PT
Информационная
безопасность

"EDRёный случай"
Как EDR спасает ИТ инфраструктуры и чему это нас учит

Алексей Жуков
Руководитель SOC | Владелец продукта RT Protect EDR

АО «РТ-Информационная безопасность»

более 100

специалистов из ведущих технических ВУЗов

Собственная экосистема продуктов ИБ

Единый центр компетенций по ИБ в ГК «Ростех»

РТ
Информационная безопасность

Алексей Жуков

Руководитель SOC I
Владелец продукта
RT Protect EDR

@AK_Zhukov

- Руководитель SOC для ГК Ростех
- Более **10 лет** в ИБ
- EX-pentester, C developer, threat analyst
- Более **5 лет** опыта развития продуктов EDR, XDR, NTA, SIEM, IPS, IRP

Современные тенденции

Расширение разнообразия используемых для написания ВПО языков программирования и технологий, усложнение архитектуры

Всё более сложные социотехнические атаки, что требует повышения осведомленности об информационной безопасности обычным работникам

Рост активности группировок, связанных с одной из сторон конфликта

Эксплуатация уязвимостей:

- Microsoft Exchange (ProxyNotShell - CVE-2022-41040)
- Apache Tomcat (Log4Shell - CVE-2021-44228)
- Microsoft Outlook Elevation of Privilege (CVE-2023-23397)
- Vmware Spring Framework (Spring4Shell - CVE-2022-22965)

Самые популярные уязвимости:

- CVE-2022-27228 (Bitrix vote module RCE)
- CVE-2021-34473 (MS Exchange RCE ProxyShell)
- CVE-2022-41040+CVE-2022-41082 (MS Exchange RCE ProxyNotShell)

Как следствие, повышение требований к защите конечных точек

PT
Информационная безопасность

Классические задачи EDR

PT Информационная безопасность

Сбор телеметрии (ingest)

- Процессы
- Файловая система
- Реестр
- Сеть
- Адреса в памяти
- Пользователи и группы
- WMI
- Автозагрузки
- Различные скрипты (PowerShell, AMSI, Bash и проч.)

Обнаружение (detection)

IoC / IoA

Автоматизированное выявление следов и TTP атакующих

YARA

Автоматизированное выявление инструментов атакующих

Vulnerability management

Своевременное оповещение об уязвимостях

Threat hunting

Ручной проактивный поиск следов / TPP атакующих

Золотой образ

Отслеживание белого списка ПО

Реагирование (response)

- Скачивание / загрузка / удаление файлов
- Завершение процесса
- Сбор данных
- Изоляция хоста
- Интерактивная консоль
- Запуск процессов / скриптов (bash)
- Антишифровальщик
- Автоматическое блокирование по хешу, имени

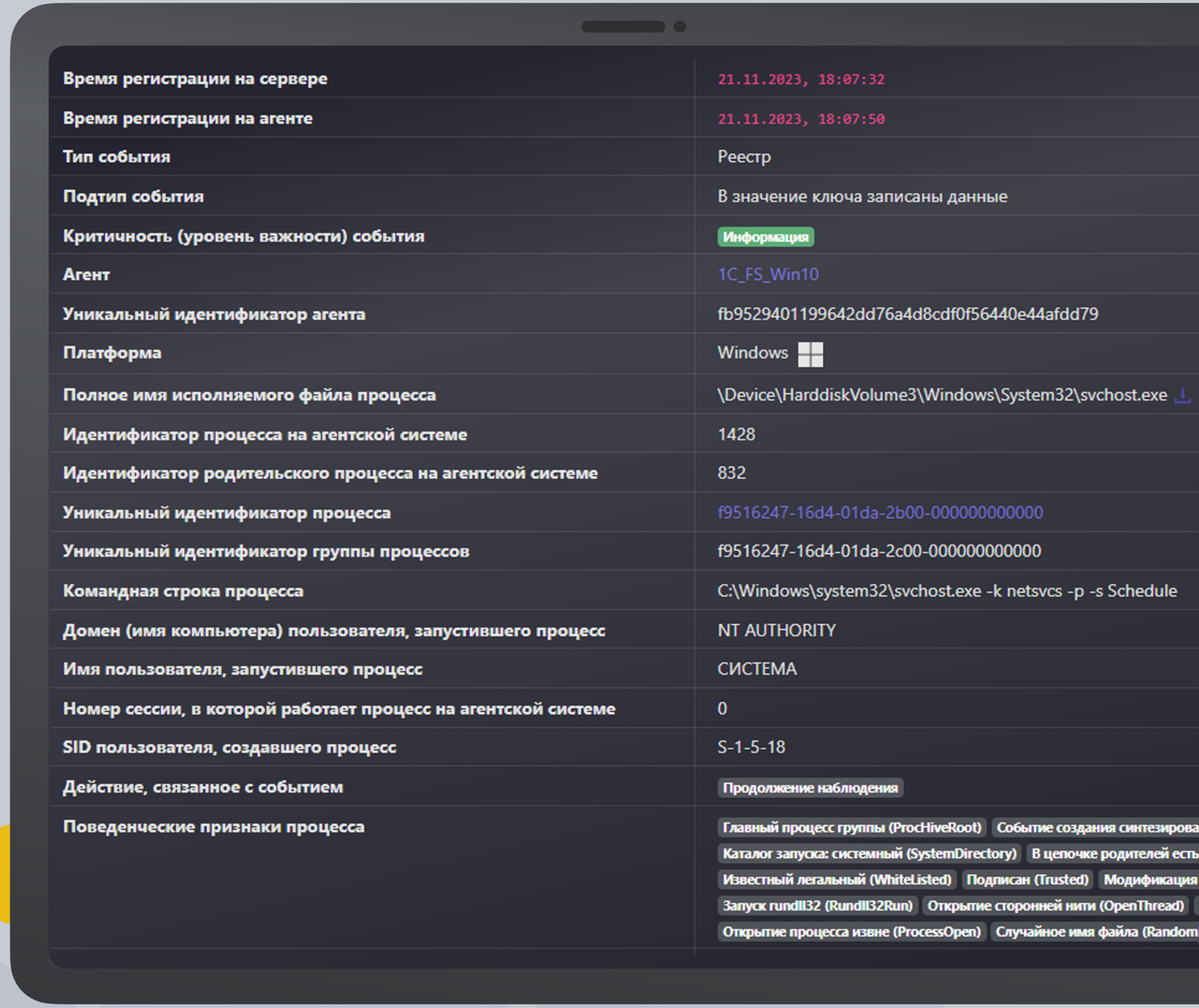
Как решать такие классические задачи EDR

