ДЕПАРТАМЕНТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ ТОМСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТОМСКИЙ ТЕХНИКУМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Внедрение программного комплекса Ankey SIEM NG в инфраструктуру предприятия ООО «НПФ «ИСБ»

СОЛОВЬЁВ АРТЁМ ДМИТРИЕВИЧ, ГРУППА 982

г. Томск, 2022 г.

Введение

- Актуальность данной темы заключается в том, что с объемами информации, обрабатываемой и передаваемой между информационными системами, организации и их сотрудники все более зависят от непрерывности и корректности выполнения данных процессов.
- В рамках реагирования на угрозы информационной безопасности (ИБ) в информационных системах недостаточно иметь набор средств защиты информации, а необходимо также располагать возможностью и средствами оперативного анализа событий в режиме реального времени.
- **Одним из решений данной проблемы является использование SIEM-систем** в информационной системе, ключевой принцип которых заключается в сборе данных о безопасности структуры, и предоставлении результата их обработки в едином интерфейсе, доступном для аналитиков безопасности.

Функции SIEM

Цель работы

- Цель дипломного проекта: внедрение программного комплекса GIS Ankey SIEM NG в инфраструктуру предприятия ООО «НПФ» «ИСБ».

Задачи

Задачами дипломного проекта в связи с указанной целью являются:

- изучение нормативно-правовой и технической документации;
- анализ предметной области, существующей инфраструктуры Предприятия;
- изучение требований к внедряемой системе для решения поставленной цели, изучение целей внедрения системы;
- процесс внедрения GIS Ankey SIEM NG;
- конфигурирование системы для корректной работы;
- проверка работоспособности системы в целом, доработка обнаруженных неисправностей;
- написание экономической части данного дипломного проекта;
- оформление проделанной работы в пояснительную записку.

Реализация

В специальной части дипломного проекта реализованы следующие пункты:

- Рассмотрение назначения, цели внедрения и требований к внедряемой системе;
- Анализ предприятия, проектирование системы в его инфраструктуре;
- Процесс установки основных компонентов системы;
- Настройка системы;
- Процесс создания задач на сбор событий ИБ (Windows, Linux, CP Gaia, Kaspersky KSC);
- Проверка корректности выполнения созданных задач на сбор событий.

