Сергей Шалин
Пресейл-инженер

PT Sandbox и PT NAD

Принципы работы продуктов для сетевой безопасности

01

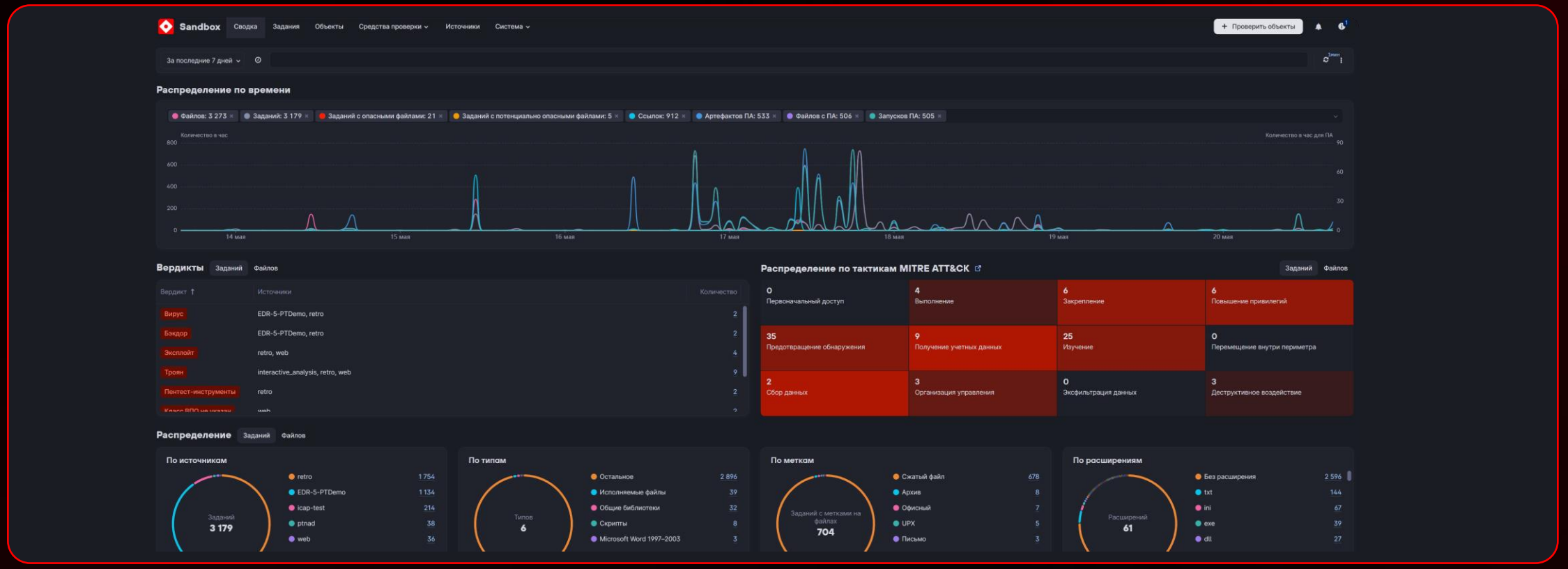
PT Sandbox

Песочница PT Sandbox

Обнаруживает вредоносное ПО на уровне гипервизора, операционной системы и виртуальной машины

Легко встраивается в инфраструктуру и контролирует основные каналы передачи файлов и ссылок

Адаптируется к особенностям бизнеса, обеспечивая защиту от целенаправленных атак



Как работает PT Sandbox

Песочница получает объекты из различных типов источников, обрабатывает файлы и ссылки, и определяет в них вредоносное содержимое

Статический анализ в PT Sandbox

Для защиты от известных угроз и проверки легитимности ссылок песочница использует комбинацию методов анализа

Собственные YARA-правила

Правила от экспертного центра PT ESC, создаваемые в ходе расследования инцидентов и анализа деятельности хакерских группировок

Категоризация веб-ресурсов

Классификация интернет-ресурсов (PT Categorizer) по их назначению и типу контента для предотвращения инцидентов ИБ

Репутационный анализ

Репутационный анализ файлов и ссылок по базе индикаторов компрометации (PT IoC) для точечного выявления угроз

Внешняя экспертиза

Антивирусный анализ: «из коробки» — «NANO Антивирус», VBA32 и ClamAV, по лицензиям — Kaspersky

Анализ содержимого ссылок

Поиск и скачивание контента по ссылкам (PT Crawler) с проверкой его легитимности, включая ссылки в QR-кодах

