МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологии
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой к.п.н., доцент Бердибаев Рат Шындалиевич

_____ «3» июня 2020г.
(подпись

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Управление безопасностью организации с применением системы Open Source Security Information Management_____

Специальность Системы Информационной Безопасности_____

Выполнил(а) Ергалиев Бекарыс Берикулы Группа СИБ-16-2___

Научный руководитель: к.т.н., профессор Тынымбаев С.Т.
Консультант: старший преподаватель Тергеусизова Алия Советжановна____
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна_____

_____ «» _____2020г.
(подпись)

по безопасности жизнедеятельности:
к.т.н доцент кафедры БТИЭ Приходько Николай Георгиевич_____

_____ «15» мая 2020г.
(подпись)

Нормоконтролер: старший преподаватель Дмитриева Маргарита Валерьевна

_____ «_____» _____2020г.
(подпись)

Рецензент: зав. кафедры «Кибербезопасность, обработка и хранение информации» КазНИТУ имени К.И Сатпаева, к.т.н.,доцент Сейлова Нургуль Абадуллаевна

_____ «» ____ 2020г.
(подпись)

Алматы 2020

Задание на выполнение дипломного проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных Технологии

Кафедра «Системы Информационной Безопасности»_____

Специальность «Системы Информационной Безопасности»____

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Ергалиев Бекарыс Берикулы _____

Тема проекта Управление безопасностью организации с применением системы Open Source Security Information Management

Утверждена приказом по университету № 563 от «15» октября 2019 г.

Срок сдачи законченного проекта «8» июня 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): Исходные материалы для выполнения задания дипломного проекта – ER-диаграмма незащищенной реляционной учебной базы данных банка, сервер OSSIM Debian Linux, Windows Server 2012R, Ubuntu Linux Server, VMware ПО для виртуализации, маршрутизатор EdgeMax_____

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы - организация SIEM системы OSSIM для компании. Акцент делается на защите каждого устройства в сети, то есть благодаря обработке данных исходящих от устройств в сети и своевременное оповещение об инциденте._____

Перечень графического материала (с точным указанием обязательных чертежей): Глава 1 содержит 16 рисунков, в главе 2 представлено 87 рисунков, в главе 3 представлено 56 рисунков, в 4 главе представлено 6 рисунков.

Основная рекомендуемая литература: David R.Miller, SIEM Implementation 1-st edition, официальная документация OSSIM SIEM, веб-сайт www.anti-malware.ru

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 9.05.2020	
Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 9.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Изучение предметной области	17.02.2020 – 25.02.2020	
Исследование SIEM систем	26.02.2020 – 4.03.2020	
Организация SIEM системы OSSIM	5.03.2020 – 24.03.2020	
Описание инструментов OSSIM	25.03.2020 - 7.04.2020	
Произведение атаки «BruteForce»	8.04.2020 – 25.04.2020	
Анализ результатов	26.04.2020 - 9.05.2020	
Анализ рисков ИБ. БЖД	29.04.2020 - 9.05.2020	

Дата выдачи задания «15» октября 2019г.

Заведующий кафедрой : _____ Бердибаев Рат Шындалиевич
(подпись)

Научный руководитель проекта: _____ к.т.н., профессор Тынымбаев С.Т.
(подпись)

Консультант:

_____ старший преподаватель Тергеусизова Алия Советжановна

(подпись)

Задание принял к

исполнению студент: _____ Ергалиев Бекарыс Берикулы

(подпись)

Аннотация

Тема дипломного проекта «Управление безопасностью организации с применением системы Open Source Security Information Management». Проект внедрялся в компанию «Просто Бэк-Офис». В данной работе была проанализирована архитектура SIEM системы, исследованы и сравнены различные SIEM системы, выбрана система OSSIM и на её основе спроектирована система сбора и корреляции событий информационной безопасности. Показаны сравнение OSSIM с платной версией системы USM, разработана структурная схема корпоративной сети после введения системы , также была произведена атака «BruteForce» на устройство в сети и были показаны результаты выявления системой. Также были рассмотрены инструменты системы, такие как хостовая система обнаружения вторжений - OSSEC, сетевая система обнаружения вторжений - Suricata, сканер активов - Nagios, сканер уязвимостей - OpenVAS.

Проведен анализ условий труда с расчетом системы кондиционирования и пожарной безопасности.

Были рассчитаны риски информационной безопасности, задачей которых являлось понимание реальных угроз, расчёт рисков, а также выбора мер направленные на уменьшение и защиту этих рисков.

Аңдатпа

Дипломдық жобаның тақырыбы: «Ұйымның қауіпсіздігін Open Source Security Information Management жүйесі арқылы басқару». Жоба «Просто Бэк-Офис» компаниясында жүзеге асырылды. Бұл жұмыста SIEM жүйесінің архитектурасы талданды, әртүрлі SIEM жүйелері зерттелді және салыстырылды, OSSIM жүйесі таңдалып, соның негізінде ақпараттық қауіпсіздік оқиғаларын жинау және өзара байланыстыру жүйесі жасалды. OSSIM-ді жүйесінің ақылы USM нұсқасымен салыстыруы көрсетілген, жүйені енгізгеннен кейін корпоративті желінің блок-схемасы жасалынған, желідегі құрылғыға «BruteForce» шабуылы жасалынған және жүйемен анықталған нәтижелер көрсетілген. Сондай-ақ, жүйенің хосстағы шабуылдарды анықтау жүйесі - OSSEC, желіні басып кіруді анықтау жүйесі - Suricata, активтерді анықтау - Nagios, осалдықты анықтау – OpenVAS сияқты құралдар қарастырылған.

Кондиционерлерді және өрт қауіпсіздігін есептеу кезінде жұмыс жағдайын талдау.

Ақпараттық қауіпсіздіктің қауіп-қатері есептелді, олардың міндеті нақты қауіп-қатерлерді түсіну, қауіп-қатерлерді есептеу, сондай-ақ осы қауіп-қатерлерді азайтуға және қорғауға бағытталған шараларға таңдау жүргізілді.

Abstract

The theme of the diploma project is “Organization security management using the system Open Source Security Information Management”. The project was implemented in the company “Просто Бэк-Офис”. In this work, we analyzed the architecture of the SIEM system, investigated and compared various SIEM systems, selected the OSSIM system, and based on it we designed a system for collecting and correlating information security events. Comparison of OSSIM with the paid version of the USM system is shown, a block diagram of the corporate network is developed after the introduction of the system, a «BruteForce» attack was also performed on a host on the network, and the results of the system detection were shown. Also, system tools were examined, such as the host intrusion detection system - OSSEC, the network intrusion detection system - Suricata, the asset scanner - Nagios, the vulnerability scanner - OpenVAS.

Working conditions were analyzed with the calculation of air conditioning and fire safety

Information security risks were calculated, the task of which was to understand real threats, calculate risks, as well as choose measures aimed at reducing, protecting these risks .

Содержание

Введение

В настоящее время число угроз, связанных с нарушением доступности, целостности и конфиденциальности в информационных системах возросло в десятки раз и хакеры представляют собой сообщество хорошо организованного и технически оснащенного криминала, о чем говорит статистика событии информационной безопасности, представленных крупными компаниями. Специалисты в области информационной безопасности считают, что необходимо создать комплексный подход в сфере реагирования и расследования инцидентов информационной безопасности в виде единого централизованного решения. Задача систем мониторинга событий информационной безопасности вполне актуальна в наше время, данная задача появляется по мере все большего увеличения числа событий, и она не будет терять своей актуальности и в будущем. Темы информационной безопасности на крупных предприятиях принимается как данность. Не являются исключением и представители химической отрасли, имеющие территориально разветвленную сеть предприятий, на которых системы информационной безопасности (ИБ) имеют тенденцию к постоянному развитию и адаптации к новым видам угроз. Таким образом, количество средств защиты информации, как и иных источников данных о текущем состоянии защищенности, неуклонно растет, усложняя тем самым не только инфраструктуру системы, но и процесс обработки этих самых данных. В таких условиях отслеживание общей картины событий, происходящих в инфраструктуре, становится все более трудоемкой задачей для администраторов ИБ, несмотря на наличие у большинства корпоративных программных продуктов функции ведения журнала событий. И проблема здесь заключается не в числе таких продуктов, а в неумении разнородных продуктов общаться между собой, обмениваться данными об угрозах и уязвимостях, нарушителях и инцидентах. Даже десяток систем обнаружения вторжений окажется бесполезным, если своевременно не реагировать на возникающие угрозы и не пытаться предотвратить их.

В данной дипломной работе рассматривается построение SIEM системы OSSIM для организации ТОО «Просто Бэк-Офис” под управлением операционной системы Debian Linux. Реализация предложенного проекта позволит управлять событиями безопасности, манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности. «Проактивный» означает «действующий до того, как ситуации станет критической».. Как следствие, появится возможность проводить корректное реагирование на возникающие угрозы ИБ и ИТ. SIEM(Security Information and Event Management) система должна быть спроектирована таким образом, чтобы обеспечить надлежащую степень защищенности сети. Целью дипломной работы является организация SIEM системы .

Для реализации поставленной цели в работе решаются следующие задачи:

- описание архитектуры SIEM систем
- исследование, а также сравнение популярных SIEM систем;
- разработка структурной схемы сети для внедрения системы;
- установка SIEM системы OSSIM;
- анализ инструментов имеющихся в системе OSSIM;
- проведение расчета анализа условий труда и расчета системы кондиционирования помещения;
- расчет рисков ИБ.

1 Теоретическая часть

В нынешних условиях проблема обеспечения информационной безопасности предприятия приобретает все больше сложный характер. Существуют инциденты, которые имеют связь с ненадёжной защищенностью данных и автоматизацией систем предприятий. Нужно брать во внимание, что как правило система защиты информации реагирует недостаточно быстро и эффективно. Из за этого в последнее время все чаще можно увидеть процессы мониторинга событий информационной безопасности, а также обнаружение и обработка выявленных инцидентов информационной безопасности в кратчайшие сроки. Отделы информационной безопасности которые имеют программно-технические средства, такие как IDS и IPS системы, антивирусное программы, DLP-системы, журналы событий, сканеры уязвимостей и т.д. все равно выявляют инциденты информационной безопасности, которые чреваты крупными потерями. Притом что с укрупнением организации, когда увеличивается число серверов, автоматизированных рабочих мест, сетевых устройств, в то время как журналы от разных источников хранится отдельно, имеет различные формы и форматы, что определяет слабую скорость анализа событий, его качества и невозможность определения их взаимосвязи, т.е. имеется некачественный мониторинг отрицательно влияющий на выявление инцидента, когда выявляются негативные последствия информационной системы в результате возникновения инцидента. Следовательно для решения такого рода проблем актуально стала система SIEM .

Security Information and Event Management - это программное средство, осуществляющее анализ в реальном времени событий безопасности, исходящих от сетевых компонентов и приложений. SIEM используется также для создания журналов данных и генерации отчетов в целях совместимости с прочими бизнес-данными. SIEM – объединение двух понятий , таких как: SEM(Security Information Management) – управление событиями безопасности и SIM(Security Event Management) – управление информационной безопасностью. SIEM системы обеспечивают анализ событий безопасности, исходящих из приложений и сетевых устройств в реальном времени. SIEM состоит из приложений, приборов, услуг, а так же используется для журналирования данных[1].

Подобные системы помогут решить нам следующие задачи:

1) Обьеденение и хранение журналов событий от различных источников

– журналов ОС, сетевых устройств, приложений и СЗИ. Посмотрев любой стандарт ИБ, мы увидим технические требования по сбору и анализу событий. Они нужны не только для того, чтобы выполнить требования стандарта, ведь бывают ситуации, когда инцидент увидели поздно, а события уже давно удалены или журналы событий почему-то недоступны и причины произошедшего выявить практически невозможно;

2) Предоставление инструментов для анализа событий и разбора инцидентов. Создает читабельный ответ. В том числе непосредственно с нужной Вам фильтрацией. Например, ежедневный отчет об инцидентах, отчет о работоспособности и т.д;

3) Корреляция и обработка по правилам. Простейший пример — «login failed»: один случай ничего не значит, но три и более таких события с одной учетной записью уже могут свидетельствовать о попытках подбора. В простейшем случае в SIEM правила представлены в формате RBR (Rule Based Reasoning) и содержат набор условий, триггеры, счетчики, сценарий действий;

4) Автоматические оповещение и инцидент-менеджмент. Основная задача таких систем – не простой сбор событий, но и автоматизация процесса обнаружения инцидентов со сбором в журнале, а также своевременное информирование о событии;

5) При наличии сканера уязвимостей, система частично поможет оценить риски (рисунок 1.1) [2].

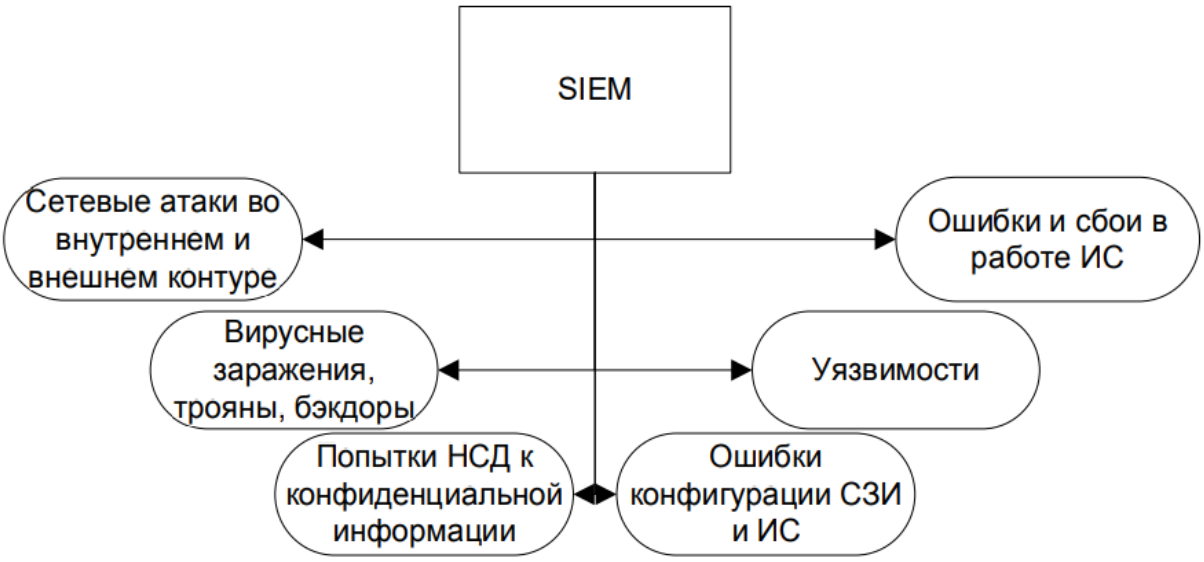


Рисунок 1.1 – Оценка рисков

Системы сбора и корреляции событий многофункциональны за счет своей логики, но для того, чтобы добиться от них желаемого результата, необходимы практичные источники и правила корреляции событий. Любое

событие (например, с DLP системы) может послужить данными для анализа. Источники выбираются на базе факторов которые указаны ниже:

– Критичность системы и информации;

– Достоверность и информативность источника событий;

– Покрытие каналов передачи информации (учитывается не только внешний, но и внутренний контур);

– Решение спектра задач ИТ и ИБ.

1.1 Архитектура SIEM системы

Как правило, SIEM-система имеет архитектуру «агенты» — «хранилище данных» — «сервер приложений», которая разворачивается поверх защищаемой информационной инфраструктуры [5]. Агенты занимаются сбором событий безопасности, их первоначальной обработкой и фильтрацией. Собранная и отфильтрованная информация далее направляется в хранилище данных или так называемый репозиторий, где уже эта информация хранится во внутреннем формате представления с целью последующего использования и анализа сервером приложений. Сервер приложений выполняет основные функции защиты информации. Он анализирует информацию, хранимую в репозитории, и преобразует ее для выработки предупреждений или управленческих решений по защите информации. Следовательно, в SIEM-системе можно указать следующие три архитектурных уровня ее построения (рисунок 1.2) [6]:

- сбора данных;
- управления данными;
- анализа данных.

Первый уровень представляет собой сбор данных от источников различных видов. К числу таковых относятся: файловые серверы, серверы баз данных, Linux-серверы, межсетевые экраны (МСЭ), рабочие машины, системы противодействия атакам (IPS, intrusion prevention systems), антивирусные программы и т.п. На следующем то есть на втором уровне осуществляется управление данными о событиях безопасности, которые хранятся в репозитории.

Данные, хранящиеся в базе(репозитории), выдаются по запросам моделей анализа данных. Результатами обработки информации в системе, получаемыми на третьем уровне, являются отчеты в предопределенной и произвольной форме, оперативная (on-line) корреляция данных о событиях, а также предупреждения, вырабатываемые в режиме on-line и (или) передаваемые по электронной почте.

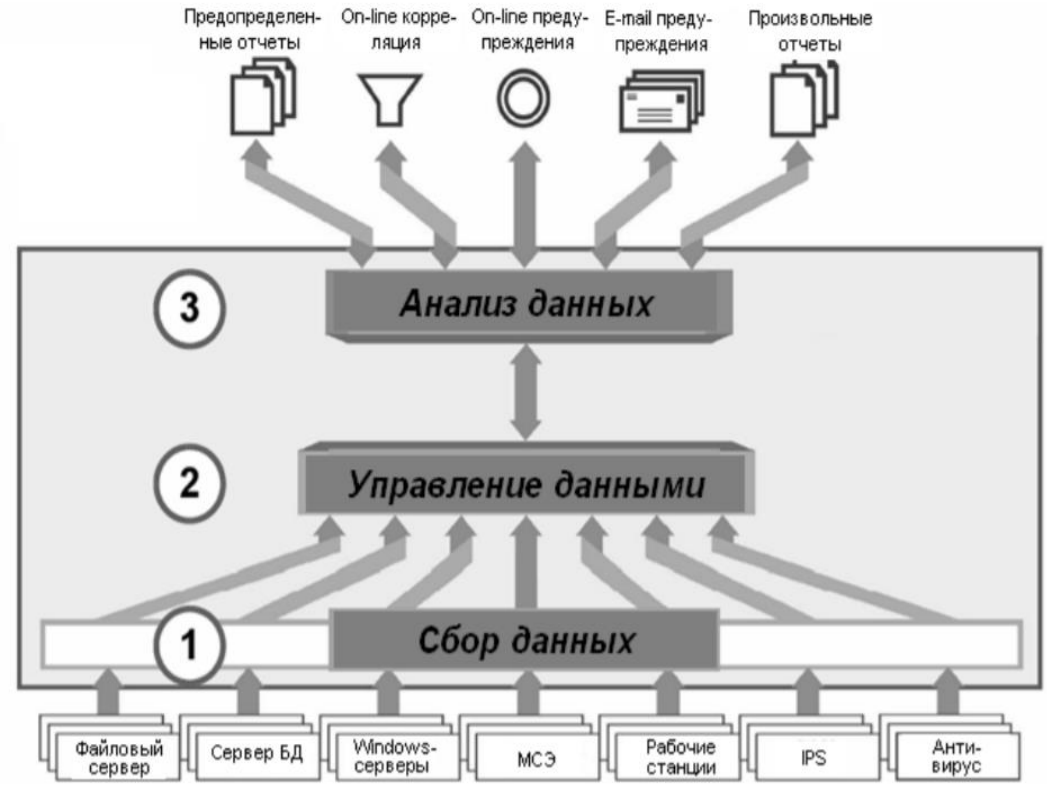


Рисунок 1.2 – Архитектура типовой SIEM системы

Данные о событиях выводятся от источников благодаря агентам, либо удаленно. В случае удаленного сбора событий возникает нагрузка на сеть, потому что некоторые устройства передают весь журнал событий, состоящий их большого количества информации которая и приводит нагрузку на сеть. Вдобавок, события должны не только собираться в хранилище для разбора в дальнейшем, но и обрабатываться. В противном случае система не оправдает затрат. Очевидно, инструментарий SIEM сократит время для расследования инцидента, но цель SIEM системы – то есть своевременное обнаруживание и предотвращение угрозы, а также оперативное реакция. Именно поэтому правила корреляции нужно разрабатывать индивидуально, в соответствии со спецификой компании или предприятия. Данные правила являются недолговечными и нуждаются в обновлении. Тоже самое в случае с системами обнаружения вторжений, если вовремя не прописывать правила или не обновлять базу правил, которое помогут обнаружить угрозу – угроза скорее всего будет реализована. Одним из достоиств систем сбора и корреляции событий информационной безопасности перед системами обнаружения вторжений в правилах – возможность показывать общее описание симптомов и использование накопленной статистики для наблюдения отклонений от нормального состояния информационных систем.

1.2 Функционирование SIEM-системы.

Рисунок 1.3 – Обобщенная иерархическая модель SIEM-системы

К главным механизмам функционирования SIEM-системы можно перечислить:

1) Нормализация определяется приведением форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки;
2) Фильтрация событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков;
3) Классификация позволяет для атрибутов событий безопасности определить их принадлежность определенным классам;
4) Агрегация объединяет события, схожие по определенным признакам;
5) Корреляция выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки на КВИ, а также нарушения критериев и политик безопасности;
6) Приоритезация определяет значимость и критичность событий

безопасности на основании правил, определенных в системе;

7) Анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов;

8) Генерация отчетов и предупреждений означает формирование, передачу, отображение и (или) печать результатов функционирования. Принятие решений определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности инфраструктуры;

9) Визуализация предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой КВИ и ее элементов;

Нужно иметь в виду, что при переключении к механизмам высокого уровня модели, показанной на рисунке 1.3, количество обрабатываемых событий сокращается, а сложность их обработки увеличивается. То есть можно считать что эффективность увеличивается. Взаимосвязь механизмов функционирования SIEM-системы нового поколения наглядно демонстрирует функциональная модель, представленная на рисунке 1.4.

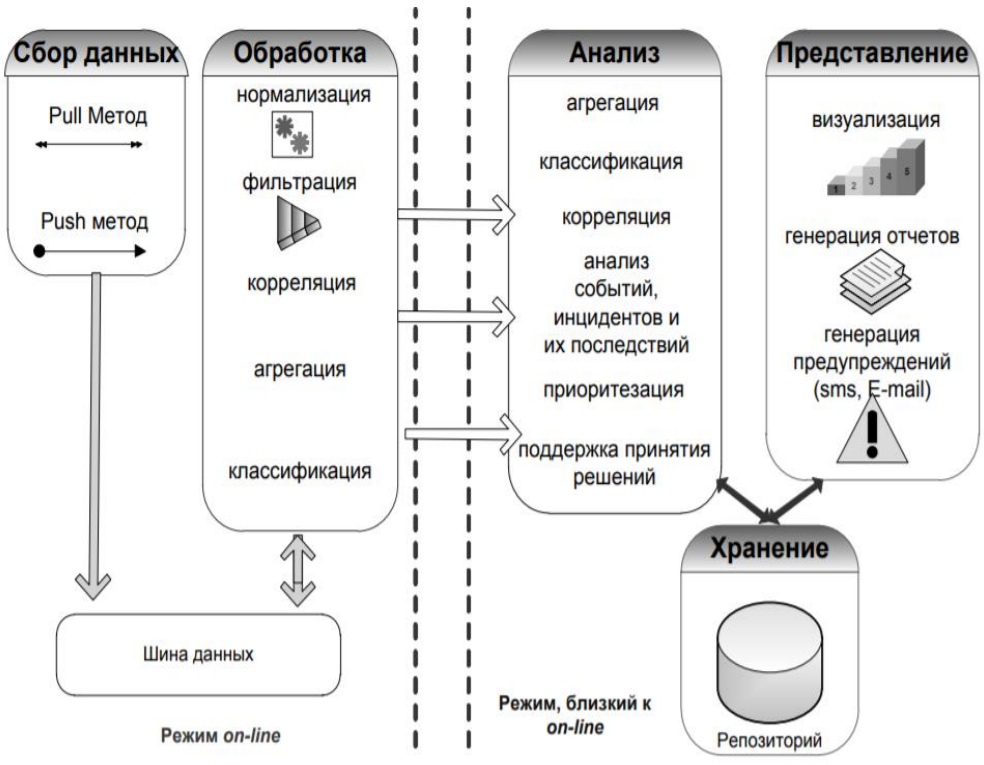


Рисунок 1.4 – Функциональная модель SIEM системы

Как видно из рисунка 1.4, в SIEM-системе можно выделить пять основных функциональных подсистем:

1) сбора данных;

2) обработки;
3) хранения;
4) анализа;
5) представления.

Вдобавок первые две функционируют в режиме on-line, остальные близкие к нему. Дадим краткую характеристику этим подсистемам.

1) Подсистема сбора данных. Для получения информации от источников существует два главных метода: Push и Pull. Смысл метода Push заключается в том, что источник сам посылает данные записей своих журналов в SIEM-систему. Соответственно в методе Pull система сама осуществляет процесс получения данных из журналов. Сбор данных можно получать от источников различных видов.

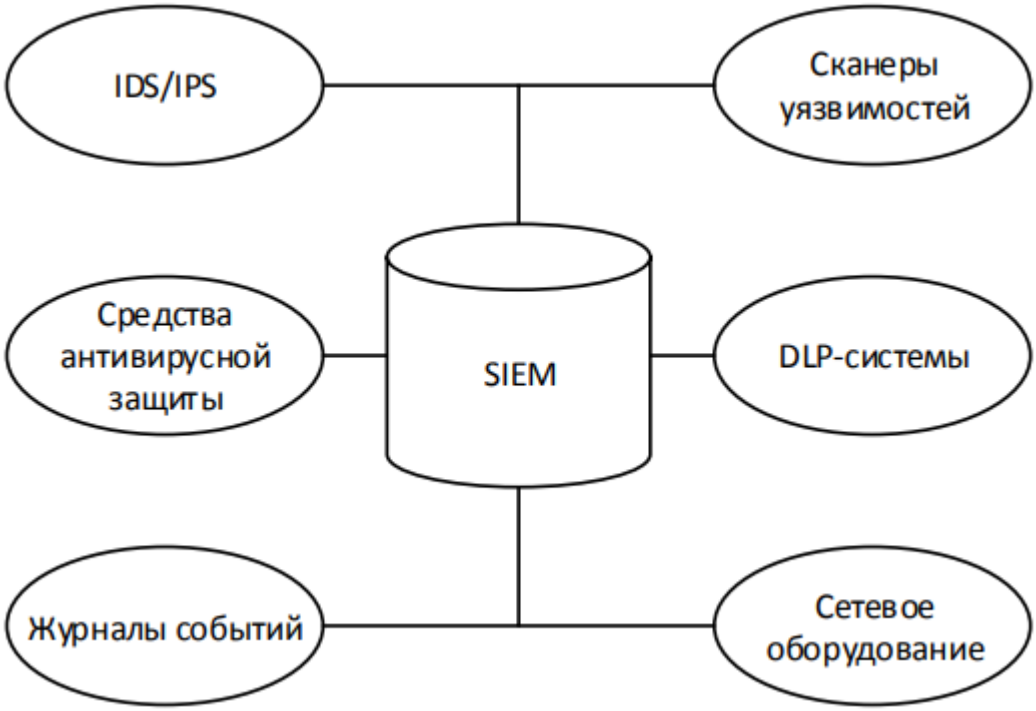


Рисунок 1.5 - Основные источники событий SIEM-системы

Информация поступает в SIEM с разных устройств — таких, как(рисунок 1.5):

- Access Control, Authentication. Применяются для мониторинга контроля доступа к информационным системам и использования привилегий;
- DLP-системы. Сведения о попытках инсайдерских утечек, нарушении прав доступа;
- IDS/IPS-системы. Несут данные о сетевых атаках, изменениях конфигурации и доступа к устройствам;

- Антивирусные приложения. Генерируют события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде;
- Журналы событий серверов и рабочих станций. Применяются для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности;
- Межсетевые экраны. Сведения об атаках, вредоносном ПО и прочем.
- Сетевое активное оборудование. Используется для контроля доступа, учета сетевого трафика;
- Сканеры уязвимостей. Данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры;
- Системы инвентаризации. Поставляют данные для контроля активов в инфраструктуре и выявления новых;
- Системы веб-фильтрации. Предоставляют данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов[3].

2) Подсистема обработки. Обработка информации включает в себя нормализацию, фильтрацию, корреляцию, агрегацию и классификацию;

3) Подсистема хранения. Отфильтрованные данные в нормализованном виде переходят для хранения в репозиторий. Репозиторий может быть создан на основе реляционной СУБД (наиболее распространенное решение), XML-ориентированной СУБД и (или) хранилища триплетов. Хранилище триплетов — это специально созданная база данных, оптимизированная для хранения и поиска триплетов, т.е. утверждений вида «субъект–предикат–объект»;

4) Подсистема анализа. Состоит анализ данных из следующих функции: корреляцию данных, классификацию, агрегацию, приоритезацию и анализ событий, инцидентов и их последствий (в том числе посредством моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов), а также поддержку принятия решений. Сам процесс анализа данных может базироваться на качественных и количественных оценках. Количественная оценка является более точной, но для нее необходимо заметно больше времени, что не всегда позволимо. Чаще всего бывает нужно быстро и качественно сделать анализ , задача которого заключается в распределении факторов риска по группам. Шкала качественного анализа может различаться в разных методах оценки, но все сводится к тому, чтобы выявить самые серьезные угрозы. Подсистема представления. Представление включает в себя несколько функций: визуализацию, генерацию отчетов и генерацию предупреждений.

1.3 Корреляция в SIEM системах

Рисунок 1.6 - Корреляция в SIEM системах

SIEM способен коррелировать:

- Угрозу, описанную правилами;
- Угрозу на базе общего шаблона;
- Аномалию в случае отключения базы накопленной статистики (baseline);
- Отклонение от правила «всё, что не разрешено – запрещено»;
- Причинно – следственную связь, если используются отдельные алгоритмы (CBR, GBR, statistical, Bayesian)[4].

Три крайних алгоритма в странах СНГ очень редко экслпатируются(рисунок 1.6). Очень сжатое количество систем могут работать с такими методами корреляции. Работы с этими алгоритмами повышает стоимость обслуживания системы за счёт потребности в выделенном квалифицированном специалисте, который будет конфигурировать и поддерживать систему в стабильном состоянии. В начале эксплуатации количество ложных срабатываний системы очень много, поэтому в большинстве случаев компании просто отключают эти механизмы обнаружения.

Многие компании не могут себе позволить иметь в штате квалифицированного аналитика, занимающегося системой SIEM и правилами корреляции, из за этого нередко обновление правил просто отсутствует. От этого исходит, что в случае однократной настройки правил корреляции инцидент обнаружится, только если о нём заявит другое средство защиты.

1.4 Принцип работы

SIEM системы автоматический объединяют и согласуют собой события ИБ, которые получаются от различный защитных устройств, позволяя аналитикам акцентироваться на более сложных критических задачах. На сегодняшний день не существует универсальных систем обнаружения и предотвращения вторжений. Так как все защитные решения имеют свои слабости и преимущества, а все защищаемые ресурсы и информационные системы крайне разнообразны. Системы для обнаружения вторжений можно сочетать и тем самым повышать эффективную работоспособность системы безопасности в целом, но в силу своего разнообразия системы обнаружения могут выдавать разную выходную информации в плане уровня тревожности, так как он связан с уровнем конфиденциальности защищаемой информации.

Вторжение происходит тогда, когда злоумышленник пытается попасть в защищаемую систему или неправильно использовать её. Термин «неправильно использовать» может толковаться по-разному и относится ко многим действиям, начиная с раскрытия конфиденциальной информации и заканчивая тривиальной рассылкой спама. Например, большинство тревожных событий, вырабатываемых системами контроля доступа к ресурсам на серверах и компьютерах персонала, не отражают непосредственно атаки. Они описывают действия пользователя, который работает с защищаемыми ресурсами, поэтому при анализе ситуации мы должны учитывать контекст, в котором появились тревожные события. Рассмотрим некоторые из них:

- Событие «введен неверный пароль» очень часто возникает во всех системах, поэтому должно игнорироваться, однако если оно 16 многократно происходило в нерабочее время компании, нужно будет создать предупреждение высокого уровня;
- Если странное поведение пользователя обнаружено на одном сервере, то это может и скорее всего, является ложной аномалией и может быть проигнорировано. Однако если же это происходит на нескольких серверах, то кто-то явно исследует сеть (например, просмотр портов);
- В некоторых компьютерных системах событие класса «не удалось войти в систему» может происходить много раз , в свою очередь в других средах таких событий не должно быть вообще.

Выше были описаны некоторые события, которые являются самой маленькой частью данных об обнаружении вторжения. События, обязательно нужно запротоколировать. После, эти данные будут участвовать в трех стадиях противодействия вторжениям:

- Обнаружение;
- Реакция;
- Предотвращение[5].

Система корреляции получает информацию на всех этих стадиях и объединяет её по ранее заданным алгоритмам. Это делает процесс обнаружения управляемым и обеспечивает нужными сведениями для

будущего предотвращения и соответствующей реакции. Стоит отметить, что корреляция событий на крупном предприятии – трудоёмкая задача по обработке больших объемов данных. Для таких случаев создаются автоматизированные системы, которые помогут объединить большое количество информации, избавиться от избытка данных, найти нужные события и действовать, опираясь на собранный материал. Каждая такая задача может быть выполнена системой сбора и корреляции событий информационной безопасности.

Основываясь на данных корреляции, производимой во время появления события, может быть запрещен доступ к атакованному устройству, таким образом, ущерб от вторжения будет снижен. Без централизованного управления системой и механизмами корреляции, невозможно иденнтифицировать вид атаки, оценить адекватность системы защиты и предпринять меры в реальном времени. Наиболее эффективной, система будет в том случае, когда системы обнаружения вторжения, межсетевые экраны, системы сетевой защиты и системы безопасности приложений будут работать вместе и совместными действиями будут уменьшать риск возникновения, проведения и реализации угроз. Такие решение осуществляет следующие функции:

- Получает информацию от одного или нескольких источников;
- Обрабатывает сообщения, основываясь на их характеристиках;
- Обрабатывает сообщения, основываясь на правилах их корреляции;
- Сохраняет сообщения в реляционной базе данных.

1.5 Преимущества SIEM системы

Оценить преимущества SIEM-решения поможет анализ по основным характеристикам.

Источники и обработка событий

Чем больше источников событий поддерживает система, тем практична защита. Но важно, чтобы SIEM-система обеспечивала индивидуальный подход к нормализации каждого события из различных источников.

Работу с программой облегчает разделение событий по опредеденным категориям. Синтаксический анализ информационных потоков (парсинг) подобных решений выполняется благодаря обозначения наиболее критичных полей. Обновляются парсеры, чаще всего, паралельно с внедрением дополнений или изменений системы.

Автоопределение, а также периодическое обновление источников эксперты относят к преимуществам. Однако общего мнения по вопросу обновления SIEM-решения не существует. Недостаток автообновления анализаторов вендоры иногда объясняют защитой от изменений логики анализа и предлагают проводить изменения SIEM под контролем собственных специалистов. Такого рода подход повышает стоимость владения системой.

Результат: лучше всего выбирать решение, которое собирает данные с максимальным количеством разных систем, которые эксплатируется в компании. Многоуровневая платформа обработки инцидентов ускорит работу с источниками и легко адаптируется к программному обеспечению. Небольшие требования к аппаратно-программным средствам при этом будут дополнительным преимуществом..

Сбор инцидентов

Практичная SIEM – это система включающяя функции нормализации, объединения и фильтрации инцидентов. Преимуществом будет обработка и хранение сырых событий. Скорость процессов при этом на общую картину не влияет. Маскирование сведений, мониторинг сетевого трафика – функции дополнительные, но не бесполезные.

Проверить корректность работы нормализации, фильтрации и агрегации возможно на уровне тестирования SIEM в «боевом» режиме. Поэтому компании больше привлекают производители, которые предоставляют бесплатный тест-драйв полнофункциональной версии продукта.

Корреляция

Оптимальное SIEM-решение сопоставляет события в режиме реального времени, умеет проводить поведенческий анализ и сравнение исторических данных.

Гибкие настройки системы корреляции, обогащение инцидентов в коннекторе или в консоли управления, дополнительная функция в виде ручной проверки, возможность одновременной работы со всеми механизмами – отличительные особенности удачной SIEM.

Визуализация

Отчетность SIEM-систем чаще всего формируется в виде графиков, гистограмм и таблиц. Большинство отчетов экспортируются в файлы пяти форматов: MS Excel, RTF, PDF, CSV, HTML.

Комфортную работу ИБ-сотруднику может обеспечит русифицированный интерфейс. Это не обязательный критерий выбора, но при других равных условиях – выгодно отличие.

Общие настройки и встроенный функционал

Комфорт работы с SIEM зависит прежде всего от наличия встроенных условий корреляции событий, графических панелей и шаблонов отчетов. Чем больше внутренних корреляционных ресурсов, тем будет меньше квалифицированной, то есть – платной помощи от сторонних специалистов потребуется при обслуживании платформы.

Удобство применения

Основным аспектом удобства работы с SIEM системой – право централизованно настраивать компоненты системы из единой консоли, а также автоматически обновлять предустановленные политики и шаблоны отчетности. Все это делает труд специалиста очень легким.

Также одним из плюсов в пользу решения – оперативность и качество технической поддержки.

1.6 Оптимизация потока событий

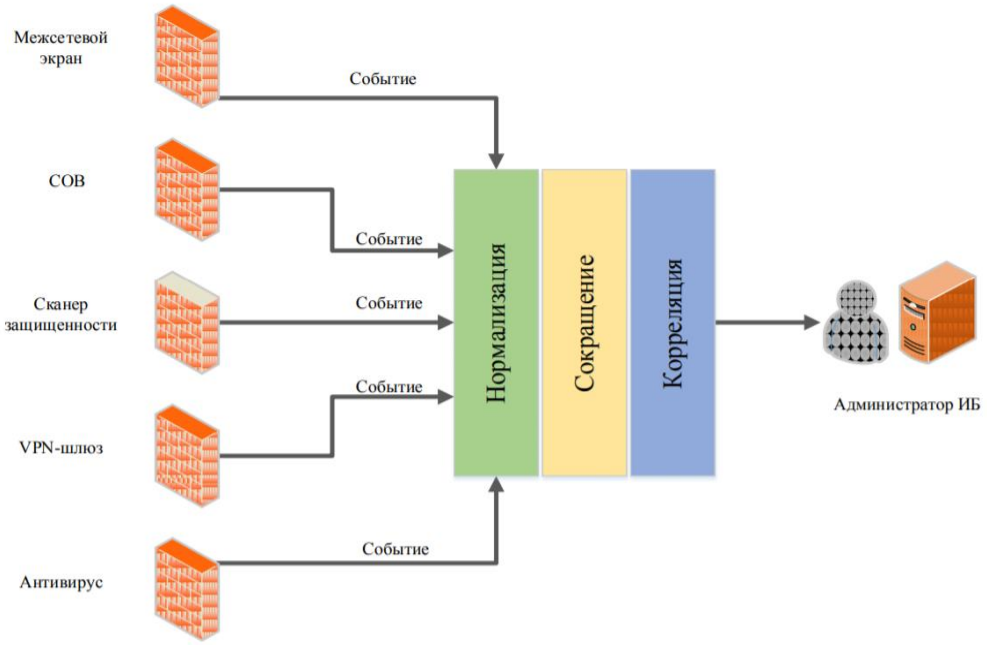


Рисунок 1.7 - Оптимизация потока событий

На рисунке 1.7 изображена корпоративная сеть обработки событий информационной безопасности и её взаимная работы вместе с различными механизмами. Все механизмы защиты (источники событий), отправляют свои данные в систему корреляции, которая сопоставляет данные то есть события друг с другом и дает администратору безопасности результаты в виде отчета .

Благодаря тому, что технология только начала развиваться, на данный момент не существует четкой теории данных систем, однако уже выработаны типовые методы корреляции, которые можно применять.

Относительно данной работе можно сделать вывод, что корреляция – это процесс сравнения, интерпретации, комбинации и равнения данных от различных компонентов защиты (агентов) производимый для поиска попыток нападения на них, либо удаленного доступа.

Из за того что это одна из новых стезей в области информационной безопасности, законченного набора методов ещё не существует. На данное время корреляция существует двух видов:

– Микрокорреляция. Относятся технологии корреляции событий, которые сосредоточены на сравнении данных в одном потоке событий;

– Макрокорреляция. Состоят в сравнении данных внутри потока событий с данными, собранными из других источников.

Если микрокорреляцию можно назвать начальной точкой при развертывании механизмов корреляции событий, то макрокорреляция, делает

возможным объединить несколько потоков, что дает возможность повысить скорость и точность поиска атак. Существует такое мнение, что для успешного управления информационной безопасностью нужно использовать оба подхода.

Представим более подробно каждый из видов.

Микрокорреляция сравнивает информацию в пределах одного потока событий. К ней относятся:

- Корреляция полей – основной тип корреляции, сравнивающий определенные события с одиночными или разными полями в нормализованных данных;
- Автокорреляция – это автоматизацией корреляции полей. В этом методе все поля целостно и систематически друг с другом для отрицательной или/и положительной корреляции;
- Корреляция правил – тоже метод автоматизации, но требует задания правил для маркировки наборов событий, как скоррелированных случаев.