Анализ предприятия, проектирование системы в инфраструктуре

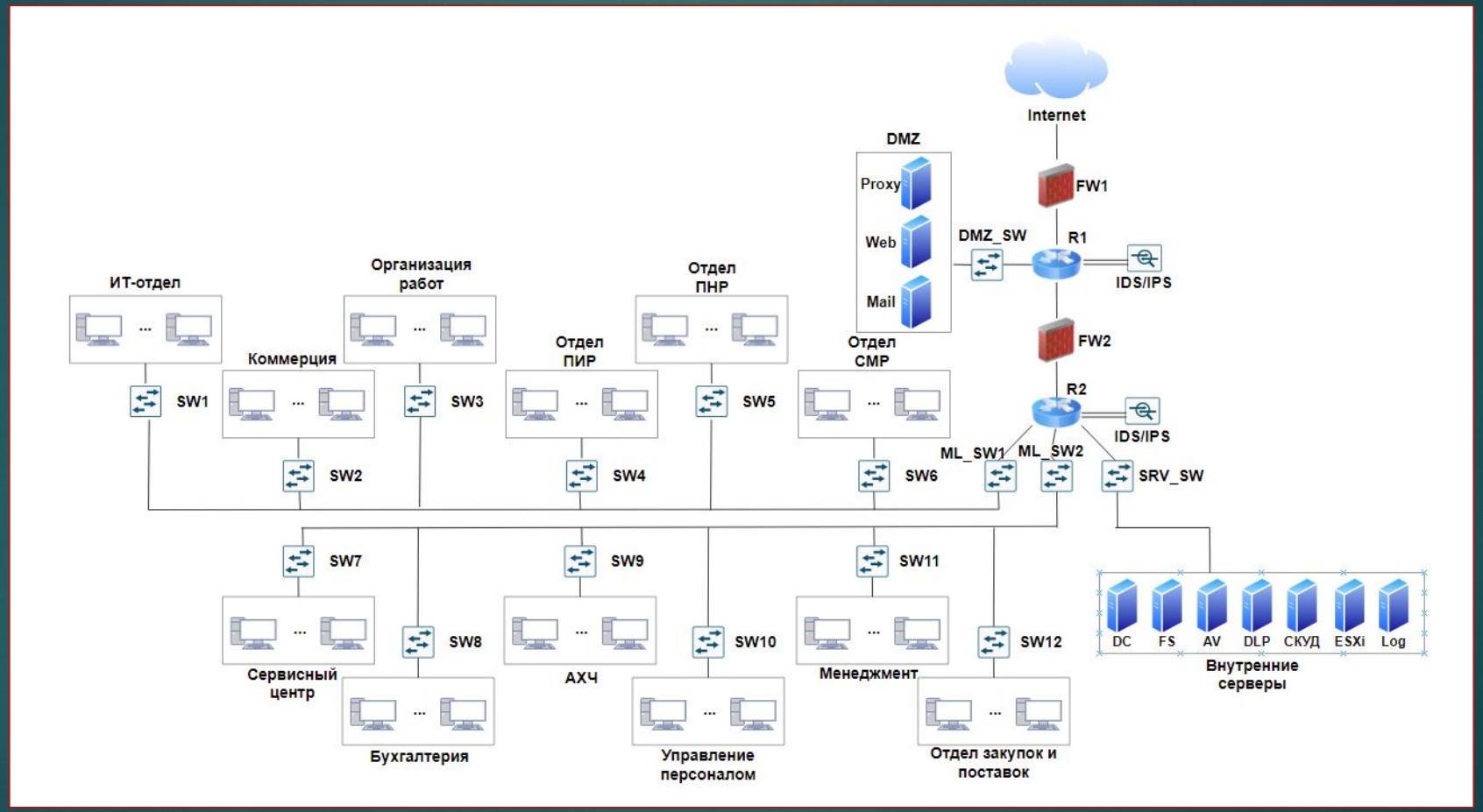


Схема инфраструктуры предприятия

Анализ предприятия, проектирование системы в инфраструктуре

Таблица 1 – Объекты автоматизации

Структурное подразделение	Наименование процесса	Возможность автоматизации	Решение об автоматизации в ходе проекта
Отдел ИТ	Управление инфраструктурой, активами	Возможна	Будет автоматизирован
Отдел ИТ	Инвентаризация активов инфраструктуры	Возможна	Будет автоматизирован
Отдел SOC	Анализ информации ИБ	Возможна	Будет автоматизирован
Отдел SOC	Централизованный сбор событий ИБ с источников	Возможна	Будет автоматизирован
Отдел SOC	Принятие решений по реагированию на инциденты ИБ	Возможна	Будет автоматизирован
Отдел SOC	Ведение отчетности по состоянию ИБ для топ-менеджмента	Возможна	Будет автоматизирован