Пользовательские YARA-правила

Для проверки объектов в PT Sandbox вы можете использовать созданные вами YARA-правила

Политики предварительной фильтрации в PT Sandbox

Для снижения нагрузки на систему поведенческого анализа можно управлять правилами проверки объектов

Пользовательские правила определения объектов с угрозами

Настройка параметров правил, по которым PT Sandbox будет относить файлы и ссылки к опасным или потенциально опасным объектам

О работе с правилами предварительной фильтрации в PT Sandbox

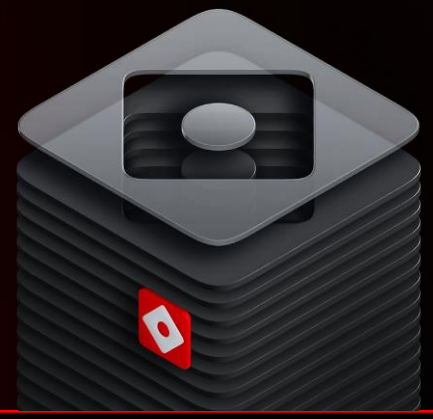
Поведенческий анализ в PT Sandbox

МНОГОУРОВНЕВАЯ ПРОВЕРКА ФАЙЛОВ

- Анализ сетевого трафика и подключений
- Анализ дампов памяти и процессов
- ML-технологии для выявления аномального поведения

Изолированная среда в PT Sandbox

Поддерживает виртуальные среды с Windows, Linux



ЭКСПЕРТНЫЕ ИНСТРУМЕНТЫ

- Кастомизация виртуальных машин в соответствии с реальными рабочими станциями
- Уникальные приманки, имитирующие настоящие файлы, процессы или данные, характерные для разных отраслей
- Механизм anti-evasion — защита от популярных техник обхода виртуальных сред

Поведенческий анализ: обновления

2024

- Образы: Windows 11, Ubuntu 22, «РЕД ОС» 8
- Управление очередью файлов на поведенческий анализ
- Поддержка до 45 виртуальных машин на узле