Корреляция событий базируется на предпосылке, что каждое событие происходящие в пределах данного временного отрезка, является причиной другого события. Если представить это в виде формулы, то мы получим:

Событие A ~ Событие B ~ => Событие C

Где A - это, например, сообщение от системы антивирусной защиты, B – последующие сообщение от системы обнаружения вторжений (A и B связанны между собой), а порожденное событие C – отправка уведомления администратору или ответственному за информационную безопасность. Таким образом, осуществляется связывание событий по определенным шаблонам и, следовательно, уменьшение их количества (рисунок 1.8, 1.9, 1.10) при повышении читабельности общего потока событий.

1.6.1 Уменьшение потока событий

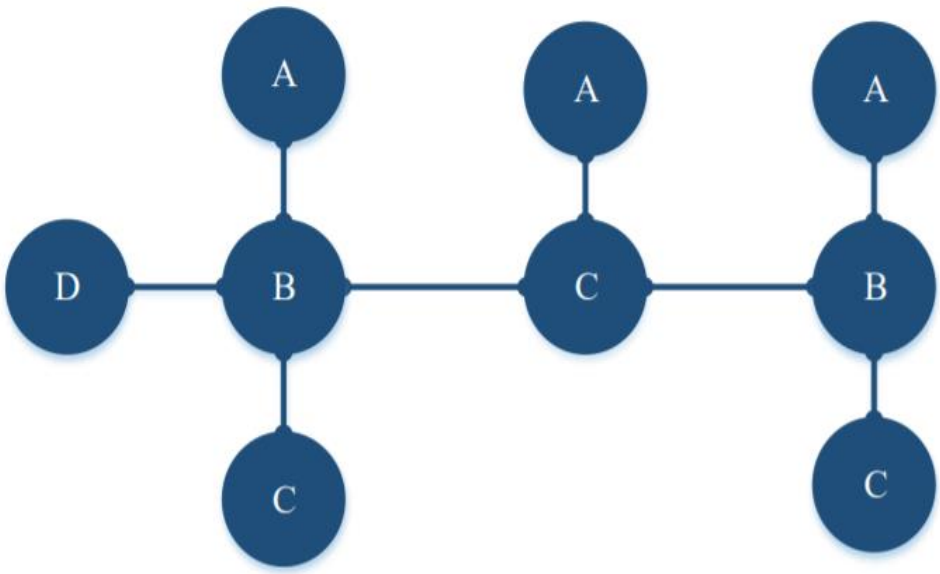


Рисунок 1.8 - Уменьшение потока событий

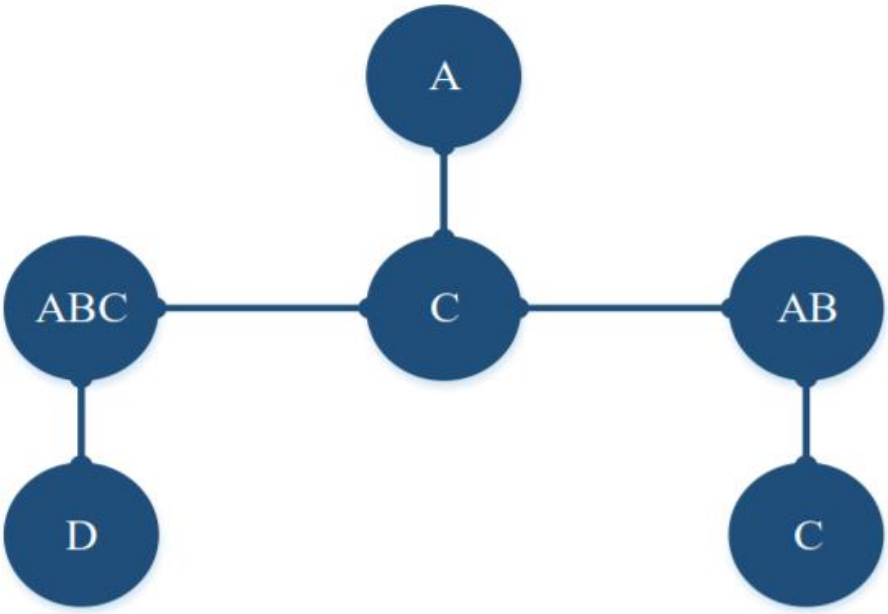


Рисунок 1.9 - Сокращение потока событий

Рисунок 1.10 - Фильтрация потока событий

На реальной практике теория отношений межсобытиями образуется в виде языков шаблонов. Эти языки, являются интерпретаторами записей, которые сотрудник информационной безопасности разрабатывает в интерфейсе системы корреляции событий. Каждая запись – это отдельная связь между событиями. Не редко человек не пишет эти отношения, а в графическом интерфейсе разрабатывает графики событий, потом объединяет их на экране – система же сама переводит эту картинку в свой внутренний скрипт. Если взять наш предыдущий пример, то запись правила будет выглядеть примерно так:

Попытка вторжения (IP-адрес источника) ~ Попытка доступа (доступ запрещен) => Эскалация проблемы (отправить сообщение на IP-адрес; заблокировать межсетевой экран)

Попытка вторжения, попытка доступа и эскалация проблемы - это внутренние описания событий на языке шаблонов. Эти события могут

содержать изменчивую информацию. Иногда правила описываются как выражения, которые выглядят как команды в языках программирования.Макрокорреляция (корреляция сплава данных) – сравнивает данные из различных наборов:

1) Корреляция профилей – определяет совокупность действий по тому или иному профилю;
2) Корреляция уязвимостей – по списку найденных уязвимостей определяет вероятность их реализации;
3) Корреляция маршрутов – изучение сетевых маршрутов атаки для выделения других допустимых вторжений;
4) Корреляция по методу Байеса – основана на статических и вероятностных методах оценки поведения пользователей или систем с применением только двух переменных;
5) Нейронная корреляция – метод похожий на предыдущий, но в отличие от него не имеет ограничений. Использует любое доступное количество переменных для анализа, анализирует их и пытается предсказать нападения. В основе данного метода лежит искусственный интеллект;
6) Временная корреляция – метод,который основывается на временных метках в системе, оценивает риск несанкционированного доступа на основе информации о том, в течение определенного времени и в какие именно временные отрезки пользователи обычно используют определенные сетевые ресурсы.

Выше мы просмотрели базовые корреляционные методы. Хотя перед тем как приступить к созданию системы, следует сделать ещё несколько шагов по определенной обработке данных, а именно:

1) Передача данных. Нужно получить начальные данные от единичных средств обеспечения информационной безопасности и переотправить их в базу данных системы корреляции. Консолидация данных – это процесс объединение регистрационных данных полученных от разных источников одну определенную базу, из которой и будет описано состояние сети. На данном уровне поддерживается защита и целостность начальных данных для корреляции – способом их верификации электронной подписью и шифрования;
2) Нормализация данных. Почти все приложения хранят записи о предупреждениях, ошибках и отказах собственных сервисах в регистрационных файлах. Например, межсетевые экраны и VPN-шлюзы(Virtual Private Network) могут следить все сомнительные соединения в момент входа в сеть и выхода. Коммутаторы и маршрутизаторы ведут журналы о состоянии сети в базах информации управления. Частенько системы скидывают важные оповещения (к примеру, SNMP-трапы) на центральную консоль управления. Из за этого данные, перемещаемые в консолидированную базу, приводятся к некому единому формату. При всем этом следует позаботиться о резервном сохранении "сырых" данных, на пример, на случай судебного разбирательства, потому что модификация

информация в виде доказательства служить уже не может. На данном уровне обеспечивается "сокращение" всех наборов данных при сохранении их целостности и полноты;

3) Сокращение данных. При реализации системы обнаружение вторжений, большие организации столкнуться с большим количеством данных, который может стать неподъемным для специалистов. Так, к примеру, огромный сервер, который работает постоянно, способен создавать до терабайта логов данных в час. В данной ситуации получение и организация поступающих данных оказывает огромную проблему, которая требует специальных исследовательских работ в сфере систем обнаружения вторжений. Из за того что все терабайты данных это и есть материал для предстоящей аналитической анализа, их позже на некоторое время необходимо сохранить. Сокращение пулла данных подразумевает использование самых различных методов и операций, нацеленных в итоге на ускорение работы программы корреляции. Уменьшение может быть проведено через сжатие данных, удаление, дублирующих комплектов, фильтрацию некой не представляющей огромной важности информации, комбинирование схожих событий воедино и так далее События, которые поступают от разнообразных источников, исследуется на предмет удвоении информации и другие данные удаляются. Далее по особым правилам обрабатываются регистрационные, информационные и аварийные сообщения. Создатель системы на данном уровне решает, что необходимо оставить и что убрать. Следовательно, для каждой компании, скорее всего, создать собственные очень необычное правила обработки событий – к примеру, фильтрирование событий ведется согласно тем уровням риска (и в том порядке), которые приняты в компании. Какое количество исходящих, "сырых" событий нужно сохранить и на какой количество времени, зависит от принятой политики защиты. Что и как сохранять для предстоящей обработки – это и есть одна из главный проблем, который стоит перед организациями, которые решают задачу действенного управления событиями. Данный окончательный шаг несмотря на прочего лучше использовать с опаской, чтобы не удалить важную доказательную информацию.

Как только данные будут собраны в единой точке, нормализованы и сокращены, системы управления информационной безопасностью могут запустить процесс корреляции.

1.6.2 Построение цепочки прохождения событий.

Корреляция очень даже полезна при определений нарушений режима безопасности, так как эти инциденты представляют собой цепочку событий, происходящих в определенно разных "сенсорных" точках сети. Данный процесс объясняется связями "многие к одному" (то есть почти все события от огромного числа сенсоров говорят об одном нападении). В сравнении с сетевым управлением, в котором, обычно, используются отношения

исключения событий (нужные – ненужные) либо взаимосвязи "один к одному", управление защитой информации гораздо сложнее. Проникновение обычно оставляет следы в разных точках сети и в различной временной очередности. Находя эти все следы, специалисты, занимающиеся информационной безопасностью, сумеют найти и с высочайшей степенью надежности предотвратить нападение.

Потому, следуя человеческой логике, необходимо также поступить и в разработке SEM-системы. После того как все данные будут собраны и подвергнуты анализу в целой базе данных(БД), нужно определить, как и в какой очередности данные события появляются, чтобы из их соединении разработать одиночное событие вторжения. Некоторые исследовательские компании используют термин "цепочка прохождения событий". Как только такая цепочка будет выстроена, ИБ специалист будет в состоянии перейти к определению самих событий и выкраиванию из них шаблонов

1.6.3 Обнаружение шаблонов в событиях

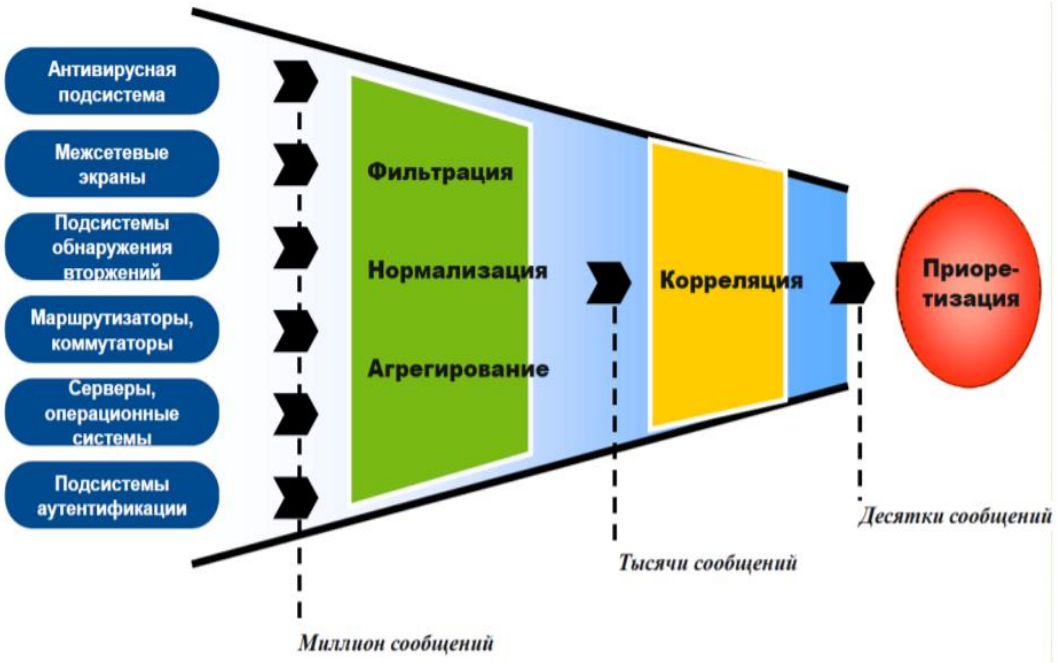


Рисунок 1.11 - Обнаружение шаблонов в событиях.

Шаблон – это некий набор взаимоотношений и правил включающий в себя свободные переменные. Например, шаблон «состояние сервера» включает в себя переменные: «Число запущенных действий», «свободная память», «численность процессов-зомби» и пр. Можно привести бесконечное количество примеров шаблонов: от низкоуровневых (отбор сетевых пакетов, которые несут в себе UDP пакеты) до высокоуровневых (помесячная характеристика трат обладателя банковского счета в точкой определенной категории риска).

Нужно подметить, что даже после мощного сокращения избыточных данных, задача поиска и корреляции, нужных образцов остается скучной и монотонной работой. Вручную синхронизировать события от всех рабочих станций и серверов, считать и интерпретировать файлы регистрации это неподъемный труд.

Существуют две похожие техники определения шаблонов из исходных данных: обнаружение аномалий и обнаружение злоупотреблений(рисунок 1.11). Суть первой состоит в том, что систему обучают на нормальных данных, в этот момент вторая техника тренируется на заранее помеченных плохих и хороших данных. Обе эти технологии появились от нового течения «data mining» - исследования данных для получения новых знаний.

Все эти техники позволяют департаментам ИБ создать базовый шаблон типичного поведения пользователя и естественно создать шаблоны для оповещения при изменении деятельности. К примеру, в некоторых ИС часто практикуют ограничение времени работы пользователей с информационными ресурсами по времени, либо дням недели – это правило создается легко и так же легко обнаруживается отклонение от него. Но проблема состоит в том, что люди слишком частенько отклоняются от правил.

Поэтому большинство существующих SIEM систем используют упрощенный набор правил для выделения шаблонов. Для корреляции в таких ситуациях часто выделяют следующие информационные поля и их соединения:

Местоположение сообщившего устройства;

1) Тип сообщившего устройства;
2) Разновидность события;
3) Источник сетевого соединения;
4) Адрес сетевого соединения;
5) Временные пороги.

1.6.4 Механизм принятия решений

Следующим уровнем в создании SIEM системы является создание механизма принятия решений. На этом этапе администратор ИБ уже имеет представление, как выглядит схема прохождения атаки, каких видов и в какое время появляются события, он имеет шаблоны различных ситуаций. Теперь, исходя из накопленной информацию, нужно внедрить в систему шаблоны привил принятия решений. К примеру: если вы получили несколько сообщений типа «доступ к внутренним адресам» от маршрутизатора, выходящего во внешний контур, а позже появилось сообщение типа «запрещенный порт» от МЭ, то нужно ожидать сообщение «атака, типа сканирование портов» от СОВ

На этом этапе разрабатывается решение, которое связывает набор замеченных действий с определенным инцидентом, а так же присваивает ему

классификацию, относительно методов нападения Проблемами при допущении ошибок на данном этапе могут быть:

- Падение производительности системы;
- Риск обхода условий мониторинга;
- Упущения в описании возможных ситуаций;
- Стадия реакции на вторжение;
- Уменьшить количество тревог.

1) Падение производительности системы

Первой опасностью, возникающей при ненадлежащем подходе к реализации механизма принятия решений, является снижение производительности. Включение любого правила может вызвать спад быстродействия системы. Не будем забывать, что в системах, построенных на сигнатурном подходе, каждый входящий элемент сравнивается с шаблонами, поэтому нужно ответственно подходить к процессу создания базы шаблонов. При увеличении входящих данных 30 или количества правил, скорость работы программы находится под угрозой;

2) Риск обхода условий мониторинга.

Вторая немаловажная проблема в корреляции событий: Компьютеры пока не могут оценивать вероятность схожести тех или иных событий с их сохраненными шаблонами. Так как правила требуют точного соответствия существует высокая вероятность того, что при желании злоумышленник может с легкостью от них уклониться. В пример можно привести правило:

IF (7 событий)
FROM (с 5 разных IP)
TO (к IP адресам важных серверов компании)
IN TIME (в течение 7 минут)
WHEN (IDS выдала ALERT и МЭ выдал DROP)
+THEN ACTION (послать уведомление администратору и заблокировать межсетевой экран)

Если атака будет осуществлена таким образом, но длительность её составит не 5 минут, а 7, то нападение пройдет незамеченным. Чтобы учесть эти особенности, нудно предусмотреть большой временной отрезок наблюдения за событиями. Это приведет к росту потребляемых ресурсов, ведь каждое событие требует процесса, либо куска программного кода для обслуживания. Чем больше временные рамки, тем больше процессов будет находиться в памяти. А это приведет к упадку производительности;

3) Упущения в описании возможных ситуаций

Понятное дело, что служба безопасности должна описать столько правил, сколько необходимо, но количество событий в сети огромное, а количество атак постоянно растет. Чтобы снизать вероятность таких ошибок нужно использовать как микро, так и макро корреляцию. Совместное использование этих технологий поможет быстрее обнаружить сбойные участки цепей прохождения событий, некорректные правила и шаблоны. Оптимальным вариантом является соединение событий из разных

источников, например: оценка работы кадра в сети проводится с учетом информации поступившей от система контроля и управления доступом (СКУД), то есть с учетом того, проходил ли он через КПП. Такие схемы гораздо более стойкие к ошибкам, чем те, которые сопоставляют меньшее количество событий от похожих источников, например: МЭ и IDS;

4) Стадия реакции на вторжение

Управление системой защиты осуществляется людьми, а, следовательно, подвержено ошибкам. Автоматизируя процессы накопления исходной информации, сокращение избыточности в ней, аналитику и корреляцию, компания хочет, чтобы была автоматизированная стадия реакции. Самой простой реакцией является: автоматизированное создание тревожных уведомлений. То есть таких, которые говорят, что было обнаружено какое-то вторжение или что-то не хорошее. Поэтому правила обработки уведомлений должны быть настолько продуманными, чтобы;

5) Уменьшить количество тревог

Сокращение число ложных и ложноположительных сообщений Необходимо определить определенный количество времени на обучение, причем не только сотрудников, но и самой системы. Так как у всех реляционных и статистических систем есть базовые пороги количества обрабатываемых чисел, связей и пр. не дойдя до которых система не сможет давать адекватных результатов, а количество ошибок будет очень большим. Например, национальная компьютерная ассоциация ЗИ советует не включать системы оповещения в течение 30 дней. За это время накопится начальный порог исходной аудиторской информации, а так же служба безопасности будет лучше понимать алгоритм работы;

Автоматический запуск программ, которые должны ответить на обнаруженное нападение (например, заблокировать доступ к информационному ресурсу или отправить уведомление об обнаружении самому нарушителю и т.п.) – наиболее активная реакция на обнаруженные атаки. Некоторые системы могут содействовать с мобильными телефонами и другими средствами связи, умеют подавать световой и звуковой сигнал. Современные SIEM системы обладают этими возможностями, но экспериментировать нужно очень осторожно, только убедившись, что действия систем под контролем. Далее рассмотрим некоторые SIEM системы, в качестве примера я решил взять несколько SIEM систем и сравнить их: HP ArcSight, MaxPatrol SIEM, Security Capsule, IBM QRadar,AlienVault.

1.7 Обзор и сравнение SIEM решений

Системы SIEM существуют в течение 10 лет, но их активное продвижение началось только в последние годы. Его причин много: от роста текущих рисков до намерения быть в тренде. Однако, можно с уверенностью сказать, что идея SIEM была очень популярной. Ведь стартовая конкурентная борьба многих независимых игроков со временем и после ряда закупок

перешла на новый уровень знаний и бюджетов не только сложно, но и на новый уровень.

Компания Gartner объявляет Magic Quadrant for Security Information and Event Management (SIEM), в рамках которого 4 производственных решения защиты от компании Softprom by ERC признаны выданными. Решения McAfee, подтвердив лидерство в этом году, имели место на квадрате Leader.Gartner rapid7 InsightIDR включает оценку комплексного решения для выявления и исследования, который объединяет анализ поведения пользователя, выявление конечных точек и визуальный поиск журналов и дает решение наивысшую позицию в квадрате визионеров. Яркими рынками IBM и Splunk прошлых лет остаются.

Казахстанский рынок как правило отличается от мирового(рисунок 1.12). В первую очередь резким доминированием HP ArcSight и относительно невысокой долей остальных лидеров из квадранта Gartner. Следующем перечислении мы рассмотрим некоторые системы в качестве примера и сравним их:

- HP ArcSight;
- Max Patrol;
- Security Capsule;
- IBM QRadar SIEM;
- OSSIM.

Рисунок 1.12 – Рынок SIEM систем

1.7.1 HP ArcSight

Данный продукт обеспечивает сбор, хранение и обработку событий информационной безопасности, которые могу поступать с различных средств защиты.

Главным в продуктовой линейки ArcSight является комплекс HP ArcSight Security Intellegence, ядром в котором служит HP ArcSight Enterprise Security Manager, который может соединяться с огромным количеством прикладных систем и девайсов. Как правило поставляется с несколькими сотнями, заранее внедренными шаблонами корреляции. Так же в состав может входить свой агент: FlexConnector, который совместим с любым типом приложений(рисунок 1.13).

HP ArcSight ESM является одним из лидеров на рынке по возможностям техническим и возможностям объеденения с бизнес-приложениями. Структура HP ArcSight ESM дает взможность развернуть решение даже в территориально-распределенной информационной системе с

низкими каналами связи. HP ArcSight ESM поставляется как в аппаратном, так и программно-аппаратном виде, что как раз таки отличает его от оставльных систем корреляции.

Для упрощения задачи по сбору, хранению и анализу журналов аудита может использоваться продукт HP ArcSight Logger – готовый программный или программно-аппаратный комплекс, которой может собирать и анализировать все данные журналов аудита организации, предоставляя сжатый и экономичный репозиторий для хранения логов. Для более простого и эффективного сбора информации о событиях безопасности в составе HP ArcSight ESM и HP ArcSight Logger могут использоваться программные комплексы HP ArcSight Connectors. Необходимо отметить, что HP ArcSight Connectors также могут поставляться в виде программно-аппаратных комплексов (HP ArcSight Connector Appliance).

Решения HP ArcSight Security Intelligence включают в себя следующие продукты:

- HP ArcSight Logger - обеспечивает сбор и фильтрацию событий;
- HP ArcSight Threat Response – обеспечивает сиюминутную реакцию на инциденты посредством анализа информации от HP ArcSight ESM, вычисление географии проблемы и принятие ответных действий;
- HP ArcSight Configuration Management - позволяет сконфигурировать сетевое оборудование и настройки безопасности;
- HP ArcSight Fraud Detection - уникальное решение для выявления и предотвращения мошенничества в области интернет-банкинга и банковских (пластиковых) карт.

Использование системы мониторинга на основе HP ArcSight помогает автоматизировать процесс реакции на события, связанные с нарушением политик безопасности. Так же применение систем мониторинга повышает эффективность уже установленных средств защиты информации.[6]

На сегодняшний день решения от HP популярны во всем мире среди финансовых организаций, государственных структур и операторов связи.

Архитектура HP Arcsight

HP Arcsight поставляется со следующими компонентами:

1) ArcSight Manager – основной серверный компонент, «ядро» системы, обеспечивающее корреляцию событий и их обработку;
2) ArcSight DB – база данных (на основе СУБД Oracle 11g), предназначенная для хранения информации;
3) ArcSight Console – консоль для управления и работой с системой, представляющая собой приложение, устанавливаемое на клиентское рабочее место администратора или пользователя системы;
4) ArcSight Web – серверный компонент web-консоли для мониторинга и получения отчетности. Для доступа к информации используется любой современный web-браузер;

5) ArcSight SmartConnectors – компоненты системы, обеспечивающие

сбор событий с источников, их предварительную фильтрацию и агрегацию, а также передачу событий в ArcSight Manager[7].

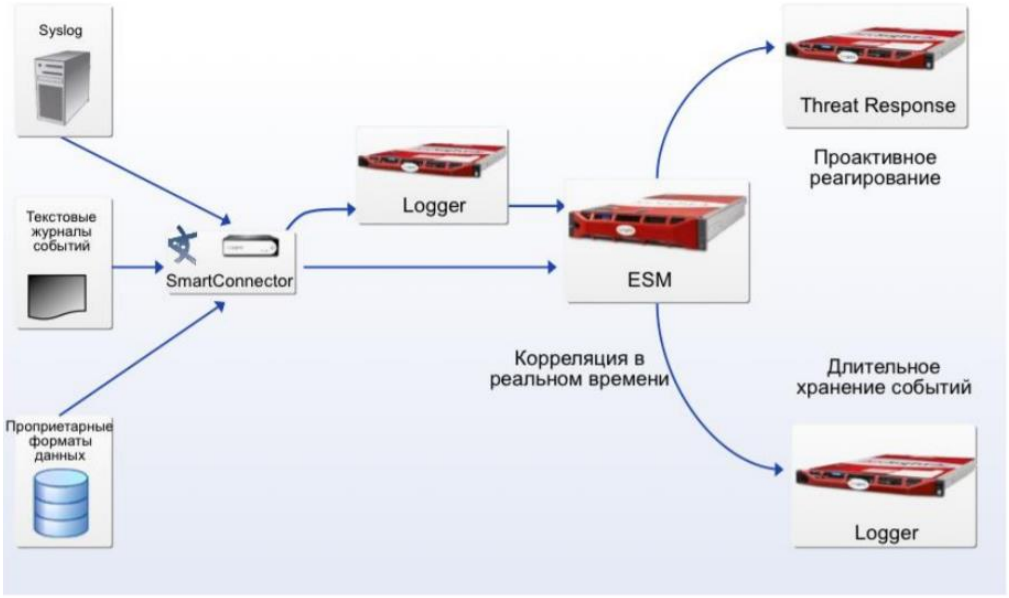


Рисунок 1.13 – Архитектура системы ArcSight

1.7.2 Max Patrol

MaxPatrol дает возможность оценить состояния защищенности всей системы, а так же определенных подразделений, приложений и узлов. Механизмы проверок системы, контроля соотношение стандартам и тестирования на проникновения, паралельно с возможностью анализа различных операционных систем, СУБД и веб-приложений, позволяют обеспечивать стабильный аудит безопасности на каждом уровне информационной системы.

Рисунок 1.14 - Ключевые возможности

Основой SIEM системы MaxPatrol 8 является сканер уязвимостей XSpider. Механизмы контроля которые находятся в нем были дополнены компонентами системных проверок и анализа безопасности без данных. Комбинация в одном комплексе возможности системных и сетевых сканеров, а так же инструментов оценки состояния защищенности систем управления баз данных и веб-приложений, дают возможность получать реальный образ защищенности системы.

Ядром Max Patrol 8 является сетевой сканер с высокой производительностью, который позволяет с высокой скорость обнаруживать открытые порты, сетевые узлы и идентифицировать серверные приложения и операционные системы. Распределенная архитектура дает возможность размещать сканер в непосредственной близости от объекта, что дает возможность снижать нагрузку на каналы связи

Эвристические механизмы анализа помогают выявить уязвимости в приложениях и сетевых службах, с низким уровнем привилегий, что позволяет получить оценку защиты сети со стороны злоумышленников. Созданные специалистами интеллектуальные виды и механизмы обнаружения уязвимостей, эффективность которых доказана специалистами в области защиты информации, предельно близки к тем, которые действительно используются хакерами, что дает возможность не только выявить ошибки, но и обнаруживать новейшие, ещё и уязвимости нулевого дня.

При наличии доступа к механизмам удаленного управления узлом модуль сканирования может использовать их для обширной проверки безопасности операционной системы и приложений. Этот метод дает возможность с меньшими ресурсами получить комплексную оценку защищенности, а также провести анализ параметров, недоступных в режиме теста на проникновение.

База знаний включает в себя системные проверки для многих популярных операционных систем таких как, Windows, Linux и 38 Unix, а также специализированного оборудования, такого как маршрутизаторы и коммутаторы Cisco IOS, межсетевые экраны Cisco PIX и Cisco ASA.

В отличие от стандартных системных сканеров, MaxPatrol 8 не требует развертывания программных модулей на устройствах, что облегчает использование и уменьшает совокупную стоимость владения. Все проверки делаются удаленно с использованием встроенных механизмов удаленного администрирования. При поддержке узлом несколько протоколов (например, Telnet и SSH) MaxPatrol 8 подбирает более безопасный из них, что дает защиту уязвимых данных при отправке по сети.

Архитектура MaxPatrol

Основными архитектурными особенностями MaxPatrol являются:

- Безопасность;
- Защита данных.

При передаче и хранении частенько используются криптографические методы защиты, обеспечивающие конфиденциальность и целостность информации, такой как пароли сотрудников, привилегии на доступ и т. д. Также предусмотрена возможность использования сертифицированных реализаций отечественных криптографических алгоритмов. Защита трафика обеспечивается благодаря цифровым сертификатам и протоколам SSL/TLS, являющегося индустриальным стандартом, что обеспечивает высокую совместимость и защиту данных. Поддерживается интеграция с существующей инфраструктурой открытых ключей (PKI). Гибкая система разграничения прав доступа дает возможность производить мониторинг информационной безопасности на различных 39 уровнях иерархии (например, на уровне администраторов, менеджеров по ИТ и ИБ подразделения, директора по ИБ Компании). Для любых пользователей системы можно предоставить список задач, с которыми он будет использовать в системе, а также разрешения на операции над конкретными объектами системы. Так, например администратору веб-серверов могут быть делегированы права на модификацию профиля сканирования, запуск и просмотр результатов задачи по оценке защищенности управляемых им серверов, но запрещено изменять список сканируемых узлов. Также разработчик веб-приложений будет иметь возможность только просматривать отчеты по результатам сканирования.

Разрешения могут устанавливаться на уровне MaxPatrol 8 Server или MaxPatrol 8 Consolidator. Такой подход позволяет адаптировать систему разграничения доступа практически под любую иерархию управления системой ИБ.[8]

1.7.3 Security Capsule

Назначение

ПАКАБ SIEM «Security Capsule» предназначен для регистрации событий информационной безопасности и выполняет следующие функции: регистрация и учет событий информационной безопасности (ИБ) в информационно-вычислительных системах и сетях, разграничение доступа пользователей к информационным ресурсам SIEM, контроль доступа SIEM, контроль целостности файлов SIEM, корреляцию событий ИБ, реакцию на события ИБ.

На базе анализа информации, собранной с помощью SIEM «Security Capsule», администратор безопасности принимает меры по обеспечению безопасности объектов информационно-вычислительных систем и сетей.

Регистрация событий информационной безопасности реализуется путем ведения журналов регистрации событий информационной безопасности:

1) доступ пользователя к приложению и завершение работы;

2) разрешенные/неразрешенные действия пользователей по доступу к информационным ресурсам;

3) сообщения, получаемые от сетевых устройств.

Структура модулей программы, наподобие разработанных коннекторов может быть внедряться и предоставляться опционально.

По договорянности с заказчиком список коннекторов может быть расширен под нужные потребности Заказчика.

Перечень разработанных коннекторов, позволяющих накапливать следующие данные о событиях информационной безопасности:

- данные от сетевых устройств, использующих протокол syslog - данные в журналах СУБД(Система Управления Базами Данных);
- данные в системном журнале ОС семейств Windows, Linux;
- данные при применении съемных носителей информации типа eToken, USB, LPT, COM. IEEE 1394, ZlocK, Device Lock;
- данные, полученные от СЗИ от НСД, например – данные, полученные от антивирусных средств;
- данные, полученные из Active Direcory; – данные реестра ОС Windows;
- данные, полученные от IDM (Identity Management) систем;
- данные, полученные от DLP (Data Leak Prevention) систем.

Архитектура

«Security Capsule» базируется на клиент-серверной технологии для распределенных неоднородных ИС, СПД, ЛВС и системы защиты конфиденциальной информации. ПАКАБ «Security Capsule» имеет модульную архитектуру, включающую в себя(рисунок 1.15):

- модуль серверной части;
- модуль мониторинга и администрирования;
- центральный модуль;
- клиентские модули;
- коннекторы;
- модуль формирования отчетов[9].

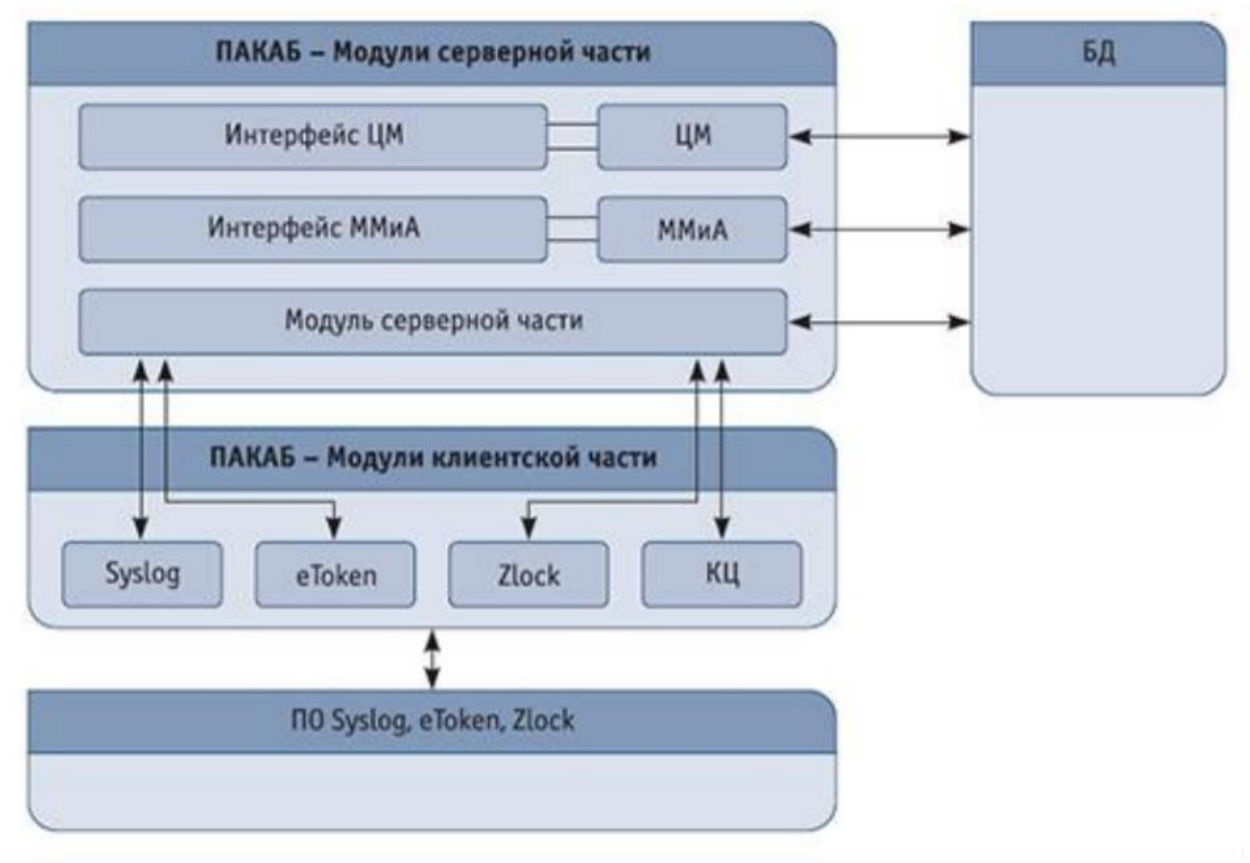


Рисунок 1.15 – Архитектура SIEM

1.7.4 IBM QRadar

Возможности и особенности QRadar SIEM

QRadar SIEM создает полную видимость внутри сети, выполняя сбор и обработку данных, которые дают возможность оперативно получать всю нужную информацию о событиях безопасности и работе сетевых девайсов, несмотря на сложности сетевой конфигурации. Тотальная прозрачность сети позволяет с огромной практичностью управлять ее безопасностью и обнаруживать все находящиеся в сети и потенциальные угрозы задолго до их реализации. QRadar SIEM - это соединенное средство, которое прекрасно справляется с задачами управления политиками по соответствию требованиям и стандартам, сбора и анализа логов и предоставляющее самый современный инструментарий для выявления угроз. Это решение базируется на упругой платформе QRadar Security Intelligence Platform, которая может развиваться одновременно с предприятием и приспосабливается под его расширяющуюся инфраструктуру, гибко и оперативно обеспечивая мониторинг корпоративной безопасности.

Сбор и анализ данных из нескольких источников

QRadar SIEM собирает информацию из следующих источников:

1) события системы безопасности - события от брандмауэров, VPNs, IDS/IPS, и т.д.;

2) сетевые события - события от свитчей, роутеров, серверов, хостов;
3) монитор активности сети - контекстные идентификаторы протоколов

7-го уровня от сетевого трафика и приложений;

4) монитор активности пользователей - данные продуктов типа IAM и сканеров уязвимостей;
5) журналы событий приложений – ERP (Enterprise Resource Planning), документооборот, базы данных приложений, административные платформы;
6) контроль угроз, логов и соответствия политикам в режиме реального времени.

Связывая разрозненную информацию, QRadar SIEM делает более эффективным обнаружение всех современных угроз. Данные нормируются и коррелируются для своевременного выявления, уведомления и реагирования на угрозы, которые не в состоянии определить другие средства защиты с ограниченной видимостью. Мониторинг, проводимый QRadar SIEM, позволит предприятиям обнаружить сложные угрозы, среди которых внутренние мошенничество, нецелевое использование приложений и многие другие.

Эффективное управление данными

Особенно практично применение QRadar SIEM для организации с крупномасштабными сетями, в которых регистрируются сотни и более событий в день. QRadar SIEM проводит сбор, анализ и хранение данных и дает возможность коррелировать события в режиме реального времени. Это позволяет между огромным количеством данных распознать те, которые влечет за собой к инцидентам безопасности. Миллиарды сетевых событий и потоков могут быть снижены, что, соответственно, облегчит процессы выявления угроз, аудита и разработку отчетности, соответствующей требованиям и стандартам.

Управление угрозами

QRadar SIEM наблюдает все серьезные инциденты и угрозы, предоставляя хронологию обслуживания и всю нужную сопутствующую информацию. Благодаря этому решению у службы безопасности появиться возможность всегда узнать ответы на вопросы такие как: кто нарушает безопасность, какой объект подвергается нападению, в каком месте лучше проводить расследование, каковы последствия этого для бизнеса? QRadar SIEM позволяет показать полную информацию о факторах, нарушающих нормальный режим работы, пользователях, моделях нарушителей, важности ресурсов, характеристиках уязвимостей, уровне активности угроз и отчетах о предыдущих нарушениях и т.д. Благодаря этому, служба безопасности сможет получить все нужные сведения для своевременного реагирования на любые инциденты безопасности.

Видимость приложений и обнаружение сетевых аномалий

Благодаря QRadar SIEM можно узнать любые аномалий и изменения в работе приложений, серверов, устройств и сегментов сети. Возможность

определения трафика на прикладном уровне позволяет QRadar SIEM достаточно точно мониторить и понимать политики и угрозы корпоративной сети организации, а также выполнять общий мониторинг сетевой активности. Функция контроля работы с таким приложением, как Skype, и социальными сетями (включая Twitter, Facebook и т.д.), также дают возможность увеличить видимости сети. Сохраняя обнаружение большого количества отступлении и поведенческих правил, QRadar SIEM имеет возможность детально ответить на вопрос о том, какой пользователь и что применяет. Контентный мониторинг и оповещение при передаче контента, корреляция с остальной сетевой активностью и логами событий позволяют определить нецелевую передачу данных. Возможности фильтрации и выбор любого временного промежутка для анализа позволяют пользователю настроить вариант вывода результатов по собственному усмотрению.

Полная видимость виртуальной среды

Специалистам ИБ доступна усиленная видимость активности широкого спектра бизнес-приложений в виртуальных сетях. Виртуальные сервера, как и физические, имеют уязвимости в системе безопасности, поэтому прозрачность виртуальной среды обработки данных требуется для точного определения необходимых мероприятий по защите приложений и данных.

Единая интуитивно понятная консоль управления

Сосредаточенная интуитивно понятная консоль управления дает ролевой доступ, дает глобальный обзор управления инцидентами и отчетности. Панели управления QRadar SIEM предлагаются как функционал, и пользователи могут сами создать и настроить свое рабочее пространство в соответствии с решаемыми задачами. Такая детализация предоставит возможность гораздо проще выявлять и выбирать всплески событий и сетевые потоки, связанные с нарушениями. QRadar SIEM показывает около 3 500 шаблонов отчетов, связанных с конкретными устройствами, ролями и требованиями регуляторов.