Бизнес-процессы ИТ отдела, подлежащие автоматизации

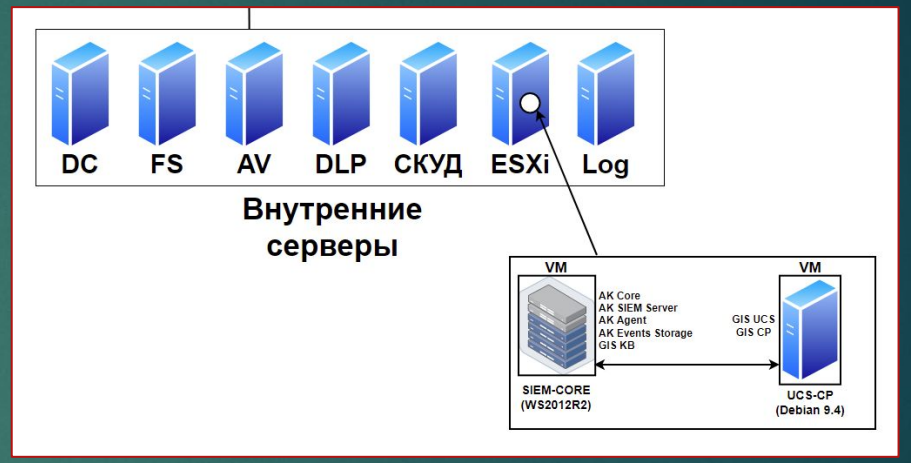
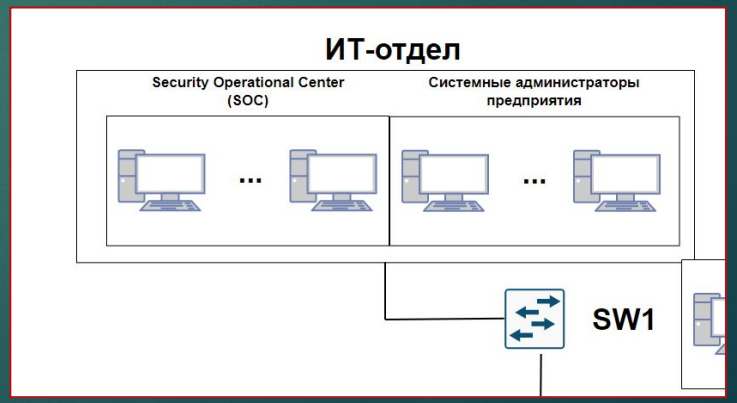
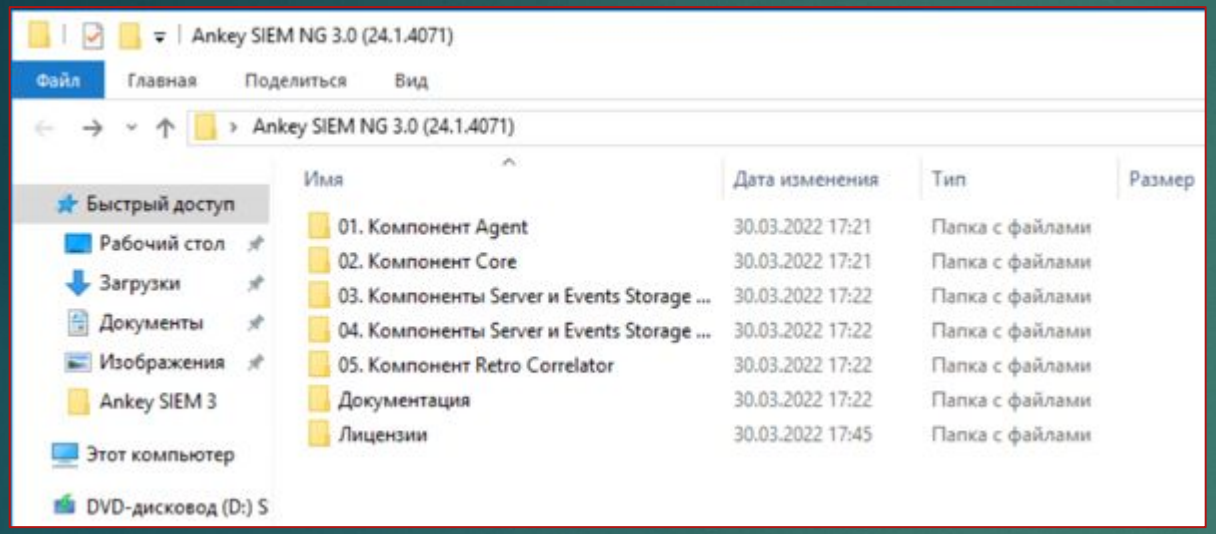


