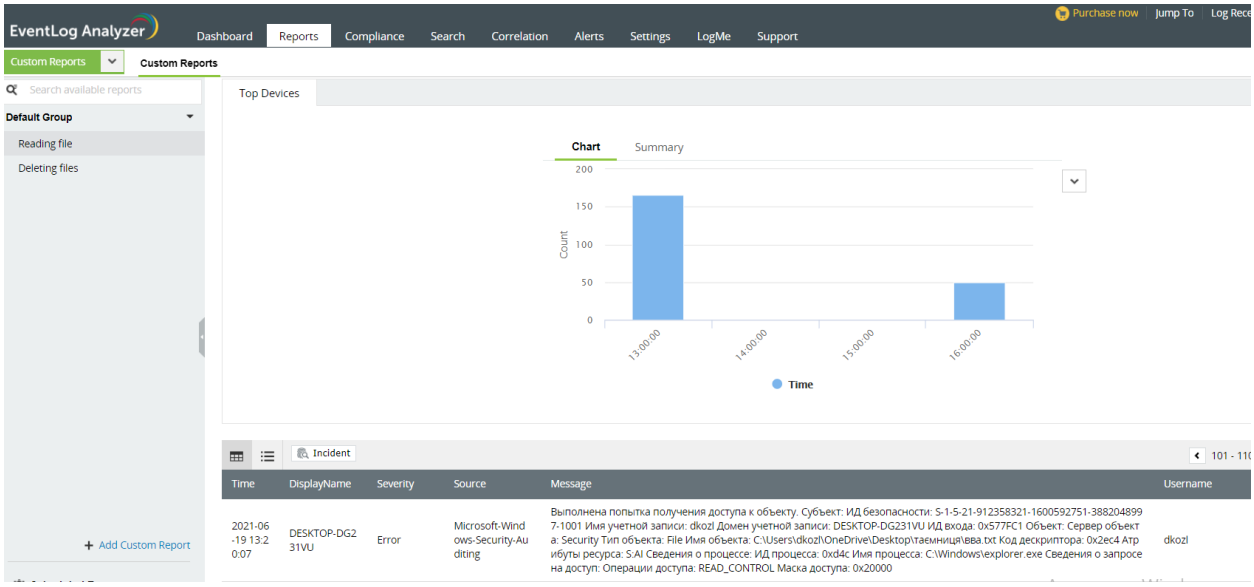

Рис. 3.24 – Результат отчета “Reading files”

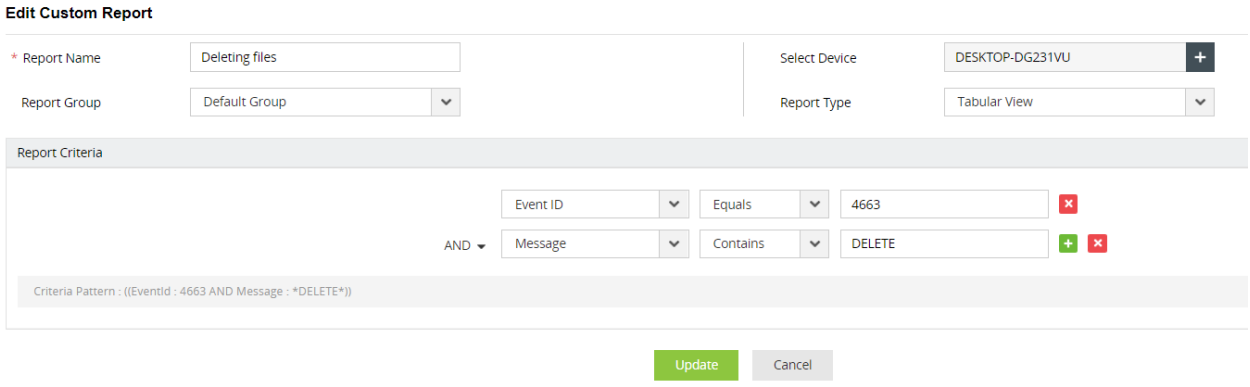

Рис. 3.25 - Настройка отчета "Deleting files"