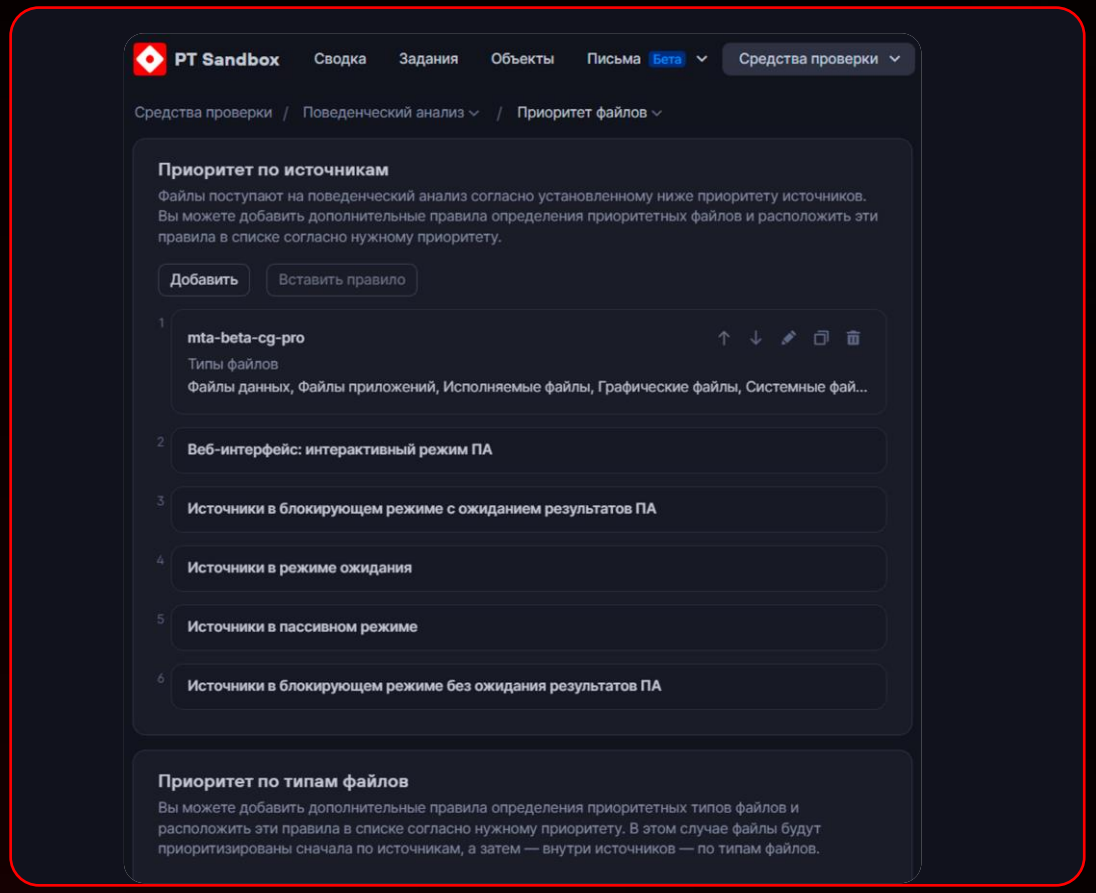
2025

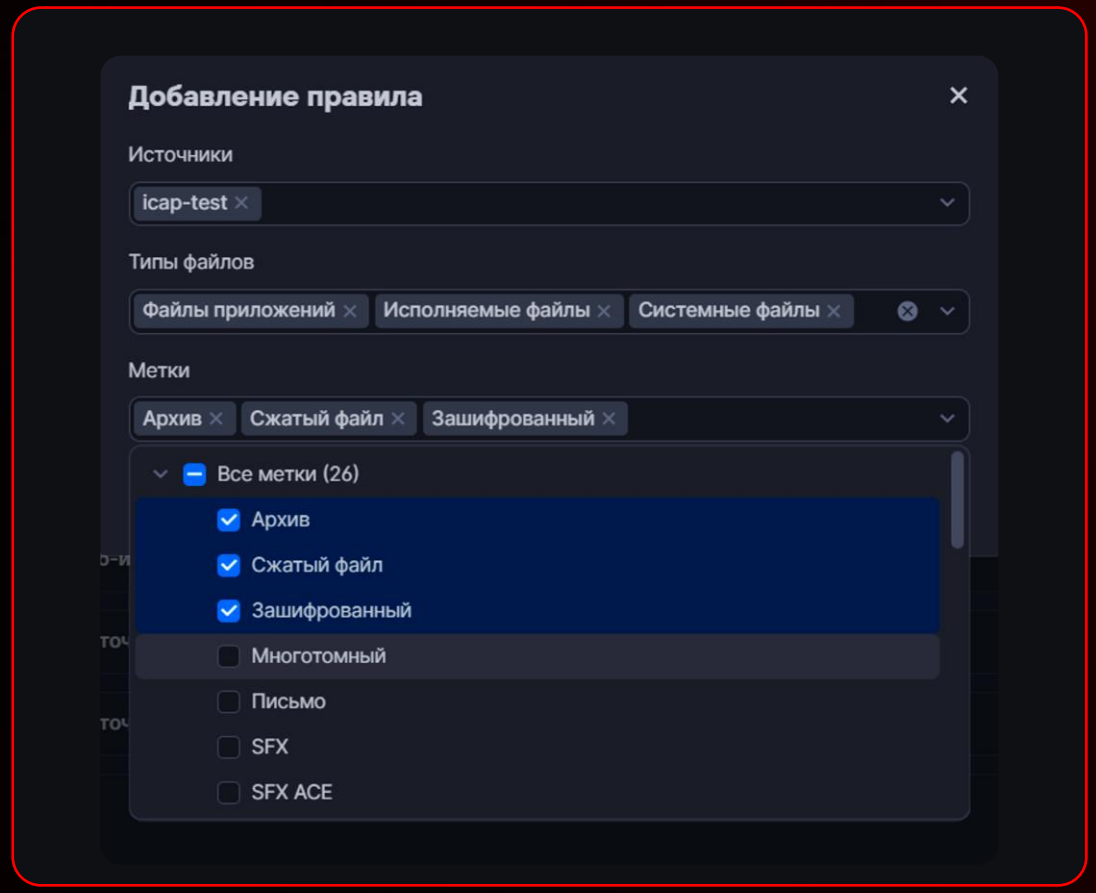
- Добавление ML-механизма анализа сетевого трафика
- Увеличение ОЗУ виртуальных машин
- Настройка расписания и очереди обновления образов
- Интерактивный анализ и запуск анализа с указанием команд
- Управление приоритетом источников и файлов