- Сбор «сырых» низкоуровневых событий с расширенной моделью данных
- Сбор классических журналов (ETW)
- Синхронная обработка индикаторов атак/компрометации на агентах
- Профили сбора событий и реагирования на инциденты
- Расширение возможностей модулей Anti-Ransomware, Deception, VM
- Расширять аналитическое обогащение

PT
Информационная безопасность

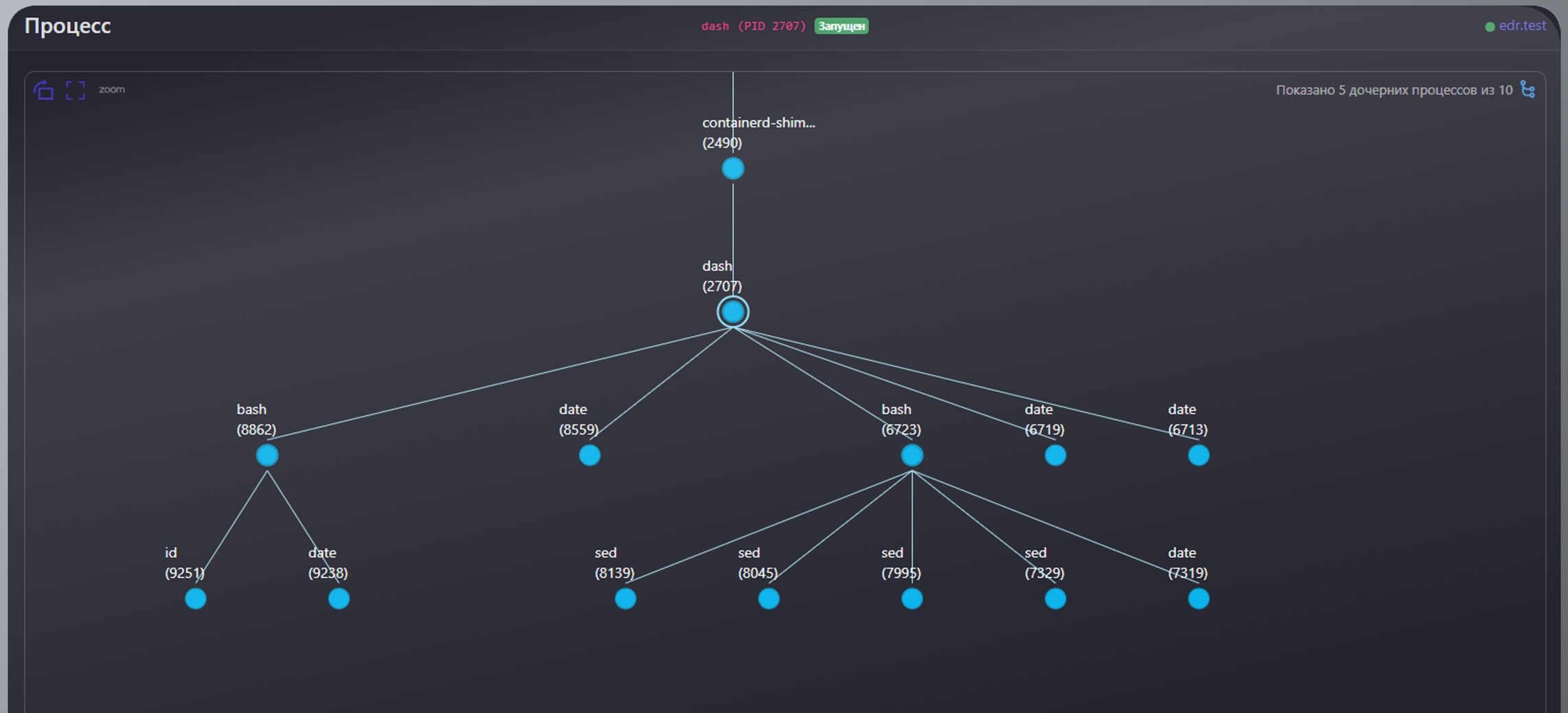
Сбор «сырых» событий

Сбор обязательных данных
от времени регистрации,
до специфических флагов
запуска



Дерево процессов

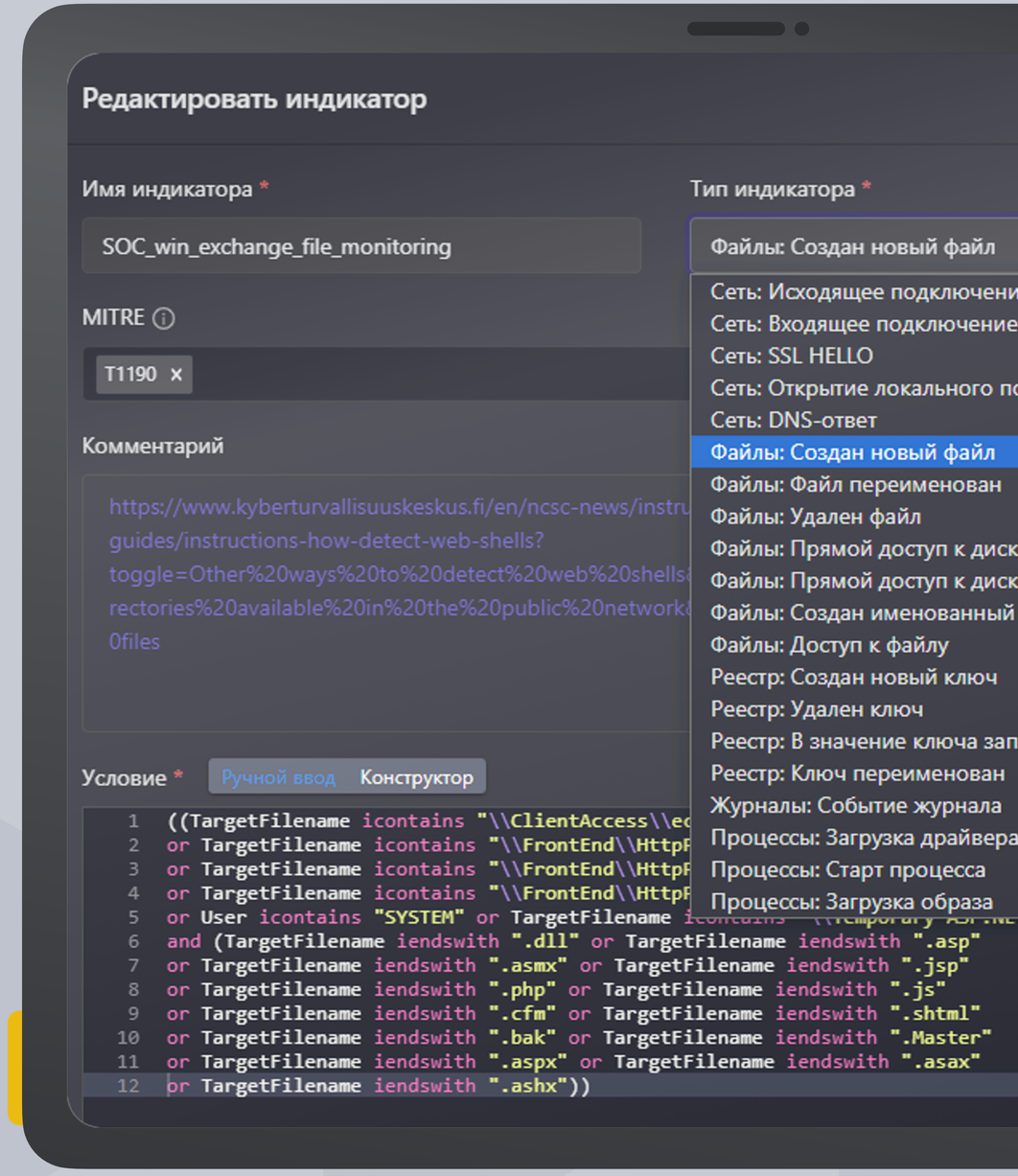
PT
Информационная безопасность



Индикаторы атак

Возможность писать правила обнаружения атак на основе событий:

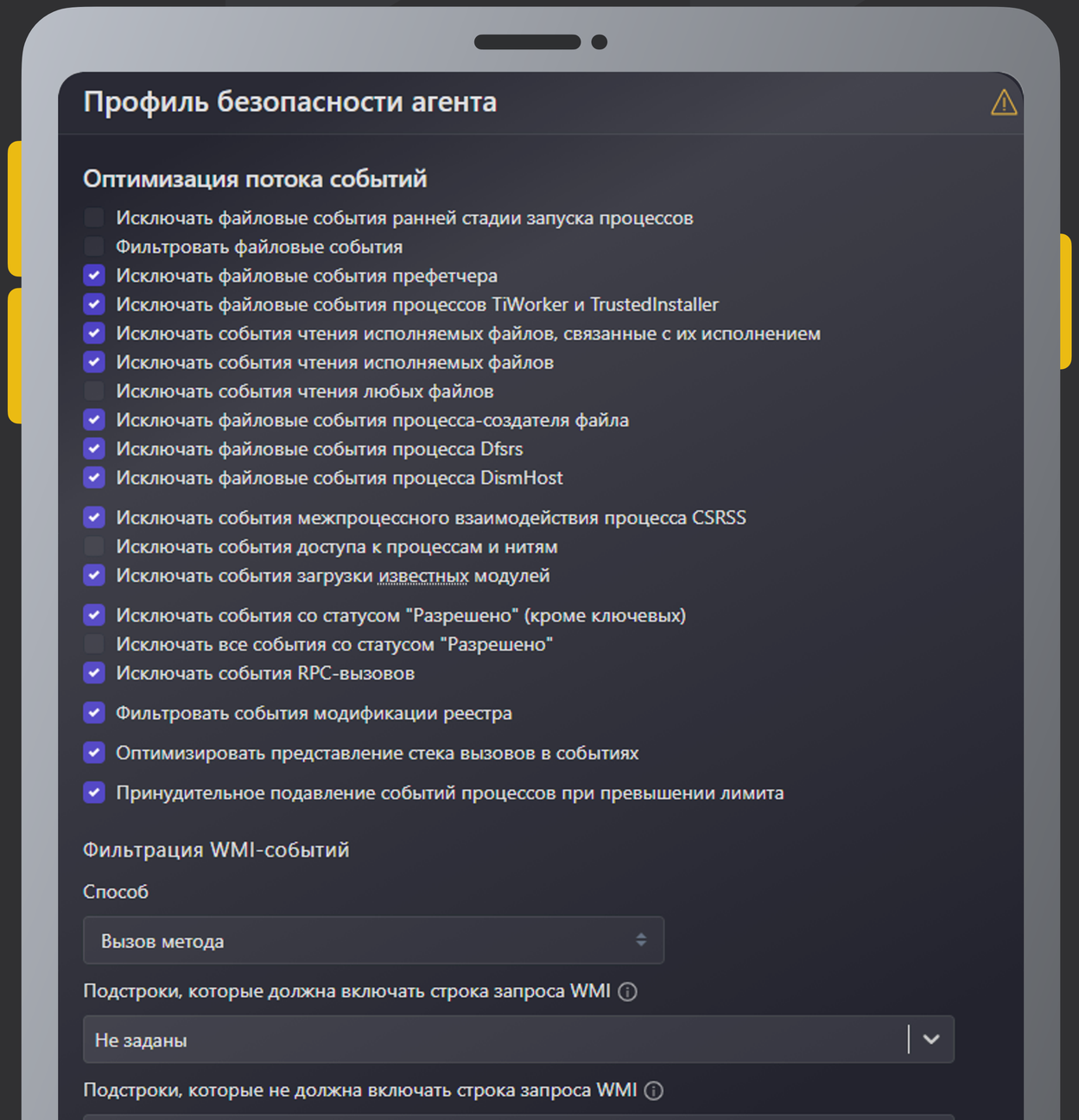
- создания процесса
- загрузки исполняемого модуля
- создания/ модификации файла
- DNS-запроса
- сетевого соединения (CONNECT)
- открытие порта для входящих соединений (LISTEN)
- и других событий