Масштабируемость и отказоустойчивость

Решение QRadar SIEM в первую очередь предназначено для малого и среднего бизнеса, но может быть с успехом развернуто в компании любого масштаба за счет своей не сложной адаптивностью. QRadar SIEM делает потенциальны быстрый переход с другого решения и полную синхронизацию между системами. Вводить дополнительные решения сторонних производителей нет нужды, так как QRadar SIEM предоставляет высокий уровень анализа и хранения данных благодаря «plug and play» устройствам, которые входят в семейство продуктов QRadar.

1.7.5 AlienVault

OSSIM (Open Source Security Information Management) — система управления, контроля и обеспечения информационной безопасности.

OSSIM продукт от компании AlienVault, предлагает решение с разными инструментами «Open Source», SIEM систему со сбором, нормализацией и

корреляцией событий. Запущенный профессионалами проект, из-за нехватки доступных Open Source решений OSSIM был разработан исключительно для того, чтобы продемонстрировать действительную ситуацию в сфере безопасности.

Система OSSIM (рисунок 1.17) является комплексным решением по управлению безопасностью, позволяющим обнаруживать и классифицировать компьютерные атаки на основе анализа, оценки рисков и корреляции событий в реальном времени.

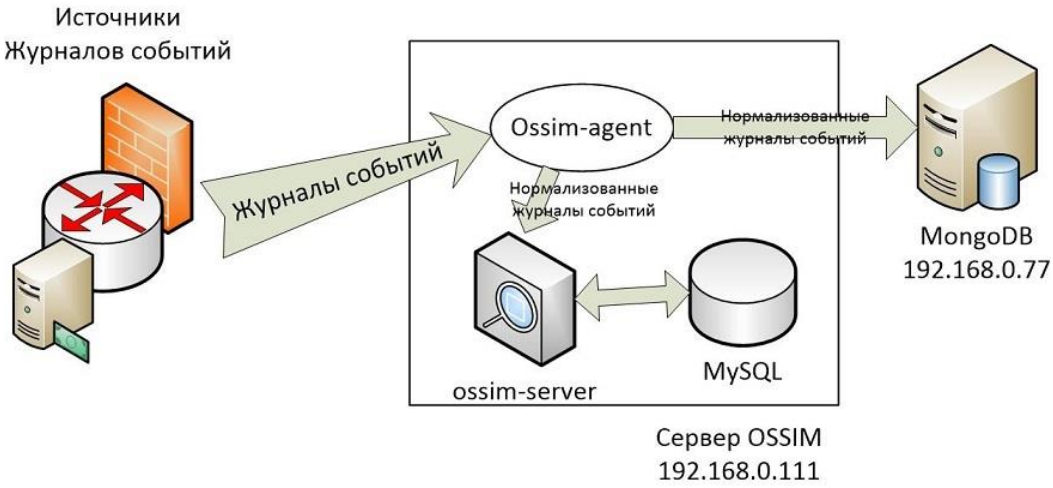


Рисунок 1.16 – Взаимодействие компонентов OSSIM

Компоненты:

- Сбор, анализ и корреляция событий — SIEM;
- Хостовая система обнаружения вторжений (HIDS) — OSSEC;
- Сетевая система обнаружения вторжений (NIDS) — Suricata;
- Беспроводная система обнаружения вторжений (WIDS) — Kismet;
- Мониторинг узлов сети — Nagios;
- Анализ сетевых аномалий – P0f, PADS, FProbe, Arpwatch и др;
- Сканер уязвимостей – OpenVAS;
- Мощнейшая система обмена информацией об угрозах между пользователями OSSIM — OTX.

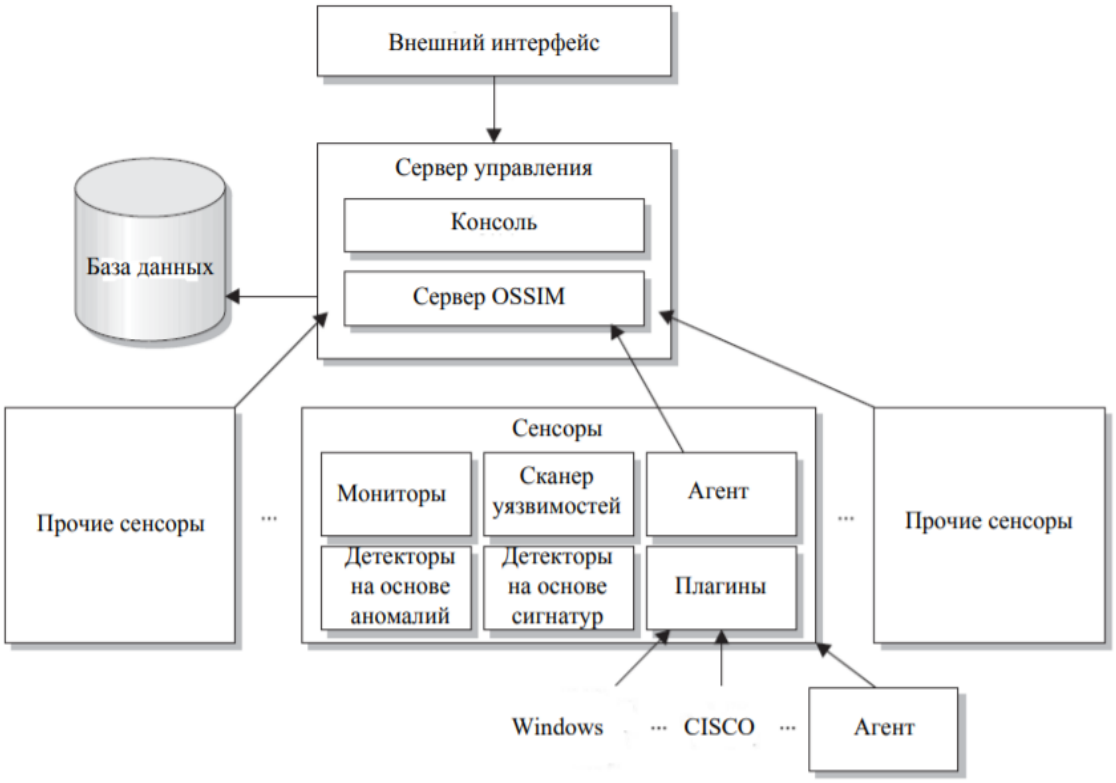


Рисунок 1.17 – Архитектура системы OSSIM

Сенсоры представляют собой низкоуровневые компоненты, которые создают интерфейс между отдельными хостами безопасности и сервером управления. Они включают множество агентов сбора данных, а также набор мониторов и детекторов. База данных является SQL-ориентированной. В ней хранится вся информация, требуемая для функционирования OSSIM. Сервер управления включает консоль, которая используется для контроля над остальными компонентами, и сервер OSSIM, который обрабатывает данные, поступающие от сенсоров(рисунок 1.16).

Выводы по главе

Таким образом, изучив принцип работы и структуру SIEM систем, можно сделать вывод, что это крайне актуальная и удобная система мониторинга.

SIEM – это сложная комплексная система, которая дает возможность получать своевременную и всеобъемлющую информацию о состоянии инфраструктуры организации. SIEM-системы являются весьма непростыми и дорогостоящими инструментами управления электронными журналами. Тяжелый процесс развертывания и требования к непрерывному обеспечению сбора событий и управлению правилами корреляции требует наличия в штате компании квалифицированных сотрудников или привлечение специалистов со стороны интегратора. Установка SIEM –системы без надлежащего контроля и управления приведет к неоправданной трате бюджета.

В случае удачного внедрения и использования SIEM-системы компания получает:

- корреляция и обработку событий безопасности, влияющих на состояние и ИТ-инфраструктуры и бизнес-процессов;
- возможность создание таких систем и центров мониторинга и реагирования как SOC(Security Operation Center);
- автоматизацию процессов обнаружения угроз и аномалии;
- реагирование на возникающие угрозы в режиме реального времени.

Новизна темы дипломной работы заключается в применении открытой технологии SIEM OSSIM для мониторинга информационных активов организации.

В главе был дан обзор системы SIEM, ее архитектуре, принципу работы, функционированию. Также был сделан обзор на виды систем мониторинга на мировом рынке. Были сделаны сравнения преимуществ нескольких систем SIEM

2 Практическая часть

2.1 Порядок выполнения работы

Работа выполняется студентом самостоятельно и состоит из следующих этапов:

1) изучение методических указаний по выполнению дипломной работы;
2) описание системы OSSIM;
3) проектирование структуры сети для внедрения системы;
4) установка системы SIEM;
5) конфигурация системы;
6) произведение «BruteForce» атаки на сервер и его перехват;
7) анализ системы после внедрения системы.

2.2 Описание системы OSSIM

В первую очередь нужно отметить что компания «AlienVault» выпускает две системы USM и OSSIM.Система USM является платной версией OSSIM. Разница систем указаны в таблице 1.

Таблица 2.1 – Сравнение USM и OSSIM

Разница	OSSIM	USM
Доступность продукта	Программа с открытым исходным кодом	Облачный сервис
Цена	Бесплатный	Ежегодная подписка
Мониторинг безопасности	Локальные физические и виртуальные среды	- Облачные среды AWS и Azure

		- Облачные приложения - Локальные физические и виртуальные среды
Архитектура развертывания	Только один сервер	Поставка SaaS с сенсоров, установленными в каждой контролируемой среде
Определение активов	+	+
Оценка уязвимости	+	+
Обнаружение вторжении	+	+
Поведенческий мониторинг	+	+
Корреляция событии	+	+
Хранилище логов	-	+
Облачный мониторинг AWS & Azure	-	+
Мониторинг безопасности облачных приложении	-	+
Автоматизация безопасности	-	+
Подключение OpenThreatExchange(Система с базами угроз)	-	+
Непрерывная обновление угроз	-	+
Поддержка по телефону или по почте	-	+
Онлайн документация продукта и база знании	-	+
Богатые аналитические графические панели и визуализация данных	-	+

На рисунках 2.1 и 2.2 показаны основные имеющиеся отличия в компонентах систем.

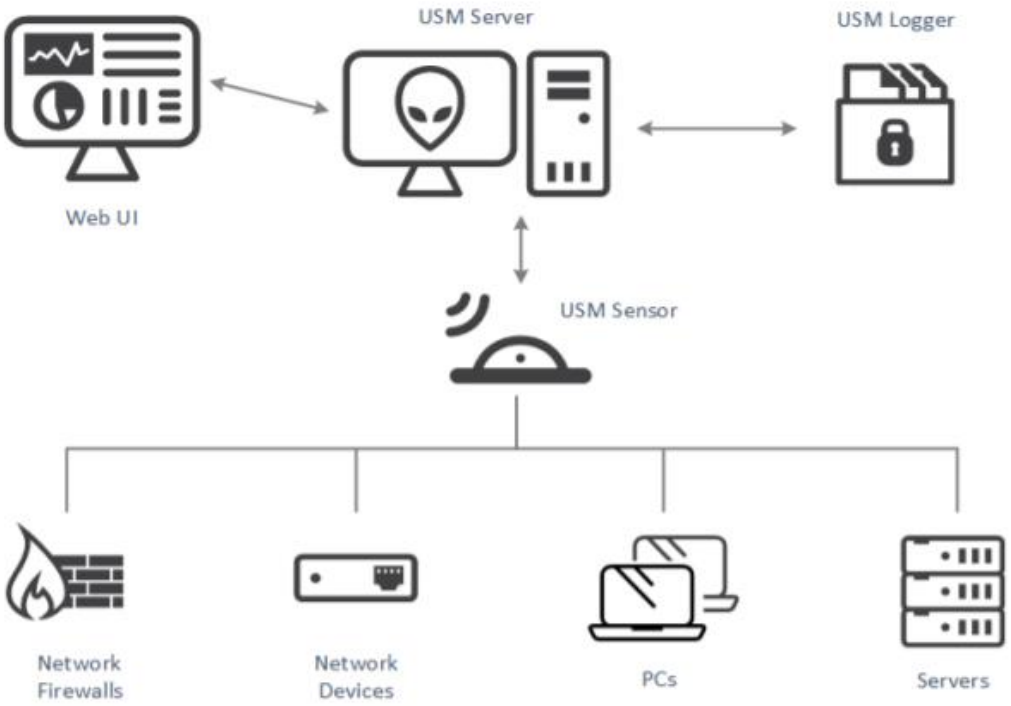


Рисунок 2.1 – Компоненты USM

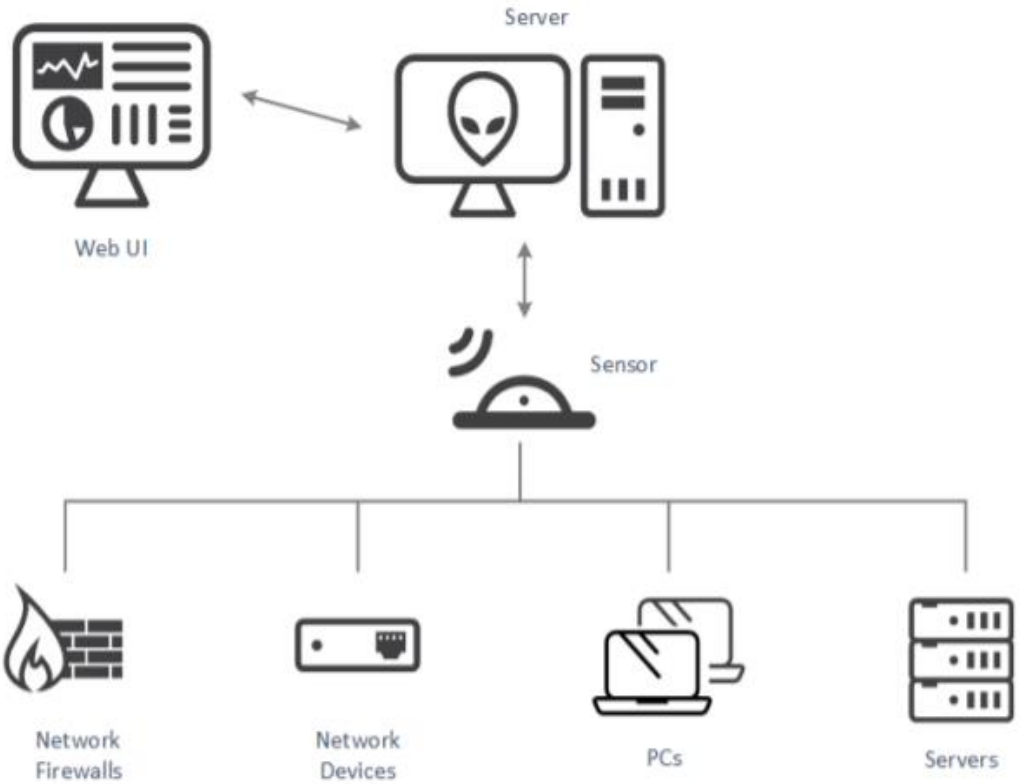


Рисунок 2.2 - Компоненты OSSIM

Особенности системы

Существует пять основных возможностей безопасности которые обеспечивает система(рисунок 2.3):

1) Обнаружение активов (Asset Discovery)

Модуль обнаружения активов идентифицирует активы и общеизвестные порты. Он способен делать это как активно, так и пассивно;

2) Оценка уязвимости (Vulnerability Assesment)

OSSIM имеет встроенную функцию для выявления уязвимостей. Для этого он использует сканер OpenvVAS. Она имеет возможность выполнить как аутентифицированное, так и не аутентифицированное сканирование по сети или хосту;

3) Обнаружение вторжений(Intrusion Detection)

Он состоит из трех частей: NIDS (Network Intrusion Detection System), HIDS(Host Based Intrusion Detection System) и FIM(File Integrity Monitoring) . В OSSIM используются инструменты IDS(Intusion Detection System), такие как Snort для идентификации аномалий сетевого трафика и Suricata для аномалий веб-трафика (SQL , XSS). OSSIM имеет встроенный сервер OSSEC для HIDS;

4) Поведенческий Мониторинг(Behavioral Monitoring)

Именно здесь анализируются аномалии сетевого трафика. В дополнение к модулю NIDS, OSSIM имеет встроенный в него Netflow. Это помогает нам определить причину "внезапного всплеска в сети", распространения вредоносных программ и т. д. В OSSIM также имеет функцию, чтобы сделать оба узла-наличие и доступность службы мониторинга. Мониторинг доступности узла проверяет, включен ли отмеченный узел или нет, а мониторинг доступности службы проверяет, включена ли конкретная служба, запущенная на компьютере. Это очень удобно при борьбе с DOS-атаками;

5) Разведка безопасности(SIEM)

Именно здесь происходит полное вычисление/обработка событий. Вся информация, которую OSSIM извлекла из всех вышеперечисленных модулей, будет использована для оценки рисков. Основная обработка материалов, таких как связывание похожих или цепных событий (корреляция), выполняется здесь. Вот одно из самых больших ограничений в OSSIM. Он получил только около 80-100 правил корреляции, в то время как, с другой стороны, USM(Unified Security Management) имеет 2000-3000 правил. Корреляция-это реальная автоматизация, которая помогает нам идентифицировать атаки. Создание пользовательской корреляции возможно в OSSIM. Но все же при сравнении 2000 + правил в USM с 80 + правилами в OSSIM, определенно USM ветры. Корреляция фактически дает нам ответы на такие вопросы, как, пытался ли кто-то использовать известную уязвимость. Есть ли у нас атака нулевого дня и т. д. Также систему можно подключить к системе OTX(Open Threat Exchange). OTX - это самый авторитетный в мире открытый обмен информацией об угрозах и аналитическая сеть.

OTXобеспечивает открытый доступ к глобальному сообществу исследователей угроз и профессионалы безопасности. В настоящее время он насчитывает более 100 000 участников по всему миру, которые вносят свой вклад более 19 миллионы индикаторов угроз ежедневно. Он обеспечивает передачу данных об угрозах, генерируемых сообществом, и импульсов OTX, что позволяет совместное исследование, а также автоматизирует процесс обновления вашей инфраструктуры безопасности с помощью данные об угрозах из любого источника. OTX позволяет любому члену сообщества безопасности активно обсуждать этот вопрос, исследуйте, проверяйте и делитесь последними данными об угрозах, тенденциями и методами, укрепляя свои позиции защиты, помогая другим делать то же самое.

Сообщество OTX и соответствующие данные об угрозах являются одним из важнейших источников данных, используемых организацией. Команда инопланетных лабораториях, чтобы создать опасный AlienVault интеллект. Инопланетные лаборатории усиливают коллектив ресурсы OTX путем анализа, проверки и кураторства данных о глобальных угрозах, предоставленных сообщество OTX.

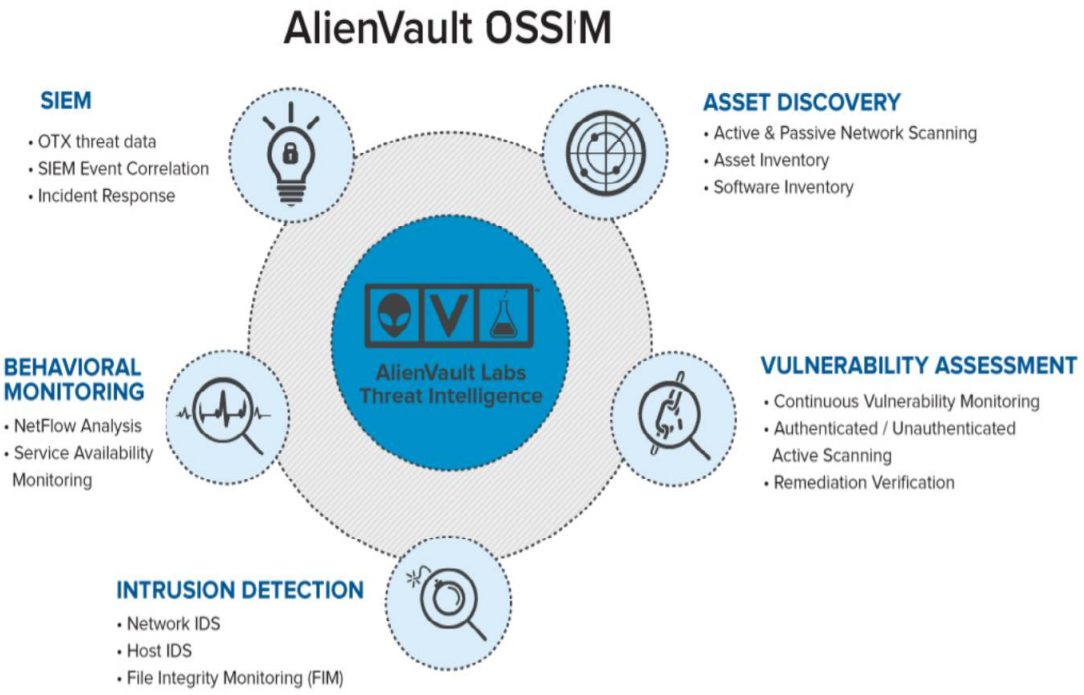


Рисунок 2.3 – Основные возможности OSSIM

Архитектура OSSIM

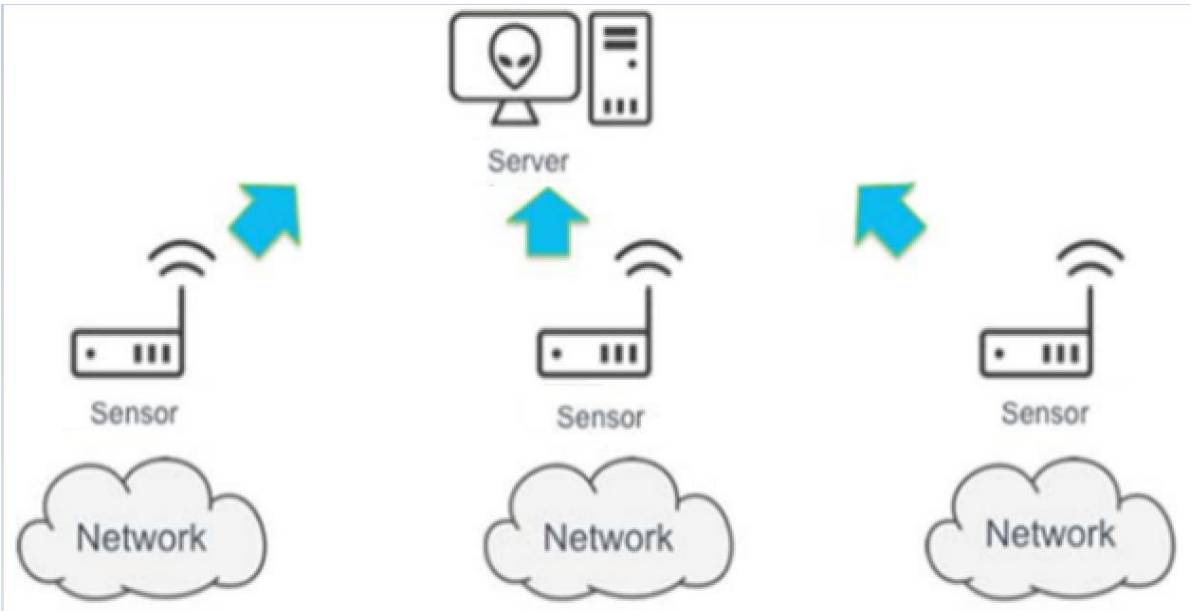


Рисунок 2.4 - Архитектура OSSIM

OSSIM состоит из двух устройств. Но поскольку это работа была построена на методике "развертывание все-в-одном", не нужно беспокоиться о настройке каждого модуля в отдельности. Датчик(Sensor)-это самое первое, что приходит в контакт с логами. Он выполняет все эти операции по обнаружению уязвимостей, обнаружению угроз, сбору журналов и т. д.. Он собирает все эти журналы информацию, которую он получил, и преобразует ее в события. Сервер (Server) фактически обрабатывает эти события, отправленные с датчика, и выполнят такие функции как, корреляция, расчет риска, распознавание образов и поведенческий анализ, а также проверяет информацию об угрозах(рисунок 2.4).

OSSIM «из коробки» включает в себя такой функционал как:

1) Сбор, анализ и корреляция событий — SIEM;
2) Хостовая система обнаружения вторжений (HIDS) — OSSEC;
3) Сетевая система обнаружения вторжений (NIDS) — Suricata;
4) Беспроводная система обнаружения вторжений (WIDS) — Kismet;
5) Мониторинг узлов сети- Nagios;
6) Анализ сетевых аномалий – P0f, PADS, FProbe, Arpwatch и др;
7) Сканер уязвимостей – OpenVAS;
8) Мощнейшая система обмена информацией об угрозах между пользователями OSSIM — OTX.

Основной рабочий процесс устройства OSSIM

Существует последовательный рабочий процесс, которому OSSIM следует при сборе необработанных данных из сети устройства, а затем разбор и нормализация этих данных в поток событий, которые затем могут быть сохранены, фильтруется и коррелируется для выявления угроз и уязвимостей. Датчик(Sensor) прибора анализирует необработанные данные из различных источников и преобразует их в поток событий, каждый из

которых имеет общий набор полей данных. Затем он отправляет события в систему Сервер(Server) устройств. Сервер(Server) устройств коррелирует события и оценивает их риск, рисунок 2.5.

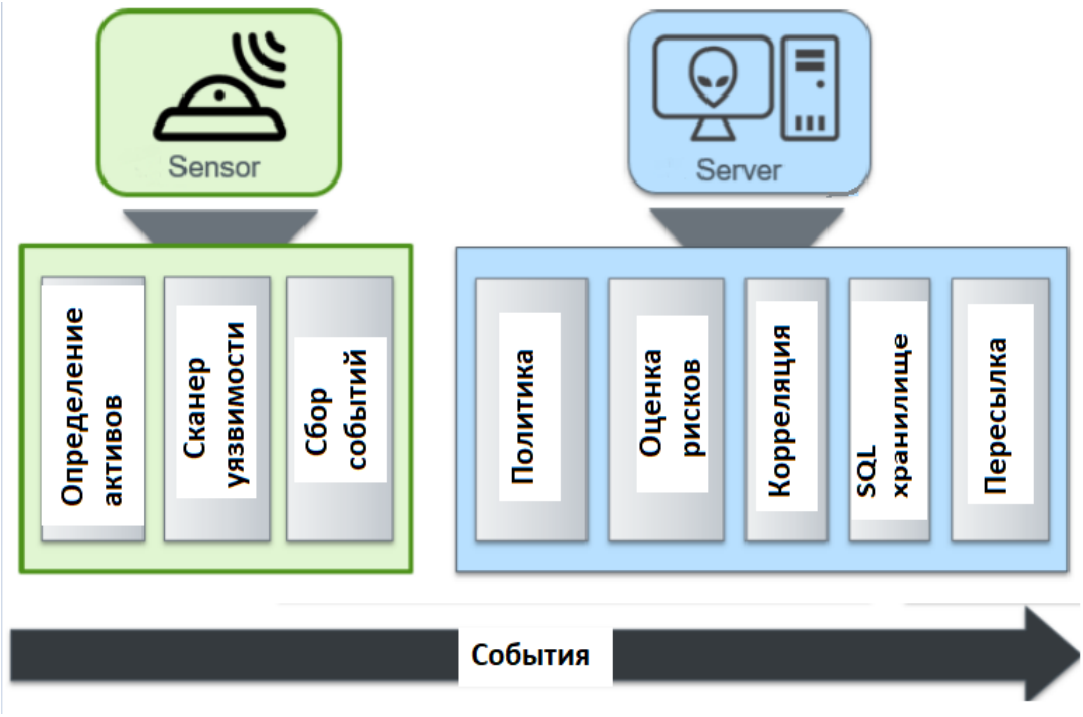


Рисунок 2.5 - Рабочий процесс системы

2.3 Проектирование SIEM системы OSSIM

В настоящее время существует множество систем мониторинга сети. Конкуренция среди вендоров систем на фоне роста в казахстане информационных атак на информационные системы , привели к масштабному внедрению такой системы как “SIEM”.

SIEM системы предоставляют систему благодаря который централизуется сетевая активность в формат которую легче усваивать. Следует сразу отметить что системы SIEM предназначены для мониторинга и реагирования на инциденты но не позволяют защищаться от угроз или предотвращать негативные события

Для примера реализации проекта, было взята система AlienVault OSSIM и внедрена в корпоративную сеть. Актуальность данной работы определяется тем, что в этой сети находятся активы с важными данными над которыми нужно производить мониторинг.

Целью данного проекта является развертывание системы мониторинга OSSIM и оптимизация под информационные активы компании. Необходимо достичь максимально надёжной, устойчивой, экономически выгодной сети. Для достижения поставленной цели требуется решить следующие задачи:

- анализ сети для которого разрабатывается система;
- разработка стратегии реализации системы OSSIM;

- подбор соответствующего оборудования;
- установка системы в сеть;
- анализ результатов.

Структурная схема сети в которую будет внедрена в итоге система OSSIM показана на рисунке 2.6:

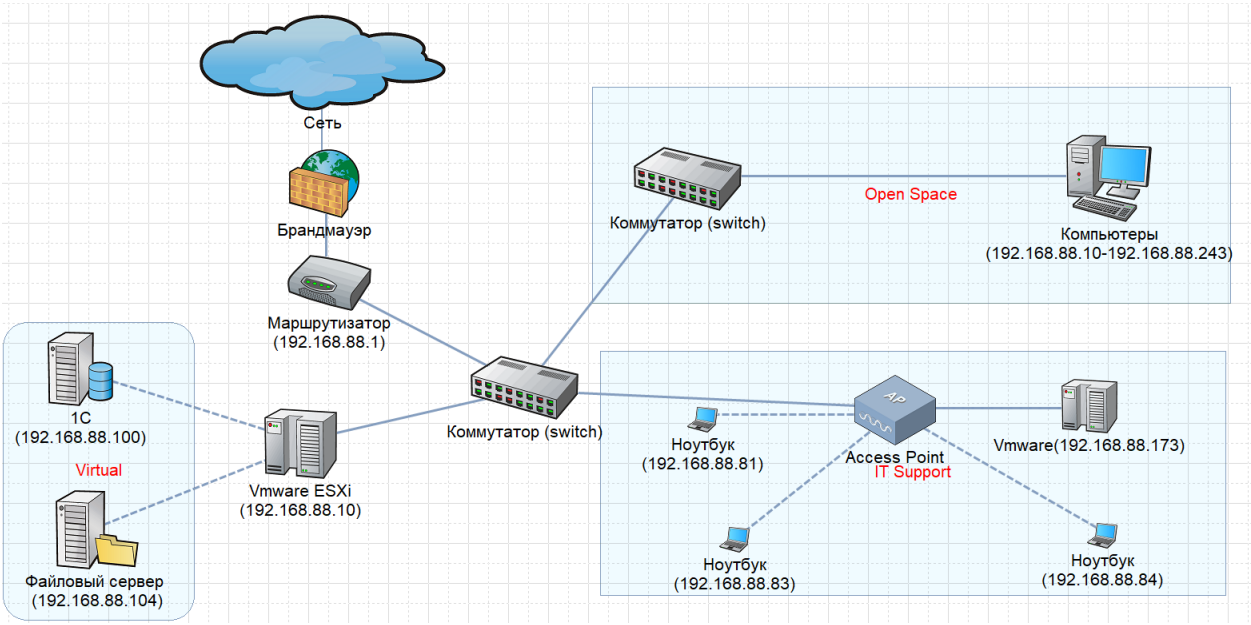


Рисунок 2.6 – Топология сети до внедрения SIEM

В практической части своей работы, было рассмотрено SOHO (Small Office/Home office) сеть. Сама сеть состоит из таких информационных активов как:

– сервер базы данных (1С);
– файловый сервер(SAMBA);
– маршрутизатор (Ubiquiti EdgeRouter 12);
– коммутаторы (TP-Link TL-SF1048);
– стационарные компьютеры;
– ноутбуки;
– сервер для виртуализации(VMware).

Из этого можно понять, что наши устройства генерируют огромное количество событий, которые администратору обрабатывать должным образом невозможно. Таким образом можно выявить основную проблему нашей системы, то есть замедленная реакция на инциденты, либо отсутствие её вовсе. В такой ситуации хорошо справляется SIEM система, которая помимо увеличения скорости реакции на инцидент дает много полезных вещей, таких как:

1. Анализ событий и создание оповещений при каких-либо аномалиях:

сетевого трафика, неожиданных действий пользователя, неопознанных

устройствах и т.д;

2. Создание отчетов. В том числе настроенных непосредственно для ваших нужд. Например, ежедневный отчет об инцидентах, отчет по работоспособности устройств и т.д. Отчеты настраиваются гибко, как и их получатели;

3. Мониторинг событий от устройств/серверов/критически важных систем, создавать соответствующие оповещения для заинтересованных лиц;

4. Сбор доказательной базы по инцидентам;

5. При наличии сканера уязвимостей, SIEM частично избавит вас от головной боли в плане рисков;

6. Уменьшение потока событий за счет фильтрации, агрегирования, нормализации, корреляции и приоретизации;

Проектируемая сеть должна предоставлять системному администратору виды информации такие как журналы и сохраненные логи которые в дальнейшем будут отображаться в нашей системе в виде таблиц и картинок.

Перейдём непосредственно к развертыванию системы. Мой выбор пал на SIEM OSSIM. Выбор мой пал на неё в связи с тем, что из рассмотренных мной систем я выбрал систему за то, что она является бесплатной системой то есть с открытым исходным кодом, также меня привлек широкий функционал, который позволяет пользоваться с системой сразу же после настройки так как не требуется установка лишнего ПО

Параметры развертывания устройства USM

Устройство AlienVault OSSIM может быть развернуто в одной из двух базовых конфигураций:

1) простая модель развертывания - все компоненты устройства OSSIM (датчик, сервер) являются совмещенный в приборе OSSIM то есть все в одном. Эта конфигурация чаще всего используется в небольших средах, а также для демонстраций и демонстрационных развертываний концепции;

2) многоуровневая распределенная модель развертывания — эта модель развертывает каждый компонент AlienVault OSSIM (датчик, сервер) как отдельное виртуальное или аппаратное устройство для создания топология распределенной системы.

В данной работе была использована техника “Все в одном” то есть сервер и сенсоры системы OSSIM устанавливается как одно целое. Ниже на рисунке 2.7 показана топология сети после внедрения системы:

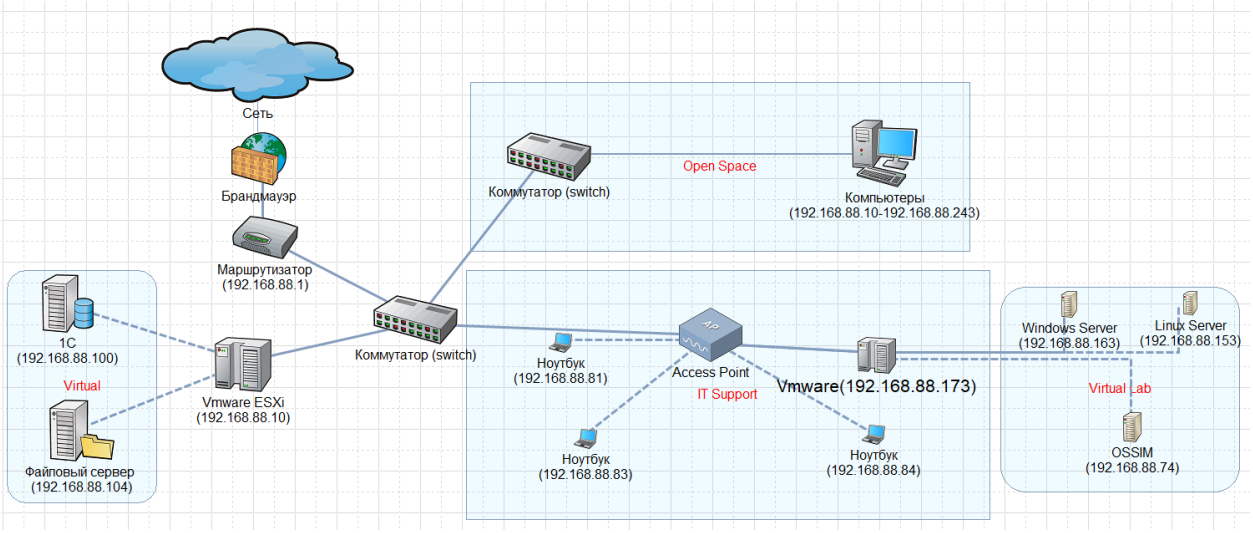


Рисунок 2.7 – Топология сети после установки системы

2.4 Развертывание OSSIM

Минимальные требования

Поскольку серверы USM и OSSIM имеют общий дизайн и системные службы, рекомендуется придерживаться требований USM для развертывания OSSIM.

Для корректной работы системы необходимо:

– Наличие на компьютерах ОС Microsoft Windows XP\7\8\10, Windows Sever 2010\2012, ОС Linux;

– Среда исполнения Microsoft .NET Framework;

– Установленные агенты на компьютерах для получения логов.

Устройство на которую будет установлена система должна иметь следующие характеристики для стабильной работы:

1) 8 ядер процессора;
2) 16 ГБ ОЗУ;
3) 1 ТБ жесткого диска;
4) сетевой интерфейс;
5) VMware или Hyper-V;
6) OSSIM ISO файл;
7) Ключ OTX.

Есть много вещей, которые следует учитывать при развертывании SIEM. Такие вещи, как EPS (события в секунду), активы, пропускная способность, географические границы, часовые пояса и хранение и т. д. Alienvault предлагает около 4 типов режимов развертывания. Но так как OSSIM - это одноуровневое,и развертывалось по методике «все-в-одном», нужно только рассмотреть несколько вещей. Первое, что необходимо рассматривать, это сфера применения. В данной работе были использованы все активы которые указаны на рисунке 2.4. Но в основном работа производилоась со следующей группой в которую вошли:

1) Linux Server (192.168.88.153);
2) Маршрутизатор (192.168.88.1);
3) Windows Server 2012 (192.168.88.163);
4) Сервер с VMware (192.168.88.74).

OSSIM-это фактически ОС Debian, которую нужно устанавливать точно так же, как и ОС. Интерфейсом является IP адрес - 192.168.88.74 который будет содержит в себе три функции:

- управления;
- сбор и сканирование журналов;
- мониторинг сети.

2.5 Установка сервера OSSIM

После настройки виртуальной машины можно приступить самой установки OSSIM сервера по ISO образу. После включения виртуальной машины система (рисунок 2.8), о типе установки то есть в качестве OSSIM сервера или сенсора. Нужно выбрать первый вариант и нажать «Ввод», чтобы продолжить.

Рисунок 2.8 – Выбор системы для установки

На рисунке 2.9 необходимо выбрать нужный язык, был выбран английский, по умолчанию. И следует нажать продолжить, чтобы начать настройку интерфейса управления

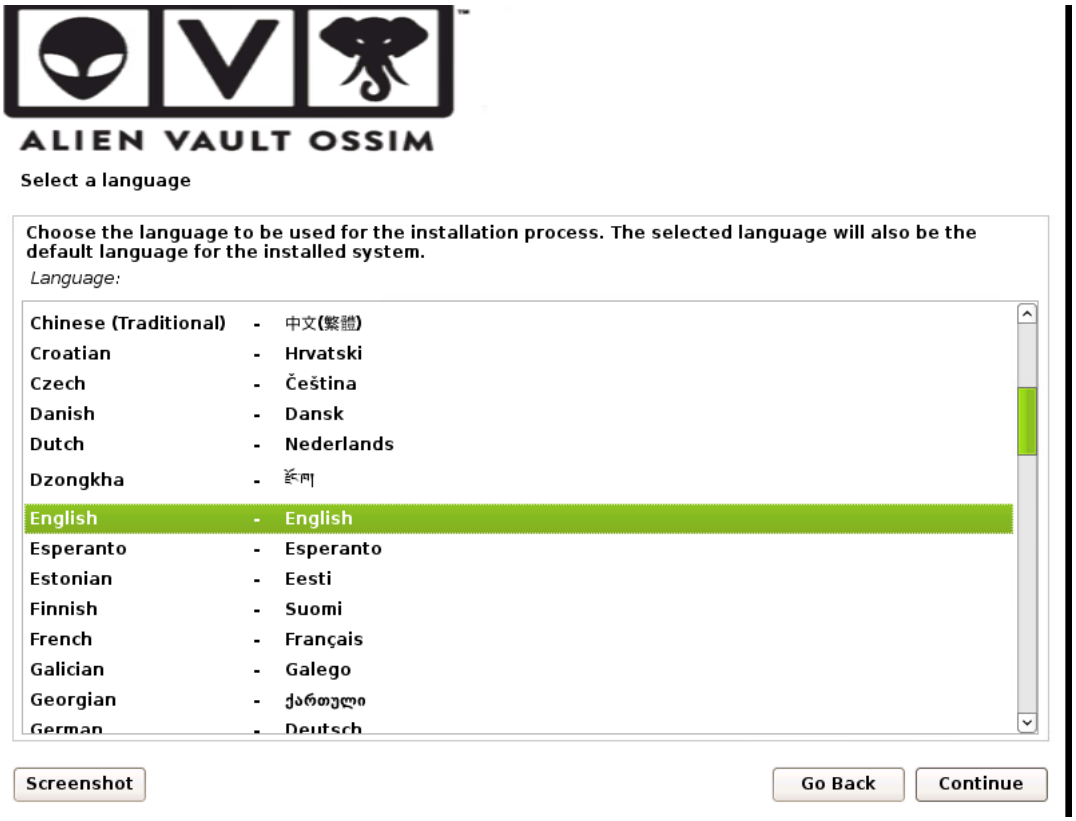


Рисунок 2.9 – Выбор языка

На этом этапе настраивается сеть виртуальной машины OSSIM. То есть настраивается интерфейс под неразборчивый режим “Promiscuous mode” который будет перехватывать весь входящий и исходящий трафик от других виртуальных машин а также хоста то есть сервера (рисунки 2.10, 2.11).

