



Опыт внедрения XDR в технологическом сегменте сети

Подготовил: Сафонов Александр

Начальник управления информационной безопасности ООО «АПИ-ФАКТОРИ»

1. Предпосылки

- Выполнение требований законодательства



- Уровень зрелости информационной безопасности

2. Защита проекта

Основные критерии

- Обеспечение непрерывности производства (ответственность, деньги)
- Выполнение законодательства (ответственность, деньги)



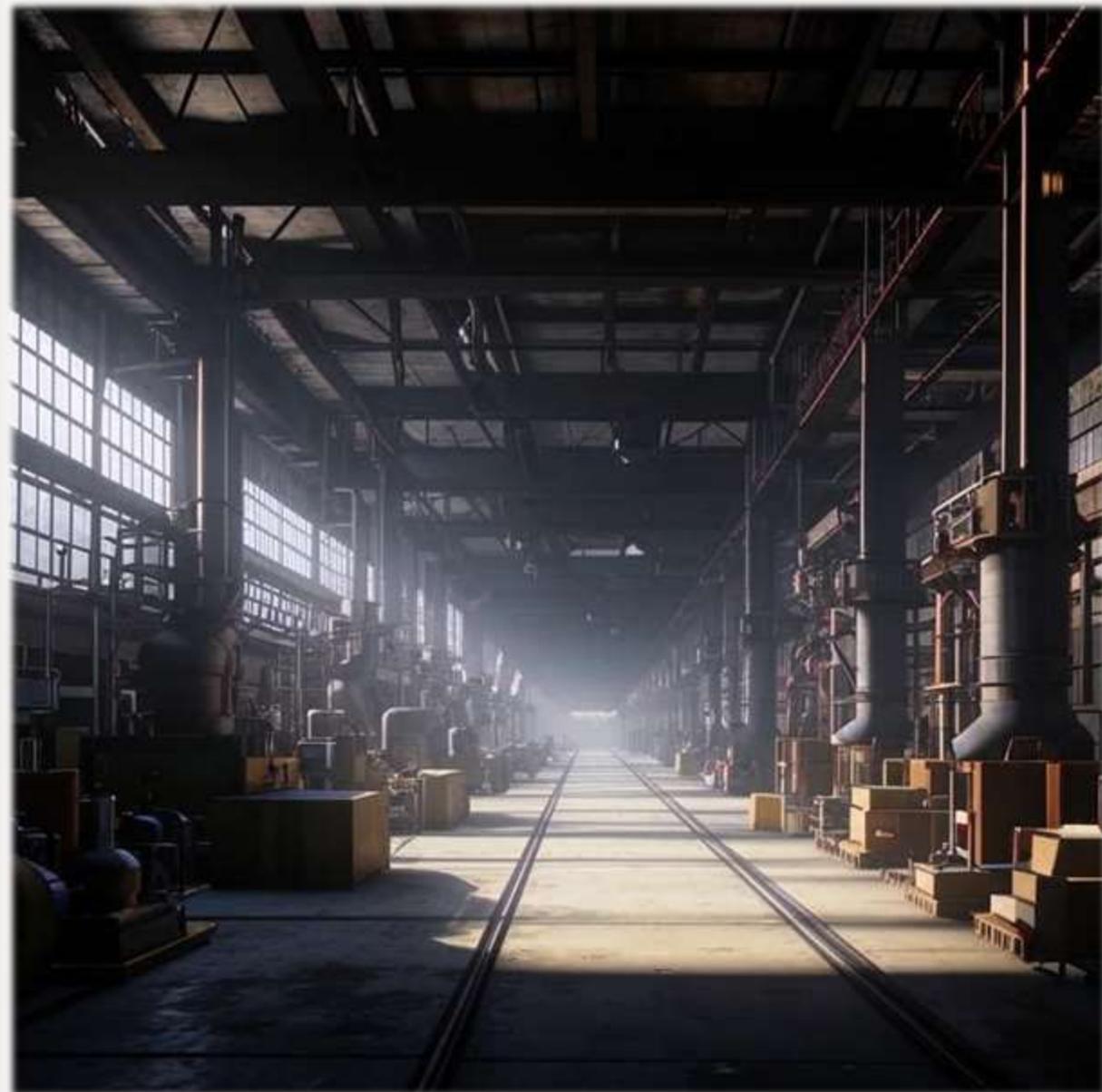
3.Выбор средств защиты

Основные критерии:

- Выполнение требований законодательства
- Поддержка промышленных протоколов
- Минимальное влияние на технические средства ТСПД
- Совместимость с уже применяемыми средствами защиты



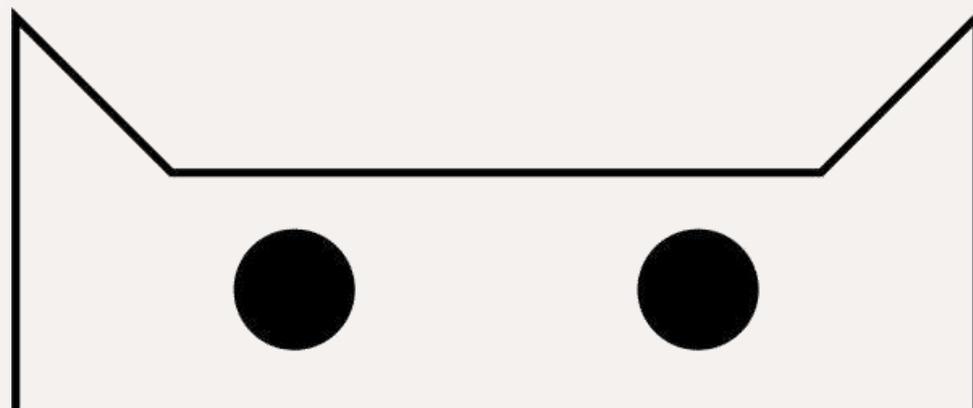
4. Внедрение решения



Где внедрили



РИМЕРА
ИЖНЕФТЕМАШ



CYBERSTEEL



РИМЕРА
АЛНАС

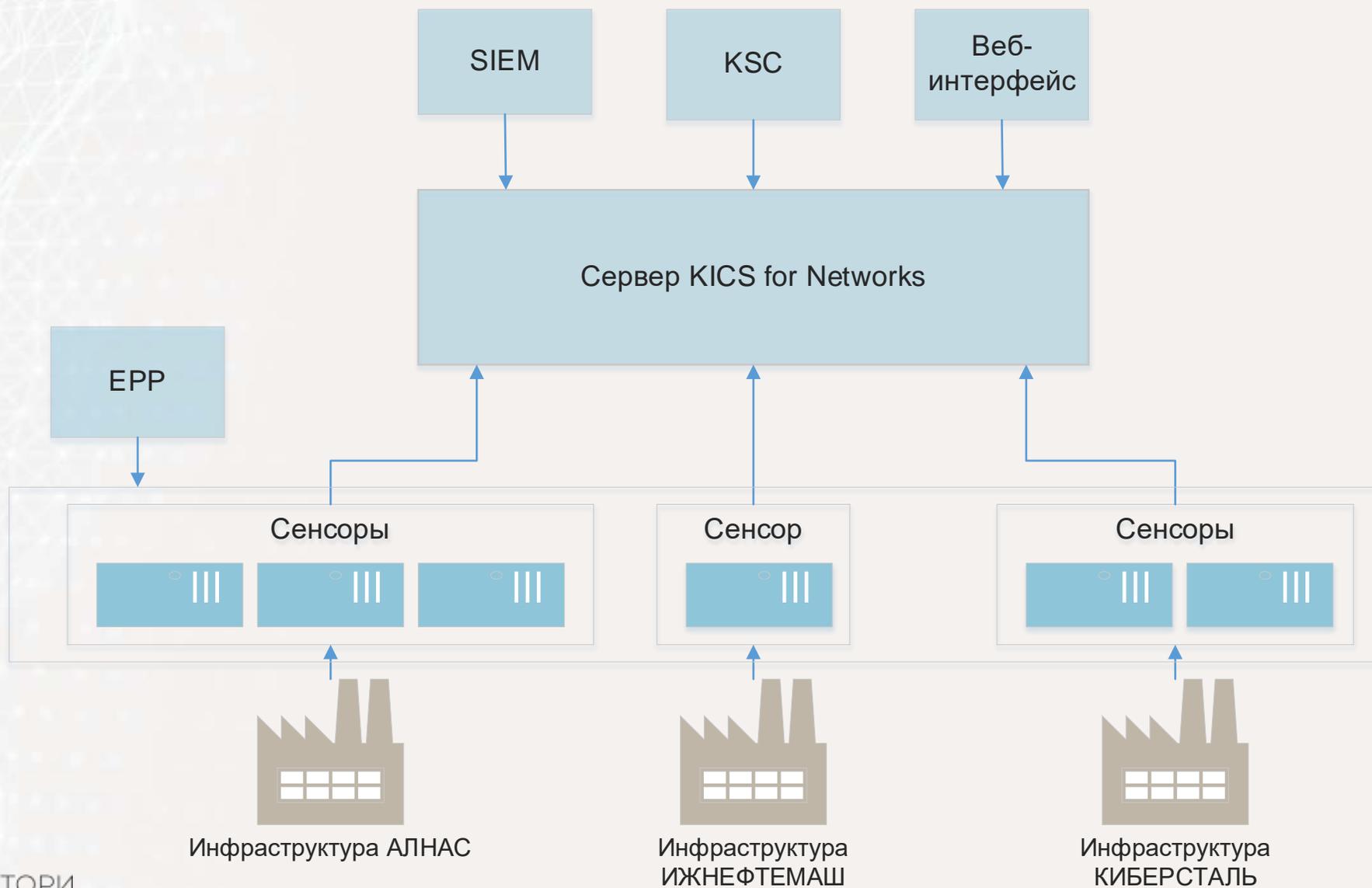
Как внедряли

- Сбор исходных данных о площадках внедрения
- Установка Сервера KICS for Networks
- Установка и подключение сенсоров
- Установка и интеграция EPP*
- Интеграция решения с KUMA SIEM
- Активация точек мониторинга
- Постановка сенсоров в режим обучения

*EPP - Endpoint Protection Platform



Итоговая структура



5. Результаты внедрения



Достижение главных целей

- Выполнение требований законодательства РФ в области защиты критической информационной инфраструктуры
- Внедрение решения для защиты от угроз информационной безопасности в ТСПД
- Отсутствие негативного влияния на ТСПД и конечные точки из сегмента АСУ ТП



Новые возможности реагирования (в ТСПД)

- Анализ сетевого трафика между узлами
- Проверка соответствия сетевого взаимодействия заданным правилам
- Обнаружение вторжений
- Сбор событий безопасности и интеграция с SIEM
- Обнаружение рисков для ресурсов информационных систем
- Защита конечных точек

Приложение 1. Анализ сетевого трафика

6 Обнаружено неразрешенное сетевое взаимодействие (TCP)

Изменить статус Показать связи Реагирование на угрозы Создать разрешающее правило Скачать трафик

Статус	Обработано	Тип события	4000002601
Технология	NIC Контроль целостности сети	Источник	Системное
ID	7871664	Сработавшее правило	—

Протокол Ethernet II / IP / TCP

Отправитель

Устройство	Неизвестное устройство
IP-адрес	10. . .
Номер порта	76
MAC-адрес	c4:00
VLAN ID	—



Получатель

Устройство	Неизвестное устройство
IP-адрес	10. . .
Номер порта	5
MAC-адрес	c4:00
VLAN ID	—