PT
Информационная безопасность

Гибкие настройки профилей

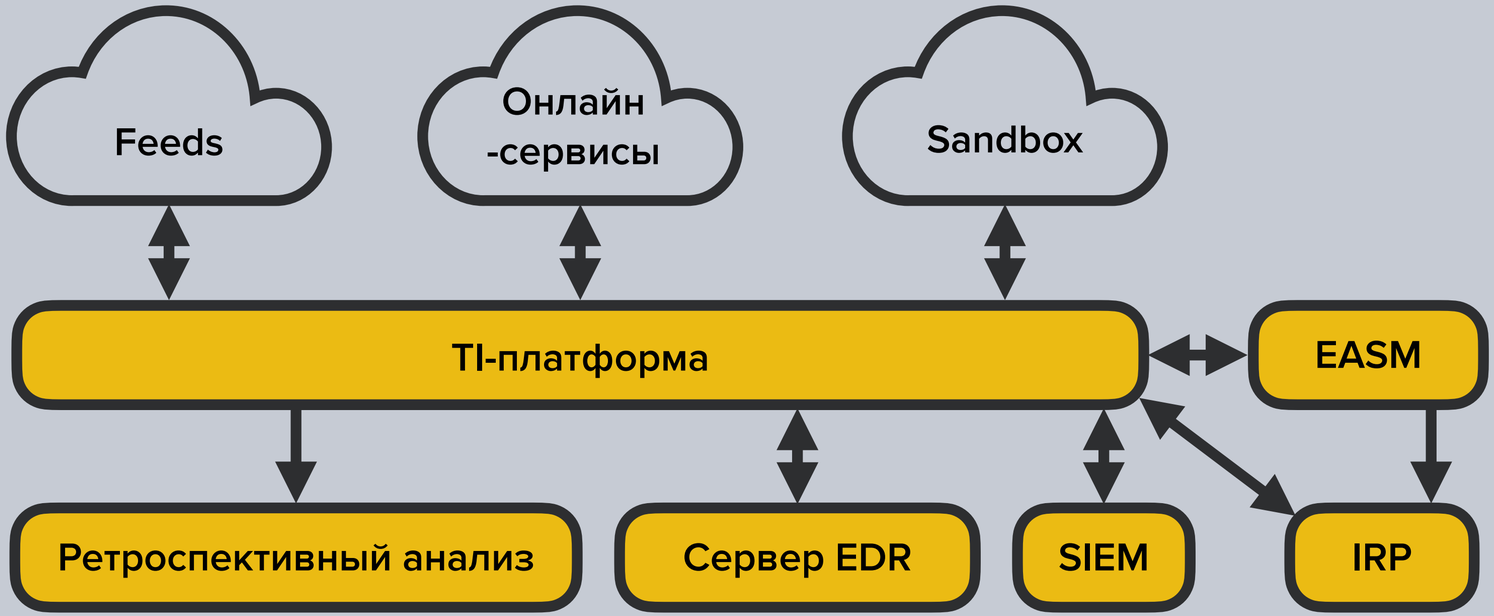
Всегда нужно иметь возможность в зависимости от типа хоста и его нагрузки «докрутить» сбор телеметрии



PT
Информационная безопасность

Расширенное аналитическое обогащение

- TI и распространение IoC/IoA
- Конвертер правил
- Detection As Code



Какие бывают EDR?