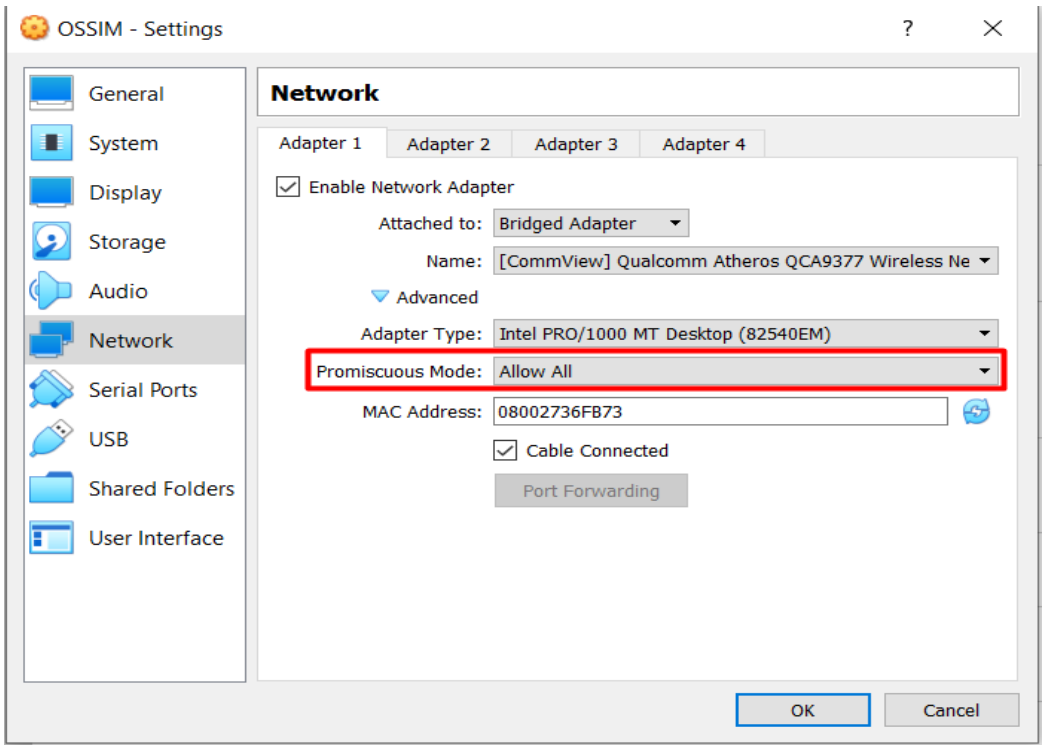


Рисунок 2.10 – Выборка неразборчивого режима

Рисунок 2.11 – Определение интерфейса

На рисунках 2.12, 2.13, 2.14 показан ввод IP адреса, маски и шлюза для интерфейс eth0 благодаря который можно подключаться к системе для удаленного управления.

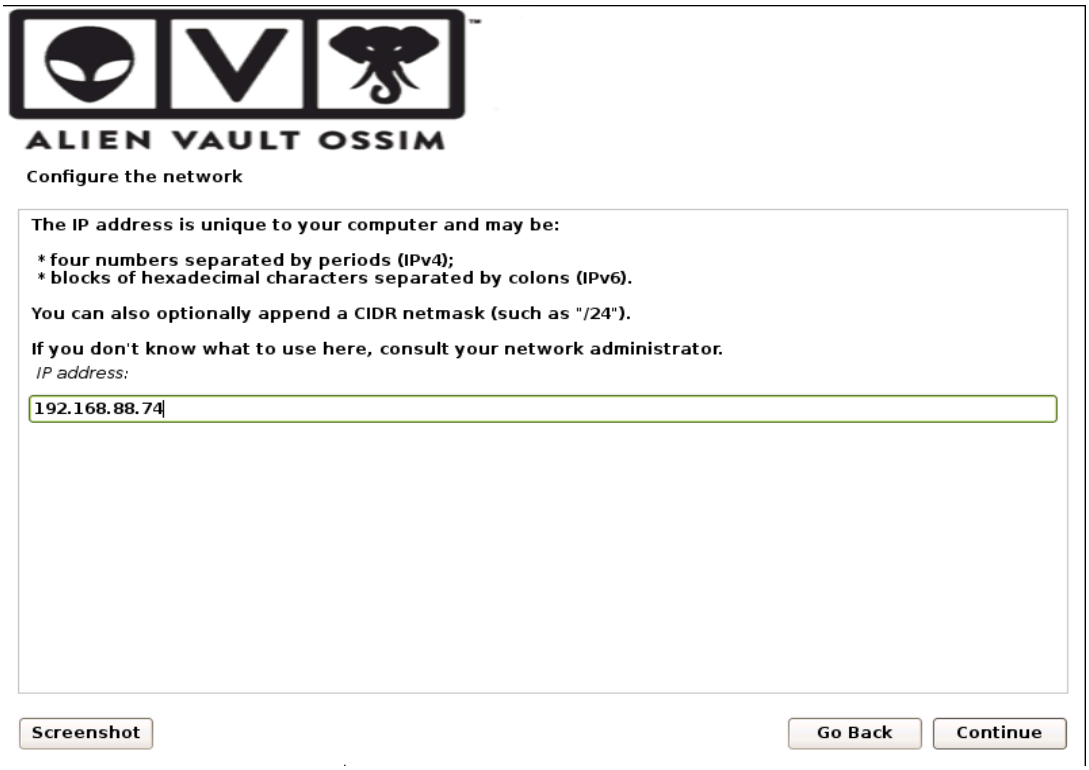


Рисунок 2.12 – IP адрес для управления

Рисунок 2.13 – Маска сети

Рисунок 2.14 – Указание шлюза

Можно оставить конфигурацию временной зоны без изменения так как далее в веб-консоли дается возможность поменять эту информацию(рисунок 2.15)

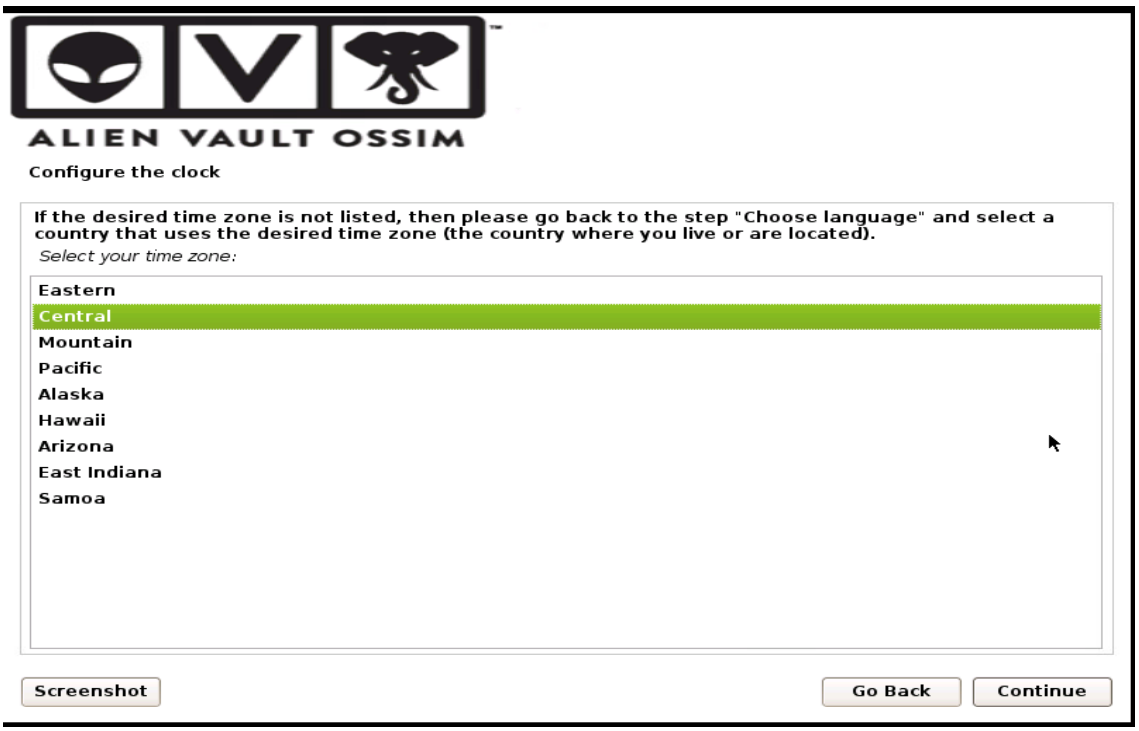


Рисунок 2.15 – Выборка временной зоны

На рисунке 2.16 производиться установка пароля для пользователя root благодаря который открывает доступ к командной консоли сервера.

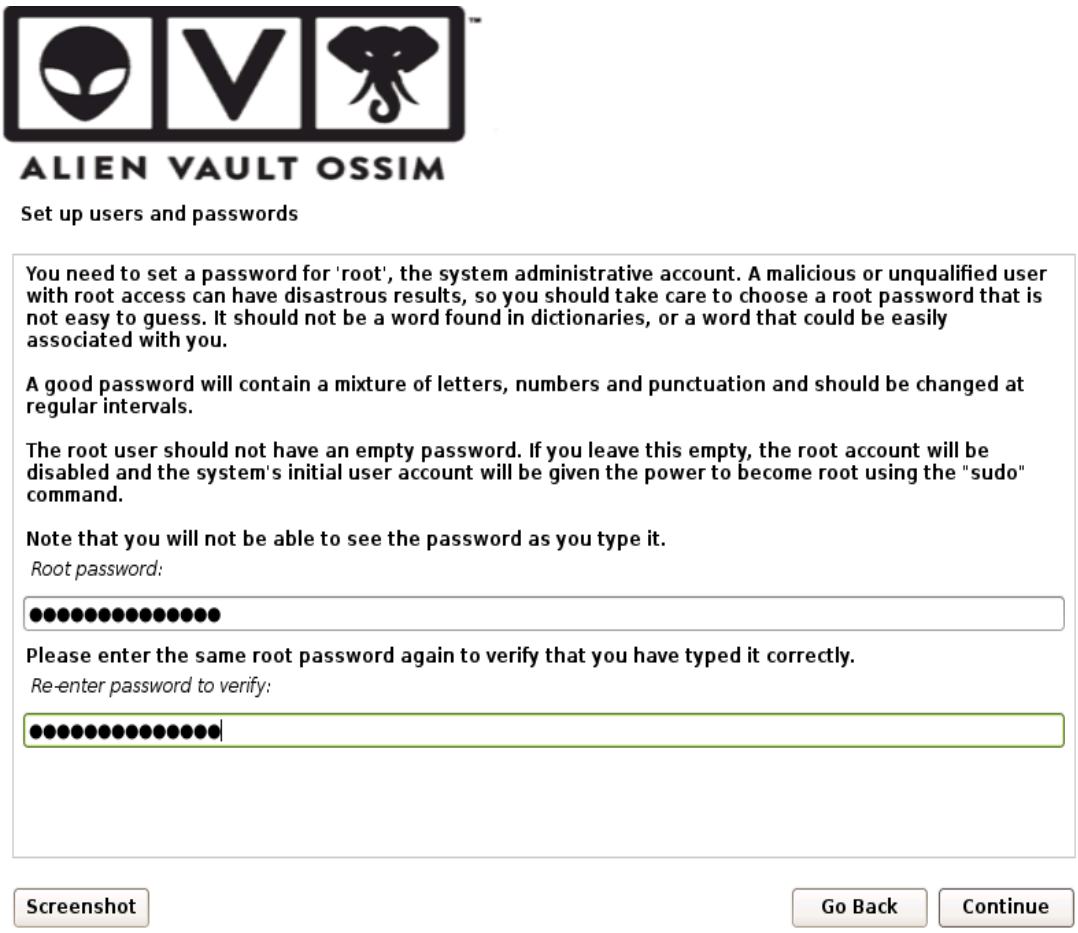


Рисунок 2.16 – Установка пароля для пользователя root

После ввода всех настроек начнётся установка. Сама установка занимает много времени, рисунок 2.17.

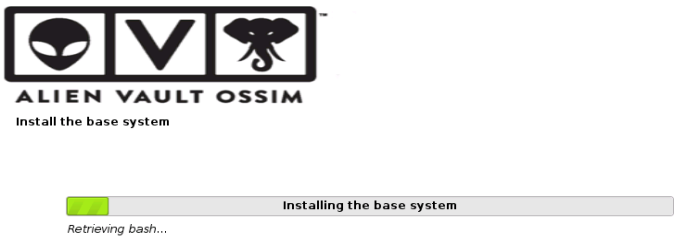


Рисунок 2.17 – Процесс установки

После завершения установки система перезагружается, и в консоли виртуальной машины, показанной ниже на рисунке 2.18, появляется экран с

вводом данных а также с IP адресом управления, который был настроен ранее. Производиться авторизация с логином root и паролем в CLI(Command Line Interface) сервера OSSIM

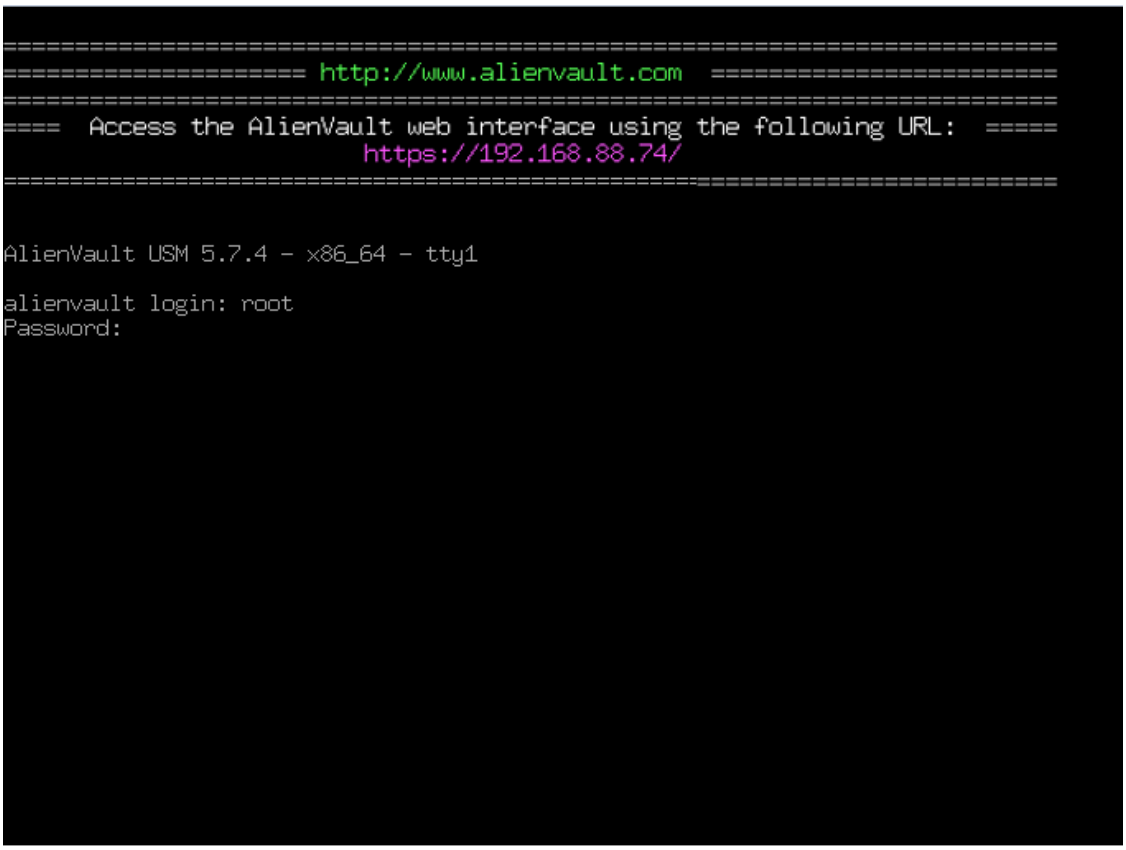


Рисунок 2.18 – Ввод логина и пароля

После авторизации следует меню настроек сервера, рисунок 2.19. Меню настроек представляет собой консоль где можно произвести настройку:

1) Системные настройки (System Preferences). Здесь можно настроить местоположение сервера, название хоста, отправку уведомлении на почту, изменение пароля, удаление API ключа AlienVault, обновление системы Настройка сенсора (Configure Sensor). Здесь можно настроить мониторинг сети, настройку CIDR, настройку IP сервера и фреймворка, настройка плагинов для данных и для мониторинга, управление Netflow;
2) Техническое обслуживание (Maintenance & Troubleshooting);
3) Командная консоль(Jailbreak System);
4) Удаленная поддержка(Support);
5) О версии системы(About this installation);
6) Перезагрузка системы(Reboot Appliance);
7) Выключение системы(Shutdown Appliance);
8) Сохранение изменение(Apply all changes).

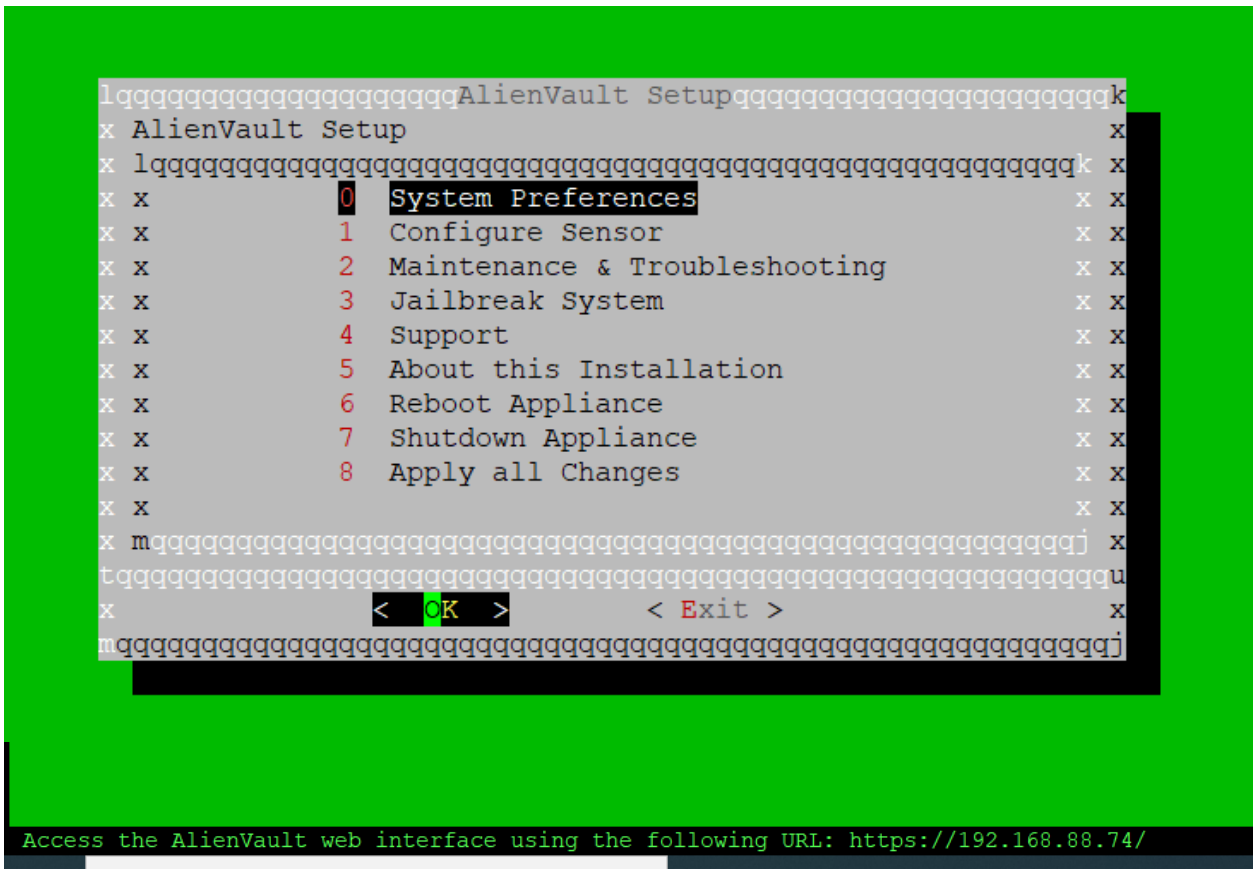


Рисунок 2.19 – Меню настроек

Далее было настроена точная дата. Для этого необходимо войти в раздел “System Preferences>Change Location>Date and Time>Configure Time Zone” и поменять на соответствующую страну, рисунки 2.20, 2.21, 2.22, 2.23, 2.24, 2.25, 2.26.

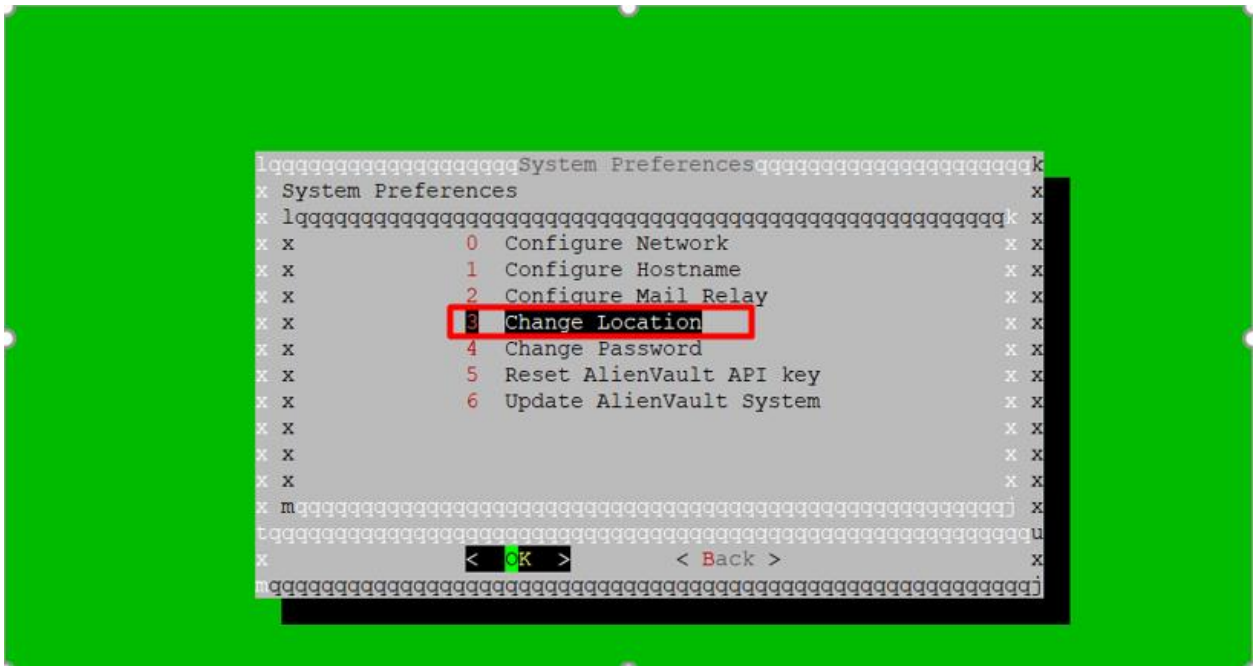


Рисунок 2.20 – Переход в раздел изменения времени

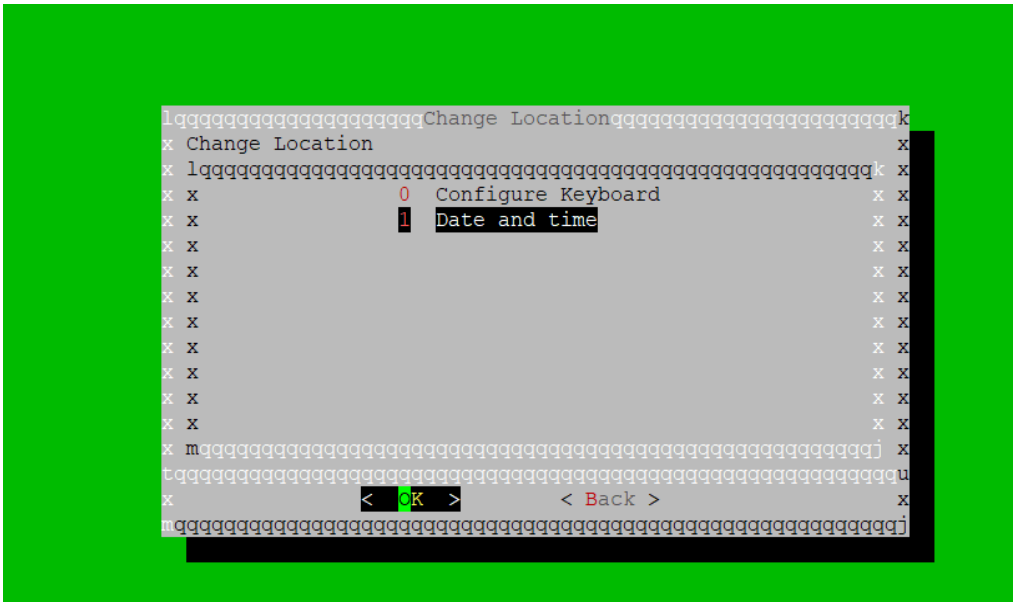


Рисунок 2.21 – Вход в раздел даты и времени

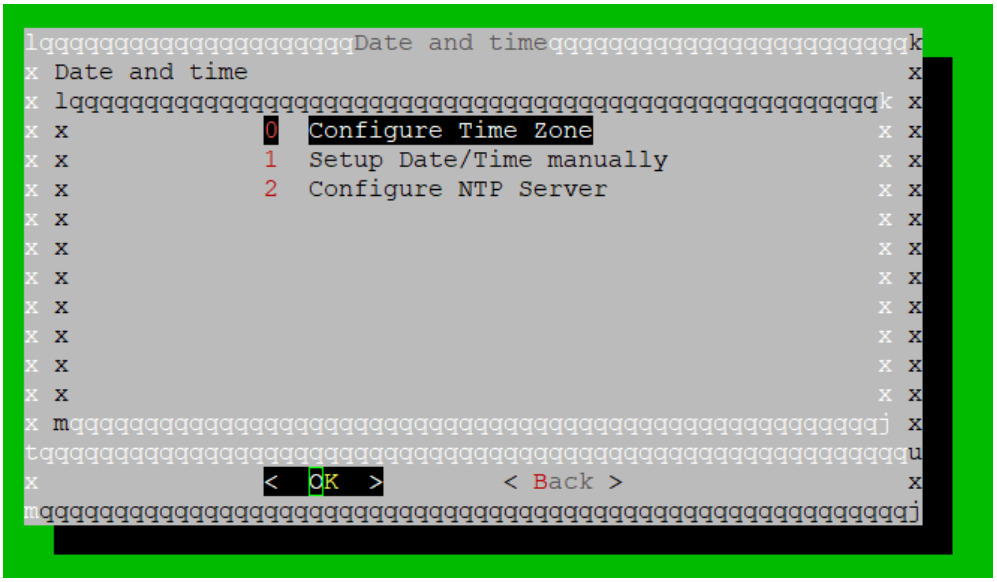


Рисунок 2.22 – Конфигурация временной зоны

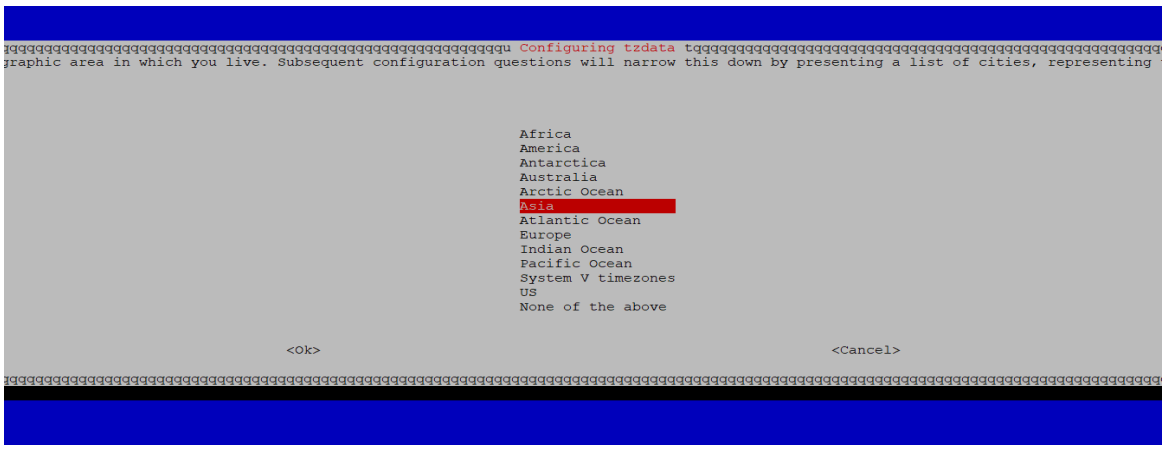


Рисунок 2.23 - Выбор зоны

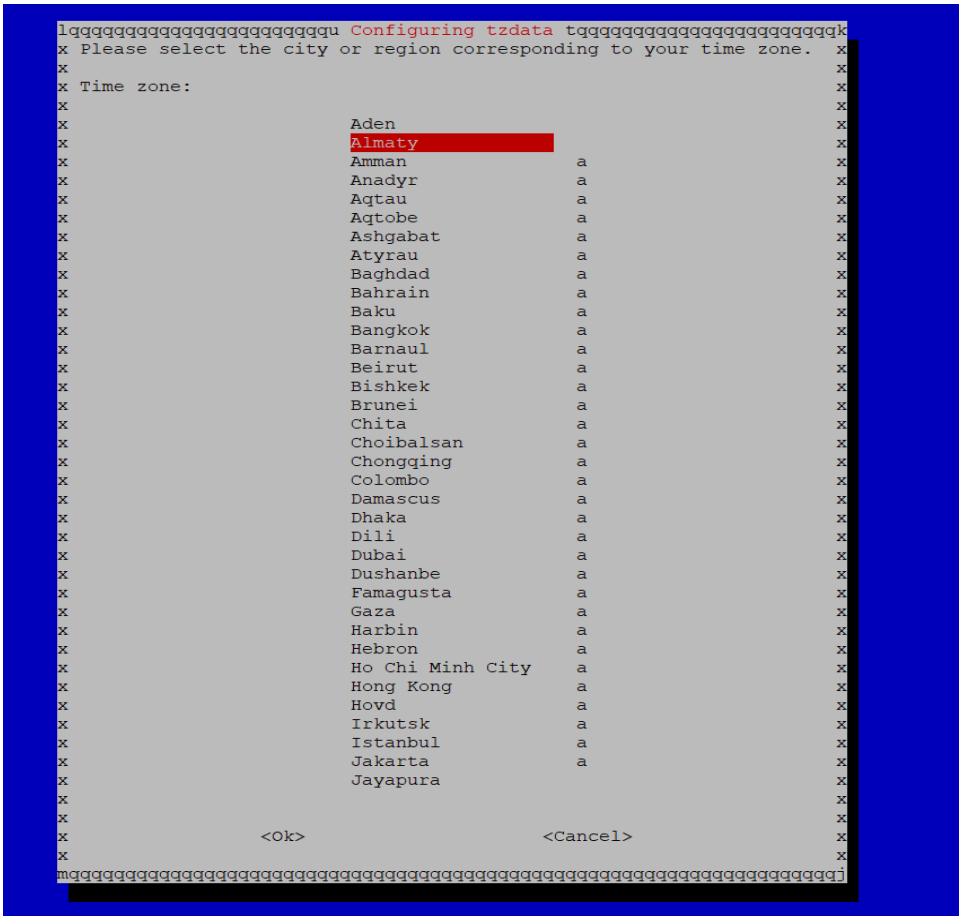


Рисунок 2.24 – Выбор города

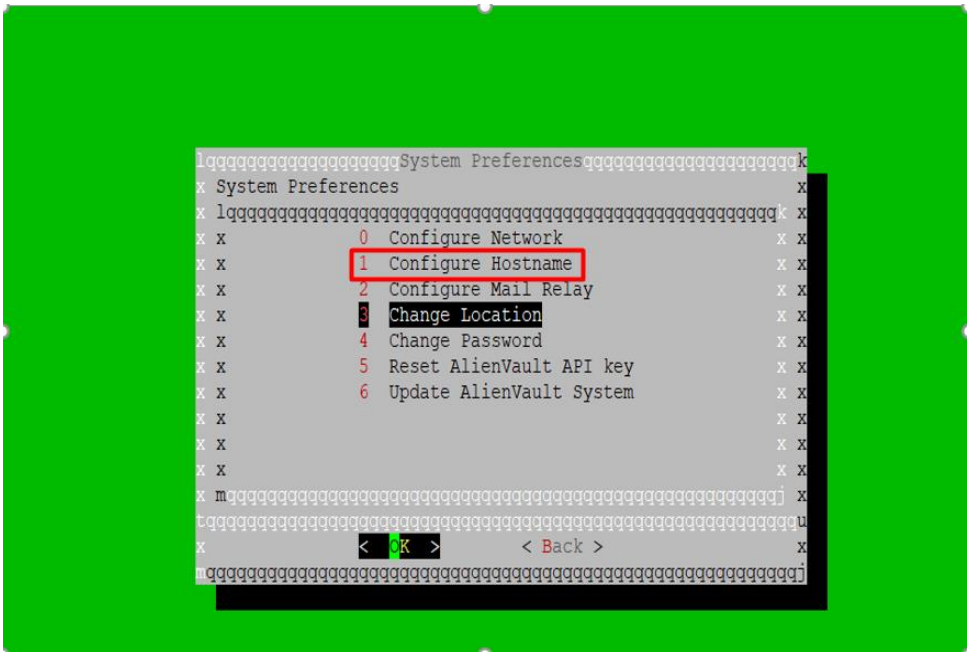


Рисунок 2.25 – Раздел конфигурации названия хоста

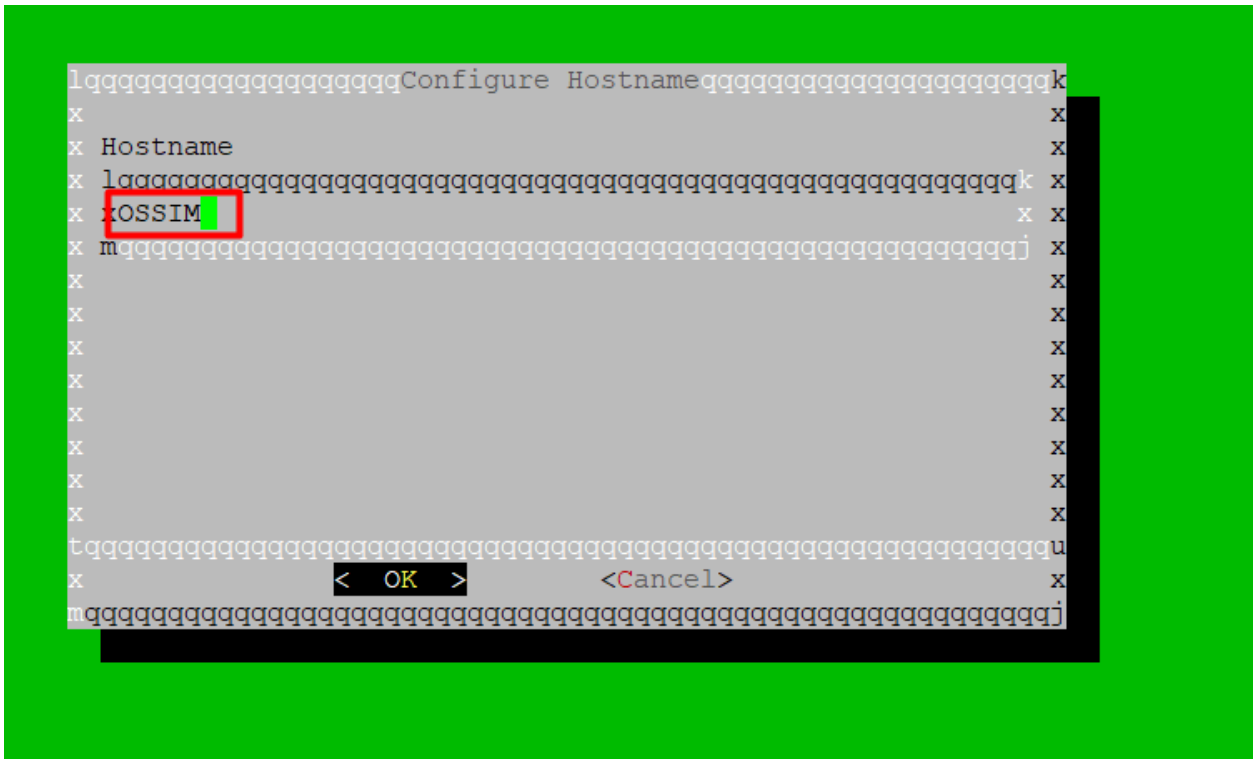


Рисунок 2.26 – Изменение названия хоста

По умолчанию OSSIM использует интерфейс управления для выполнения мониторинга сети, сбора журналов и сканирования. Можно разделить эти интерфейсы для того чтобы не нагружать систему. Следовательно, нет необходимости настраивать какие-либо дополнительные

интерфейсы, так как все они функционируют на одном интерфейсе управления, рисунки 2.27, 2.29, 2.30.