Изолированная среда в PT Sandbox

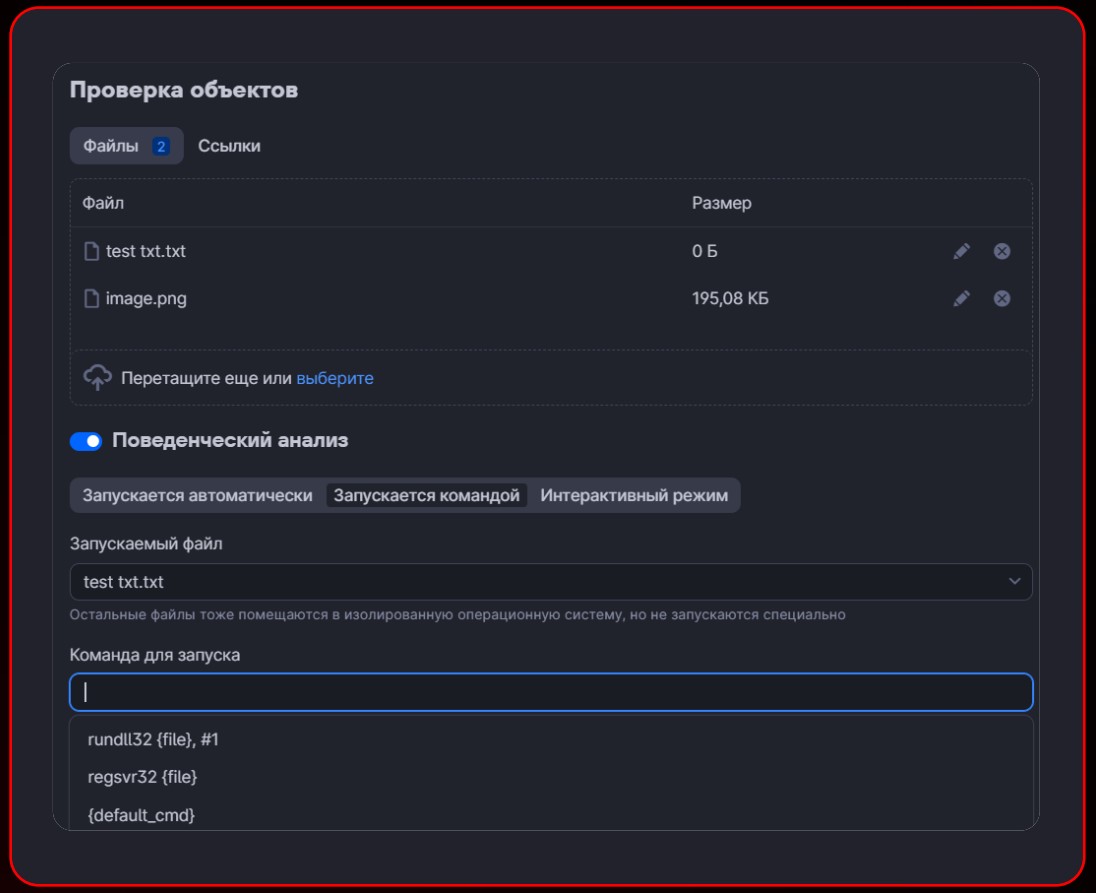
Поддерживает виртуальные среды с Windows, Linux