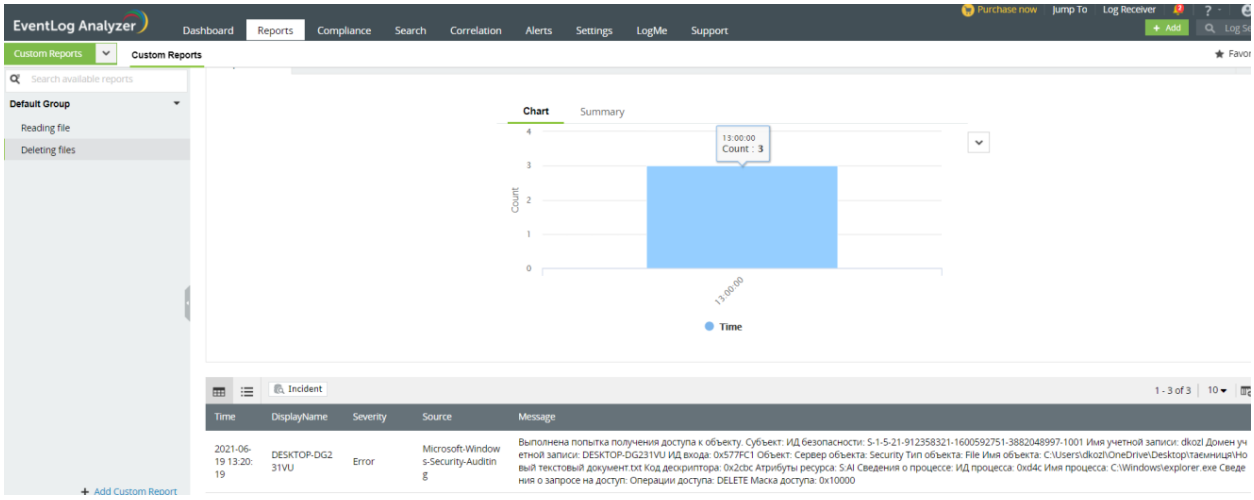

Рис. 3.26 -Результат отчета "Deleting files"

3.4. Расчёт рисков на основе оценок в узлах SIEM-системы.

3.4.1. Расчёт вероятности атак на узлы.

Единый аспект к прогнозированию атак и оцениванию безопасности, исполненный в AMSEC, базируется в прогнозировании действия нападающего, генерации графов атак и связей сервисов, вычислении разных характеристик безопасности и предоставлении операций многостороннего рассмотрения рисков.

Единая процедура оценивания безопасности разделяется в 3 стадии:

(1) получение входной данных;

(2) создание графов атак;

(3) расчет характеристик безопасности.

AMSEC обладает 2 порядка функционирования: offline (постоянный) и online (динамичный). В постоянном порядке входными сведениями с целью расчеты характеристик считаются топология узы, представление определенного программного обеспечения, сведения о популярных уязвимостях, а кроме того, сгенерированные графы атак и модификации нападающих. В динамическом порядке сведениями с целью пересчета характеристик предназначаются подвергнутые обработке действия и сигналы тревоги.

Attack Potential способен рассчитываться статично, в базе наибольшей трудности допуска в разных шагах атаки

$$(P) = \begin{cases} High, AccessDelicacy(P) = Low \\ Low, AccessDelicacy(P) = High \end{cases} \quad (3.1)$$

где P – комплект атакующих действий, AccessDelicacy(P) – максимальная сложность атаки.

Attack Potential способен рассчитываться динамически, в базе числа реализованных деяний атаки и единого числа деяний вплоть до миссии.

Для вычисления AccessDelicacy была выбран метод подхода, так как он может использоваться в статическом, а также в динамическом режиме, приближенным реальному времени, которая дает точную оценку показателя.

При расчете учитывается уровень угрозы, использование backdoor и теорема Байеса:

- любое положение обусловливается равно как участок раздел атак, вместе с учетом его пред- и постусловий;
- начальному узлу атаки назначается возможность, характеризуемая модификацией атакующего (High – 0.7, Medium – 0.5, Low – 0.3);
- возможность перехода с 1-го участка к иному обусловливается сложностью допуска надлежащей уязвимости;

с целью любого участка рассчитываются местные распределения возможностей. В их базе рассчитываются абсолютные вероятности состояний согласно составе общего распределения возможностей: для набора состояний

$$R = \{R_1 \dots . R_n\}, \Pr(R_1 \dots R_n) = \prod_{i=1}^{n} \Pr(R_i | Pa[R_i]), \quad (3.2)$$