Начало	10.10.2024 13:41:38.752
Последнее появление	10.10.2024 13:41:38.752
Завершение	10.10.2024 14:02:20.927
Всего появлений	1
Метка	☆

Приложение 2. Разрешающие правила

Разрешающие правила

+ Добавить правило | ▶ Включить | ⊘ Выключить | 🗑️

Статусы		Типы правил			Адресная инт		
Включено	Выключено	CC	NIC	EVT	Все адреса		
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
ID п...	▼	🕒	▼	Ти...	↓≡	▼	Протоко
<input checked="" type="checkbox"/>	16026	●	NIC	Ethernet			
<input type="checkbox"/>	16025	●	NIC	Ethernet			
<input type="checkbox"/>	16024	●	NIC	Ethernet			
<input type="checkbox"/>	16023	●	NIC	Ethernet			
<input type="checkbox"/>	16022	●	NIC	Ethernet			
<input type="checkbox"/>	16021	●	NIC	Ethernet			
<input type="checkbox"/>	16020	●	NIC	Ethernet			

Ethernet II / IP / TCP

×

✎ Изменить | 🗑️ Удалить | ⊘ Выключить | 📄 Копировать правило

Статус: Включено | ID правила: 16026
Тип правила: **NIC** Контроль целостности сети | Источник: Система

Создано: 10.10.2024 19:45:13.451
Изменено: 10.10.2024 19:45:13.451
Протоколы/Команды: Ethernet II / IP / TCP

Сторона 1

АП-МАС: Киберсталь
MAC: 44:b6:
АП-IP: Киберсталь
IP: 62. . . .
Порт: 1

Сторона 2

АП-МАС: Киберсталь
MAC: 5c:e9:
АП-IP: Киберсталь
IP: 10. . . .
Порт: Любой

Приложение 3. Сбор событий безопасности

События и инциденты

Экспорт | Изменить статус | Показать связи | Обновление | Выбрано: 1 из 2000+ | Поиск событий

706 тыс. Новых событий | 0 Событий в обработке | Оценки: 0 - 10 | Технологии: DPI, NIC, IDS, CC, EXT, AM, EPP | Период: 10.10.2024 12:18:54 - 11.10.2024 12:18:54

Фильтр по умолчанию

Посл...	Заголовок	Оце...	Отп...	Пол...	Про...	Техн...	Всег...	ID	Ста...	
<input type="checkbox"/>	10.10.2024 1...	В трафике приз...	9	Киберстал...	Киберстал...	IP	EXT	1	7872208	✓
<input checked="" type="checkbox"/>	10.10.2024 1...	Сработало п...	9	Киберстал...	Киберстал...	FTP	IDS	1	7872207	✓
<input type="checkbox"/>	11.10.2024 0...	Обнаружена ано...	3	Киберстал...	Киберстал...	HTTPS	IDS	1	7872886	⚙️
<input type="checkbox"/>	10.10.2024 1...	Обнаружено нер...	6			ARP	NIC	18	7870063	✓
<input type="checkbox"/>	10.10.2024 1...	Обнаружено нер...	6			ARP	NIC	54	7869747	✓

Приложение 4. Виджеты

Мониторинг

Виджеты

Процессор

Server
2 %

Оперативная память

Server
27 %

Занято на диске

Server
7 %

Время работы

Эффективное врем...
1 сут 01:13:34

Трафик

Вся программа
11 Мбит/с

Теги

Вся программа
61 тегов/с

Устройства

Марш-р: 7, ПЛК: 157, Другое: 1688, Сетевое устр-во: 7, HMI / SCADA: 2, Сервер: 22, Рабочая станция: 91, Мобильное устр-во: 1, Ноутбук: 8, Шлюз: 3

Поиск устройств

Маршрутизаторы, требующие внимания: 1
C9300-24T

ПЛК, требующие внимания: 4
MH241, Schneider EL..., Schneider EL..., Schneider EL...