Схема разворачивания системы в инфраструктуре

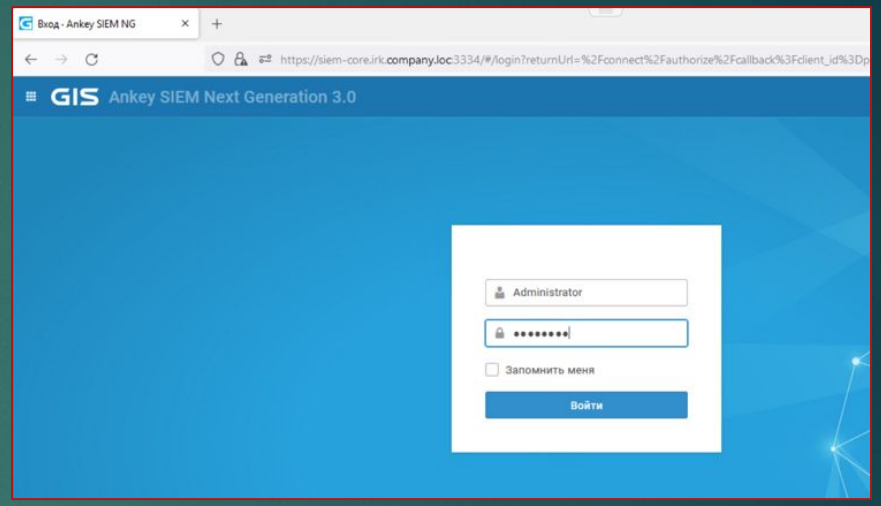


Новая структура ИТ-отдела предприятия

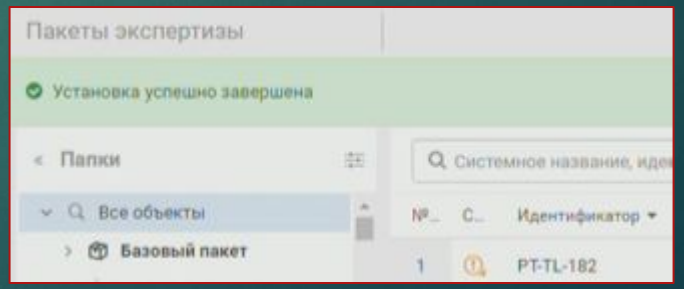
Процесс установки основных компонентов системы