где $Pa[S_i] -$ набор всех S_i

Форма пересчета показателя представлена на рисунке 3.27

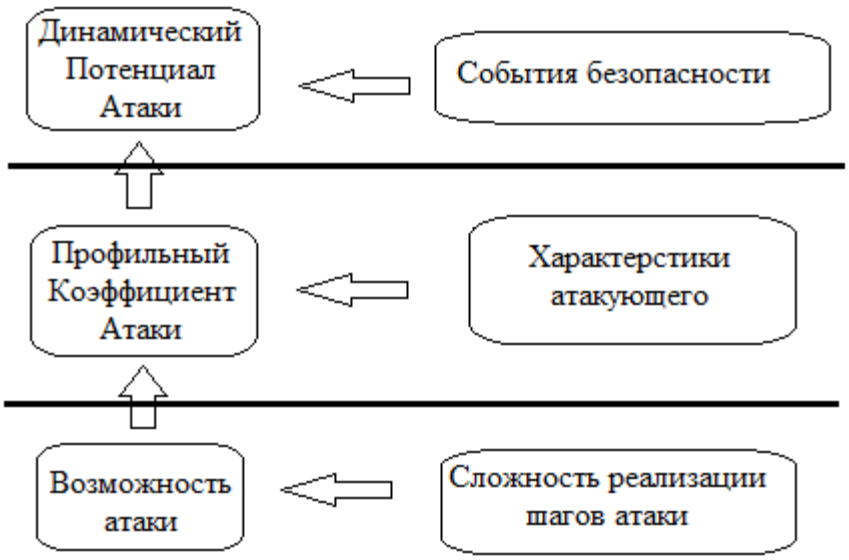

Рис. 3.27. Изменения показателя Уровня Атаки
в зависимости от учитываемых данных.

В последующем степени, степени нападающего, включится коэффициент Dynamic Attack Potential. В основании этого признака Возможности Атаки пересчитывается, создавая другой коэффициент Однопрофильный Attack Potential. Новейшие сведения в степени происшествий, надлежащем интернет системе деятельность AMSEC, кроме того дают возможность скорректировать характеристики. К примеру, сведения касательно реализованных нападающих деяниях дает возможность оценивать касательно способностях нападающего а также сосчитать коэффициент Степень Способностей Нападающего. Кроме того сведения, содержащаяся в действиях защищенности, дает возможность считать вероятности осуществлении нападающих операций в основании теоремы Байеса:

$$Pr(R_1|R_2) = Pr(R_2|R_1) \times Pr(R_1)/Pr(R_2), \quad (3.3)$$

где $Pr(R_1)$, $Pr(R_1)$ - предшествующие вероятности R_1 и R_2.

Это дает возможность откорректировать показатель Attack Potential, сформировав новый показатель Dynamic Attack Potential (уровень событий на рис. 3.27).

3.4.2. Вычисление Attack Potential и Dynamic Attack Potential

Разберем перемена значимости признака Attack Potential в период в образце вычислений с целью испытательной компьютерной сети. На рис. 2 изображены взятые для примера пути атак и соответствующие уязвимости хостов сети:

(1) Внешний пользователь с ноутбуком Шлюз Внешний маршрутизатор Межсетевой экран Внутренний маршрутизатор 1 Хост-1 (CVE-2001-1572, CVE-2006-0038);

(2) Внешний пользователь с ноутбуком Шлюз Внешний маршрутизатор Межсетевой экран Внутренний маршрутизатор 1 Хост-1 Хост-2 (CVE-2001-1572, CVE-2006-0038, CVE-2013-0073);

(3) Внешний пользователь с ноутбуком Шлюз Внешний маршрутизатор Межсетевой экран Внутренний маршрутизатор 1 Хост-1 Хост-3 (CVE-2001-1572, CVE-2006-0038, CVE-2013- 0073).