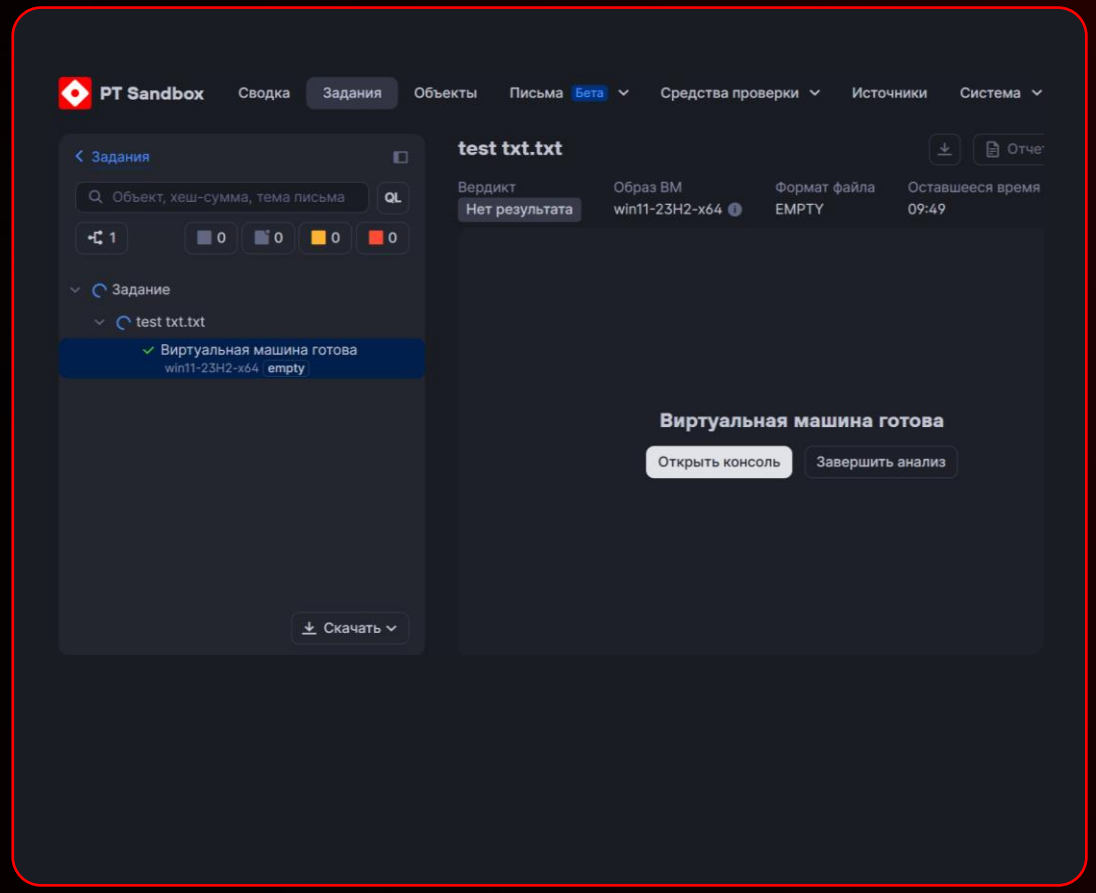
Управление приоритетом проверок





Запуск по команде и в интерактивном режиме



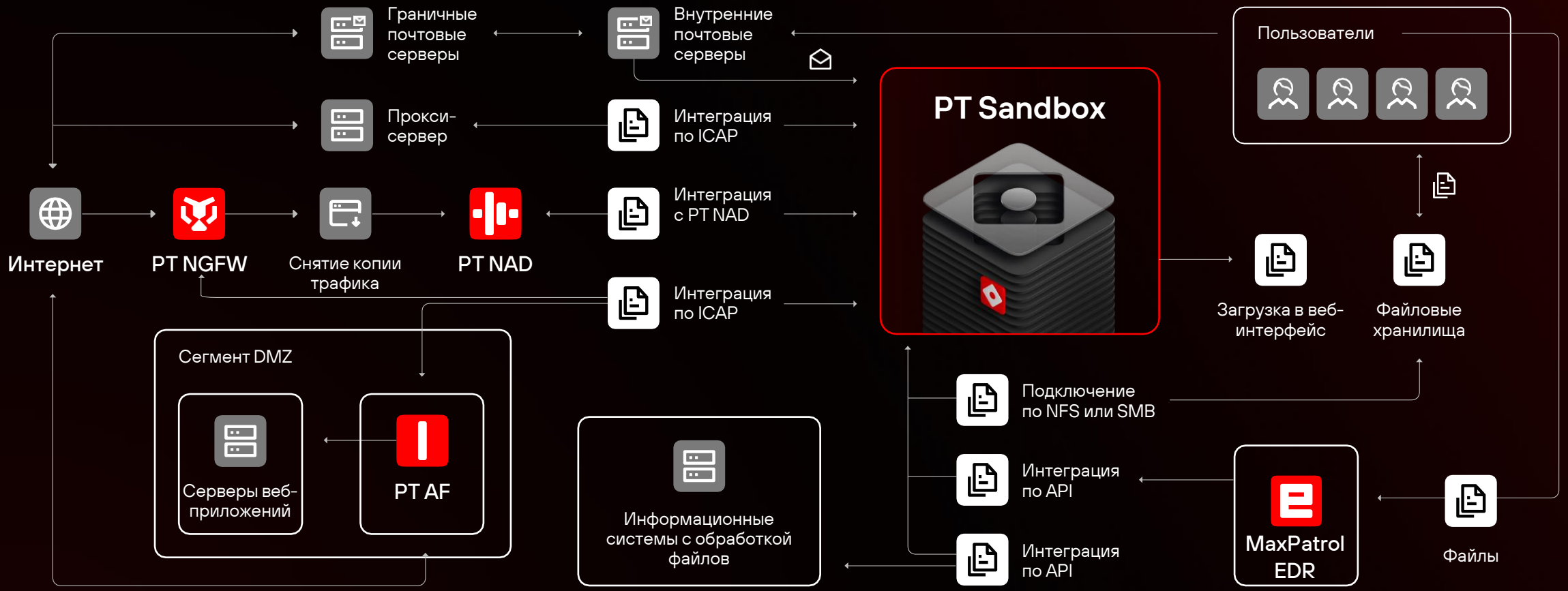


Режимы работы PT Sandbox

		РЕШАЕМЫЕ ЗАДАЧИ
Обнаружение ВПО	Подключение песочницы к различным источникам, сбор файлов и ссылок на анализ с последующим уведомлением об угрозах **Не влияет на бизнес-процессы**	▪ Определение активности ВПО ▪ Выявление хакерских инструментов ▪ Обнаружение эксплуатации уязвимостей
Блокировка ВПО	Взаимодействие с почтовыми системами, системами контроля сетевого трафика и коннекторами API для блокировки вредоносного содержимого **Минимальное влияние на бизнес-процессы**	▪ Блокировка неизвестного ВПО ▪ Защита от хакерских инструментов ▪ Доставка пользователям сообщений и файлов без вредоносных вложений
Исследование угроз	Автоматизация труда специалистов SOC: анализирует объекты, включая загруженные вручную, предоставляет результаты и дает возможность выгрузить нужные артефакты **Сокращает время на исследование угроз**	▪ Получение безопасных обновлений программного обеспечения ▪ Автоматизация анализа объектов ▪ Ретроспективный анализ инцидентов