Содержимое диска с дистрибутивами Ankey SIEM NG

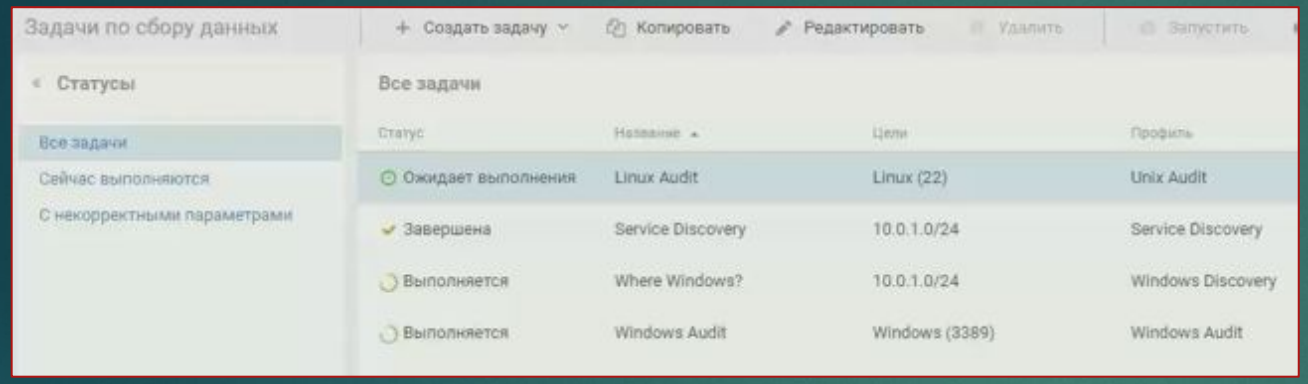


Окно входа в веб-консоль системы



Успешная установка системной базы знаний

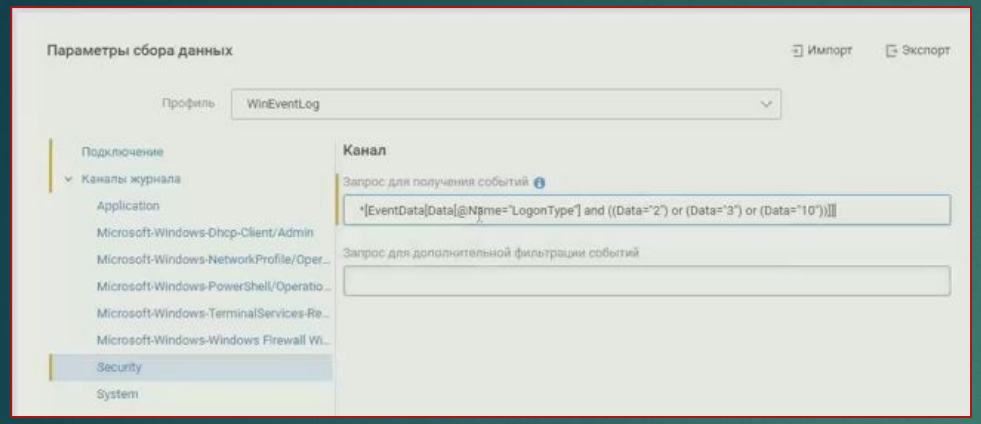
Настройка системы



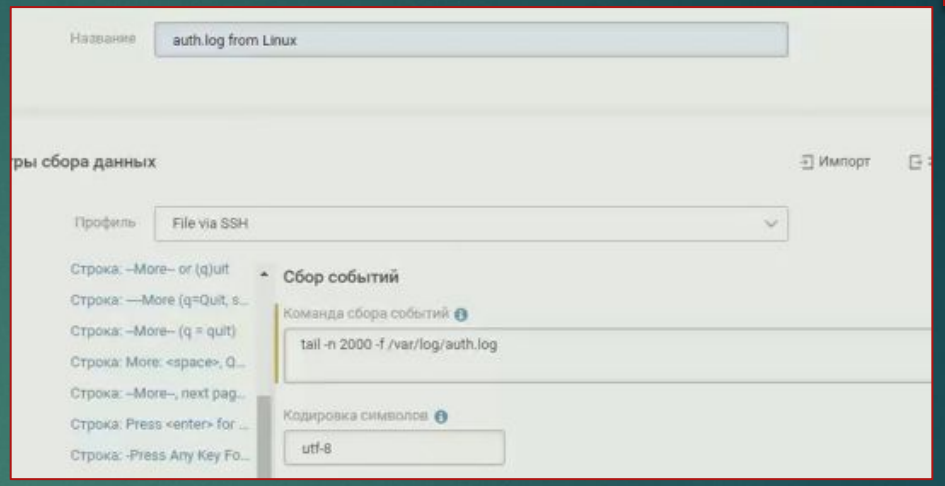
Выполнение задач на сбор данных об активах (инвентаризация)

Собранная информация о конкретном активе

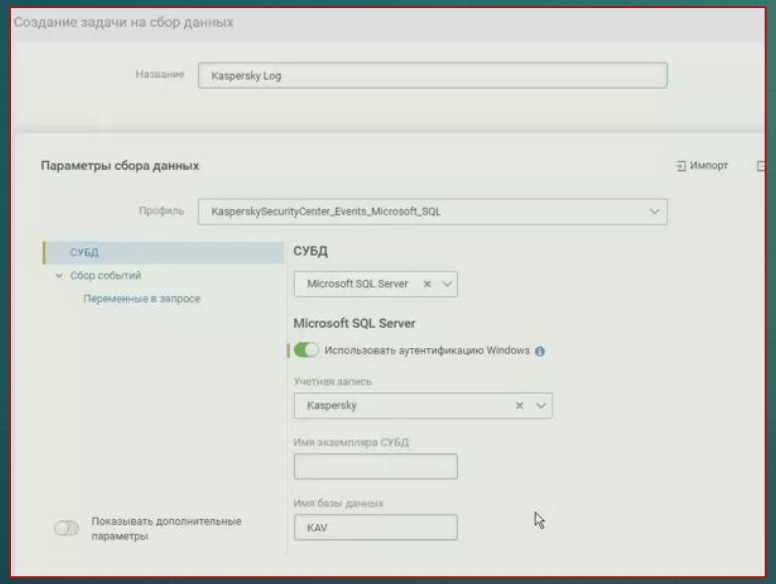
Создание задач на сбор событий ИБ с активов



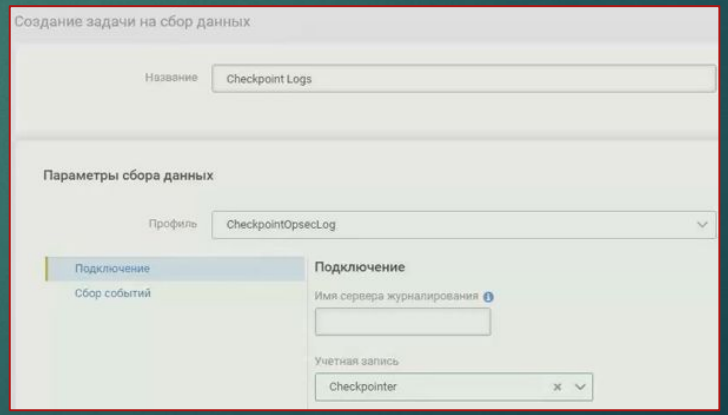
Процесс создания задачи на сбор событий Windows