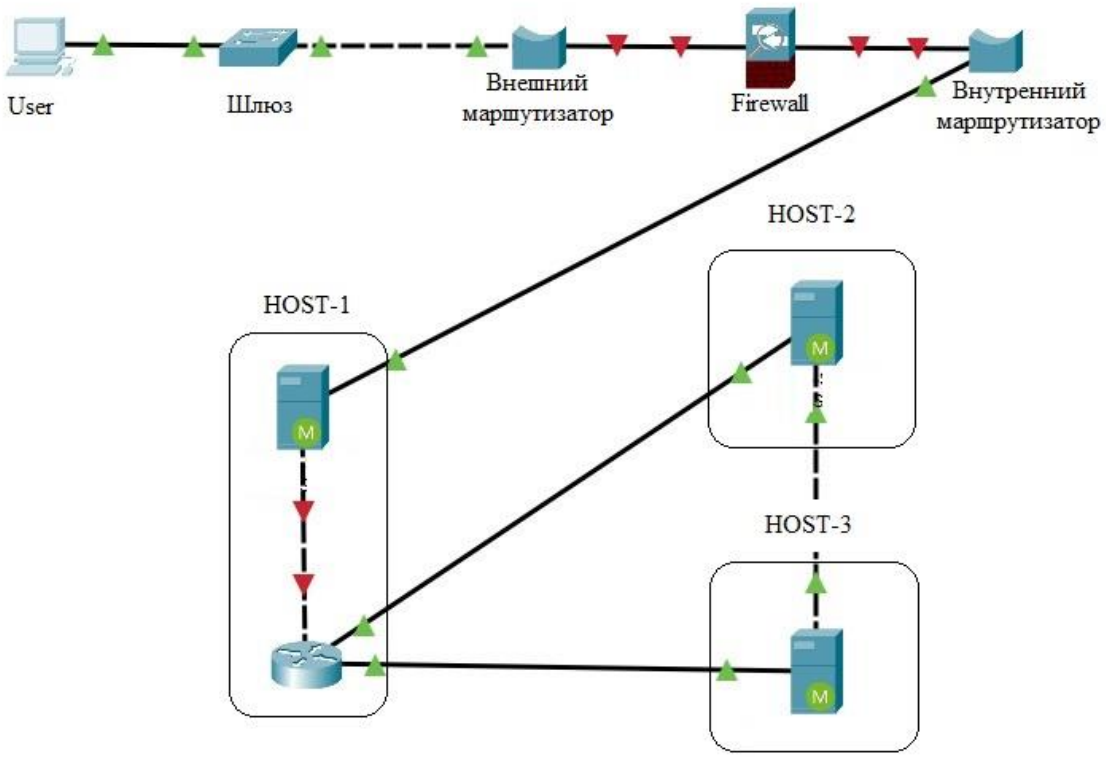

Рис. 3.28. Пример путей атаки.

Attack Potential определяются следующим образом. На данном этапе не учитывается навыки атакующего объекта,

Пользователь с компьютером проходит шлюз, внешний маршрутиза-тор, фаервол и внутренний маршрутизатор до фаервола HOST-1 и HOST-2 или HOST-3 и способен скомпрометировать их качества защищенности.

Используя уязвимости хостов, будем определять узлы, которые соответствуют использованию:

- A – CBE-2013-00073 (e_A=0.71)
- B – CBE-2013-00038 (e_B=0.61)
- C – CBE-2001-01572 (e_C=0.71)

- X – Пользователь

Учитывая Attack Potential, а также использование уязвимостей для проникновения определим вероятность условного распределения:

Узел X: Pr(X)=1 (Dynamic Attack Potential равна 1), Pr(¬X) =0;

Узел C: Pr(C)=0.71 (вероятность использования уязвимости e_c= 0.71) Pr(¬C) = 0.29 для X = 0 – Pr(C) = 0 Pr(¬C) =1;

Узел B: C=1 - Pr(B) = 0, 61 (вероятность использования уязвимости $e_в$= 0.61), Pr(¬B) = 0.39; для C = 0 – Pr(B)=0, Pr(¬B) =1;

Узел A: B=1 – Pr(A) = 0.71 (вероятность использования уязвимости e_A= 0.71), Pr(¬A) = 0.29; для B = 0 – Pr(A)=0, Pr(¬A) =1;

Для каждого узла определим вероятности. Для узла X есть только одно состояние. Чтобы найти показатели на узле C нужно вычислить успех на узле X Pr(C)= 1·0.71=0.71. Показатели узла B вычитываются на основе узла C: Pr(B)=0.61·0.71=0.433. Для узла A учитываем успех на узле B: Pr(A)=0.433·0.71=0.307. Вычисляя данные выводим данные на узлах:

- Attack Potential карт-бланш узла HOST-1 (C) = 0.433
- Attack Potential карт-бланш узла HOST-2 (B) = 0.307
- Attack Potential карт-бланш узла HOST-3 (A) = 0.307

Рассмотрим, как влияет Dynamic Attack Potential на Attack Potential. Определим уровень атакующего как средний (Pr(X)=0.5).