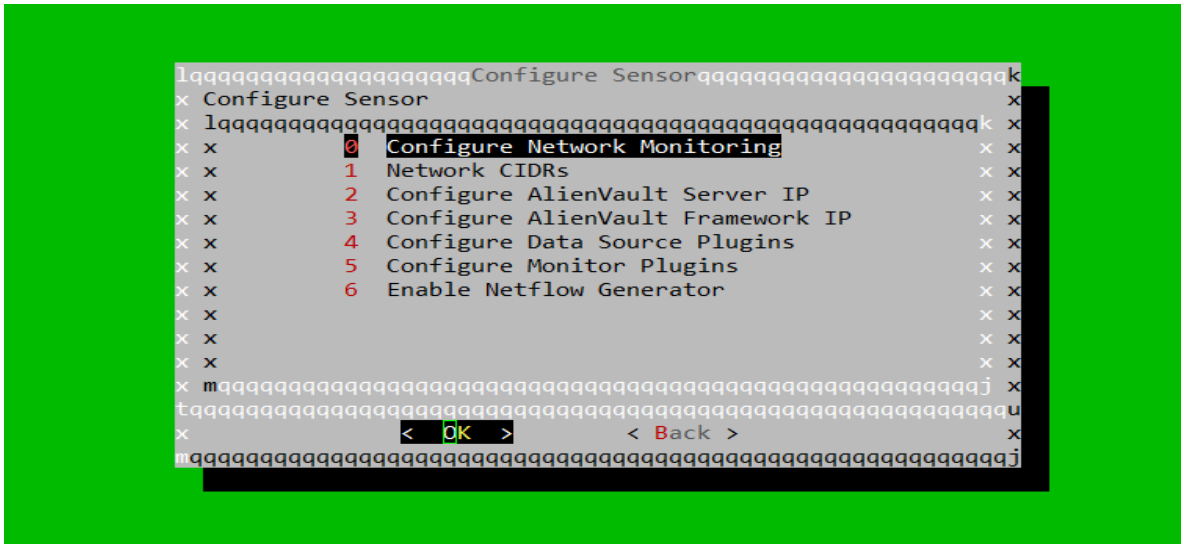


Рисунок 2.27 - Вход в раздел настройка интерфейса мониторинга

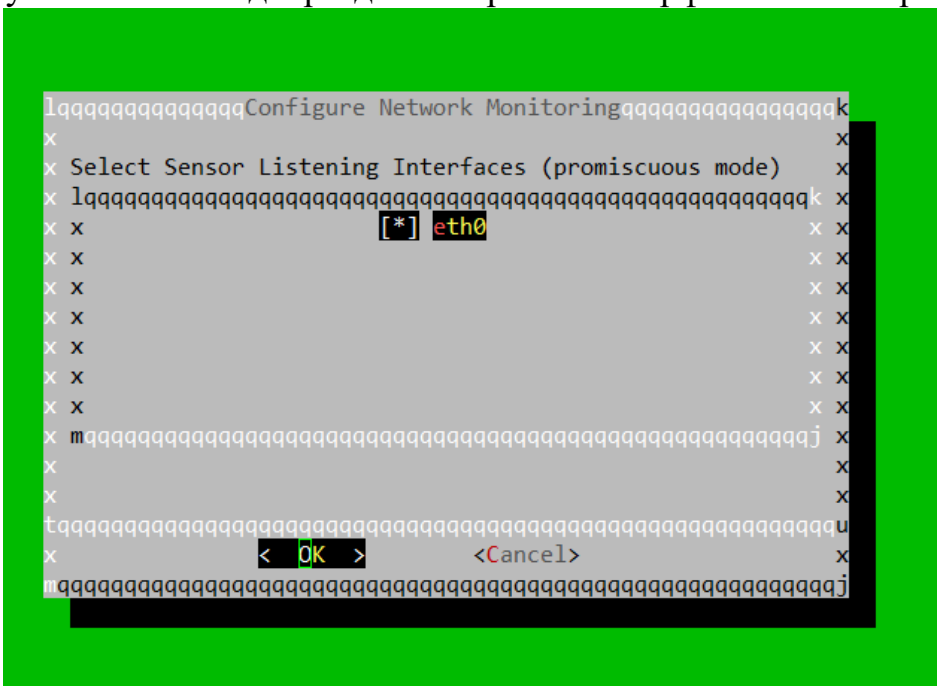


Рисунок 2.28 - Интерфейс мониторинга

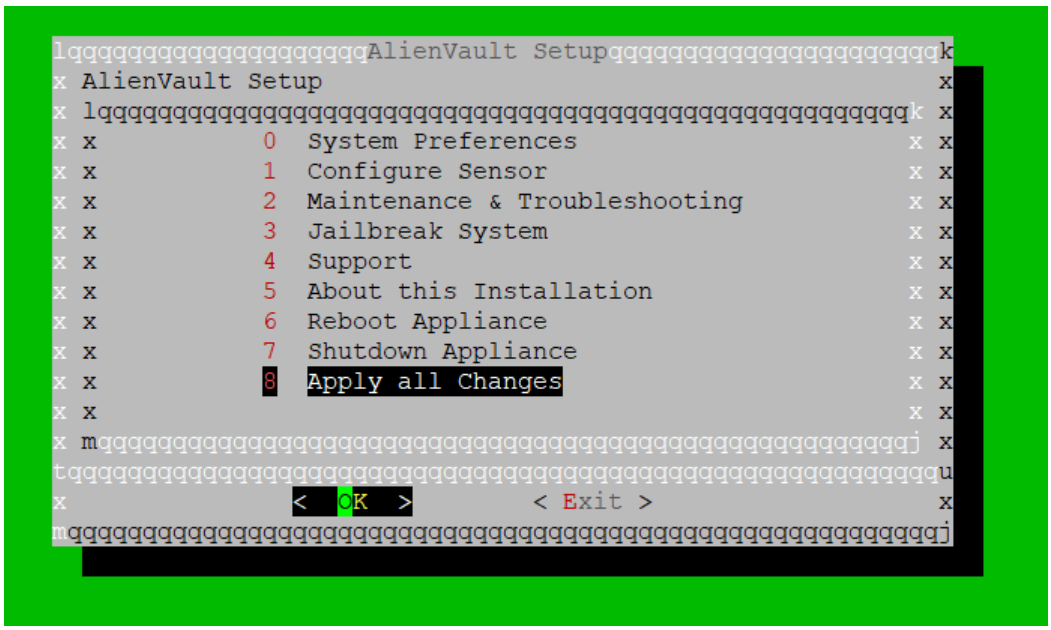


Рисунок 2.29 – Сохранение всех изменении

Рисунок 2.30 – Измененное название хоста

2.6 Веб интерфейс системы

После настройки консоли появится возможность подклкючения к веб интерфейсу через IP адрес:192.168.88.74. Для этого нужно открыть браузер и ввести в адресной строке этот IP. Браузер Mozilla Firefox не открывает ссылку, поэтому был использован браузер Chrome для доступа к веб-интерфейсу. Chrome предложит предупреждающее окно, в котором говорится, что сертификат не является доверенным, поскольку OSSIM использует самозаверяющий сертификат. После принятия исключения, сервер OSSIM потребует ввести следующую информацию. Заполнение необходимых данных, которые запрашивались были отражены на следующих рисунках 2.31, 2.32

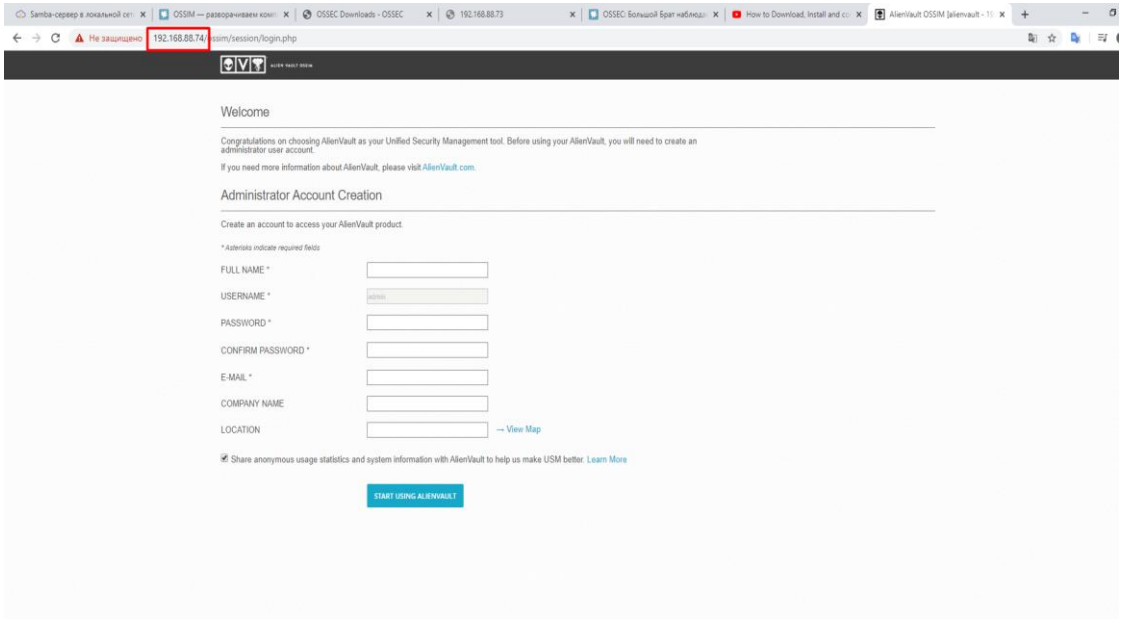


Рисунок 2.31 – Ввод необходимых данных

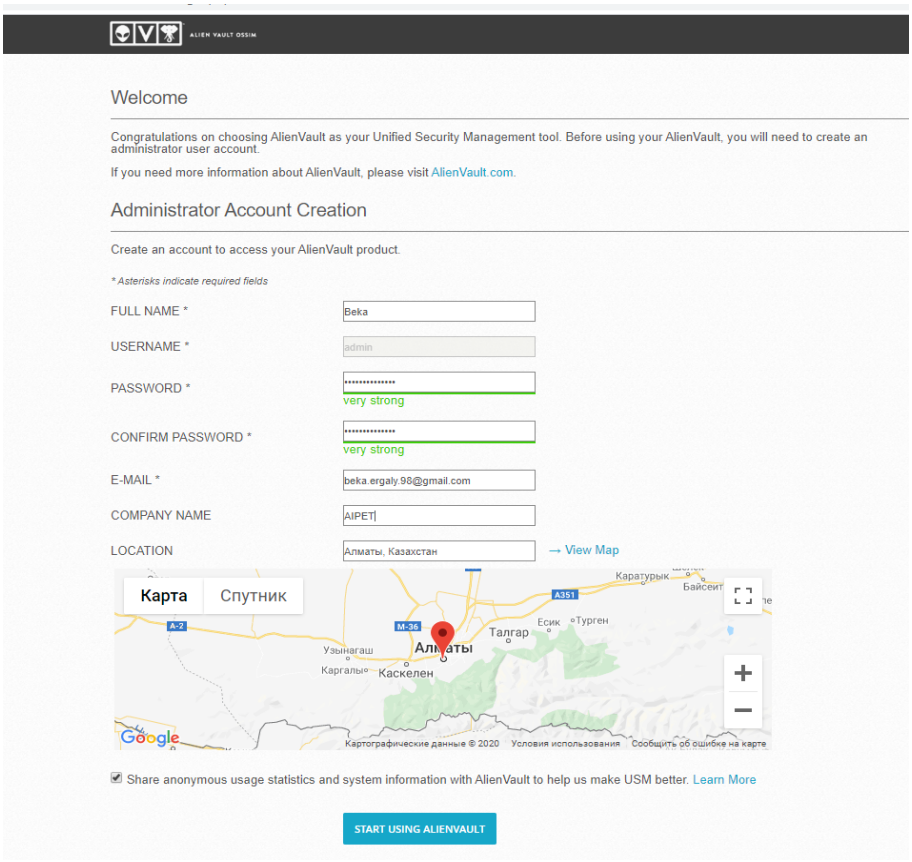


Рисунок 2.32 – Введенные данные

Следующие окно появятся после создания учетной записи администратора, рисунок 2.33. Необходимо ввести имя пользователя и пароль для пользователя которые были созданы выше.

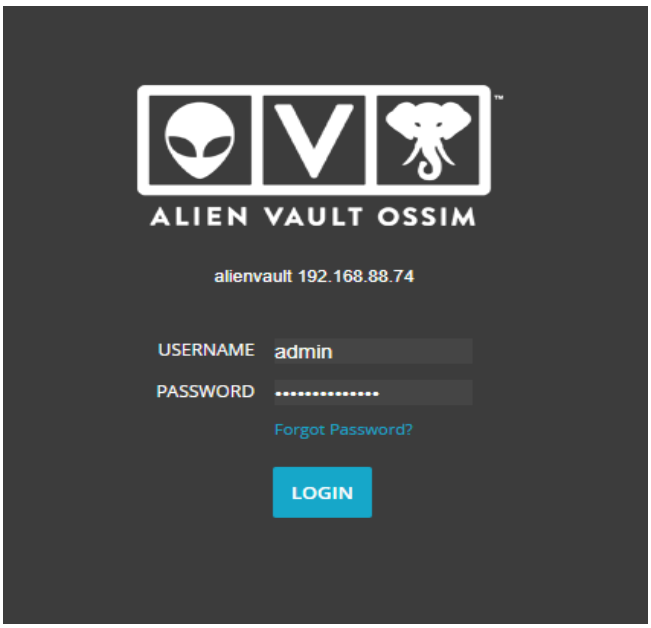


Рисунок 2.33 – Авторизация в веб-интерфейсе

После успешного входа в веб-интерфейс нужно ввести данные в мастере настроек для дальнейшей стабильной работы сервера OSSIM.

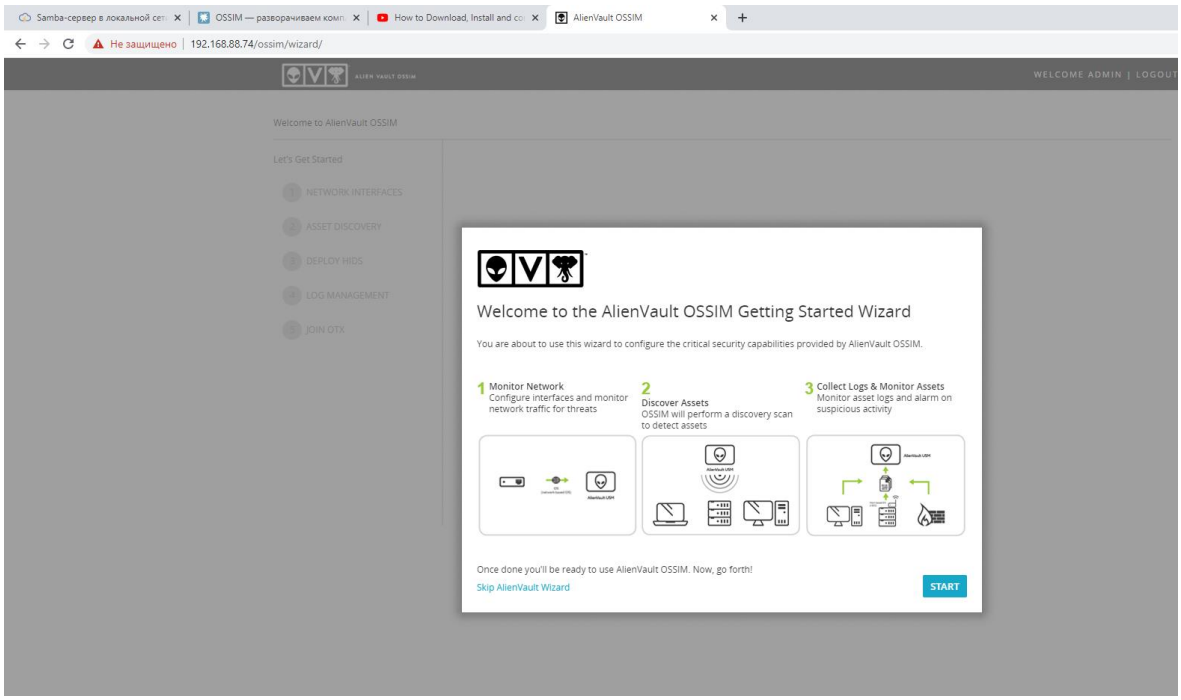


Рисунок 2.34 – Мастер настройки

Мастер настройки показывает следующие три варианта:

1. Monitor Network — Мониторинг сети (настройка сети, мониторинг которой осуществляет сервер OSSIM);
2. Assets Discovery — Обнаружение устройств (Автоматическое обнаружение сетевых устройств в организации);

3. Collecting logs and monitoring of network nodes — Сбор логов и мониторинг сетевых узлов.

Для настройки сервера OSSIM требуется нажать на кнопку «START» на рисунке 2.34. После нажатия другое окно запросит конфигурацию сети, которая показана на рисунке 2.35. Были настроены интерфейсы: “eth1” - для сборщика логов и мониторинга сети, а также для управления сервером OSSIM.

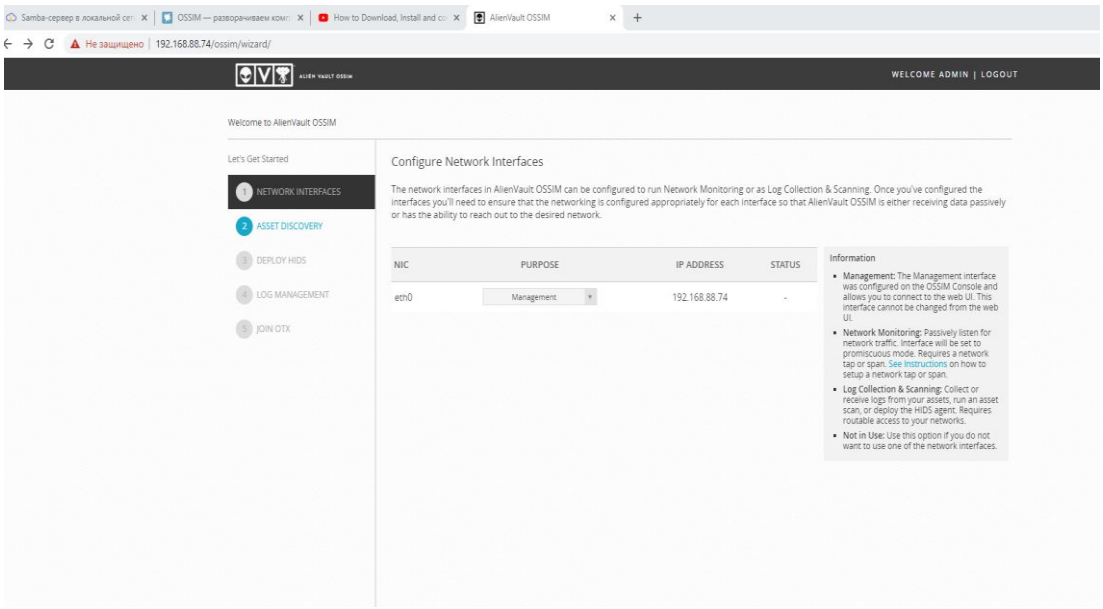


Рисунок 2.35 – Настройка сети

На втором этапе OSSIM выполнит автоматическое обнаружение сетевых устройств(рисунок 2.36). Оно поддерживает автоматическое и ручное обнаружение устройств.

Существует три типа хостов в системе OSSIM:

- Windows;
- Linux;
- Сетевое устройство.

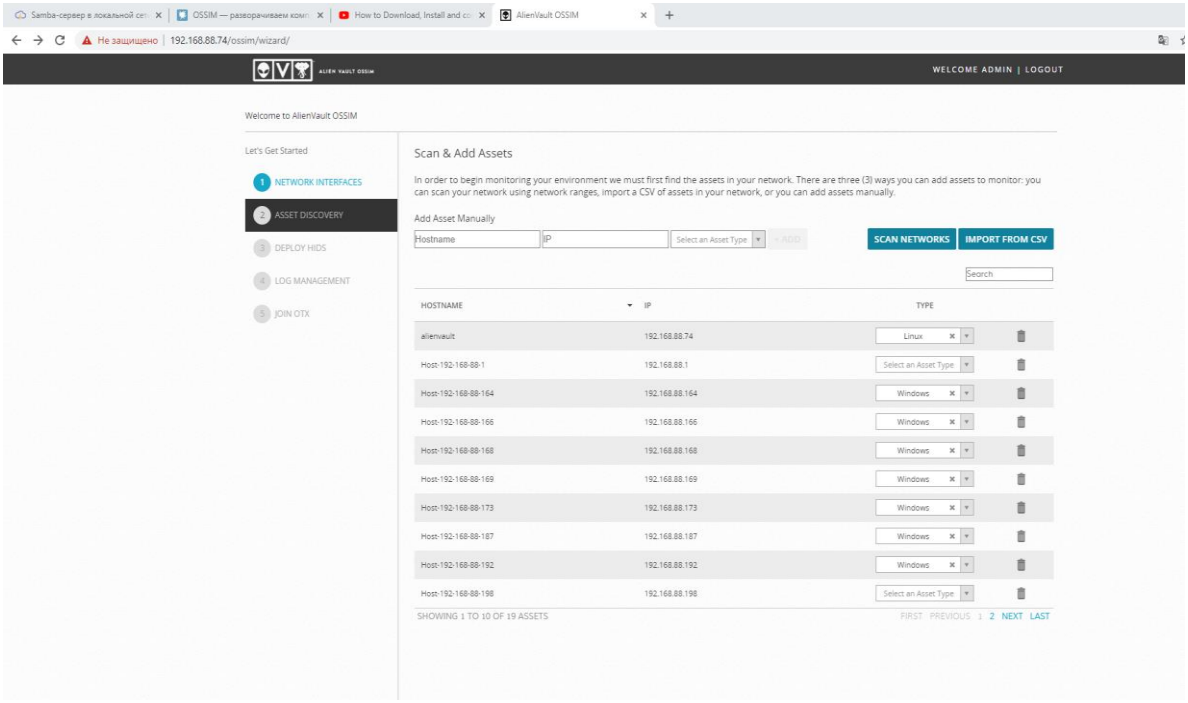


Рисунок 2.36 – Поиск активов

После настройки сети и обнаружения устройств следующим шагом является развертывание хостовой системы обнаружения вторжении то есть установка агентов на устройства Windows и Linux для обеспечения целостности файлов, мониторинга, обнаружения руткитов и сбора логов событий, а также добавление сетевых устройств, устройств безопасности и сервера для сбора логов с этих устройств. Эти пункты показаны как “Log Management” и “Deploy HIDS” на рисунке 2.37. Эти шаги также последний шаг(присоединение к базе с угрозами OTX), пропускаем так как их можно настроить позже.

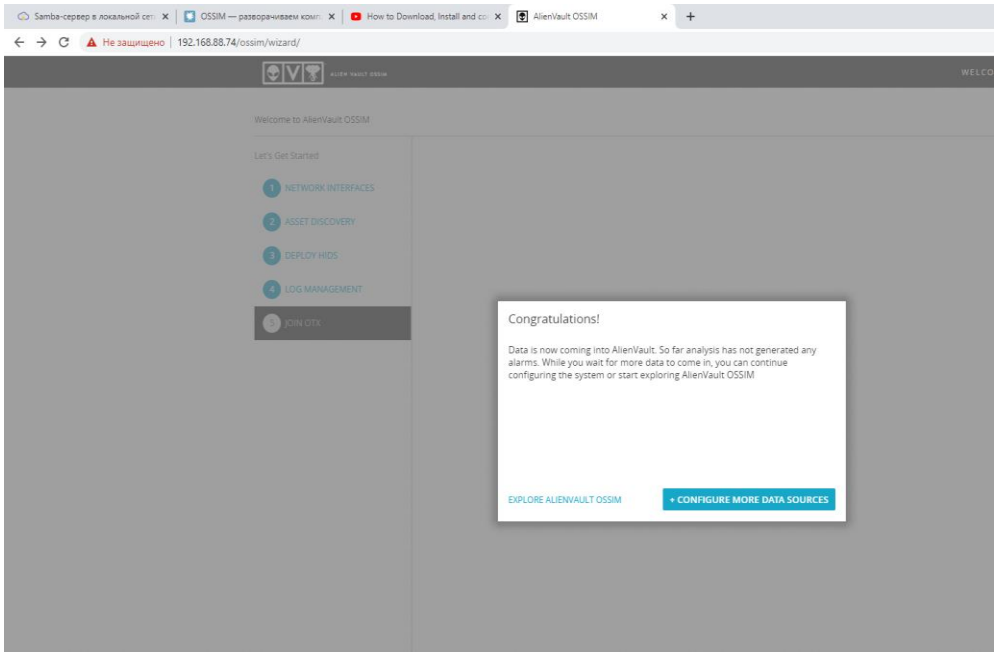


Рисунок 2.37 – Успешное завершение конфигурации

Далее после утверждения ввода данных появится основная панель управления сервером OSSIM которая показана ниже на рисунке 2.38

Основная панель управления сервером OSSIM состоит из следующих опций в основном графическом интерфейсе:

- Дашборд(Dashboard);
- Анализ(Analysis);
- Среды(Environment);
- Отчеты(Reports);
- Конфигурация(Configuration).

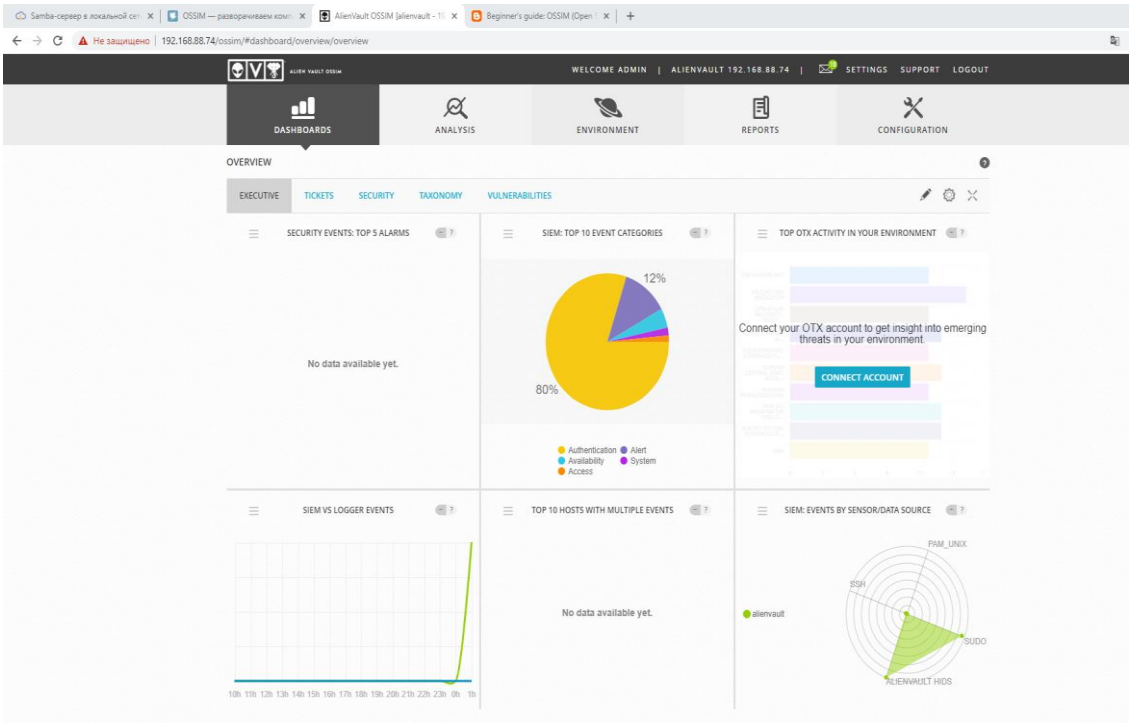


Рисунок 2.38 – Вид на веб-интерфейс системы

Дашборд

Этот раздел показывает полное представление обо всех компонентах сервера OSSIM, таких как серьезность угрозы, уязвимости в сетевом узле, состояние развертывания, карты рисков и статистика OTX. Подменю дашборда показаны на следующем рисунке 2.39.

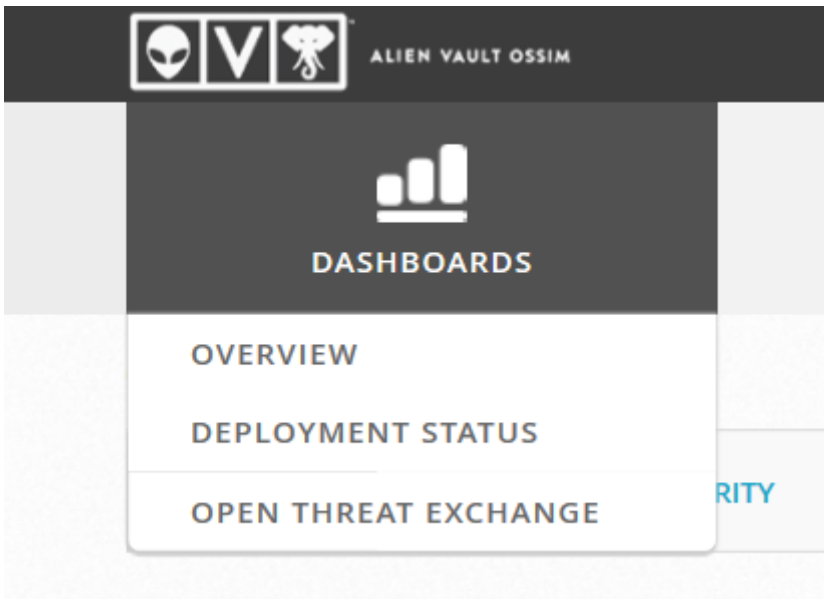


Рисунок 2.39 – Раздел дашборда

Анализ

Анализ 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. Меню анализа далее разделено на следующие подменю рисунок 2.40.

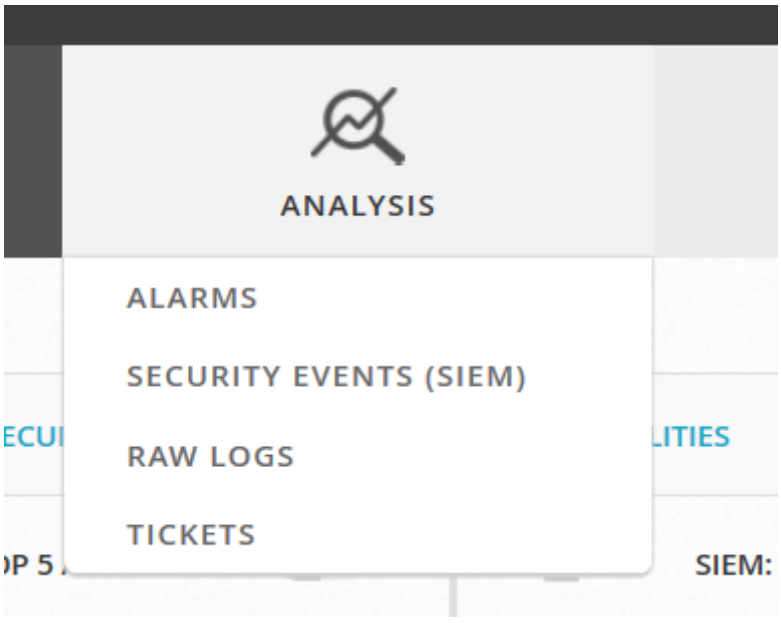


Рисунок 2.40 –Раздел анализа

Среда

В этом меню сервера OSSIM настройки связаны с устройствами организации. Оно показывает устройства, группу и сеть, уязвимости, сетевой

поток и настройки обнаружения. Подменю для всех этих настроек показаны на рисунке ниже, рисунок 2.41:

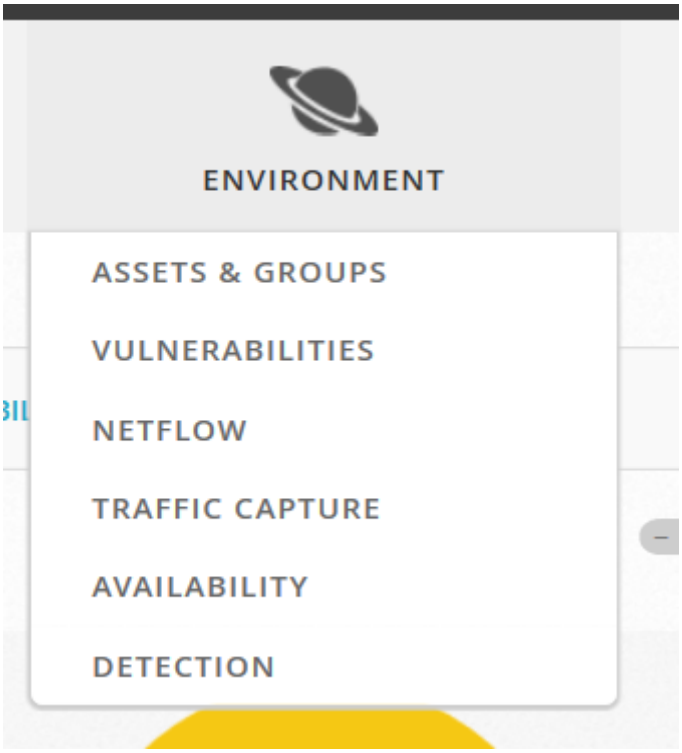


Рисунок 2.41 –Раздел среды

Отчеты

Отчетность является важным компонентом любого сервера регистрации. Сервер OSSIM также генерирует отчеты, которые очень полезны для детального исследования любого конкретного хоста, рисунок 2.42.

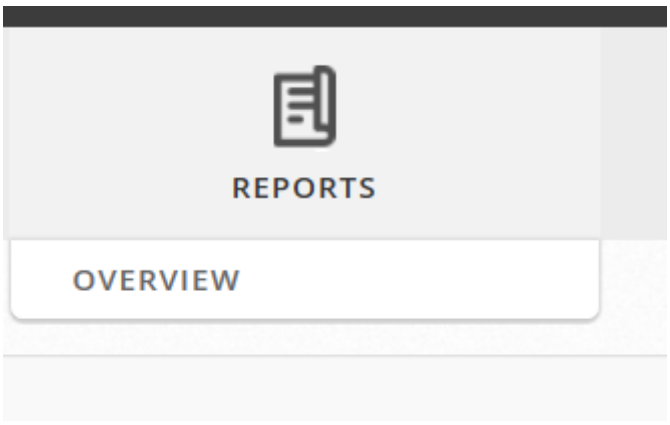


Рисунок 2.42 - Раздел отчета

Конфигурация

В меню конфигурации для установки и настройки AlienVault SIEM

(OSSIM) пользователь может изменить настройку сервера OSSIM, например, изменить IP-адрес интерфейса управления, добавить дополнительный хост для мониторинга и логирования, а также добавить/удалить различные датчики или плагины. Подменю для всех сервисов показано на рисунке 2.43.

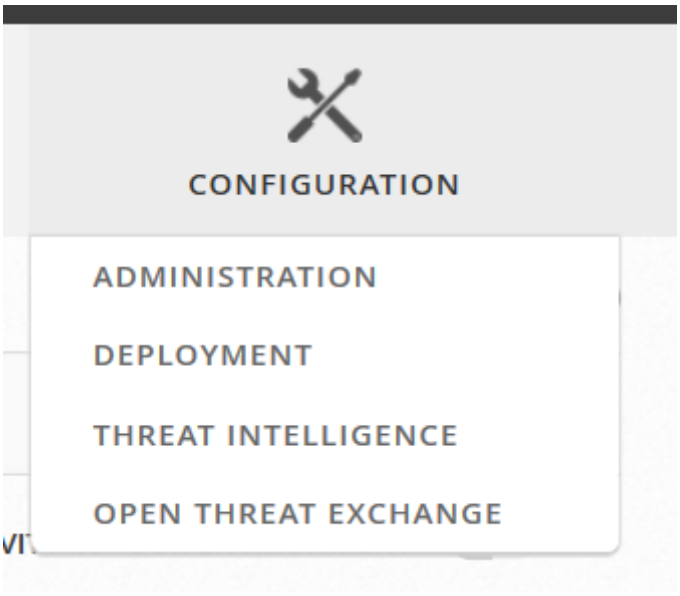


Рисунок 2.43 – Раздел конфигурации

2.7 Регистрация OTX

Для следующего шага нужен ключ OTX. OTX - это платформа разведки угроз по всему миру. Благодаря этой базе можно защитить свое устройство от глобальных угроз. Для этого нужен уникальный ключ, чтобы получать обновления от OTX. Сперва нужно создать учетную запись на сайте AlienVault, рисунок 2.44.

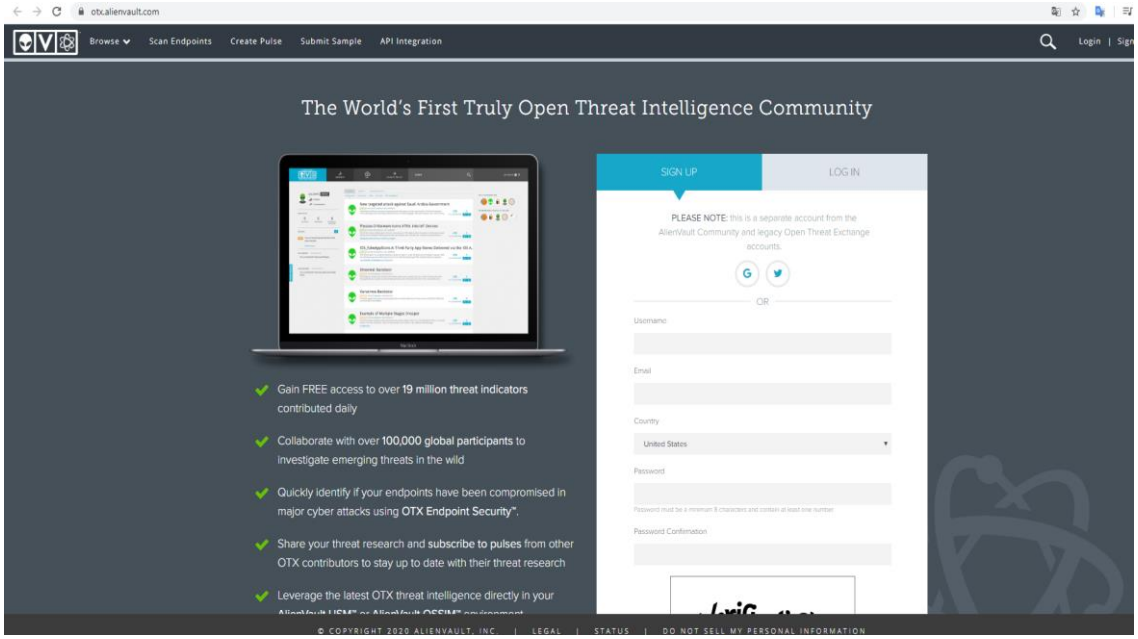


Рисунок 2.44– Переход на сайт AlienVault

После входа в систему необходимо перейти во вкладку настройки и скопировать ключ , рисунках 2.45, 2.46, 2.47.

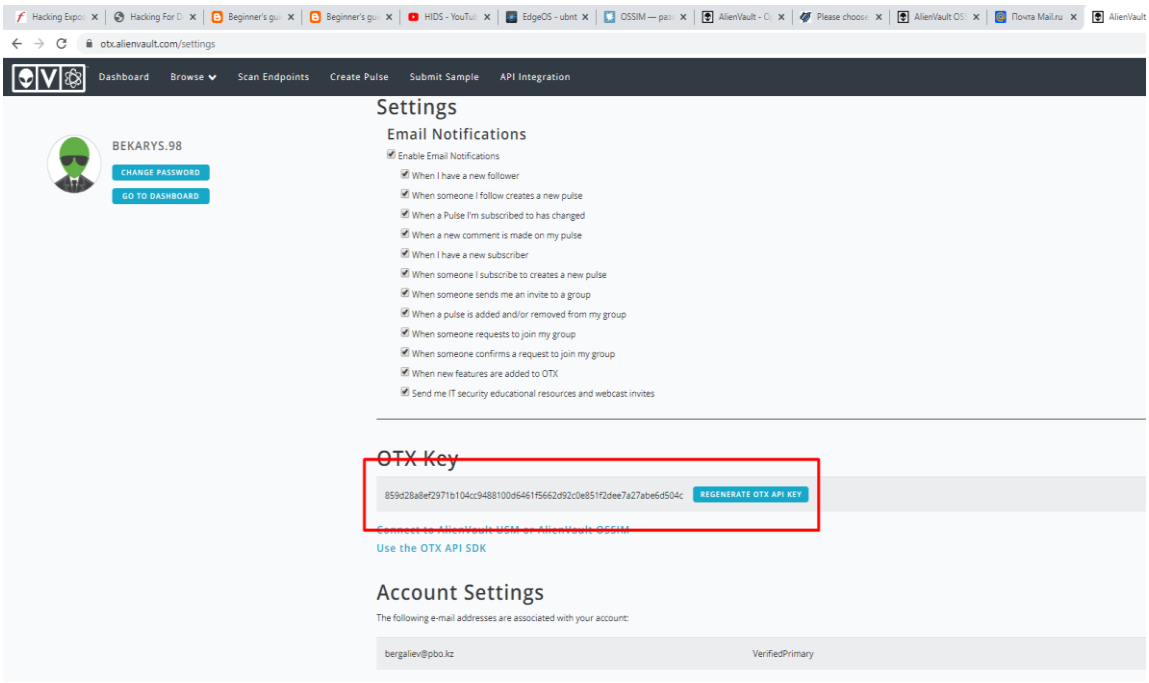


Рисунок 2.45 – ключ OTX

Затем нужно вернуться в веб-интерфейс OSSIM и вставить туда ключ. После успешного подтверждения ключа система будет подключена к базе с уязвимостями.

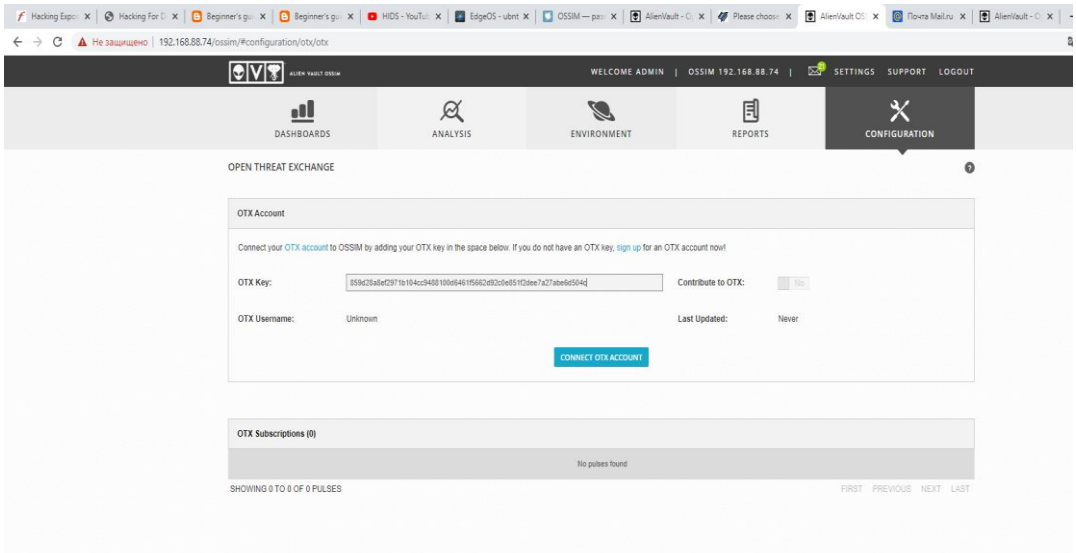


Рисунок 2.46– Ввод ключа в систему

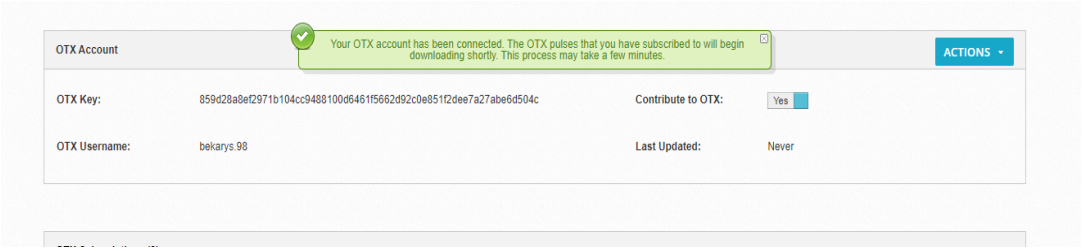


Рисунок 2.47 – Успешное подключение к системе

2.8 Добавление и сканирование активов

Все, что имеет IP-адрес, может называться активом. Активы такие как: мобильные устройства, сервера и IP-камеры, сетевые принтеры и т.д могут быть добавлены в OSSIM. Для демонстрации было отсканировано все устройства в сети. Чтобы добавить активы, нужно перейти в меню «Среда > активы и группы > добавить активы». Существует 4 способа добавления активов. В нашем случае был использован 4-й метод «Сканирование новых активов», который является быстрым и простым методом добавления активов, рисунках 2.48, 2.49, 2.50, 2.51, 2.52, 2.53.