Процесс создания задачи на сбор событий Linux

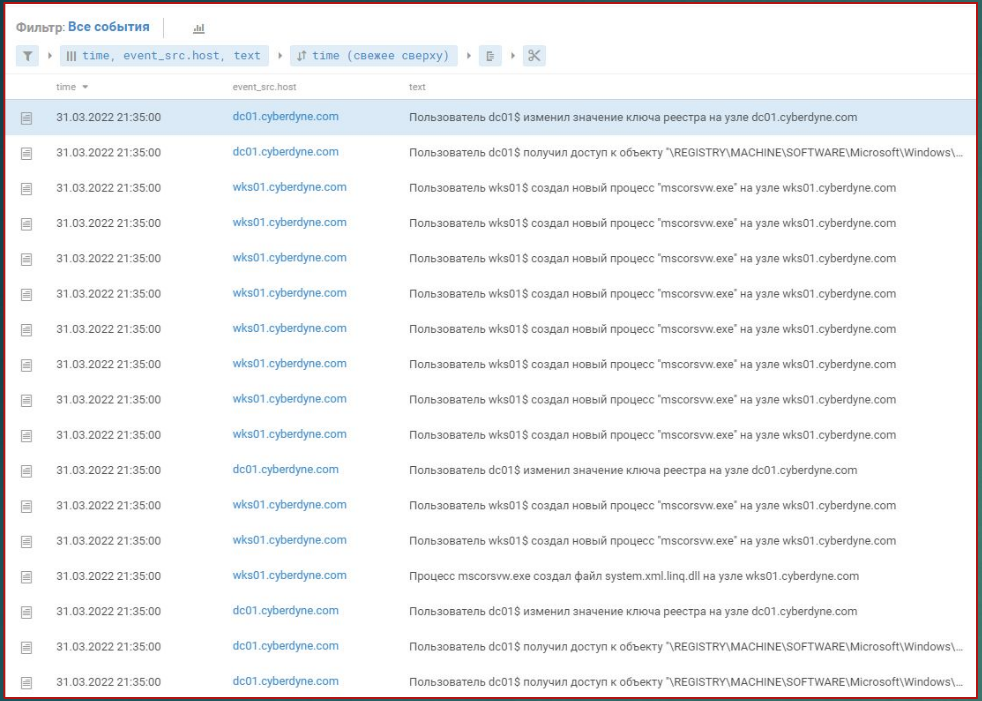


Процесс создания задачи на сбор событий KSC



Процесс создания задачи на сбор событий CheckPoint

Проверка корректности отработавших задач

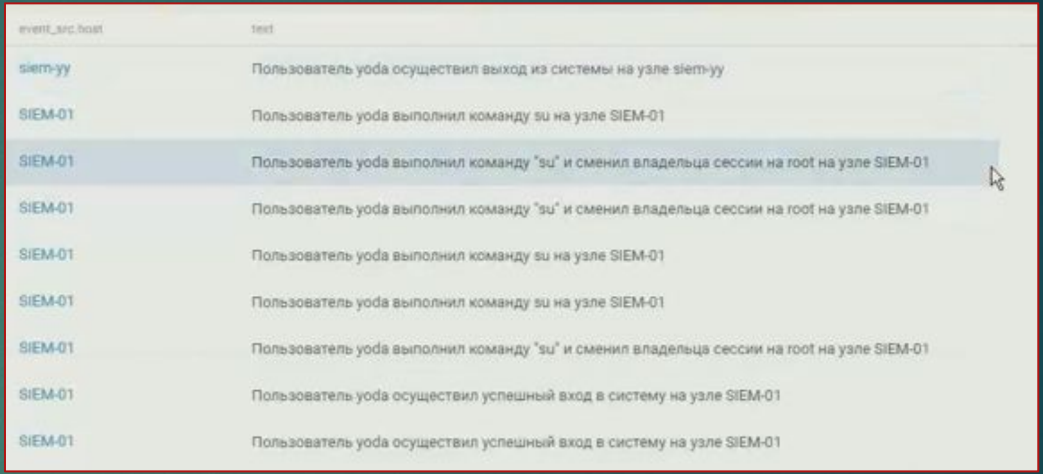


Фильтр: Все события

time, event_src.host, text | time (свежее сверху)