Другие устройства, требующие внимания: 3
ILOCN79510..., Устройство ..., Устройство ...

Сетевые устройства, требующие внимания: 1

События

1ч 12ч 24ч 7д

Поиск событий

- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:15:49.465
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:15:19.456
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:14:49.447
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:14:19.437
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:11:29.375
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:10:49.364
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:10:19.355
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:09:49.346
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:09:19.337
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:08:49.328
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:08:19.319
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:07:49.309
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:07:19.300
- Отсутствует трафик на точке мониторинга ... 11.10.2024 15:06:50.292

Приложение 5. Обнаружение рисков

Риски			
Изменить статус			
Показать связи			
Экспорт			
Период обнаружения	Категории		
Последние 30 дней	Уязвимость	Конфигурация	АСУ ТП
Категория	Название		
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input checked="" type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	
<input type="checkbox"/>	Небезопасная архитектура сети	Взаимодействие по нежелательному протоколу	

8.1 Взаимодействие по нежелательному протоколу Ethernet II / IP / UDP / DNS/LLMNR поверх UDP в ОТ-подсети

Изменить | Изменить статус | Показать связи | Экспорт

Категория	Небезопасная архитектура сети	ID риска	64568
Статус	Актуальный	Тип риска	5000009104
Устройство	 .cybersteel.co m		

Описание

Обнаружено взаимодействие по нежелательному протоколу в подсети с типом Частная, ОТ.

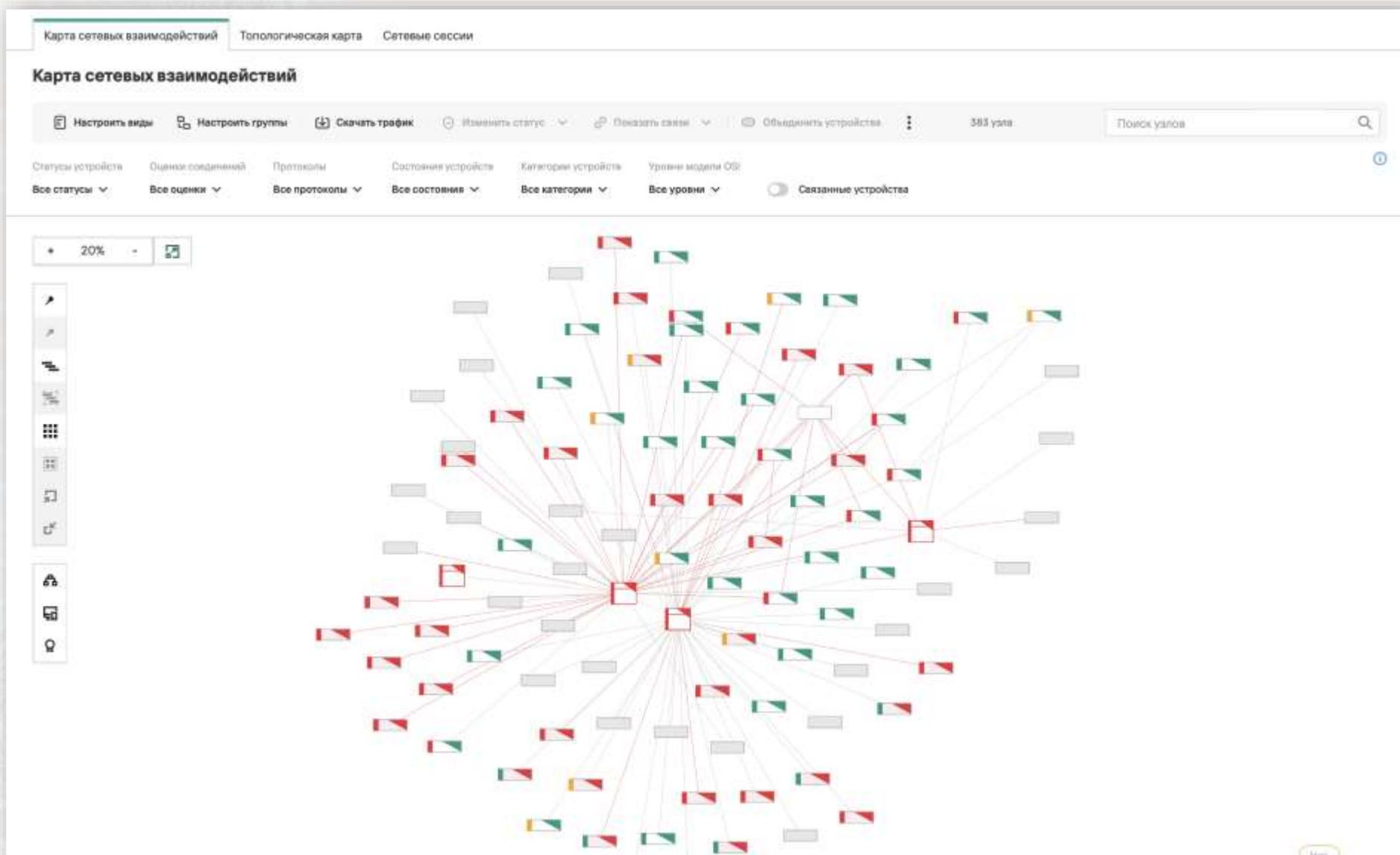
Возможные последствия.