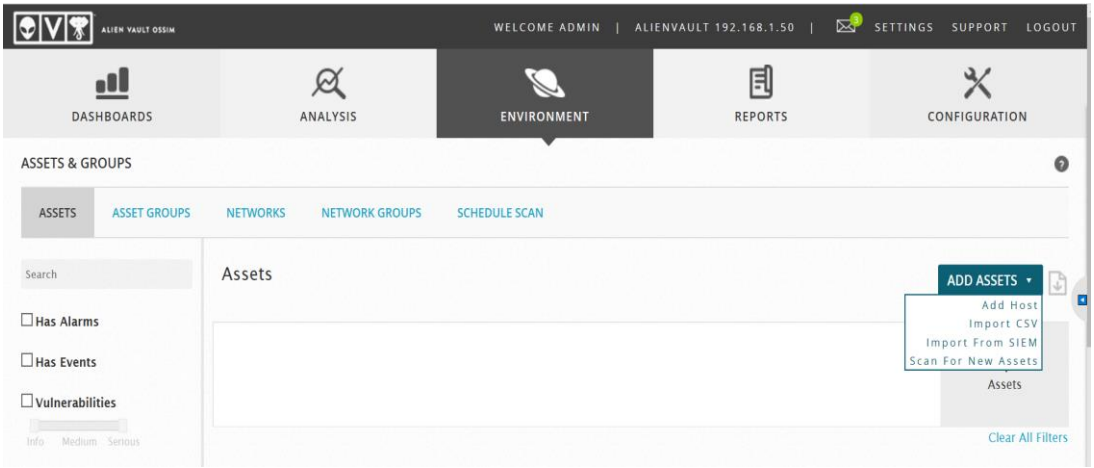


Рисунок 2.48 – Добавление активов

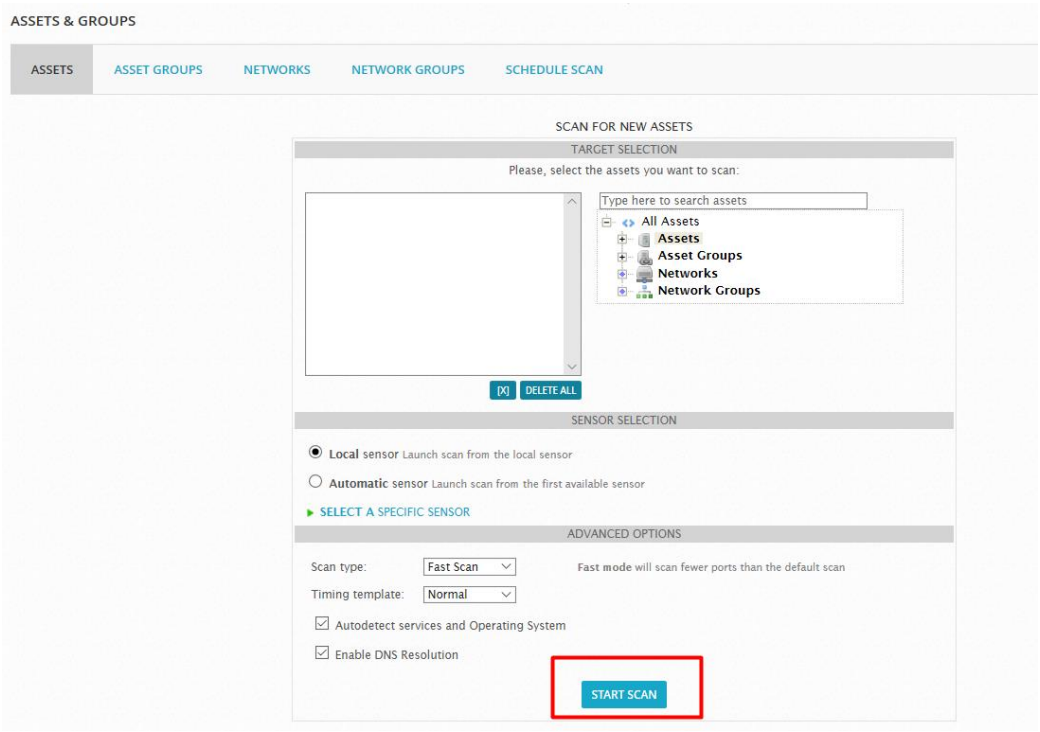
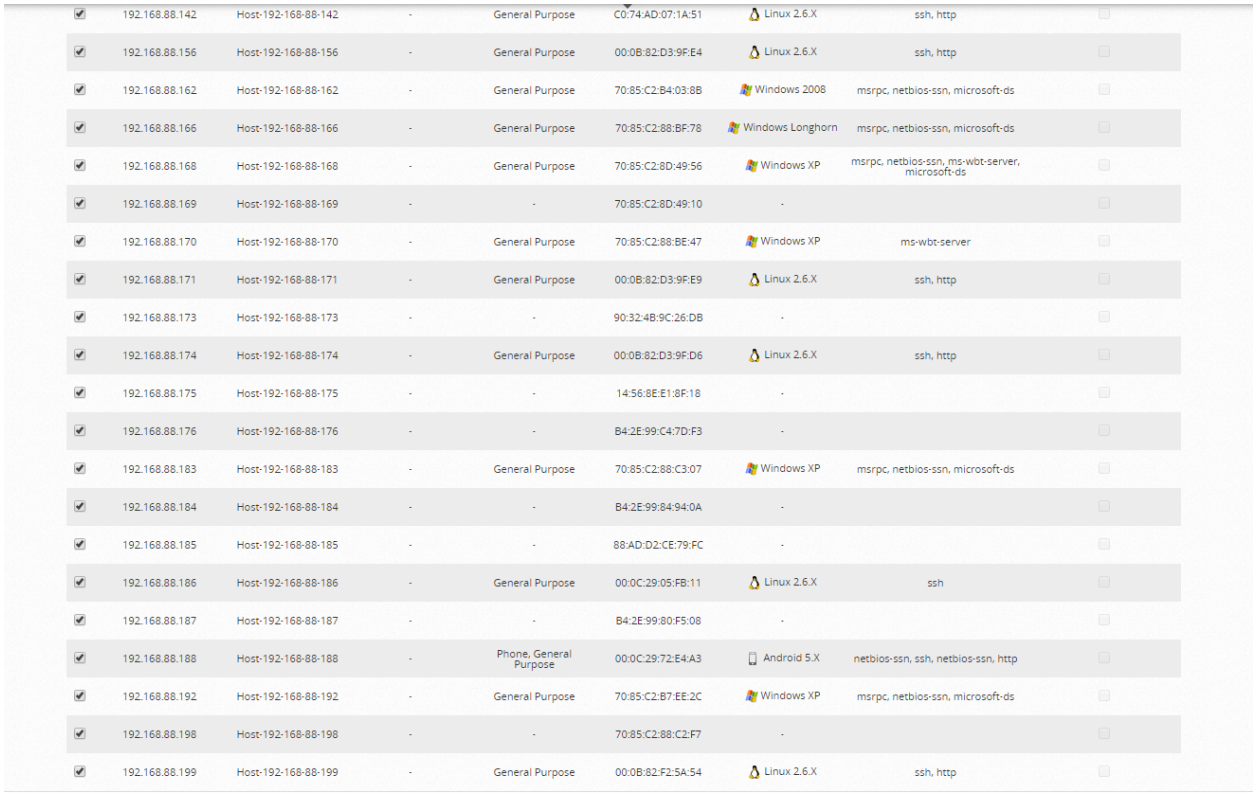


Рисунок 2.49 – Начало сканирования

SCAN RESULTS

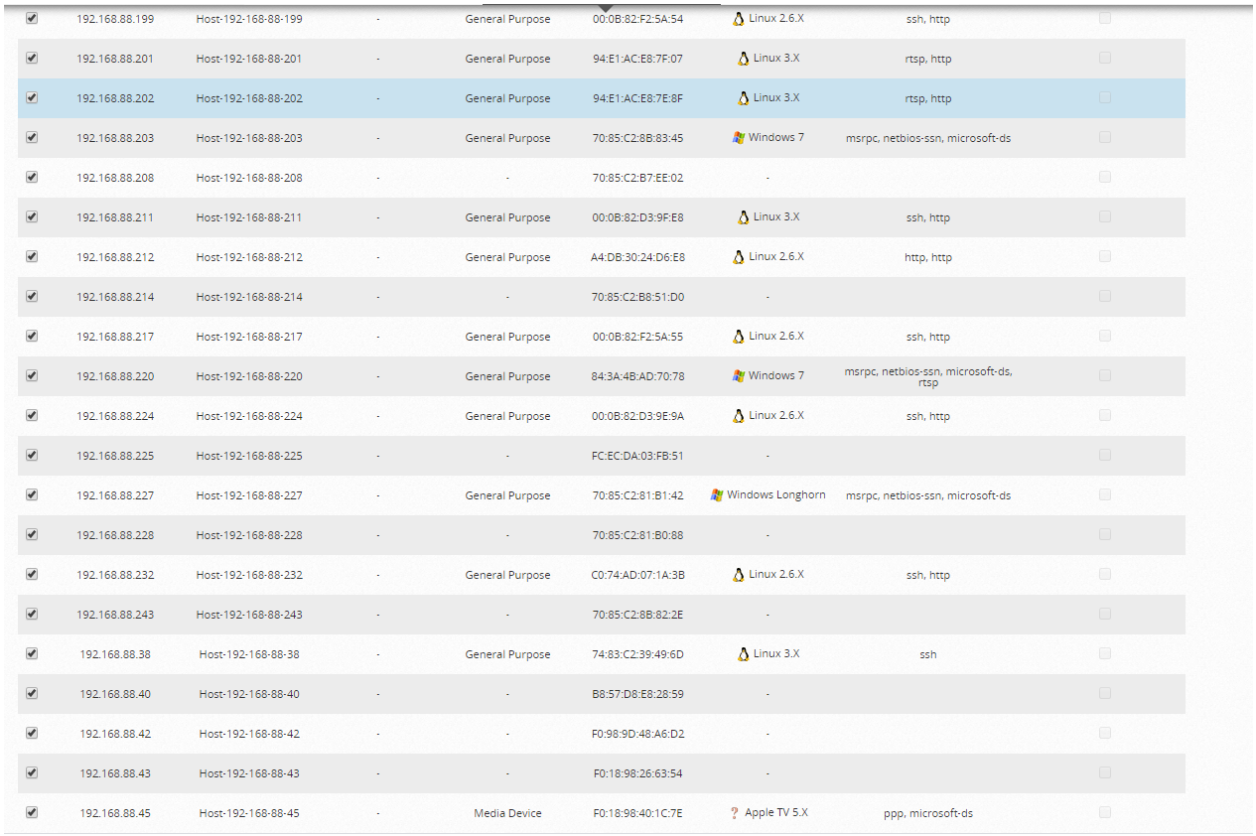
HOST	HOSTNAME	FQDN	DEVICE TYPES	MAC	OS	SERVICES	FQDN AS HOSTNAME
192.168.88.1	Host-192-168-88-1	-	General Purpose	FC:EC:DA:03:FB:51	Linux 3.X	ssh, https, domain, http	
192.168.88.10	Host-192-168-88-10	-	Specialized	00:22:19:65:22:68	ESXi 6.X	https, http	
192.168.88.100	Host-192-168-88-100	pbo-1c	General Purpose	00:0C:29:72:E4:A3	Linux 2.6.X	netbios-ssn, ssh, netbios-ssn, http	
192.168.88.101	Host-192-168-88-101	-	General Purpose	00:0C:29:05:FB:11	Linux 2.6.X	ssh	
192.168.88.102	Host-192-168-88-102	-	General Purpose	B8:27:EB:E9:0E:64	Linux 3.X	ssh	
192.168.88.104	Host-192-168-88-104	-	General Purpose	50:E5:49:86:45:F3	Linux 3.X	netbios-ssn, ssh, netbios-ssn	
192.168.88.105	Host-192-168-88-105	-	General Purpose	FC:4D:D4:D7:F0:79	Linux 2.6.X	netbios-ssn, ssh, netbios-ssn, http	
192.168.88.106	Host-192-168-88-106	-	General Purpose	00:0B:82:E2:9D:7A	Linux 2.6.X	ssh, http	
192.168.88.109	Host-192-168-88-109	-	-	70:85:C2:B4:0B:37	-		
192.168.88.113	Host-192-168-88-113	-	-	80:91:33:58:23:07	-		
192.168.88.118	Host-192-168-88-118	-	General Purpose	70:85:C2:B4:03:87	Windows XP	msrpc, netbios-ssn, microsoft-ds	
192.168.88.138	Host-192-168-88-138	-	-	00:B5:D0:2C:A1:89	-		
192.168.88.139	Host-192-168-88-139	-	General Purpose	00:0B:82:D3:9F:E1	Linux 2.6.X	ssh, http	
192.168.88.142	Host-192-168-88-142	-	General Purpose	C0:74:AD:07:1A:51	Linux 2.6.X	ssh, http	

Рисунок 2.50 – Отсканированные устройства



☑	192.168.88.142	Host-192-168-88-142	-	General Purpose	C0:74:AD:07:1A:51	Linux 2.6.X	ssh, http	
☑	192.168.88.156	Host-192-168-88-156	-	General Purpose	00:0B:82:D3:9F:E4	Linux 2.6.X	ssh, http	
☑	192.168.88.162	Host-192-168-88-162	-	General Purpose	70:85:C2:B4:03:8B	Windows 2008	msrpc, netbios-ssn, microsoft-ds	
☑	192.168.88.166	Host-192-168-88-166	-	General Purpose	70:85:C2:88:BF:78	Windows Longhorn	msrpc, netbios-ssn, microsoft-ds	
☑	192.168.88.168	Host-192-168-88-168	-	General Purpose	70:85:C2:8D:49:56	Windows XP	msrpc, netbios-ssn, ms-wbt-server, microsoft-ds	
☑	192.168.88.169	Host-192-168-88-169	-	-	70:85:C2:8D:49:10	-		
☑	192.168.88.170	Host-192-168-88-170	-	General Purpose	70:85:C2:88:BE:47	Windows XP	ms-wbt-server	
☑	192.168.88.171	Host-192-168-88-171	-	General Purpose	00:0B:82:D3:9F:E9	Linux 2.6.X	ssh, http	
☑	192.168.88.173	Host-192-168-88-173	-	-	90:32:4B:9C:26:DB	-		
☑	192.168.88.174	Host-192-168-88-174	-	General Purpose	00:0B:82:D3:9F:D6	Linux 2.6.X	ssh, http	
☑	192.168.88.175	Host-192-168-88-175	-	-	14:56:8E:E1:8F:18	-		
☑	192.168.88.176	Host-192-168-88-176	-	-	B4:2E:99:C4:7D:F3	-		
☑	192.168.88.183	Host-192-168-88-183	-	General Purpose	70:85:C2:88:C3:07	Windows XP	msrpc, netbios-ssn, microsoft-ds	
☑	192.168.88.184	Host-192-168-88-184	-	-	B4:2E:99:84:94:0A	-		
☑	192.168.88.185	Host-192-168-88-185	-	-	88:AD:D2:CE:79:FC	-		
☑	192.168.88.186	Host-192-168-88-186	-	General Purpose	00:0C:29:05:FB:11	Linux 2.6.X	ssh	
☑	192.168.88.187	Host-192-168-88-187	-	-	B4:2E:99:80:F5:08	-		
☑	192.168.88.188	Host-192-168-88-188	-	Phone, General Purpose	00:0C:29:72:E4:A3	Android 5.X	netbios-ssn, ssh, netbios-ssn, http	
☑	192.168.88.192	Host-192-168-88-192	-	General Purpose	70:85:C2:B7:EE:2C	Windows XP	msrpc, netbios-ssn, microsoft-ds	
☑	192.168.88.198	Host-192-168-88-198	-	-	70:85:C2:88:C2:F7	-		
☑	192.168.88.199	Host-192-168-88-199	-	General Purpose	00:0B:82:F2:5A:54	Linux 2.6.X	ssh, http	

Рисунок 2.51 – Отсканированные устройства



☑	192.168.88.199	Host-192-168-88-199	-	General Purpose	00:0B:82:F2:5A:54	Linux 2.6.X	ssh, http	
☑	192.168.88.201	Host-192-168-88-201	-	General Purpose	94:E1:AC:E8:7F:07	Linux 3.X	rtsp, http	
☑	192.168.88.202	Host-192-168-88-202	-	General Purpose	94:E1:AC:E8:7E:8F	Linux 3.X	rtsp, http	
☑	192.168.88.203	Host-192-168-88-203	-	General Purpose	70:85:C2:8B:83:45	Windows 7	msrpc, netbios-ssn, microsoft-ds	
☑	192.168.88.208	Host-192-168-88-208	-	-	70:85:C2:B7:EE:02	-		
☑	192.168.88.211	Host-192-168-88-211	-	General Purpose	00:0B:82:D3:9F:E8	Linux 3.X	ssh, http	
☑	192.168.88.212	Host-192-168-88-212	-	General Purpose	A4:DB:30:24:D6:E8	Linux 2.6.X	http, http	
☑	192.168.88.214	Host-192-168-88-214	-	-	70:85:C2:B8:51:D0	-		
☑	192.168.88.217	Host-192-168-88-217	-	General Purpose	00:0B:82:F2:5A:55	Linux 2.6.X	ssh, http	
☑	192.168.88.220	Host-192-168-88-220	-	General Purpose	84:3A:4B:AD:70:78	Windows 7	msrpc, netbios-ssn, microsoft-ds, rtsp	
☑	192.168.88.224	Host-192-168-88-224	-	General Purpose	00:0B:82:D3:9E:9A	Linux 2.6.X	ssh, http	
☑	192.168.88.225	Host-192-168-88-225	-	-	FC:EC:DA:03:FB:51	-		
☑	192.168.88.227	Host-192-168-88-227	-	General Purpose	70:85:C2:81:B1:42	Windows Longhorn	msrpc, netbios-ssn, microsoft-ds	
☑	192.168.88.228	Host-192-168-88-228	-	-	70:85:C2:81:B0:88	-		
☑	192.168.88.232	Host-192-168-88-232	-	General Purpose	C0:74:AD:07:1A:3B	Linux 2.6.X	ssh, http	
☑	192.168.88.243	Host-192-168-88-243	-	-	70:85:C2:8B:82:2E	-		
☑	192.168.88.38	Host-192-168-88-38	-	General Purpose	74:83:C2:39:49:6D	Linux 3.X	ssh	
☑	192.168.88.40	Host-192-168-88-40	-	-	B8:57:D8:E8:28:59	-		
☑	192.168.88.42	Host-192-168-88-42	-	-	F0:98:9D:48:A6:D2	-		
☑	192.168.88.43	Host-192-168-88-43	-	-	F0:18:98:26:63:54	-		
☑	192.168.88.45	Host-192-168-88-45	-	Media Device	F0:18:98:40:1C:7E	? Apple TV 5.X	ppp, microsoft-ds	

Рисунок 2.52 – Отсканированные устройства

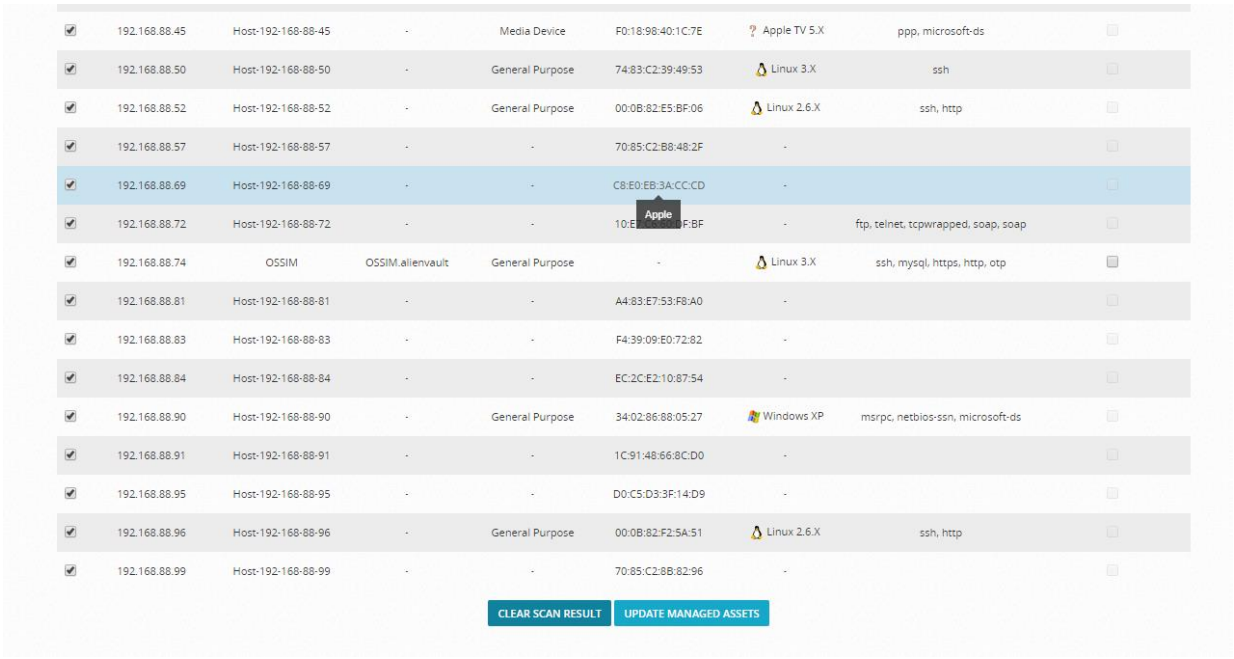


Рисунок 2.53 – Отсканированные устройства

Далее было создана группа с которой была произведена дальнейшая работа, рисунки 2.54, 2.55, 2.56.

Рисунок 2.54 – Создание группы

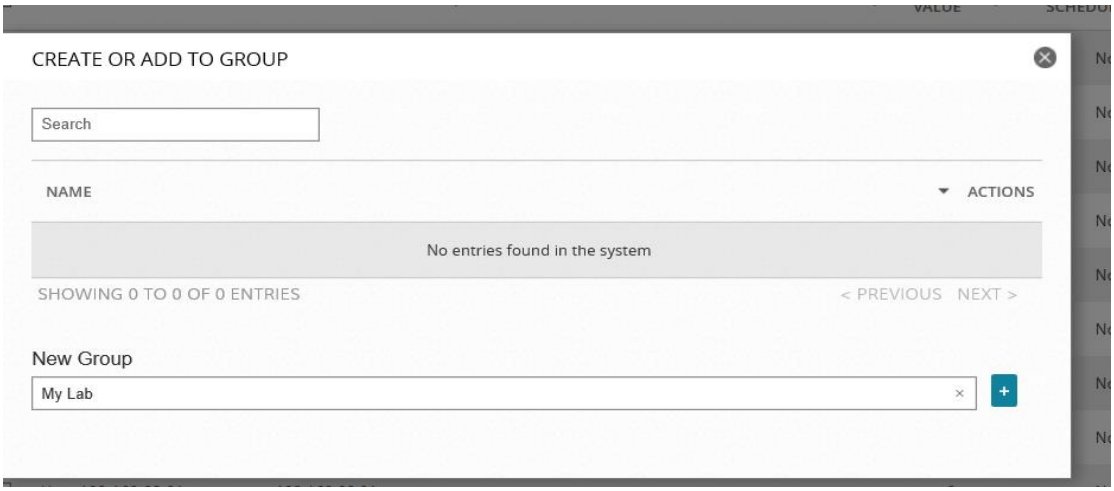


Рисунок 2.55 – Название группы

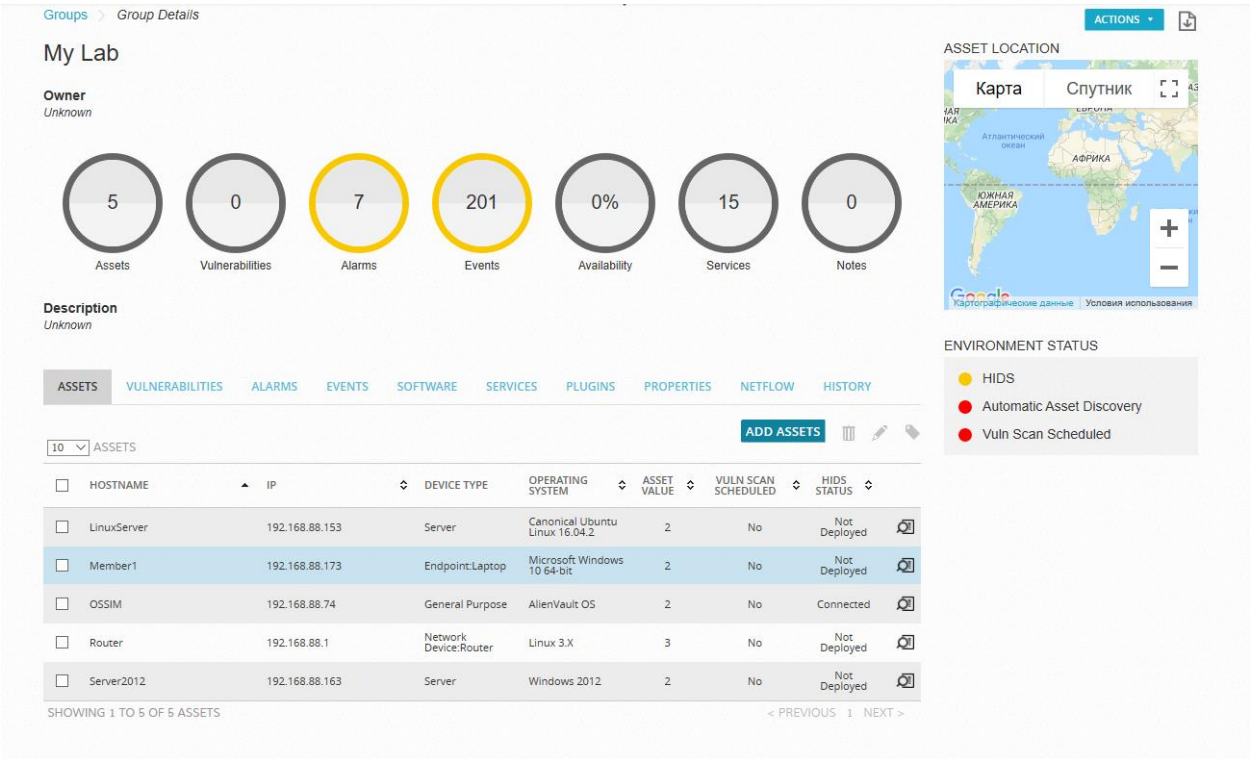


Рисунок 2.56 – Информация о группе

2.9 Внедрение HIDS

Настройка HIDS является следующей задачей. Установка HIDS на устройствах Windows очень проста так как нет необходимости физический устанавливать что либо на устройстве, но сложна при развертывании на устройствах Linux. Для того чтобы настроить хостовую систему нужно перейти в меню «Среда > Обнаружение > добавление агента», во всплывающем окне необходимо заполнить данные актива и нажать «Save» , рисунках 2.57 – 2.63.

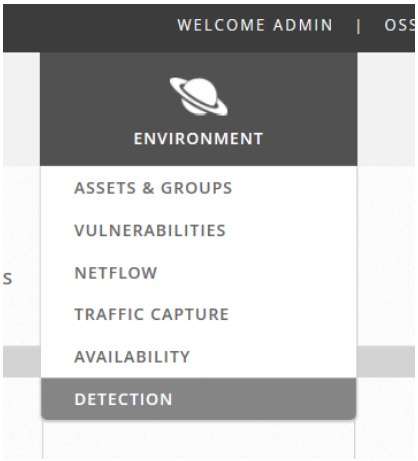


Рисунок 2.57– Переход в меню HIDS

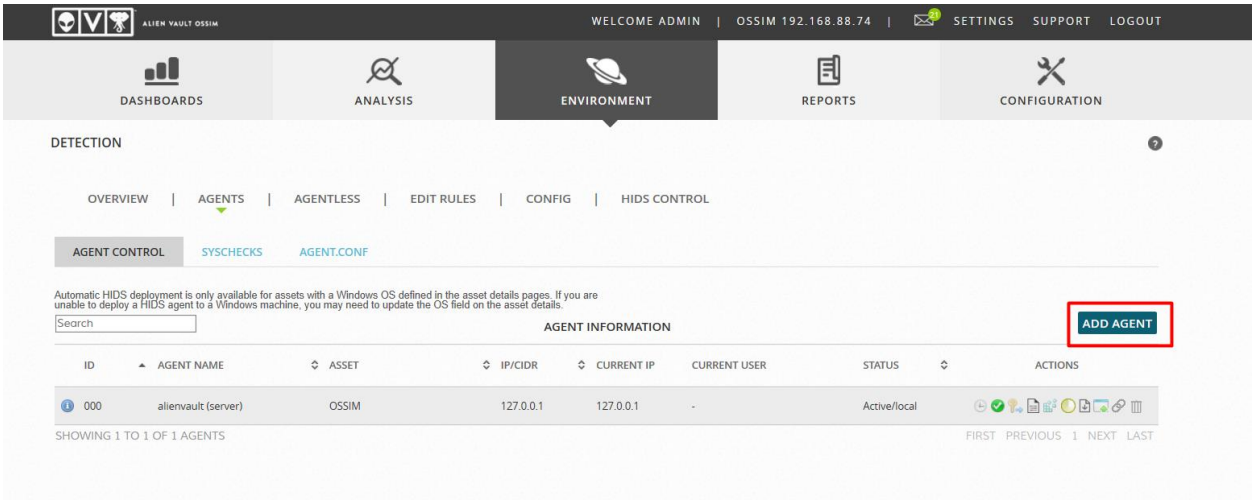


Рисунок 2.58 – Добавление агента

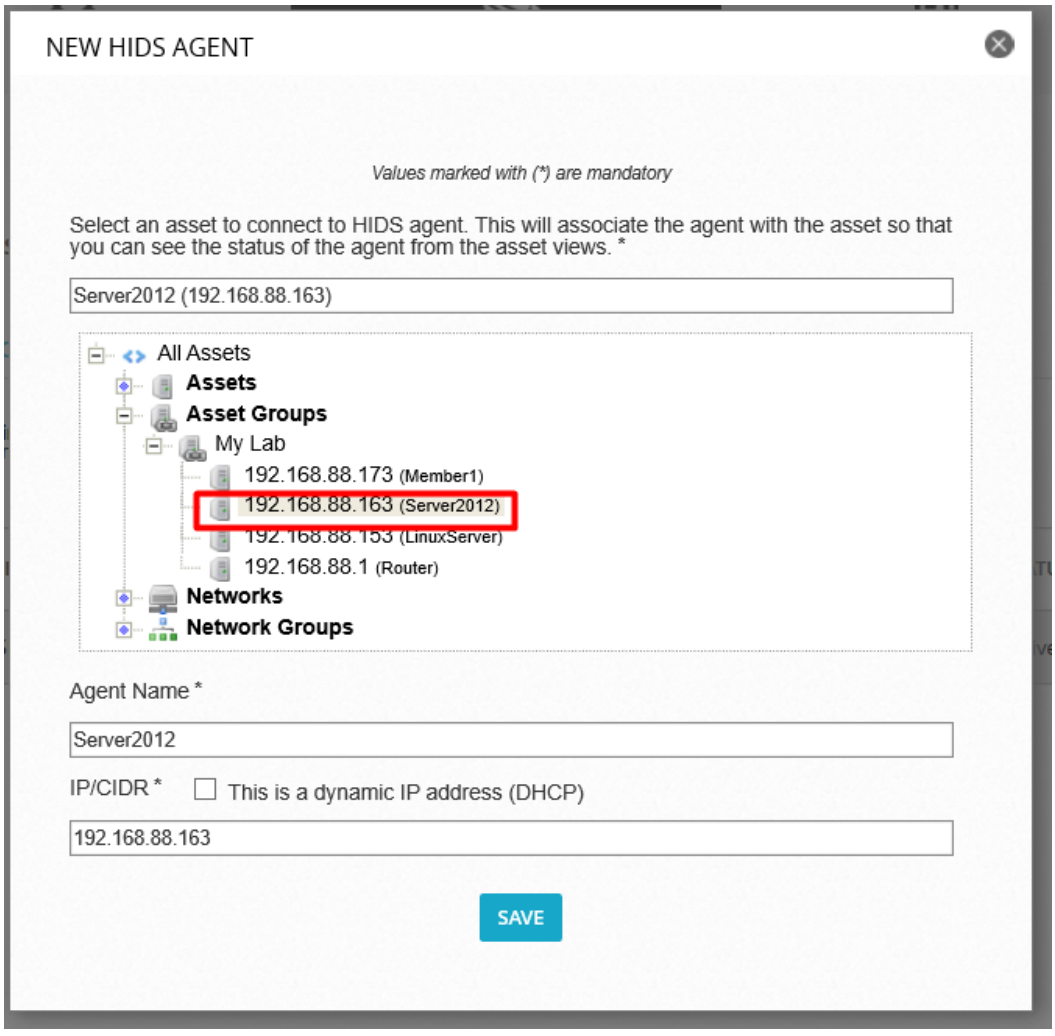


Рисунок 2.59 – Поиск устройства для внедрения агента

Рисунок 2.60 – Автоматическая установка

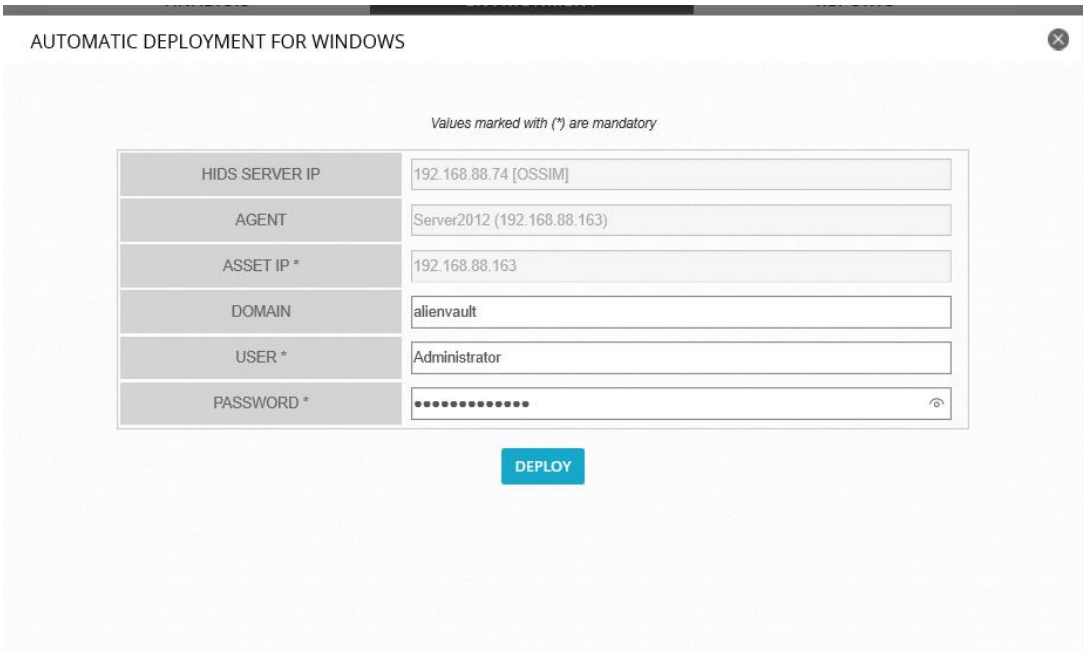


Рисунок 2.61 – Ввод пользовательских данных

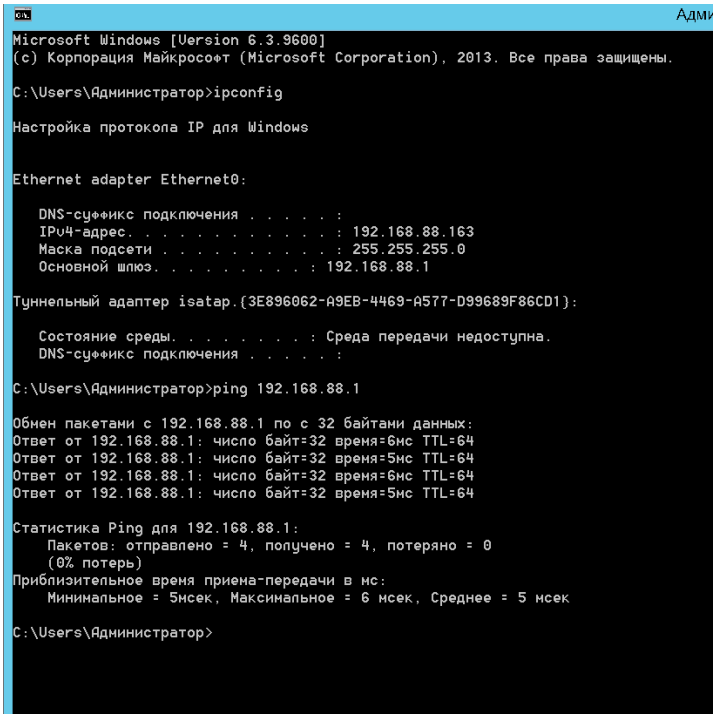


Рисунок 2.62 – Сервер Windows 2012

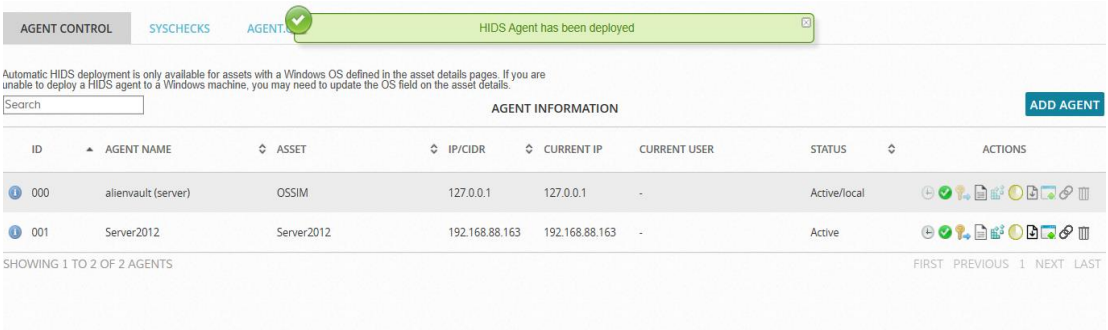


Рисунок 2.63 – Успешная установка

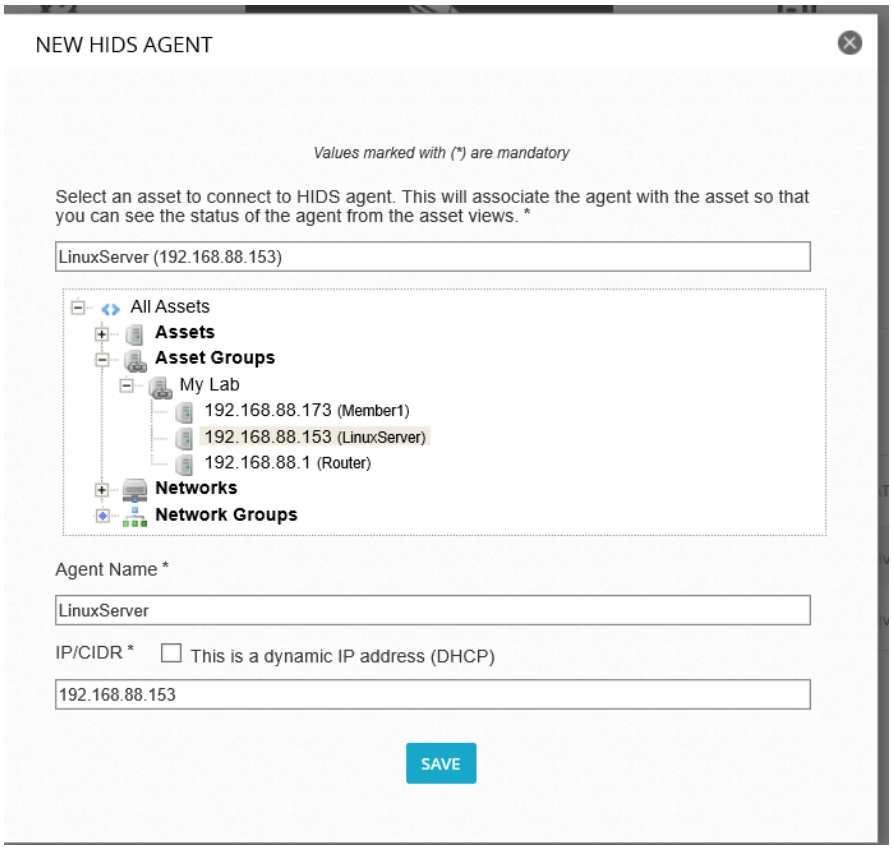


Рисунок 2.64 – Переход в меню HIDS

```
server@server:~/ossec-hids-3.3.0$ wget https://github.com/ossec/ossec-hids/archi
ve/3.3.0.tar.gz
```