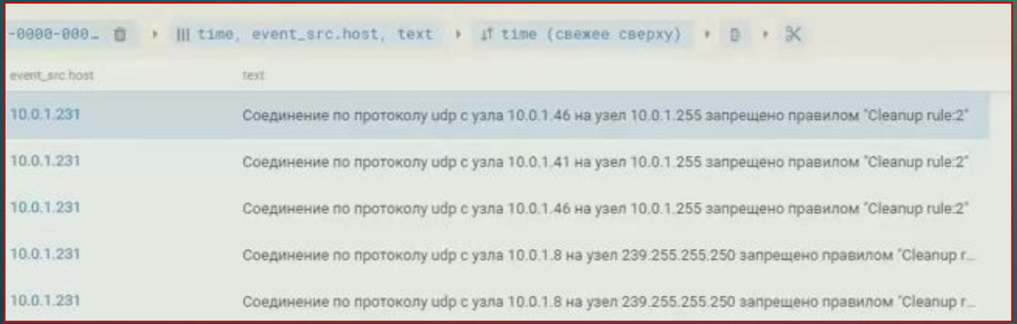
time	event_src.host	text
31.03.2022 21:35:00	dc01.cyberdyne.com	Пользователь dc01$ изменил значение ключа реестра на узле dc01.cyberdyne.com
31.03.2022 21:35:00	dc01.cyberdyne.com	Пользователь dc01$ получил доступ к объекту "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\...
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	dc01.cyberdyne.com	Пользователь dc01$ изменил значение ключа реестра на узле dc01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Пользователь wks01$ создал новый процесс "mscorsvw.exe" на узле wks01.cyberdyne.com
31.03.2022 21:35:00	wks01.cyberdyne.com	Процесс mscorsvw.exe создал файл system.xml.linq.dll на узле wks01.cyberdyne.com
31.03.2022 21:35:00	dc01.cyberdyne.com	Пользователь dc01$ изменил значение ключа реестра на узле dc01.cyberdyne.com
31.03.2022 21:35:00	dc01.cyberdyne.com	Пользователь dc01$ получил доступ к объекту "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\...
31.03.2022 21:35:00	dc01.cyberdyne.com	Пользователь dc01$ получил доступ к объекту "\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\...

События Windows



event_src.host	text
siem-yy	Пользователь yoda осуществил выход из системы на узле siem-yy
SIEM-01	Пользователь yoda выполнил команду su на узле SIEM-01
SIEM-01	Пользователь yoda выполнил команду "su" и сменил владельца сессии на root на узле SIEM-01
SIEM-01	Пользователь yoda выполнил команду "su" и сменил владельца сессии на root на узле SIEM-01
SIEM-01	Пользователь yoda выполнил команду su на узле SIEM-01
SIEM-01	Пользователь yoda выполнил команду su на узле SIEM-01
SIEM-01	Пользователь yoda выполнил команду "su" и сменил владельца сессии на root на узле SIEM-01
SIEM-01	Пользователь yoda осуществил успешный вход в систему на узле SIEM-01
SIEM-01	Пользователь yoda осуществил успешный вход в систему на узле SIEM-01