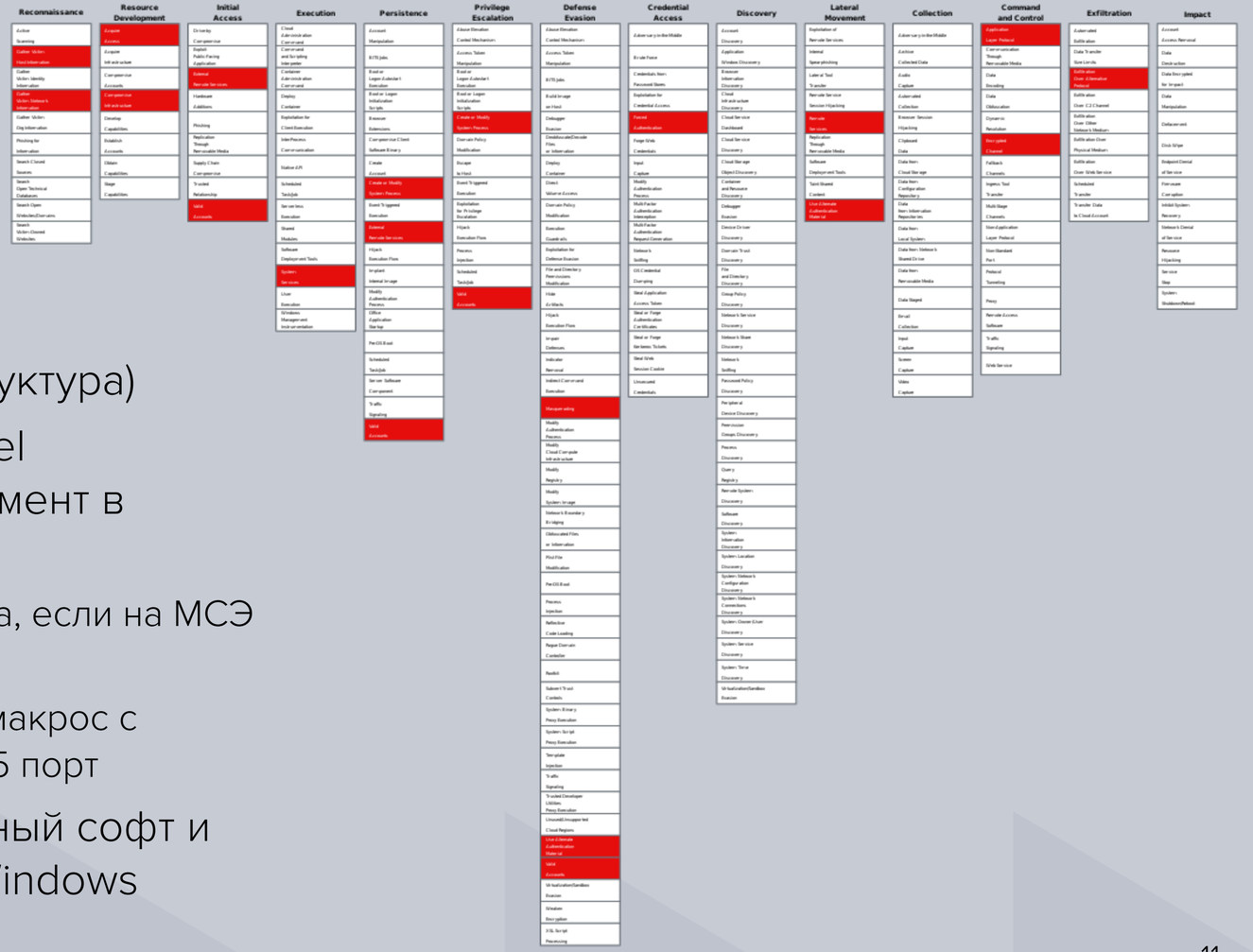
PT
Информационная безопасность

Must Have	Middle	Advanced
Сбор сырой телеметрии, стандартные журналы	Терминал доступа	Модуль уязвимостей
Запуск скриптов и/или файлов	Синхронная работа правил прямо на агенте	Threat Hunting
Базовая работа с сетью и изоляция	Работа с процессами и файлами, в т.ч. Anti-ransomeware	Профили мониторинга и реагирования в зависимости от типов хостов
Сбор инвентаризационной информации	Различные метрики работоспособности агентов	Цепочки автореспонса
IoC	Расширенные IoA, YARA	Конвертер правил
Гибкость в исключениях	Интеграция с TI, гибкость API	Возможность искать неуправляемые хосты и строить карту сети

Что мы ловили: кейс 1

PT
Информационная безопасность

APT Stealth Sword
Mitre ATT&CK



Техники закрепления группировки:

- SSH-ключи на сервере, о котором никто из администраторов не знал (теневая IT-инфраструктура)
- Внешние ссылки в часто используемых MS Excel документах. Указание внешней ссылки на документ в ячейке листа MS Excel позволяет:
  - перехватить Net-NTLM-v2 хеш пользователя домена, если на МСЭ не заблокирован 445 порт
  - запустить свою вредоносную нагрузку (например, макрос с реверс-шеллом), если на МСЭ не заблокирован 445 порт
- Служба Windows, маскирующаяся под легитимный софт и использующая в работе легитимные утилиты Windows

Что пошло не так?

Не хватило покрытия по сканированию инфраструктуры – не увидели «теневой сегмент», из которого шли атаки. Нужна интеграция ASM

PT
Информационная безопасность

Кейс 2. Не хватило самого EDR

APT Lazarus со своим ВПО была замечена как минимум в 3 организациях контура Корпорации

- **ВПО:** Trojan.Win64.Matadoor
- **Индикатор компрометации:** Связка из {имя}.dll и {имя}Helper.dll в C:\Windows\System32\ (загрузчик и образец фреймворка MATA)
- **Закрепление:** служба Windows
- **Распространение:**

  компрометация СЗИ

  ➜ удаленное выполнение команд с использованием СЗИ

  ➜ компрометация инфраструктуры

После установки, агент EDR:

- Пресёк запуск службы
- Начал блокировать индикаторы атак, что увидели на инциденте, пока шло расследование
- Блокировал powershell скрипты вредоноса

PT
Информационная безопасность

Кейс 3, где не хватило технологий

PT Информационная безопасность

ВПО Cobalt Strike

- В рамках одного из расследований зафиксировано использование одной из версий **CobaltStrike**
- ВПО распространялось с использованием протокола **SMB**
- Запуск исполняемых файлов осуществлялся с помощью **RPC**
- AMSI провайдер заблокировал выполнение **dotnet кода**

Вшитая в ВПО строка с названием именованного канала

```
// Token: 0x04000004 RID: 4
private static string name = "[redacted]";
```