Вычислим изменённые показатели для каждого узла: для узла X - Pr(X)=0.5; для узла C - Pr(C)=0.5·0.71=0.355; для узла B - Pr(B)=0.355·0.61=0.2166; для узла A - Pr(A)=0.2166·0.71=0.1538. По полученным значениям получаем выводы: значение HOST-1 равен 0.2166,
значения HOST-2 и HOST-3 равны 0.1538.

В последующем стадии исследований ведется обрабатывание происшествий защищенности. AMSEC исследует действия защищенности и исчисляет вероятности вероятных предстоящих и предшествующих операций нападающего. Элементарное представление действия защищенности, что

способен анализироваться AMSEC, включает 3 степь: хост ключа, хост направления и вид атаки.

Данное явление включает данные о обнаружении хода распознавания портов. Прокси-сервер 10.10.1.30 был просканирован программой Nmap вместе с пользовательским хостом в наружном узле 192.168.0.1/24. В случае если в докладе согласно действиям защищенности не имеется данных касательно иных нападающих деяниях, AMSEC создает заключение, то что вместе с значительной ступенью вероятности в узы выявлен внешний вид нападающий.

Допустим была произведена успешная атака на узел B. Посчитаем Attack Potential при помощи теоремы Байеса, для получения Dynamic Attack Potential на уровне событий. Произведем вычисления для узла C. Вероятности узлов B и C вычислили выше Pr(B) = 0.2166, Pr(C) = 0.355.

Pr(B÷C) = 0.61. Таким образом Pr(C/B) = 0.61·0.355÷0.2166 = 0.999, при происхождении событий на узле B, вероятность на узле C возросла.

Изменения Attack Potential были показаны на рисунке 3.29. Изменения происходят при добавлении информации на разных уровнях показателей защиты. Новейшая сведения о степени умений нападающего уменьшает значимость признака, нападающий никак не способен применять все без исключения уязвимости. В степени происшествий значимость признака увеличивается из-за выявления новейшего действия. Данное дает возможность совершать теории касательно предшествующих и дальнейших шагах атаки. Кроме того, в базе трудности предшествующих деяний и тенденции атаки возможно совершать теории о степени познаний нападающего.

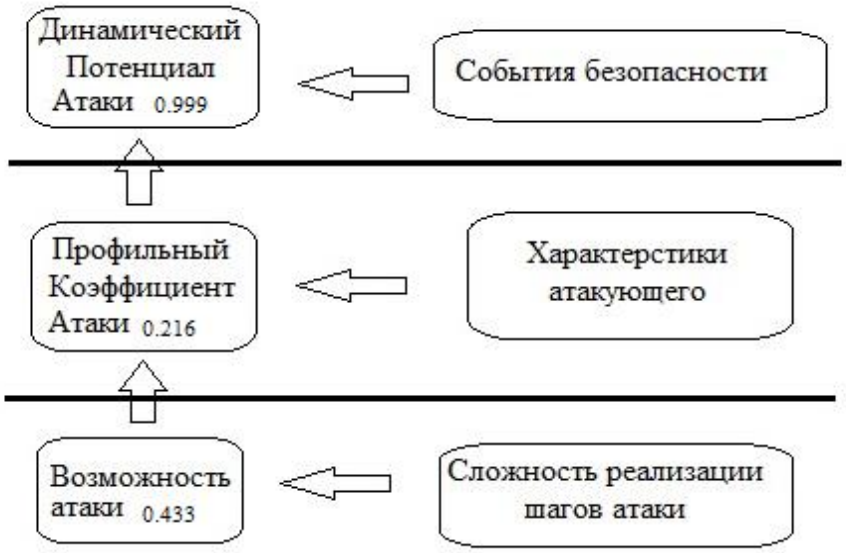

Рис. 3.29. Изменения значения Attack Potential.

ЗАКЛЮЧЕНИЕ

Технологический прогресс не стоит на месте, и системы защиты информации развиваются и эволюционируют вместе с ним. SIEM-системы не являются исключением. Ранее функционал классического SIEM решения больших и средних компаний более-менее удовлетворял имеющимся требованиям. Однако в настоящее время необходимы новые механизмы и функции, способные своевременно и адекватно выявлять, обрабатывать и анализировать текущие потоки информации и событий безопасности для гораздо большего количества устройств с учетом существенно возросших объемов информации, в том числе данных о пользователях, трафике, сервисах, событиях и так далее.