Рисунок 2.65 – Скачивание файла

```
server@server:~$ ls
3.3.0.tar.gz  ossec-hids-3.3.0
```

Рисунок 2.66 - Скачанные файлы

```
server@server:~$ cd ossec-hids-3.3.0/
server@server:~/ossec-hids-3.3.0$ sudo ./install.sh
```

Рисунок 2.67 – Запуск скрипта

```
  - User: root
  - Host: server


  -- Press ENTER to continue or Ctrl-C to abort. --


1- What kind of installation do you want (server, agent, local, hybrid or help)? agent

  - Agent(client) installation chosen.

2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]: yes
 - Choose where to install the OSSEC HIDS [/var/ossec]:

    - Installation will be made at  /var/ossec .

3- Configuring the OSSEC HIDS.

  3.1- What's the IP Address or hostname of the OSSEC HIDS server?: 192.168.88.74

   - Adding Server IP 192.168.88.74

  3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

   - Running syscheck (integrity check daemon).

  3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y

   - Running rootcheck (rootkit detection).

  3.4 - Do you want to enable active response? (y/n) [y]: n

   - Active response disabled.

  3.5- Setting the configuration to analyze the following logs:
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/dpkg.log

 - If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .


   --- Press ENTER to continue ---
```

Рисунок 2.68 – Процесс установки

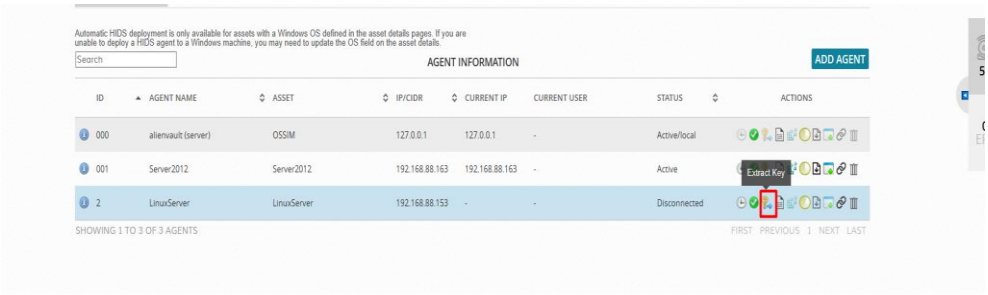


Рисунок 2.69 – Вывод ключа для установки

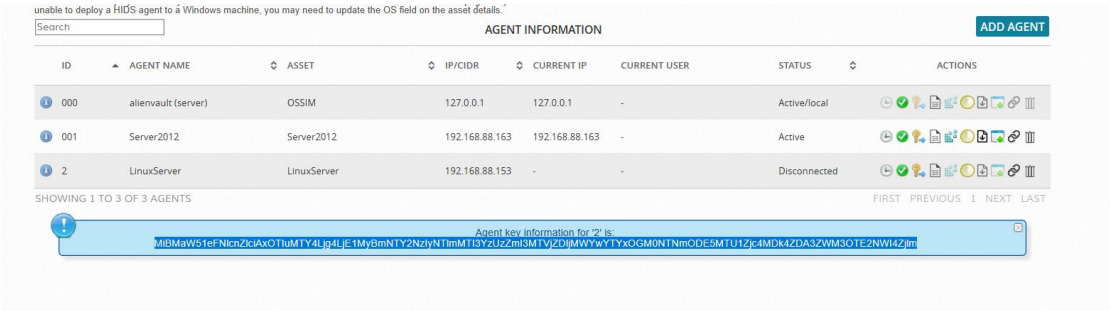


Рисунок 2.70 – Копирование ключа

Рисунок 2.71 – Ввод ключа для установки

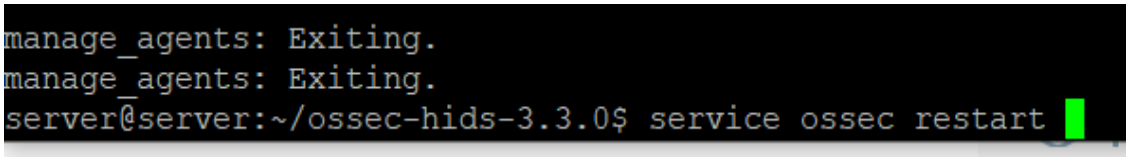


Рисунок 2.72 – Перезагрузка агента OSSEC

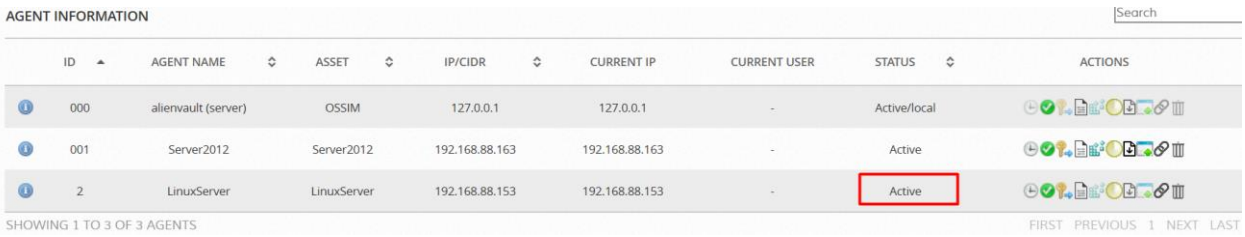


Рисунок 2.73 – Успешная установка агента

2.10 Сканирования хоста на уязвимости

Еще одной функцией системы является сканер уязвимости которая работает при установке HIDS агента на устройства. Она позволяет выявить уязвимые места хоста. Ее можно установить на определенный режим чтобы она сканировала устройства в нужное время. Далее показана сканирование Linux сервера, рисунки 2.74 – 2.77.

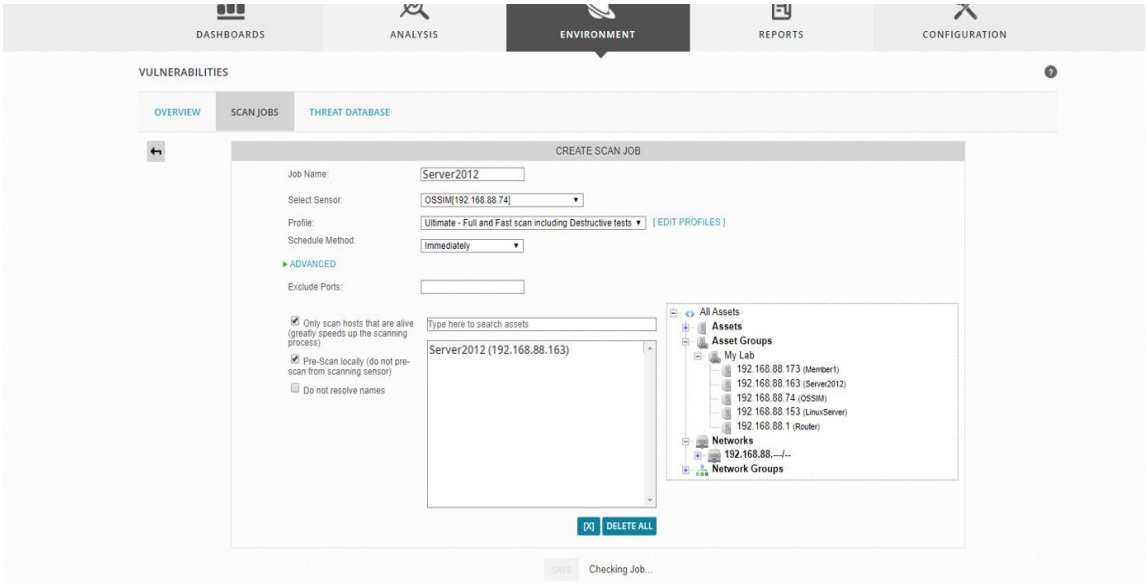


Рисунок 2.74 – Указание хоста

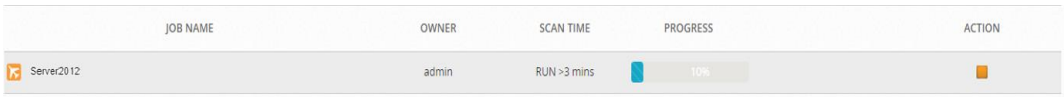


Рисунок 2.75 – Запущенный сканер

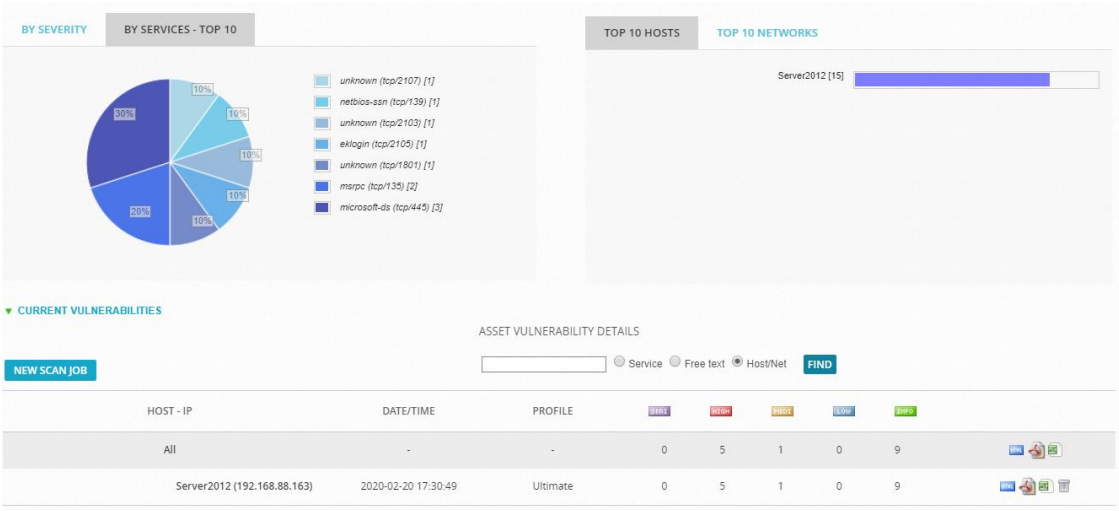


Рисунок 2.76 – Результат по сервисам

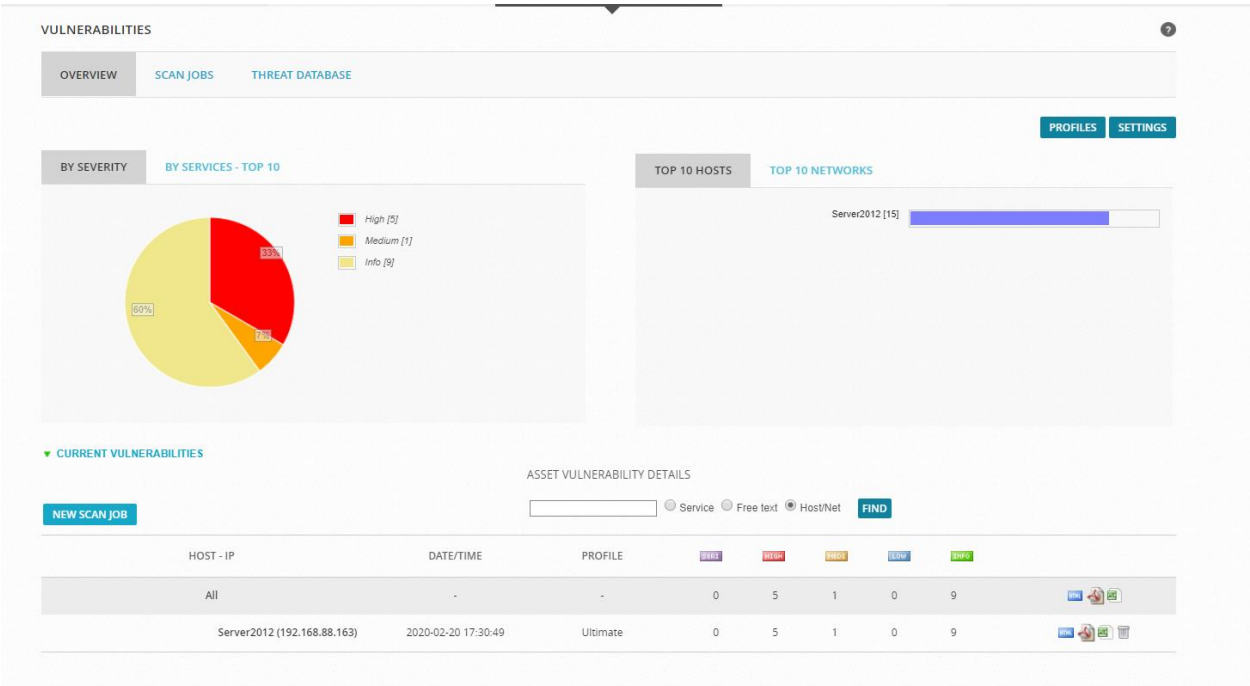


Рисунок 2.77 – Результат по по серьезности

2.11 Атака на сервер

В данном разделе была произведена «Bruteforce» атака на Linux сервер с IP адресом – 192.168.88.153. Для этого была использована ОС Kali Linux на которую была установлен инструмент для атаки “Metasploit Framework”.

```
server@server:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:3b:73:2d
          inet addr:192.168.88.153  Bcast:192.168.88.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3b:732d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1159726 errors:0 dropped:0 overruns:0 frame:0
          TX packets:925079 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:94063321 (94.0 MB)  TX bytes:59047374 (59.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:240 errors:0 dropped:0 overruns:0 frame:0
          TX packets:240 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:26759 (26.7 KB)  TX bytes:26759 (26.7 KB)
```

Рисунок 2.78 – Информация об интерфейсах Linux сервера

```
server@server:~$ sudo service ssh status
[sudo] password for server:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-02-17 03:36:24 EST; 3 days ago
  Process: 982 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 1070 (sshd)
    Tasks: 1
   Memory: 5.5M
      CPU: 43.576s
   CGroup: /system.slice/ssh.service
           └─1070 /usr/sbin/sshd -D
```

Рисунок 2.79 – Включенный сервис SSH

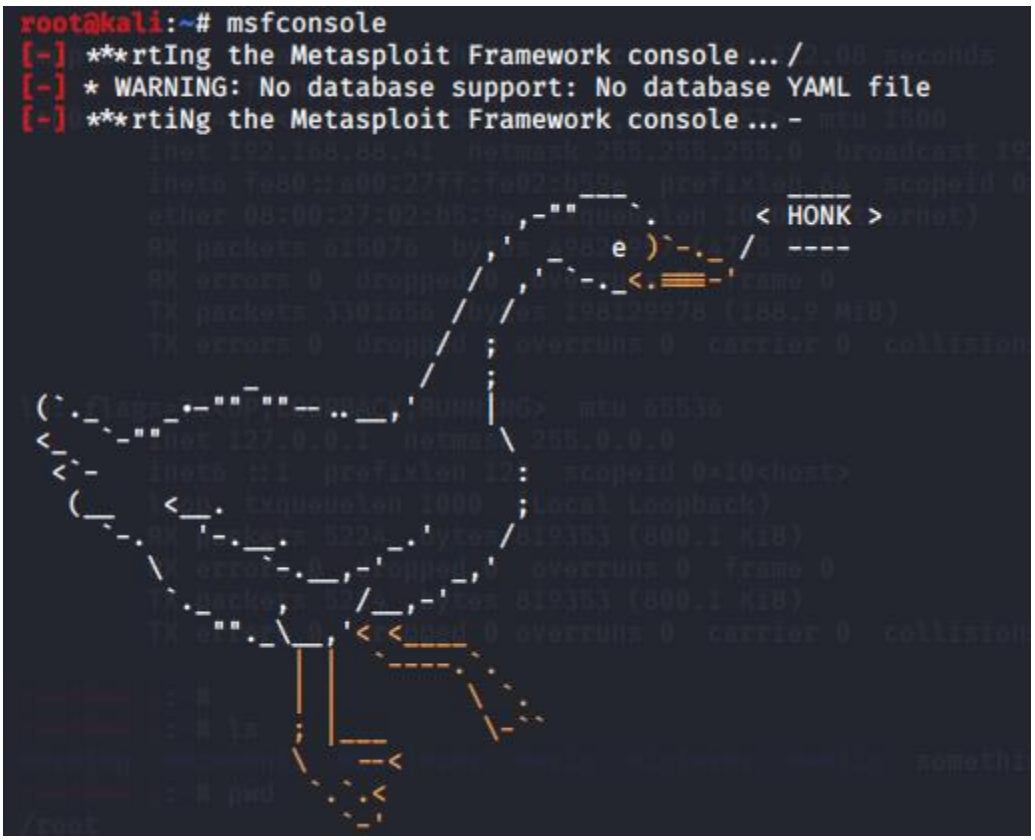


Рисунок 2.80 – Вход в Metasploit Network

На рисунке 2.81, были заданы данные о хосте на которую была произведена атака. «USERPASS_FILE» - файл в котором хранится база ключей, «RHOSTS» - IP атакуемого хоста.

```
msf5 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.88.153
RHOSTS ⇒ 192.168.88.153
msf5 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /root/bruteforce-database/1000000-password-seclists.txt
USERPASS_FILE ⇒ /root/bruteforce-database/1000000-password-seclists.txt
msf5 auxiliary(scanner/ssh/ssh_login) > run
```

Рисунок 2.81 – Задание параметров уязвимого хоста

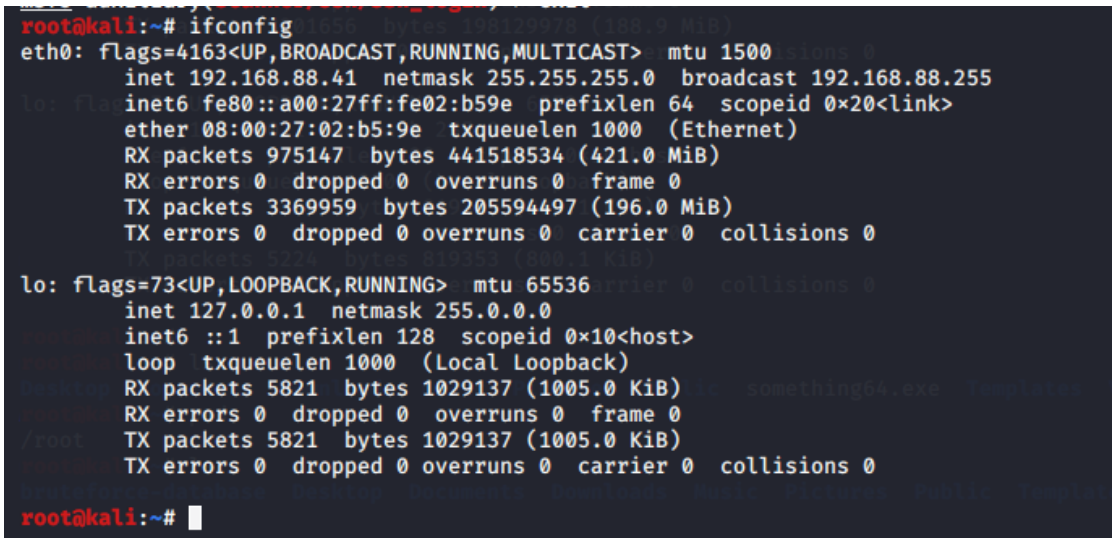


Рисунок 2.82– Информация об интерфейсах Kali Linux

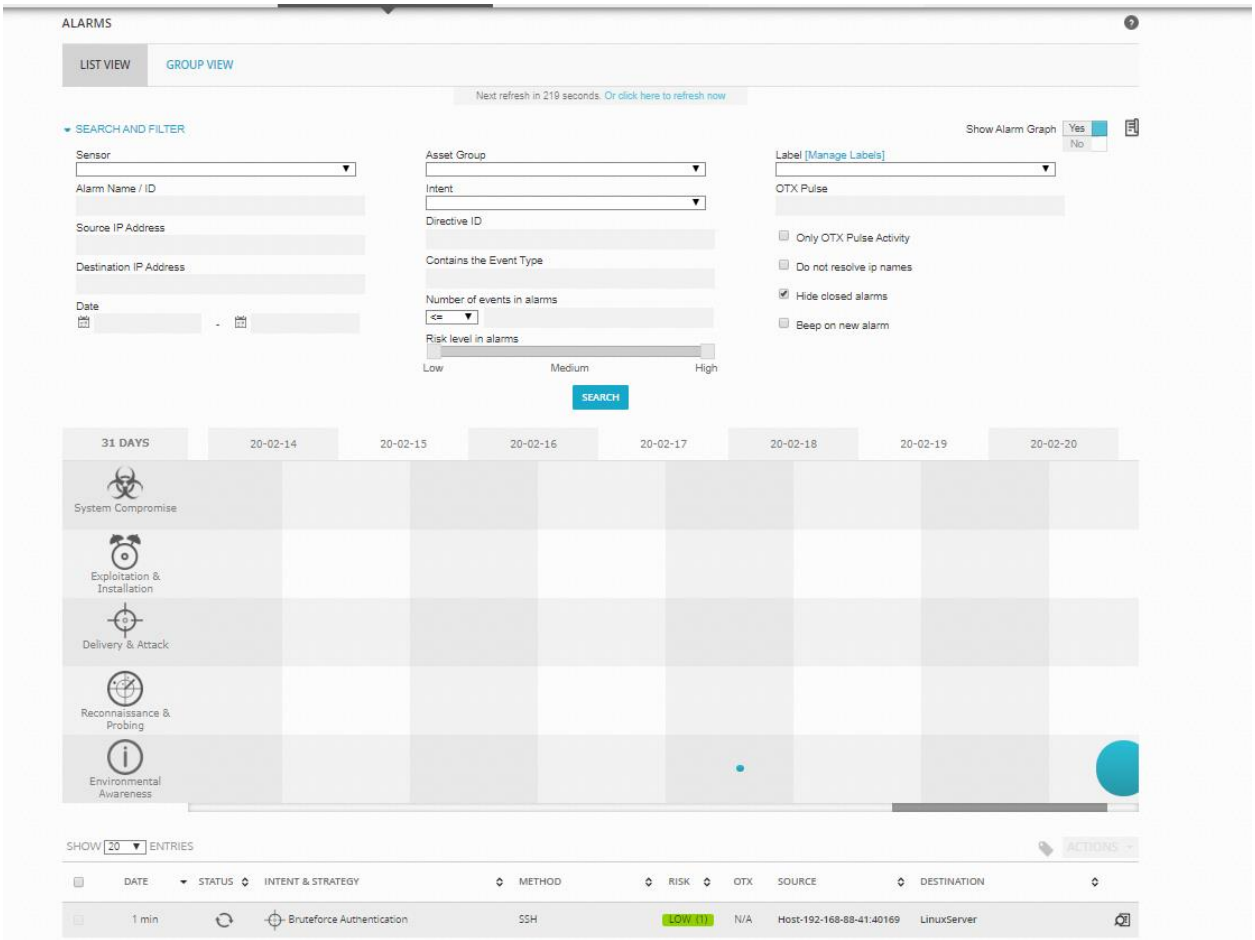


Рисунок 2.83 – Оповещение SIEM системы об атаке

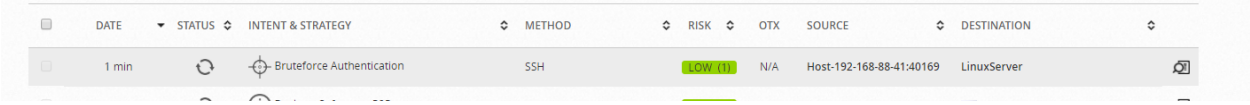
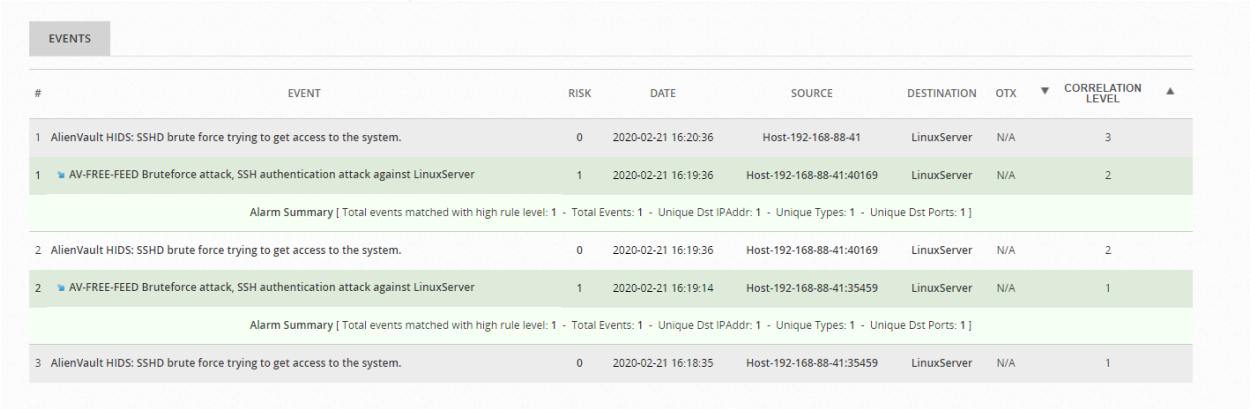


Рисунок 2.84 – «BruteForce» атака



EVENTS

#	EVENT	RISK	DATE	SOURCE	DESTINATION	OTX	CORRELATION LEVEL
1	AlienVault HIDS: SSHD brute force trying to get access to the system.	0	2020-02-21 16:20:36	Host-192-168-88-41	LinuxServer	N/A	3
1	AV-FREE-FEED Bruteforce attack, SSH authentication attack against LinuxServer	1	2020-02-21 16:19:36	Host-192-168-88-41:40169	LinuxServer	N/A	2
	Alarm Summary [Total events matched with high rule level: 1 - Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
2	AlienVault HIDS: SSHD brute force trying to get access to the system.	0	2020-02-21 16:19:36	Host-192-168-88-41:40169	LinuxServer	N/A	2
2	AV-FREE-FEED Bruteforce attack, SSH authentication attack against LinuxServer	1	2020-02-21 16:19:14	Host-192-168-88-41:35459	LinuxServer	N/A	1
	Alarm Summary [Total events matched with high rule level: 1 - Total Events: 1 - Unique Dst IPAddr: 1 - Unique Types: 1 - Unique Dst Ports: 1]						
3	AlienVault HIDS: SSHD brute force trying to get access to the system.	0	2020-02-21 16:18:35	Host-192-168-88-41:35459	LinuxServer	N/A	1

Рисунок 2.85 – Вывод информации об атаке в событиях системы

Выводы по главе

В данной работе были рассмотрены различные SIEM системы, как лидеры рынка, так и не очень популярные. Была показана установка и исследован функционал системы OSSIM. До внедрения SIEM решения разные устройства генерировали сотни тысяч событий в сутки, обработка которых была непосильна администратору информационной безопасности, однако после установки системы сбора и корреляции событий информационной безопасности количество событий сократилось до десятков в сутки. Так же теперь события с нескольких источников обрабатываются по определенному шаблону, что помогает выявить дополнительные нарушения и инциденты. Вдобавок была сделана атака на хост в сети и показаны результаты выявления данной атаки.

3 Оценивание рисков информационной безопасности

3.1 Активы и анализ рисков ИБ

Для расчета рисков информационной безопасности были определены защищаемые активы такие как, виртуальный сервер Windows Server 2012, виртуальное хранилище и сетевая инфраструктура.

Риски информационной безопасности были рассчитаны с учетом темы дипломного проекта. Были рассчитаны риски для вышеперечисленных активов (незащищенных). Расчет остаточных рисков был произведен с учетом данных защитных мер.

Для расчета рисков был выбран алгоритм из стандарта ISO-27005. Расчет по первому алгоритму (по двум шкалам) производится на основе приложения Е стандарта ISO-27005: Подходы к оценке риска информационной безопасности.

Таблица 3.1 – Ценность активов, уровни угроз и уязвимостей

Степень	Низкая	Средняя	Высокая

вероятности возникновения угрозы										
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Принципы упрощают некоторые значения ценности по числовой шкале.

Таблица 3.1 является итогом рассмотрения степени вероятности сценария инцидента, отображенного на количественно оцененное влияние бизнеса.

Общий рейтинг рисков:

- низкий риск:0-2;
- средний риск:2-5;
- высокий риск:6-8. [18]

Остаточный риск – это риск, который остается после мер по контролю над рисками. Расчет остаточного риска осуществляется по формуле, представленной ниже.

Остаточные риск=Первичный риск–Влияние мероприятий по контролю над рисками. [19]

Таблица 3.2 – Анализ рисков информационной безопасности

№	Угрозы	Уязвимости	риска	Меры по обработке риска	риска	Комментарии, ресурсы, ответственный
Актив №1. Windows Server 2012						
1	Угроза перехвата паролей в режиме реального	Отсутствие шифрации передаваемых данных	8	Шифрование трафика между сервером и клиентом	3	Специалист ИБ

	времени					
2	Угроза повышения привилегий	Использование недостаточно надежного пароля	6	Использование OSSIM HIDS для мониторинга аномалий на хостах	2	Системый аднинистратор
3	Угроза заражения компьютера при посещении неблагонадёжных сайтов	Недостаточная проверка безопасности сайта	5	Слежение за опасными сайтами благодаря базе OSSIM OTX	2	Системый аднинистратор
4	Угроза исследования механизмов работы программы	Своевременно не обновленная ОС	6	Внедрение OSSIM HIDS для слежением за программами на хосте	2	Специалист ИБ
5	Угроза переполнения программного буфера	Отсутствие ограничения на количество получаемых пакетов	6	Использование инструмента Nagios OSSIM для оповещения о превышении количества пакетов	1	Системный администратор
6	Угроза установки кейлоггера	Присутствие бэкдора в ОС	6	Создание правил OSSIM NIDS для выявления изменения данных и слежения за ними	2	Специалист ИБ
Актив №2. Виртуальное хранилище						
7	Несанкционированный	Неправильная распределения	8	Аудит, корректное	3	Специалист ИБ

	доступ и чтение конфиденциальных данных	прав и отсутствие шифрования		распределение привилегии		
8	Угроза несанкционированного удаления защищаемой информации	Отсутствие защиты от несанкционированного доступа	7	Система резервного копирования, использование система защиты от НСД	2	Системный администратор
Актив №3. Сетевая инфраструктура						
9	Угроза определения топологии вычислительной сети	Незащищенность передаваемого трафика	6	Шифрование трафика между веб-сервером и клиентом	1	Сетевой администратор
10	Атака на открытый порт 22 SSH методом подбора паролей	Отсутствие ограничений подбора паролей и фильтрации подключающихся портов	6	Настроить параметры OSSIM OpenVAS для сканирования открытых портов	1	Специалист ИБ

Расчёт рисков информационной безопасности - это один из ключевых этапов при исследовании и расчетов рисков. Наглядно показывает эффективно ли были приняты меры, на ту или иную угрозу и остаточный риск, а также сведения об уязвимостях, угроз и показатели максимального риск

3.2 Методология Coras

Суть методологии CORAS состоит в адаптации, уточнении и комбинировании таких методов проведения анализа рисков, как Event-Tree-Analysis, цепи Маркова, HazOp и FMECA. Метод CORAS использует модель UML (унифицированный язык моделирования – язык графического описания для объектного моделирования в области разработки программного обеспечения). Для документирования промежуточных результатов и для того, чтобы представить полные заключения об анализе рисков информационной безопасности, используются специальные диаграммы CORAS, которые встроены в UML. [3]

Метод CORAS – это компьютеризированный инструмент, который поддерживает документирование, создание отчетов о результатах анализа

путем моделирования риска. Все работы относительно рисков проводятся посредством следующих процедур:

1) подготовительные мероприятия – сбор общих сведений об объекте анализа;
2) представление клиентом объектов, которые необходимо проанализировать;
3) детализированное описание задачи аналитиком;
4) проверка корректности и полноты документация, представленной для анализа;
5) мероприятия по выявлению рисков, (осуществляется, например, в форме семинара) возглавляемые аналитиками;
6) оценка вероятностей и последствий инцидентов информационной безопасности;
7) выявление приемлемых рисков и рисков, которые должны быть представлены на дальнейшую оценку для возможного устранения;
8) устранение угроз, с целью сокращения вероятности и последствий инцидентов в области информационной безопасности.

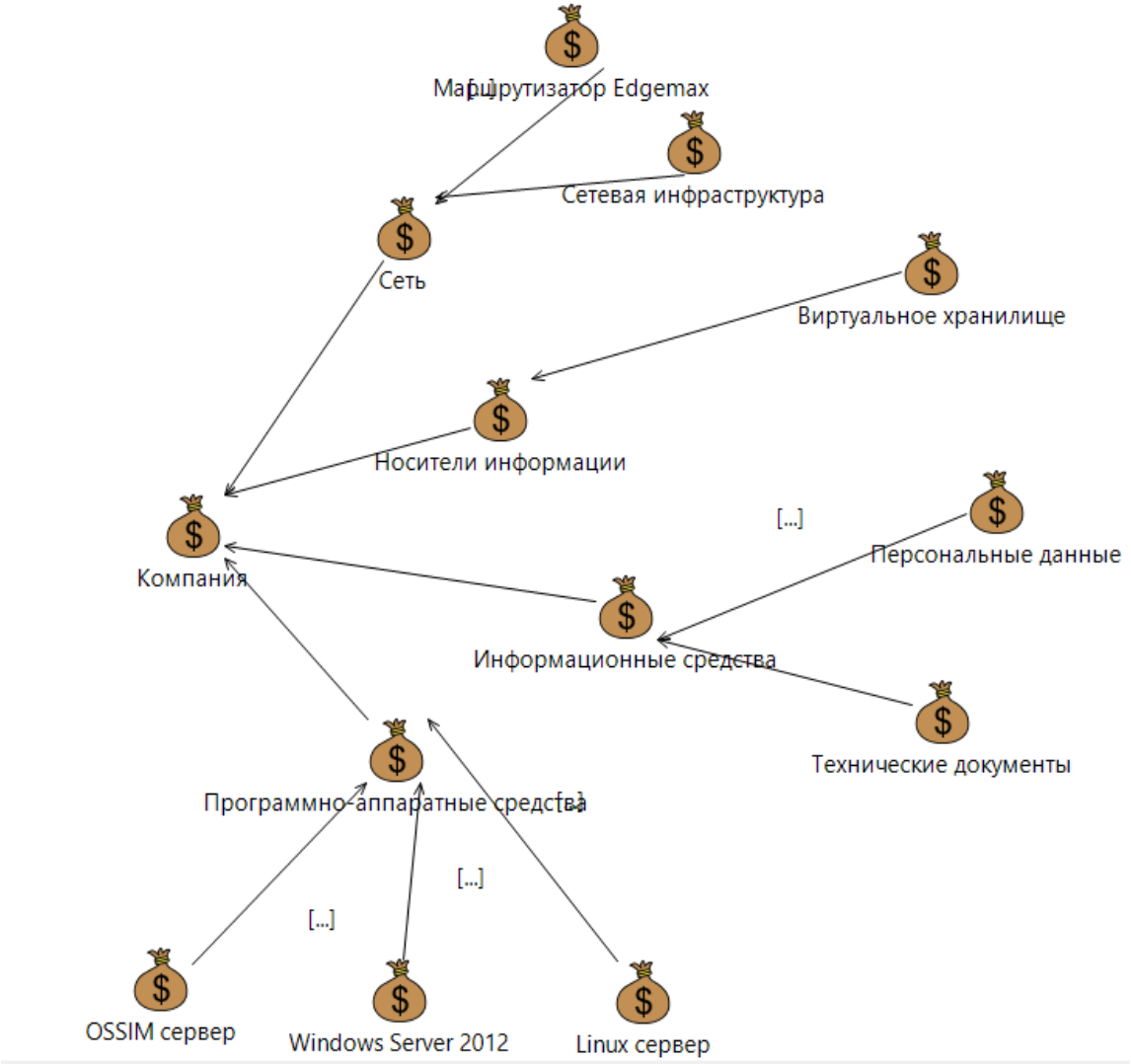


Рисунок 3.1 – диаграмма активов

На рисунке 3.1 представлена диаграмма активов, которые разделены на категории: «Программно-аппаратные средства» и «Информационные средства», «Носители информации», «Сеть» . К программно-аппаратные средствам входит Windows Server 2012, Linux сервер, OSSIM сервер, к информационным относится персональные данные, технические документы, к носителям относится виртуальное хранилище, к сети относится сетевая инфраструктура и маршрутизатор Edgemax.

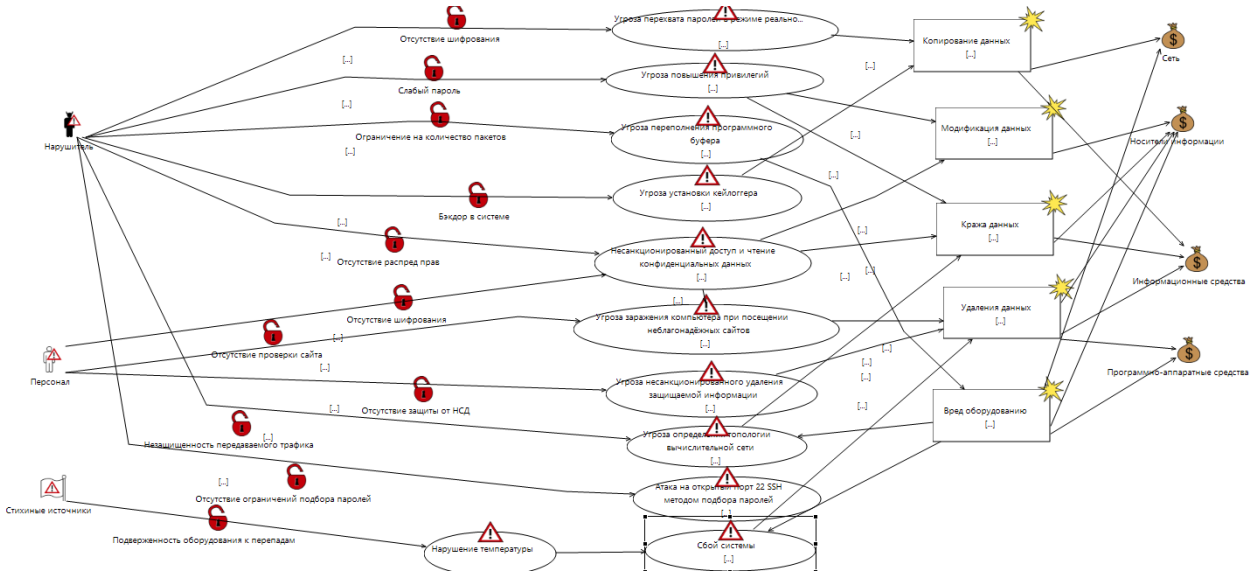


Рисунок 3.2 – Модели угроз

На рисунке 2 представлена диаграмма модели угроз. Элементы диаграммы: источники угроз – уязвимости – этапы реализации угроз – последствия – активы

То есть, сначала источники, затем уязвимости, с помощью которых реализуют угрозу, из которого мы получаем некоторые последствия на определенный актив.

Например, источник угрозы «Нарушитель», используя уязвимость «отсутствие шифрования», реализует перехват пароля и получает доступ к информации. Актив, на который направлена данная угроза – «программно аппаратные средства».