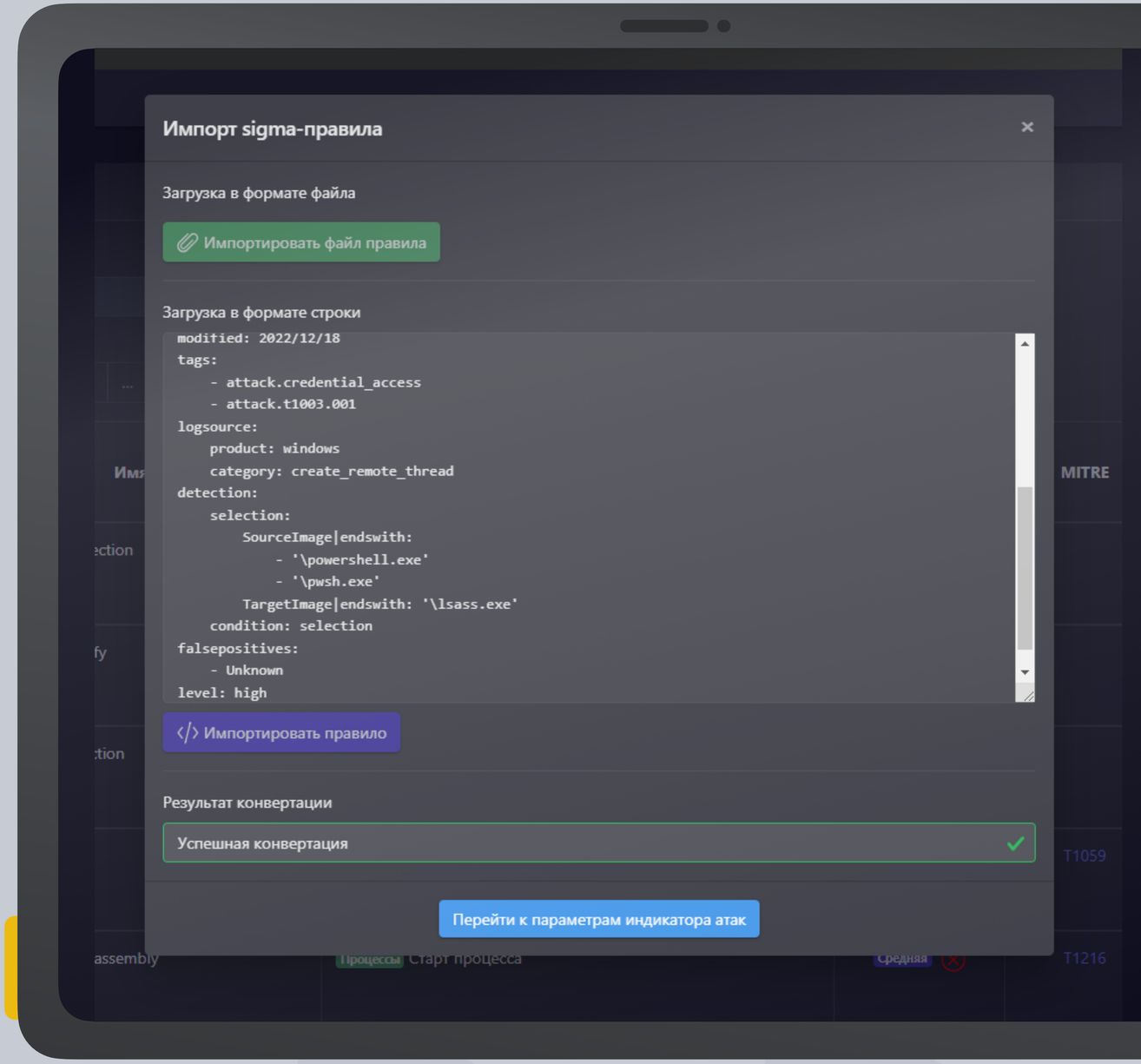
- Как-то происходил инжект в **w3wp.exe** – не хватило сканирования памяти.
- Взаимодействие между экземплярами ВПО осуществлялось с использованием именованных каналов (**named pipes**)
- Выполнение команд, реализованное в виде плейбуков **Ansible**, осуществлялось **в памяти** вредоносных процессов

Детектирование с использованием RT Protect EDR

[redacted] 19:37:45	DC / [redacted]	Файлы Создан именованный канал \Device\NamedPipe\uv-0000DF6E6D234AAD-BC85	OneDriveServerPresentationFramework.exe (5804)
[redacted] 19:37:36	DC / [redacted]	Файлы Создан именованный канал \Device\NamedPipe\crashpad_2824_TDCRYICWSDGDYJUC	OneDriveServerPresentationFramework.exe (5804)
[redacted] 19:37:32	DC / [redacted]	Файлы Создан именованный канал \Device\NamedPipe\aba6230a0e826892	OneDriveServerPresentationFramework.exe (5804)

Чему в итоге это нас учит

- Нужно постоянное совершенствование детекта и респонса, делать его более простым и удобным для аналитиков
- Взаимосвязь продуктов и обязательное API, полная интеграция
- Конвертер правил



Как расширить превент и детект через EDR и не только

Модули **Deception** в экосистеме

Интеграция с различными **Sandbox**

Модули уязвимостей и контроль утечек (**VM, EASM**)

NTA для обнаружения аномалий и записи трафика под расследование по команде экосистемы

PT
Информационная безопасность

Как расширить респонс?