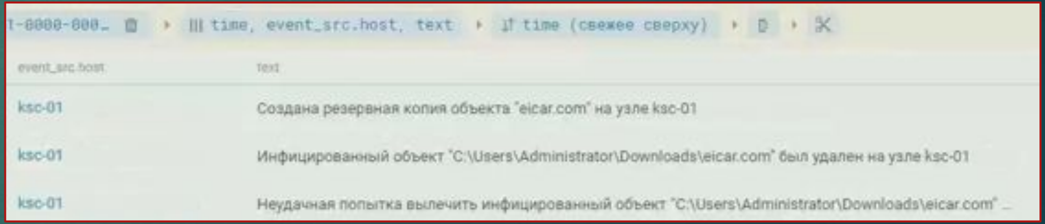
События Linux



-0000-000... | time, event_src.host, text | time (свежее сверху)

event_src.host	text
10.0.1.231	Соединение по протоколу udp с узла 10.0.1.46 на узел 10.0.1.255 запрещено правилом "Cleanup rule:2"
10.0.1.231	Соединение по протоколу udp с узла 10.0.1.41 на узел 10.0.1.255 запрещено правилом "Cleanup rule:2"
10.0.1.231	Соединение по протоколу udp с узла 10.0.1.46 на узел 10.0.1.255 запрещено правилом "Cleanup rule:2"
10.0.1.231	Соединение по протоколу udp с узла 10.0.1.8 на узел 239.255.255.250 запрещено правилом "Cleanup r...
10.0.1.231	Соединение по протоколу udp с узла 10.0.1.8 на узел 239.255.255.250 запрещено правилом "Cleanup r...

События CheckPoint



t-0000-000... | time, event_src.host, text | time (свежее сверху)

event_src.host	text
ksc-01	Создана резервная копия объекта "eicar.com" на узле ksc-01
ksc-01	Инфицированный объект "C:\Users\Administrator\Downloads\eicar.com" был удален на узле ksc-01
ksc-01	Неудачная попытка вылечить инфицированный объект "C:\Users\Administrator\Downloads\eicar.com" ...

События KSC

Экономическая часть

- Технико-экономическое основание показывает, что проект технически возможен и экономически выгоден, а также содержит анализ затрат и результатов проекта.

Бф – AK SIEM NG
Бк1 – PT MaxPatrol SIEM
Бк2 – HPE ArcSight

Таблица 9 – Расчет себестоимости разработки

Наименование статей расходов	**Стоимость, руб.**
Затраты на оплату труда (фонд оплаты труда)	52403
Амортизация	61358,58
Затраты на электроэнергию	16876,8
Итого:	130638,38

Итоговая себестоимость реализации проекта

Таблица 10 – Оценочная карта для сравнения конкурентных технических решений

Критерии оценки	**Вес критерия**	**Баллы**			**Конкурентоспособность, средневзвешенное значение**		
		Бф	Бк1	Бк2	Кф	Кк1	Кк2
Технические критерии оценки ресурсоэффективности							
Повышение производительности труда пользователя	0,15	5	5	5	0,75	0,75	0,75
Удобство во внедрении	0,05	4	4	3	0,2	0,2	0,15
Удобство в эксплуатации	0,1	5	5	4	0,5	0,5	0,4
Качество продукта	0,2	5	5	4	1	1	0,8
Техническая поддержка от производителя	0,05	4	5	3	0,2	0,25	0,15
Простота эксплуатации	0,05	5	4	4	0,25	0,2	0,2
Надежность	0,15	5	5	4	0,75	0,75	0,6
Экономические критерии оценки эффективности							
Конкурентоспособность решения	0,08	4	5	3	0,32	0,4	0,24
Уровень проникновения на рынок	0,05	4	5	3	0,2	0,25	0,15
Цена	0,07	5	3	2	0,35	0,21	0,14
Предполагаемый срок эксплуатации	0,05	5	4	4	0,25	0,2	0,2
Итого:	**1**	-	-	-	4,77	4,71	3,78

Оценочная карта сравнения конкурентных решений

Заключение

Цель дипломного проекта была достигнута путем выполнения следующих поставленных задач:

- изучена нормативно-правовая и техническая документация;
- проанализирована предметная область, инфраструктура Предприятия, изучены требования к системе, изучены цели внедрения;
- произведен процесс внедрения и настройки системы;
- произведена конфигурация системы, связанная со сбором событий ИБ с источников, проверена работоспособность системы.

Достигнут желаемый результат: мониторинг, управление и реагирование событиями и инцидентами ИБ в инфраструктуре Предприятия были централизованы, информация обрабатывается до легко воспринимаемого аналитиками ИБ состояния, для дальнейшего администрирования и использования системы на Предприятии был организован отдел – центр управления безопасностью (SOC), являющийся частью ИТ-отдела.

Спасибо за внимание!