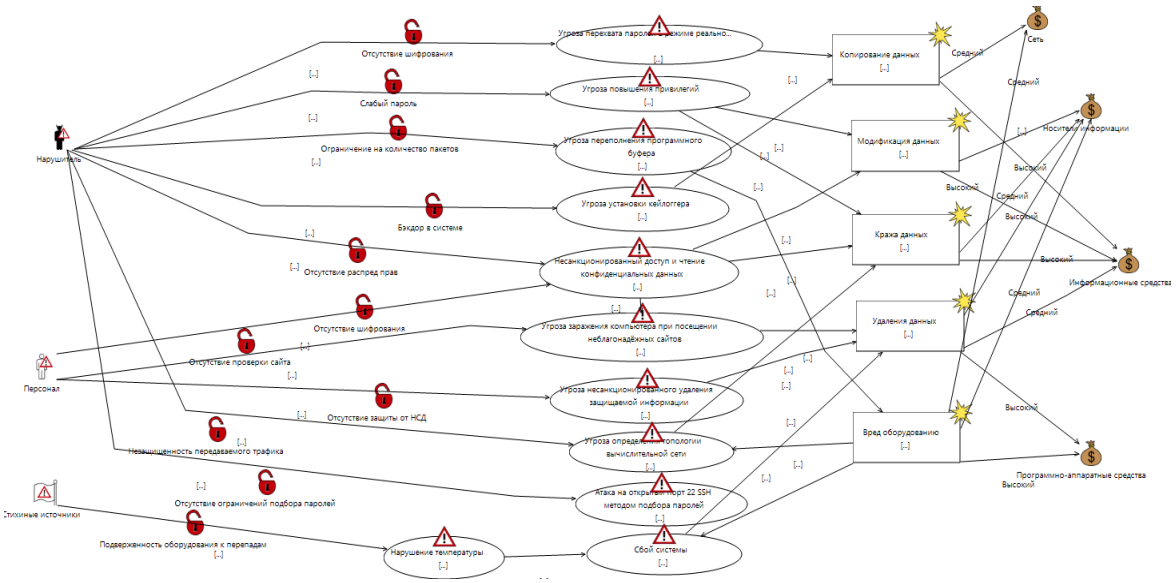


Рисунок 3.3 – Модель угроз с учетом вероятности возникновения инцидента

На рисунке 3.3 представлена диаграмма модели угроз с учетом вероятности возникновения инцидентов. Ее следует читать также, как и предыдущую диаграмму, представленную на рисунке 3, с учетом того что добавлен параметр вероятности возникновения инцидентов. Вероятности возникновения инцидента могут быть высокой, средней и низкой. Например, копирования данных с информационных средств имеет высокую вероятность возникновения.

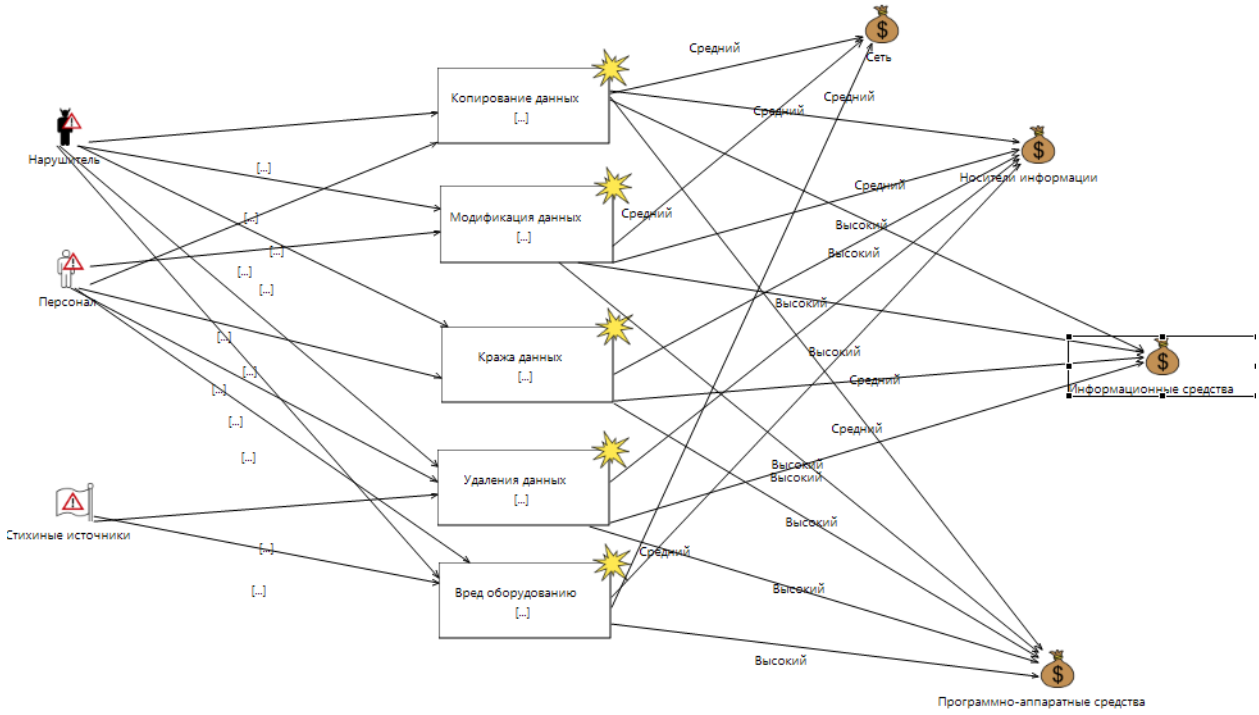


Рисунок 3.4 – Диаграмма рисков с характеристиками влияния угроз

На рисунке 3.4 представлена диаграмма рисков с характеристиками воздействия угроз. То есть для каждого актива определяем последствия в случае осуществления этого риска. Элементы диаграммы слева направо: источники угроз, уязвимости, способы реализации угроз, степень влияния реализации угроз, понесшие от реализации угрозы ущерб активы.

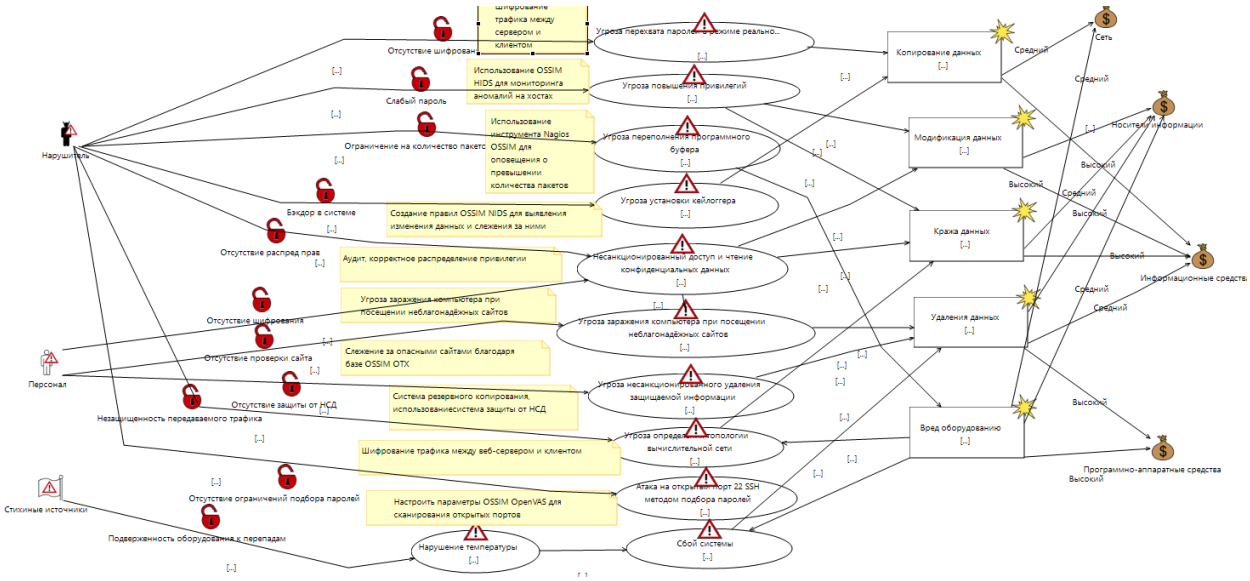


Рисунок 3.5 – Модель угроз с учетом защитных мер

На рисунке 3.5 представлена диаграмма модели угроз с возможными мерами защиты. Ее следует читать так же, как и диаграмму, представленную на рисунке 3.2, с единственным отличием: между уязвимостями и способами реализации угроз добавлены защитные меры для уменьшения рисков, то есть между уязвимостями и способами реализации угроз добавлены защитные меры для уменьшения рисков. К примеру, для уязвимости «Отсутствия ограничений подбора паролей» внедрена защитный сканер «OpenVAS».

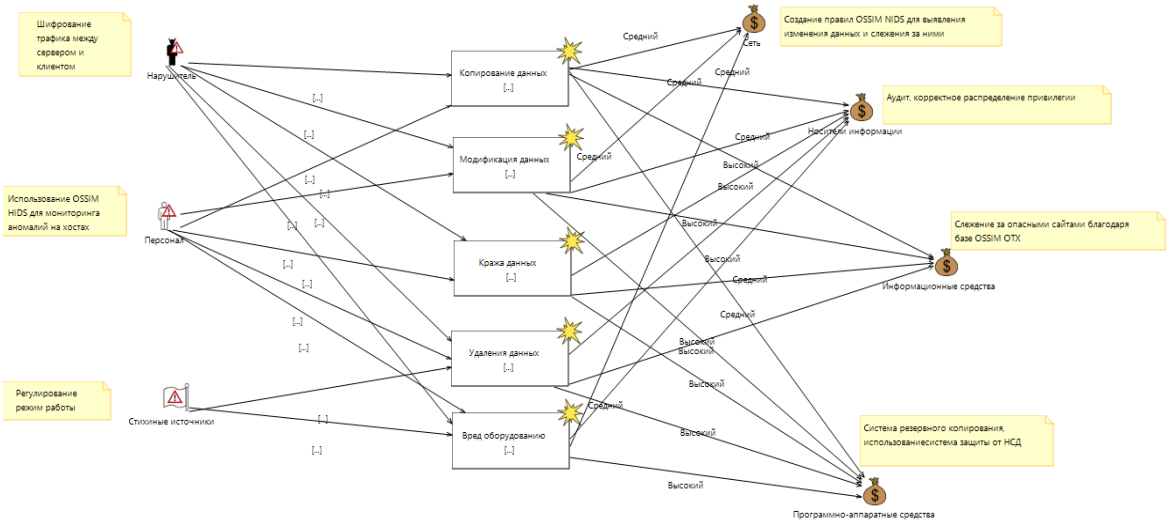


Рисунок 3.6 – Диаграмма недопустимых рисков

На рисунке 3.6 представлена диаграмма недопустимых рисков. Она построена на базе диаграммы, представленной на рисунке 3.4, но здесь представлены те риски, которые имеют высокую степень влияния угроз.

Выводы по главе

В данном разделе дипломного проекта, были произведены расчёты рисков. Задачей данных методик являлось понимание реальных угроз, расчёт рисков, а также выбора мер направленные на уменьшение этих рисков и защитных мер. Количественный пример представляет объект и стоимость и оценки. Произведен обзор рисков, определение активов. Также были рассчитаны максимальные и остаточные риски. Так как угрозы в основном направленные на виртуальые машины, в особенности на местоположение серверов: OSSIM, Windows, Linux, 1C, Файловый. Были исследованы комплексы защитных мер которые были направлены на минимизацию данных угроз и остаточного риска, такие как настройка сервера OSSIM, применены инструменты системы такие как HIDS и NIDS для мониторинга вторжения , Nagios для мониторинг поведения узлов, OpenVAS для сканера уязваимости. Данные меры позволяет полностью минимизировать направленные угрозы связанный с сетью, удаленного доступа и изменения конфигурации серверов..

Так как все риски оказались неприемлемы (от 6 до 8 по 8-ми балльной шкале), для всех рисков были описаны защитные меры. После введения мер для обработки рисков риски были пересчитаны, получены остаточные риски. Все риски, оставшиеся после перерасчета с учетом защитных мер, стали приемлемыми (от 0 до 3 по 8-ми балльной шкале).

4. Безопасность жизнедеятельности

Основной целью данного дипломного проекта является проектирование программного комплекса SIEM OSSIM для обеспечения безопасности объекта. Актуальность этой темы заключается в том, что на данный момент количество данных увеличивается и обработка такого количества информации стало невозможным и решением является внедрение SIEM системы для обработки данных. Это исследование может быть использовано для реализации SIEM системы OSSIM для корпоративной сети.

Проблемы БЖД а также их решения состоит в обеспечении нормальных и комфортных условий труда для людей в их жизни, в защите человека и окружающей его среды от воздействия вредных факторов, превышающих нормативно-допустимые уровни. Поддержание и создание удобных и хороших условий деятельности и отдыха человека способствует его высокой продуктивности.

Предоставление безопасности труда и отдыха способствует сохранению жизни и поддержанию здоровья человека за счет снижения травм и заболеваемости.

Проблемы связанные с безопасной жизнедеятельности человека необходимо решать на всех циклах жизни, будь то разработка, эксперимент или использование разработанной методики на практике.

Работа с вычислительной техникой по вредности относится к безопасным (риск смерти на человека в год составляет менее 0.0001). Нагрузка труда у работника вычислительной техники также минимальна, так как уровень психической нагрузки по этому роду деятельности предусматривает энергетические затраты 2000...2400 ккал в сутки.

Анализ условий труда и мероприятия по защите от воздействия вредных производственных факторов.

4.1 Анализ условий труда при разработке проекта SIEM системы OSSIM

Главным инструментом используемым при разработке указанного проекта является - персональный компьютер (ПК). Нормальная и безопасная работа специалиста за ПК во многом зависит от того, в какой мере условия его работы соответствуют оптимальным. При этом, под условиями работы подразумевают комплекс физических, химических, биологических и психофизических факторов, установленных стандартами по безопасности труда [11].

К физическим факторам относятся:

- шум из-за движущихся машин, механизмов и их элементов, загазованность воздуха, температура выделяемая оборудованием;
- плотность воздуха, ее резкое изменение, подвижность и ионизация воздуха;
- ионизирующие и электромагнитные излучения, статические заряды и повышение напряжения в цепи, электрические и магнитные поля;
- отсутствие или недостаток естественного света, повышенная или пониженная освещенность, яркость и контрастность, пульсация светового потока;
- ультрафиолетовое или инфракрасное излучение.

К биологическим факторам относятся:

- микроорганизмы (бактерии, вирусы, грибы и т.д.);
- макроорганизмы (растения и животные).

К психофизическим факторам относятся перегрузки:

- физические (статические, динамические, гиподинамия);
- нервно-психические (умственное перенапряжение, монотонность труда, эмоциональные перегрузки).

При проектировании места для работы пользователя ПК необходимо нормировать и учитывать все указанные группы факторов, так как при определенных условиях они могут вызвать нежелательные функциональные изменение в организме сотрудника, снизить качество и эффективность его работы, повлиять отрицательно на его здоровье.

Работа с операционной системой, программными продуктами и приложениями на ПК относится к категории работ 1а.

4.1.1 Микроклимат производственной среды в кабинетах вычислительной техники

Особо значительным фактором является микроклимат которая создается в кабинете [11], особенно температура и влажность воздуха. Исследования показывают, что высокая температура в сочетании с высокой влажностью воздуха оказывают огромное влияние на работоспособность человека. Сильно увеличивается время сенсорных и моторных реакций, нарушается координация движений, увеличивается количество ошибок. Высокая температура плохо сказывается и на ряде психологических функций человека. Уменьшается объем оперативной памяти, резко суживается способность к ассоциациям. При +11ºС начинается окоченение конечностей, такая температура минимально допустима. Наиболее благоприятный диапазон температур в летнее время считается от +18ºС до +24ºС, в зимнее время от +17ºС до +22ºС.

Движение воздуха позволяет увеличить рабочий диапазон температур. Так при скорости движения воздуха 0.1, 0.5, 0.9 м/с верхняя допустимая граница рабочего диапазона изменяется соответственно до +22º, +24º, +26ºС.

Атмосферное давление в пределах 80-106 кПа считается допустимой для человека. При давлениях, выходящих за эти пределы, человеку потребуется предварительная акклиматизация.

Фактические показатели соответствуют приведённым выше нормам.

Результаты работы пользователя ПК в большой степени зависят и от освещенности рабочего места. Чтобы правильно рассчитать рациональную систему освещения, необходимо учесть яркость источников света, их места в помещении, яркостной контраст между устройствами ПК и фоном, блёсткость поверхностей, качество и цвет светильников и поверхностей. Для большой контрастности при светлом фоне наименьший уровень освещенности должен быть 200 лк.

Фактические показатели соответствуют приведённым выше нормам.

Зрительная работа является работой средней точности согласно [2].

В объектах, где эксплуатируют ПК, необходимо предусмотреть систему искусственного освещения из люминесцентных ламп дневного света или ламп накаливания, которые сегодня уступили место, энергосберегающим лампам. Энергосберегающая лампа – это электрическая лампа, обладающая существенно большей светоотдачей, в сравнении с классическими лампами накаливания. Благодаря этому замена ламп накаливания на энергосберегающие способствует экономии электроэнергии. Часто энергосберегающие лампы называют компактными люминесцентными лампами, которые имеют изогнутую форму колбы, что позволяет разместить лампу в светильнике меньших размеров.

Часто встречается отравление парами ртути. Люминесцентные лампы содержат в своем составе в небольшом количестве пары ртути, в связи с чем их нельзя выбрасывать как обычный бытовой мусор, а требуется сдавать в утилизацию в специализированные организации. Опасно не только острое

отравление парами ртути, но и долговременное хроническое отравление малыми дозами паров, вызывающее неврологические заболевания, а также длительное воздействие сверх малых доз.

Ультрафиолетовое излучение люминесцентных ламп. При работе люминесцентных ламп небольшое количество ультрафиолетового излучения выходит наружу через стеклянную колбу, что может потенциально представлять опасность для людей с кожей, слишком чувствительной к этому излучению. Ультрафиолетовое излучение (УФ) может вызывать появление кожных мутаций. Наиболее опасным является воздействие УФ – излучения на роговицу и сетчатку глаза. Поэтому энергосберегающие лампы не стоит располагать ближе 30см. от глаз (ночник, настольные лампы, освещение жилых помещений).

Полосатый спектр люминесцентных и светодиодных ламп. Энергосберегающие лампы обладают выраженными пиками на отдельных участках спектра. На некоторых же участках излучение может отсутствовать (провал в области фиолетовых и синих лучей есть и у ламп накаливания). В связи с неблагоприятным воздействием прерывистого спектра на сетчатку глаза и нервную систему человека (подавление продукции мелатонина), не рекомендуется применение светодиодных ламп в детских и школьных учреждениях, палатах интенсивной терапии, кабинах машинистов.

Использование источников искусственного освещения в соответствии с указанными предостережениями и рекомендациями.

Есть прямая, отраженная и диффузная системы искусственного освещения. При прямом освещении свет попадает на объект непосредственно от источников света. При этом 90-100% мощности светильника направлено на рабочую поверхность, что вызывает яркостные контрасты, резкие тени и блёсткость (свойство ярко освещенной поверхности вызывать ослепление или дезадаптацию наблюдателя). При освещении отраженным светом 90-100% света направляется на потолок и верхнюю часть стен, от которых свет более или менее равномерно отражается по всему помещению. При этом достигается равная освещенность без теней и блесткости. Диффузное освещение обеспечивает рассеянный свет, одинаково распределенный по всем направлениям. Такая система освещения требует меньшей мощности, чем две предыдущие, но вызывает частичное образование теней и блёсткости.

Большое влияние на деятельность сотрудника (сетевого специалиста) оказывает и уровень акустического шума. Шум резко снижает производительность труда и увеличивает травматизм. Физиологически шум воздействует на органы зрения и слуха, повышает кровяное давление, при этом притупляется внимание.

Шум оказывает также и эмоциональное воздействие: он является причиной возникновения таких отрицательных эмоций, как досада, раздражение. Особенно неприятны высокочастотные и прерывистые шумы.

В соответствии с [13] уровни звукового давления для сотрудников вычислительного центра и/или отдела информационных технологий лежат в пределе 38-68 дБ в зависимости от частоты шума. Фактически уровень звукового давления не превышает 30дБ, что соответствует установленным нормам и требованиям.

Также к числу неблагоприятных факторов относятся электромагнитные поля (ЭМП) высоких частот [14]. Их воздействие на человека может вызвать функциональные сдвиги в организме: быструю утомляемость, головные боли, нарушение сна, раздражительность, утомление зрения и т.п.

Благоприятными условиями газового состава воздуха считается содержание кислорода 19-20%, углекислого газа около 1%; допустимые значения, при которых не происходит выраженного снижения работоспособности, составляют: кислорода – 18-29%, углекислого газа – 1-2%. Снижение содержания кислорода ниже 16% и повышение содержания углекислого газа выше 3% являются недопустимыми и могут привести к нежелательным последствиям. Важнейшим способом борьбы с неблагоприятным воздействием на человека химических факторов является соблюдение их предельно допустимых концентраций в производственных помещениях. Предельно допустимыми считаются такие максимальные концентрации вредных веществ, которые при ежедневной работе не могут вызывать у работающих заболевания или отклонения в состоянии здоровья. Такими концентрациями считаются, например, для аммиака – 20 мг/м, анилина – 3 мг/м, ацетона – 200 мг/м, бензола – 5 мг/м, бензина – 100 мг/м, серной кислоты – 1 мг/м, но так как тип работы не относится к производственному, данные виды вредных веществ, можно исключить.

Фактические показатели соответствуют приведённым выше нормам.

Персональный компьютер питается напряжением 220В/50Гц, которое превышает безопасный предел 42 В. Следовательно, возникает опасность поражения электрическим током.

Воздействие на человека электрического тока приводит к общим травмам (электроудары) и местным (ожоги, металлизация кожи, электрические знаки, электроофтальмия, механические повреждения).

Данное помещение можно классифицировать как помещение без повышенной опасности поражения людей электрическим током, в соответствии с Правилами Устройства Электроустановок.

При работе на персональном компьютере человек попадает под воздействие статического электричества. Под действием статических электрических полей дисплея пыль помещения электризуется и переносится на лицо пользователя, что приводит к заболеваниям (раздражению) кожи (дерматит, угри).

Разработка осуществляется с использованием компьютерной техники и электронного оборудования. В рассматриваемом помещении работает 1 сотрудник, который имеет свое рабочее место.

Характеристики рабочего помещения:

Рассматривается рабочее помещения, расположенное в здании, которое не находится в непосредственной близости от железнодорожной магистрали или нагруженной автомагистрали, аэропорта и так далее, поэтому внешних источников шума, влияющих на процесс работы – нет.

Помещение имеет следующие параметры:

- находится на первом этаже одноэтажного здания;
- размеры помещения (комнаты): длина 8м, ширина 6м, высота 3м;
- вид светопропускающего материала – стекло листовое, двойное;
- вид переплета – стальные двойные открывающиеся;
- солнцезащитные устройства – убирающиеся регулируемые жалюзи и

шторы;

- два окна размером 1,5*1,2;
- внутренняя отделка стен – светлая;

помещение по зрительным условиям работы относится к категории легких работ (легкая физическая, категория 1а, работа производится сидя и не требует физического напряжения);

- искусственное освещение – 2 светильника с двумя люминесцентным лампами.

Характеристики используемого в работе оборудования:

- Ноутбук с процессором Intel(R) CoreTM i5 – 8500U, оперативная память 16GB SSD - 512Гб, жесткий диск 1TB;
- электропитание: переменное напряжение 220-250 В, частотой 50 Гц. Мощность 400 Вт;
- 2 светильника, 4 люминесцентные лампы;
- электропитание: переменное напряжение 220-250 В, частотой 50 Гц, мощность светильника 2х28 Вт.

Электротехническое оборудование является потенциальным источником возникновения пожарной опасности. Оборудование малошумящее - вредность в качестве повышенного шума отсутствует.

4.2 Анализ и расчет пожарной безопасности кабинета инженера - разработчика

Согласно утвержденному постановлением Правительства РК от 16.01.2009г. №14 Техническому регламенту «Общие требования к пожарной безопасности», здание по степени опасности развития пожара, от функционального назначения и пожарной нагрузки горючих материалов, относится к 1-ой группе категории Д – пониженная пожароопасность.

Причинами возникновения пожара могут быть:

- резкое возгорание элементов аппаратуры;
- несоблюдение режимов эксплуатации оборудования, неправильное действие персонала.

При возникновении пожара может пострадать не только помещение, но и дорогостоящая аппаратура, а самое главное, могут быть человеческие жертвы. Поэтому необходимо чтобы были приняты меры по раннему выявлению и ликвидации пожаров. Источниками зажигания могут оказаться электронные схемы ЭВМ, приборы, применяемые для технического обслуживания, устройства электропитания, кондиционеры воздуха, где в результате различных нарушений образуются перегретые элементы, и др.

В соответствии с пунктом 5.9, Государственного стандарта РК: «Техника пожарная. Огнетушители», общественные и промышленные здания и сооружения должны иметь на каждом этаже не менее двух переносных огнетушителей [16].

Также по нормам обеспечения объектов первичными средствами пожаротушения, расстояние от возможного очага пожара до места размещения огнетушителя не должно превышать 70м. – для помещений категории Д [17].

В соответствии с требованиями правил пожарной безопасности помещение оборудованы углекислотными огнетушителями ОУ-5 с учетом – один огнетушитель на 100 м2. Общая площадь помещения составляет 48м2, таким образом устанавливается 1 огнетушитель. В качестве огнетушащего вещества применяется комбинированный углекислотно-хладоновый состав. Расчетная масса комбинированного углекислотно-хладонового состава md, для объемного пожаротушения определяется по формуле:

$$m_d = k g_n v \quad (4.1)$$

где k = l,2 – коэффициент компенсации не учитываемых потерь углекислотно-хладонового состава, gn = 0,04 – нормативная массовая концентрация углекислотно-хладонового состава, V – объем помещения, который можно вычислить по следующей формуле:

$$V = A \times B \times H \quad (4.2)$$

где A = 8 м - длина помещения, B = 6 м - ширина помещения, H = 3м - высота помещения.

Тогда:

$$V = 8 \times 6 \times 3 = 144 \text{ м}^3$$

Следовательно:

$$m_d = 1{,}2 \times 0{,}04 \times 144 \approx 6{,}9 \text{ кг}$$

Расчетное число баллонов x определяется из расчета вместимости в 20-литровый баллон 12 кг углекислотно - хладонового состава.

Внутренний диаметр магистрального трубопровода di (мм), определяется по формуле:

$$d_i = 12 \times \sqrt{2} \approx 17 \text{ мм.}$$

Эквивалентная длина магистрального трубопровода l2 определяется по формуле:

$$l_2 = k_1 \times l \quad (4.3)$$

где k1=1,2 - коэффициент увеличения длины трубопровода для компенсации не учитывающих местных потерь, l=3м - длина трубопровода по проекту тогда:

$$l_2 = 1{,}2 \times 3 = 3{,}6 \text{ м.}$$

Расход углекислотно-хладонового состава Q, в зависимости от эквивалентной длины и диаметра трубопровода равна 1,4 кг/с.

Расчетное время подачи углекислотно-хладонового состава t, определяется по формуле:

$$t = \frac{m_d}{V * Q} \quad (4.4)$$

Тогда:

$$t = \frac{6{,}9}{144 \times 1{,}4} = 0{,}033 \text{ мин.}$$

Масса основного запаса углекислотно-хладонового состава m определяется по формуле:

$$m = 1{,}1 \times m_d \times (1 + \frac{k_2}{k_1}) \quad (4.5)$$

где $k2 = 0{,}2$ – коэффициент учитывающий остаток углекислотно-хладонового состава в баллонах и трубопроводах. Тогда:

$$m = 1{,}1 \times 6.9 \times \left(1 + \frac{0{,}2}{1{,}2}\right) = 8.855 \text{ кг.}$$

Таким образом, из полученных результатов можно сделать вывод, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 6.9 кг. Автоматические установки газового пожаротушения имеют устройства для автоматического пуска. Данный огнетушитель будет установлен непосредственно в помещении специалиста центра информационных технологий (IT – отдел), плюс, можно учитывать 2 общих ручных огнетушителя на этаже.

4.3 Расчет системы кондиционирования кабинета ИТ специалиста

В таблице 4.1 приведены оптимальные нормы параметров микроклимата с учетом периода года согласно [15] для легкой физической работы. Оборудование, установленное в рабочем помещении, не является источником выделения тепла (очень незначительное выделение тепла аппаратурой никаким образом не оказывает влияние на микроклимат рабочего помещения). Климатические условия эксплуатации оборудования полностью совпадают с климатическими условиями, нормируемыми для рабочего персонала.

Таблица 4.1 − Оптимальные нормы температуры, относительной влажности и скорости движения воздуха в обслуживаемой зоне жилых, общественных и административно-бытовых помещений [15]

Период года	Категория работ	Температура воздуха, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Легкая - 1а Легкая – 1б	22-24 21-23	40-60 40-60	0,1 0,1
Теплый	Легкая - 1а Легкая – 1б	23-25 22-24	40-60 40-60	0,1 0,2

Для вентиляции офисного помещения используются каналы естественной вентиляции, прокладываемые при строительстве здания и открытые окна летом. В теплый период года при достижении температуры в офисе свыше норм, приведенных в таблице 4.1, для поддержания оптимального микроклимата используется кондиционер. Нормальный микроклимат в офисе обеспечивает хорошее самочувствие сотрудника в любое время года, и соответственно продуктивность работы увеличивается. Таким образом, для поддержания условий микроклимата в помещении, целесообразно оборудовать его системой кондиционирования.

Ниже представлен расчет системы кондиционирования в рабочем помещении. Кондиционирование обеспечит соответствие климата в рабочем помещении нормативам.

Количество приточного воздуха $L_{\text{пр}}, \frac{\text{м}^3}{\text{ч}}$ определяем по формуле:

$$L_{\text{пр}} = \frac{Q_{\text{изб}}}{cp_{\text{пв}}(t_{\text{выт}} - t_{\text{пв}})} \quad 4.6)$$

где $Q_{\text{изб}}$ - избыточное выделение явной теплоты, кДЖ/ч; c - удельная теплоемкость воздуха при постоянном давлении, равная $c = 1$кДж/кг°С; $p_{\text{пв}}$ - плотность поступающего в помещение воздуха, равная 1,2 кг/м3; $t_{\text{выт}}$ - температура удаляемого из помещения воздуха за пределы рабочей или обслуживаемой зоны,°С; $t_{\text{пв}}$ - температура приточного воздуха,°С.

Температура удаляемого из помещения воздуха $t_{\text{выт}}$ °С, определяется по формуле:

$$t_{\text{выт}} = t_{\text{рз}} + \Delta t(h_{\text{вп}} - z) \quad 4.7)$$

где: $t_{\text{рз}}$ - температура в рабочей зоне, которая не должна превышать допустимую по нормам ($t_{\text{рз}} \leq t_{\text{доп}}$),°С; $h_{\text{вп}}$ - расстояние от пола до центра вытяжных проемов (кондиционера),м.

Поскольку расчет производится для теплого периода года, то примем $t_{\text{рз}} = 22$°С. Внутренняя часть кондиционера расположена на высоте $h_{\text{вп}} = 2{,}7$м.

$$t_{\text{выт}} = 22 + 1{,}2(2{,}7 - 3) = 21{,}64\ ℃$$

Температура приточного воздуха $t_{\text{пр}}$ при наличии избытка явной теплоты должна быть на $5-7$ °С ниже температуры воздуха в рабочей зоне:

$$t_{\text{пр}} = 22 - 7 = 15\ ℃$$

Величину избыточного выделения явной теплоты $Q_{\text{изб}}$ находят на основании баланса теплоты в помещении по формуле:

$$Q_{\text{изб}} = \sum Q - \sum Q_{yx} \quad 4.8)$$

где $\sum Q$ - суммарное количество поступающей в помещение явной теплоты; $\sum Q_{yx}$ - суммарное количество уходящей из помещения теплоты (за счет теплопотерь ограждениями, нагрева поступающего в помещение воздуха).

Основными источниками избыточного тепла являются светильники, люди и др. Кроме того, необходимо учитывать теплопоступления от солнечной радиации. В данном помещении тепловыделением электронного оборудования можно пренебречь, т.к. выделение тепла от ПК, который к

тому же само охлаждается вентилятором, очень мало. Поэтому учитываем тепловыделения от искусственного освещения, от людей, количество тепла, поступающего в помещение через окна от солнечной радиации.

Тепловыделения от искусственного освещения Q_2, рассчитывают, предполагая, что практически вся затрачиваемая энергия, в конечном счете, преобразуется в тепло, по формуле:

$$Q_2 = 1000N \quad (4.9)$$

где N – расходуемая мощность светильников, кВТ.

$$Q_2 = 1000 \times 0{,}27 \times 4 = 1080 \text{ кВТ}$$

Тепловыделения от людей Q_3 определяют по формуле:

$$Q_3 = nq_ч \quad (4.10)$$

где n - число работающих; $q_ч$ - количество тепла, выделяемое одним человеком, представлено в таблице 4.2.

Таблица 4.2 – Количество тепла, выделяемое одним человеком в зависимости от категории работ и температуры окружающей среды

Категория работ	Количество тепла, Вт (мужч.) при температуре воздуха в помещении, °С			
	Полное		Явное	
	при 10°С	При 20°С	при 10°С	При 20°С
Легкая	180Вт	145Вт	150Вт	100Вт

$$Q_3 = 1 \times 145 = 145\text{Вт}$$

Количество тепла, поступающего в помещение от солнечной радиации $Q_{\text{солн.рад.}}$, определяют по формуле:

$$Q_{\text{солн.рад.}} = F_{\text{ост}} q_{\text{ост}} A_{\text{ост}} \quad (4.11)$$

для покрытий:

$$Q_{\text{п.рад.}} = F_n q_n k_n \quad (4.12)$$

Где $F_{\text{ост}}$ и F_n - площадь поверхности и покрытия, м2; $q_{\text{ост}}$ и q_n - теплопоступления через 1м2 поверхности остекления и поверхности покрытия, при коэффициенте теплопередачи, равном 1Вт/м2℃; $A_{\text{ост}}$ - коэффициент остекления; k_n- коэффициент теплопередачи покрытия, 1Вт/м2℃.

Значение $q_{\text{ост}}$ в зависимости от географической ориентации поверхности и характеристики окон или фонарей принимается в пределах $70-210$, а коэффициента $A_{\text{ост}}$ в зависимости от вида остекления и его солнцезащитных свойств - в пределах $0{,}25-1{,}25$, средние значения теплопоступления от солнечной радиации через покрытие в зависимости от географической широты и вида покрытия принимают в пределах 6 - 24.

$$F_{\text{ост}} = 1{,}5 \times 1{,}2 \times 2 = 3{,}6 \text{ м2}$$

Окна рабочего помещения направлены на север, поэтому примем значение $q_{\text{ост}}$ равным 140Вт/м2℃. Примем $A_{\text{ост}} = 0{,}35$.

$$Q_{\text{ост.рад.}} = 3{,}6 \times 140 \times 0{,}35 = 176{,}4\text{Вт}$$

Среднее значение теплопоступления для покрытия с учетом географической широты примем равным $Q_{\text{п.рад.}} = 18\text{Вт}$.

Потери тепла из помещения Q_{yx} кВТ, через стены двери, окна оценивают ориентировочно по формуле:

$$Q_{yx} = \frac{\lambda S(t_{\text{выт}} - t_{\text{пр}})}{\delta} \quad (4.13)$$

Где λ - теплопроводность стен, Вт/м℃; S - площадь, м2; δ - толщина стен,м.

Стены рабочего помещения изготовлены из тяжелого бетона М600, теплопроводность которого равна 12Вт/м℃. Толщина стен δ = 0,5м.

$$Q_{yx} = \frac{1{,}2 \times 24(21{,}64 - 15)}{0{,}5} = 382{,}464 \text{ Вт}$$

Вычислим суммарное количество поступающей в помещение явной теплоты:

$$\sum Q = Q_2 + Q_3 + Q_{\text{ост.рад.}} + Q_{\text{п.рад}} \quad (4.14)$$

$$\sum Q = 1080 + 145 + 176{,}4 + 18 = 1419.4 \text{ кВТ}$$

Так как расчет производится для летнего периода величина избыточного выделения явной теплоты равна:

$$Q_{\text{изб}} = 1419.4 \text{ кВт}$$

Вычислим количество приточного воздуха:

$$L_{\text{пр}} = \frac{1419.4}{1 \times 1{,}2(21{,}64 - 15)} = 178{,}1 \text{м3/ч}$$

Чтобы обеспечивать расход воздуха $L = 178{,}1$ м3/ч, можно использовать 1 кондиционер фирмы LG AR5500 с функцией ускоренного охлаждения:

- мощность охлаждения – 6,8 кВт;
- мощность обогрева – 8 кВт;
- максимальная длина/высота трубопровода – 20/12м.;
- уровень шума внутреннего блока - 44/28 дБ:;
- уровень шума наружного блока – 54 Дб.

Что является сверх достаточным для обеспечения комфортного микроклимата.

Выводы по главе

В данном разделе был произведён анализ условий труда в рабочем помещении. Уровень условий труда признан допустимым, и данные, полученные из расчетов полностью удовлетворяют требованиям стандартов безопасности жизнедеятельности.

Электротехническое оборудование в помещении является потенциальным источником возникновения пожара. Из расчетов получили, что для обеспечения нормального функционирования системы автоматического пожаротушения потребуется 1 баллон углекислотно-хладонового состава вместимостью 20 литров, с массой смеси 4,6 кг.

Также приведен расчет системы кондиционирования помещения, с учетом суммарного количества поступающей в помещение явной теплоты и количеством приточного воздуха.

Заключение

В данном дипломном проекте была произведена организация SIEM системы OSSIM. Для достижения поставленных целей и решения предложенной задачи была проделана следующая работа:

- была описана архитектура SIEM системы;
- исследованы популярные SIEM системы;
- разработана структурная схема сети для внедрения системы OSSIM;
- установлена SIEM система OSSIM;
- проанализированы инструменты имеющиеся в системе OSSIM;
- проведен расчет анализа условий труда и расчет системы кондиционирования помещения;
- рассчитаны риски ИБ.

Практическую ценность в данной работе представляет освоение навыков работы с SIEM системой. Кроме того, проект был успешно внедрен и использован по назначению и имеет актуальность на данный момент.

В ходе выполнения дипломной работы была создана полноценная и рабочая топология корпоративной сети с настроенным оборудованием.

Данная система предназначена для компаний с небольшими активами в сети. С помощью данной системы над каждым устройством корпоративной сети будет вестись мониторинг.

В разделе безопасности жизнедеятельности был произведён анализ условий труда в рабочем помещении. Уровень условий труда признан допустимым, и данные, полученные из расчетов полностью удовлетворяют требованиям стандартов безопасности жизнедеятельности. Также приведен расчет системы кондиционирования помещения, с учетом суммарного количества поступающей в помещение явной теплоты и количеством приточного воздуха.

В разделе оценки рисков были произведены расчёты рисков, задачей которых являлось понимание реальных угроз, расчёт рисков, а также выбора мер направленные на уменьшение этих рисков и защитных мер.

Перечень сокращении

СМСБ	–	системы мониторинга событий безопасности
НСД	–	несанкционированный доступ
ПО	–	программное обеспечение
КВИ	–	критический важная инфраструктура
ИБ	–	информационная безопасность
ИТ	–	информационные технологии
СЗИ	–	система защиты информации
ИС	–	информационные системы
ОС	–	операционная система
СОВ	–	система обнаружения вторжений
МЭ	–	межсетевые экраны
ЛВС	–	локальная вычислительная сеть
СПД	–	сети передачи данных
ИТ	–	информационные технологии

Список литературы

1. Википедия. «SIEM» https://ru.wikipedia.org/wiki/SIEM
2. Олеся Шелестова «Что такое SIEM?», http://www.securitylab.ru/4300777.php
3. Канев А.Н. Мониторинг событий и обнаружение инцидентов безопасности с использованием SIEM – систем. Международный студенческий научный вестник. – 2015. – № 3;
4. Дмитрий Хамакев «SIEM: ответы на часто задаваемые вопросы», https://habrahabr.ru/post/172389/
5. Максим Гарусев. «Системы корреляции событий: революция или эволюция?», http://www.setevoi.ru/cgi-bin/text.pl/magazines/2003/7/30
6. Артем Медведев «самый безопасный SOC», http://www.jetinfo.ru/stati/samyj-bezopasnyj-soc/#1
7. Официальный сайт компании HP. «ArcSight SIEM» http://www8.hp.com/ru/ru/software-solutions/siem-security-informationevent-management/index.html
8. Официальный сайт Positive Technologies. «MaxPatrol SIEM» , http://www.ptsecurity.ru/products/mpsiem/
9. Официальный сайт «ООО ИТБ». «Security Capsule SIEM», https://www.itb.spb.ru/3_2_2.php
10. Алексей Герасимов. «Сравнение SEIM – систем», http://siem.guru/compare_SIEM_systems.php
11. ГОСТ 26883-86. Внешние воздействующие факторы. Термины и определения.
12. СП РК 2.04-104-2012. Естественное и искусственное освещение.
13. ГОСТ 12.1.003-2014 «ССБТ. Шум. Общие требования безопасности.
14. СанПиН 2.2.4.1191-03. Электромагнитные поля в производственных условиях
15. СНиП РК 4.02-05-2001 Отопление, вентиляция и кондиционирование. Общие требования. – АИЭС, 2004.
16. Zhiger-orleu.kz/standards/126-technika-pozharnaya-ognetushiteli-treboaniya-k-ekspluatacii.html
17. https://online.zakon.kz/m/document/?doc_id=31483044
18. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности, дата введения 2011-12-01. (Дата обращения: 07.05.20)19.
19 Остаточный риск – URL:.https://ru.wikipedia.org/wiki/BA (Дата обращения: 10.05.20)