PT Sandbox в инфраструктуре

Подключается ко множеству источников, обеспечивая своевременное обнаружение неизвестного ВПО по целому ряду сценариев



Интеграция PT Sandbox со сторонними системами

PT Sandbox может интегрироваться по API со сторонними системами. Продукт отдает результаты проверки в коннектор API*, который может выполнять блокировку на основе полученных данных

PT Sandbox обеспечивает безопасность данных в репозиториях, хранилищах и корпоративных системах коммуникации

* Написать коннектор можно с помощью руководства разработчика

Интернет

- Небезопасные публичные и приватные репозитории
- Системы документооборота
- Облачные хранилища
- Корпоративные средства коммуникации
- Системы обновления ПО

Коннекторы API

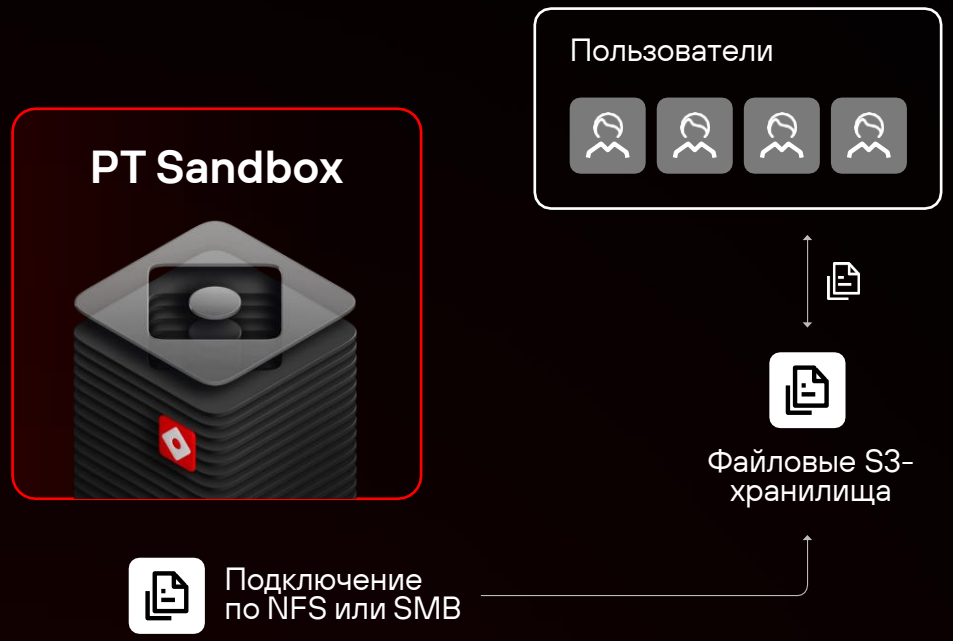
Файлы на проверку

Результаты проверки

Безопасные объекты

- Безопасные репозитории
- Системы документооборота
- Облачные хранилища
- Корпоративные средства коммуникации
- Системы обновления ПО