Основой оперативного и адекватного реагирования на инциденты безопасности является правильная обработка событий безопасности, которые собирает SIEM-система, что обеспечивается грамотно построенным процессом нормализации.

В данной магистерской диссертации была разработана методика обработки информации в системах мониторинга событий информационной безопасности, которая определяет обработку информации со стороны процесса нормализации. Особенностью данной методики является углубленное рассмотрение процесса нормализации, в частности, в рамках данной методики была разработана схема полей событий безопасности. Отличием данной схемы является более индивидуальный подход к рассмотрению событий, каждое событие рассматривается отдельно, в нем выделяются поля, которые действительно полезны для дальнейшей обработки SIEM-системой. При разработке данной схемы были проанализированы схемы полей событий безопасности таких решений мониторинга информационной безопасности, как IBM Security Qradar SIEM, Splunk Enterprise Security, McAfee Enterprise Security и AlienVault OSSIM.

Выводы по данной диссертации могут быть следующими:

1. Был проведен анализ предметной области с учитыванием угроз и рисков компьютерных сетей малого предприятия
2. Проведен анализ систем и принципов их работы. Выбрана опен соурс программа и была модифицирована под актуальную форму работы.
3. Предложена методика определения актуальных угроз безопасности информации, в отличие от известных, позволяющая в автоматизированном режиме формировать перечень актуальных УБИ, гипотетически исключая ошибки экспертов. Позволяющая определять большее количество актуальных УБИ, минимизировать трудоемкость процесса и вычислительные ресурсы.
4. На основе трехрубежной модели защиты информации проведены расчеты, позволяющие получить в количественном выражении оценку числа путей распространения атак к узлам в сегментах. Введен показатель «Attack Potential», позволяющий отнести совокупность аномальных событий информационной системы к атаке с использованием механизма нечеткого логического вывода.

Список использованной литературы

1. Зубок М.И. Інформаційна безпека в підприємницькій діяльності. Киев: ГНОЗІС, 2015, – 216 с.
2. Миллер Д.Р. Implementing and Configuring a Security Information and Event Management (SIEM) System. Флорида: Network Pro Library, 2010, 300 стр.
3. В.В. Масленников. Анализ данных безопасности в SIEM-системах. Москва: АСВ, 2021, – 256 с.
4. Quin K. Computer Networking and Cybersecurity. Астен: Primasta, 2020, – 240 с.
5. Хорошко В.О. Основи інформаційної безпеки. Киев: ДУІКТ, 2008, 186 стр.
6. David R. M. SIEM Implementation. Флорида: Network Pro Library, 2010. – 464 с.
7. Kelley D. Practical Cybersecurity Architecture. Birmingham: Packt Publishing Ltd., 2020, – 386 с.
8. Brattle. P. Security Information and Event Management (SIEM) - Implementation Guide, Монтреаль: Basel, 2021, – 350 с.
9. Скрынников, В.В. Управление информационной безопасностью с использованием SIEM-систем. – Москва: Издательство, 2016, 240 стр.
10. Ritvik Kh. How to use Elasticsearch, Logstash and Kibana to visualize logs in Python in real-time. [Электронный ресурс] Ссылка: https://www.freecodecamp.org/news/how-to-use-elasticsearch-logstash-and-kibana-to-visualise-logs-in-python-in-realtime-acaab281c9de/.
11. IBM QRadar Security Intelligence Platform. [Электронный ресурс] Ссылка: https://www.ibm.com/docs/ru/qsip/7.5.
12. Splunk. [Электронный ресурс] Ссылка: https://www.splunk.com/en_us/products/cyber-security.html.
13. McAfee SIEM. [Электронный ресурс] Ссылка: https://roi4cio.com/catalog/product/mcafee-enterprise-security-manager.

14. AlienVault OSSIM. [Электронный ресурс] Ссылка: https://cybersecurity.att.com/products/ossim.
15. Галицкий А. В. Защита информации в сети: анализ технологий и синтез решений. Москва: ДМК Пресс, 2004. – 616 с.
16. Липаев В. В. Функциональная безопасность программных средств. Москва: СИНТЕГ, 2014. – 348 с.
17. Садыг-заде Н.А. Актуальность SIEM-систем на предприятиях. Баку, 2023. – 4 с.