- Использование нежелательных протоколов в промышленной сети позволяет злоумышленнику реализовать широкий спектр векторов атак.
- Наличие таких взаимодействий может свидетельствовать о нарушении политик безопасности, неверной конфигурации сетевого оборудования или неправильно спроектированной архитектуре сети.

Меры по устранению угроз.

- Проверить устройства, на которых зафиксировано использование нежелательных протоколов, на наличие неразрешенного ПО.
- Выполнить антивирусную проверку устройств, на которых зафиксировано использование нежелательных протоколов.
- Проверить параметры сетевых устройств на правильность конфигурации правил фильтрации протоколов.

Приложение 6. Карта сетевых взаимодействий



Приложение 7. Интерфейс управления технологиями защиты

Server ✕

 Изменить  Выключить все  Включить все  Проверить целостность 

Управление технологиями Параметры

[Включить все](#) [Выключить все](#) [Обучение](#) ▼

<input checked="" type="checkbox"/> AM Обнаружение активности устройств	Обучение ▼	 Указать срок
<input checked="" type="checkbox"/> CC Контроль системных команд	Обучение ▼	 Указать срок
<input checked="" type="checkbox"/> DPI Контроль процесса по правилам	Обучение ▼	 Указать срок
<input checked="" type="checkbox"/> NIC Контроль целостности сети	Обучение ▼	 Указать срок
<input type="checkbox"/> AM Контроль проектов ПЛК		
<input checked="" type="checkbox"/> AM Обнаружение сведений об устройствах		
<input checked="" type="checkbox"/> AM Обнаружение рисков		
<input checked="" type="checkbox"/> DPI Обнаружение неизвестных тегов		
<input checked="" type="checkbox"/> DPI Обнаружение устройств для контроля процесса		
<input checked="" type="checkbox"/> IDS Обнаружение ARP-спуфинга		
<input checked="" type="checkbox"/> IDS Обнаружение аномалий в протоколе IP		
<input checked="" type="checkbox"/> IDS Обнаружение аномалий в протоколе TCP		
<input checked="" type="checkbox"/> IDS Обнаружение вторжений по правилам		
<input checked="" type="checkbox"/> IDS Обнаружение атак подбора и сканирования		
<input checked="" type="checkbox"/> AM Обнаружение сетевых сессий		

Благодарю за внимание!

Сафонов Александр

Начальник управления информационной безопасности ООО «АПИ-ФАКТОРИ»

Aleksandr.Safonov@rimera.com