Цепочки автоправил

Блокировка сетевых устройств

Призыв к действию для аналитиков от системы на различные действия по блокировке/изоляции

PT
Информационная безопасность

PT
Информационная безопасность

Портрет злоумышленников

Как от них защититься:

UTM • Антивирус • Антиспам • EDR • WAF
SA • Sandbox • Сегментация сети
NTA • EDR • IRP • СЗИ АСУ ТП • Anti-APT
Продвинутый SOC с маппингом по Killchain+Mitre ATT&CK

UTM • Антивирус • Антиспам • EDR • WAF
SA • Sandbox • Сегментация сети • NTA • EDR
IRP • СЗИ АСУ ТП • Anti-APT • Продвинутый SOC

UTM • Антивирус • Антиспам • EDR • WAF
SA • Sandbox • Сегментация сети • SOC •

WAF • UTM • Patch-менеджмент • Антивирус
Анализ журналов аудита СЗИ • Антиспам • EDR

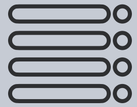
WAF • UTM • Patch-менеджмент

Аспекты на масштабах сервис провайдера и не только

Множество разнородных сегментов и инфраструктур

Распространение правил и аналитики

Дефицит кадров



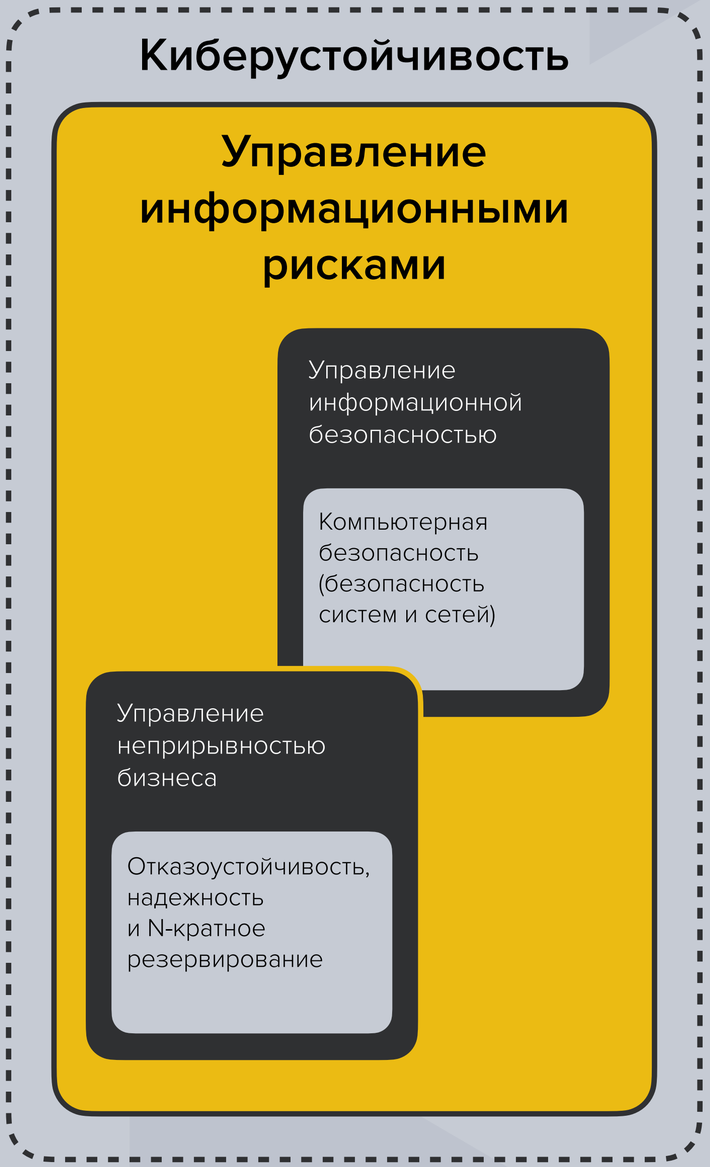
Хочется унифицированную модель данных для правил различных типов решений (шаблоны настроек на различных типах устройств для оперативности)

PT
Информационная безопасность

TDRP

Экосистемные или интеграционные продукты

К чему это должно привести?



Кибербезопасность

Активная защита от злоумышленников и инсайдеров, а также непреднамеренных ошибок сотрудников.

+

Информационная безопасность

Пассивная защита – обеспечение целостности, доступности и конфиденциальности информации.

=

Общая цель ИБ и ИТ – КИБЕРУСТОЙЧИВОСТЬ

Способность ИТ-объекта сохранять работоспособное состояние в условиях различных взаимодействий (внешний хакер, сотрудник, другая ИТ-система)

Нам доверяют

Ростех
РТ-Энергоэффективность

РТ
Развитие бизнеса

Ростех
Техприемка

Ростех

KAMAZ

ОАК
Объединенная авиастроительная корпорация

ОДК

КБП

СИБЕР

Нацимбио

Высокоточные комплексы

УВЗ

Акционерное общество
Рязанский радиозавод

Контакты

Адрес: 117587, г. Москва,
Варшавское шоссе,
дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru

РТ
Информационная безопасность