Новые источники: поддержка S3-хранилищ

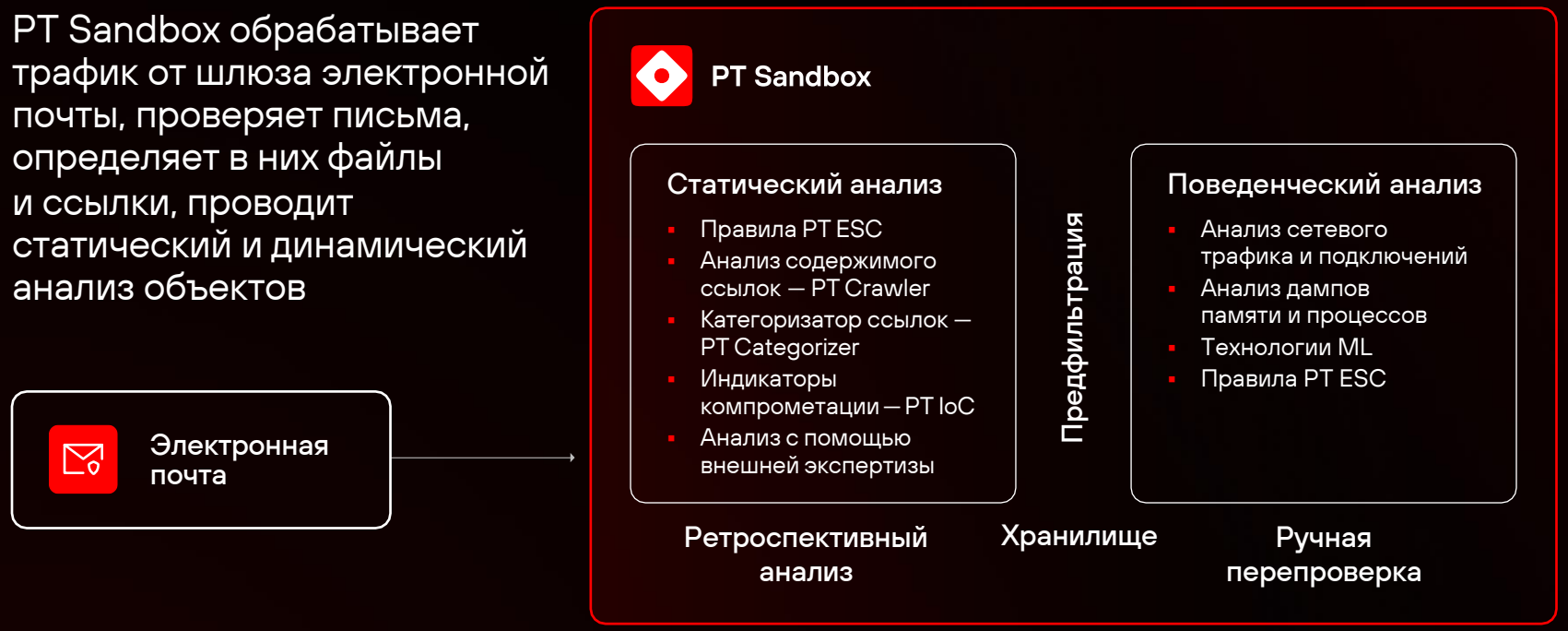


В дополнение к «обходчику» для привычных файловых хранилищ добавлено подключение для универсальных решений Simple Storage Service

Примеры инструкций для подключения S3-хранилищ

PT Sandbox и почтовые системы

PT Sandbox обрабатывает трафик от шлюза электронной почты, проверяет письма, определяет в них файлы и ссылки, проводит статический и динамический анализ объектов



Блокирует электронные письма с вредоносным содержимым или доставляет обезвреженные письма

Блокировка

Блокировка ВПО в почтовом трафике

SOC

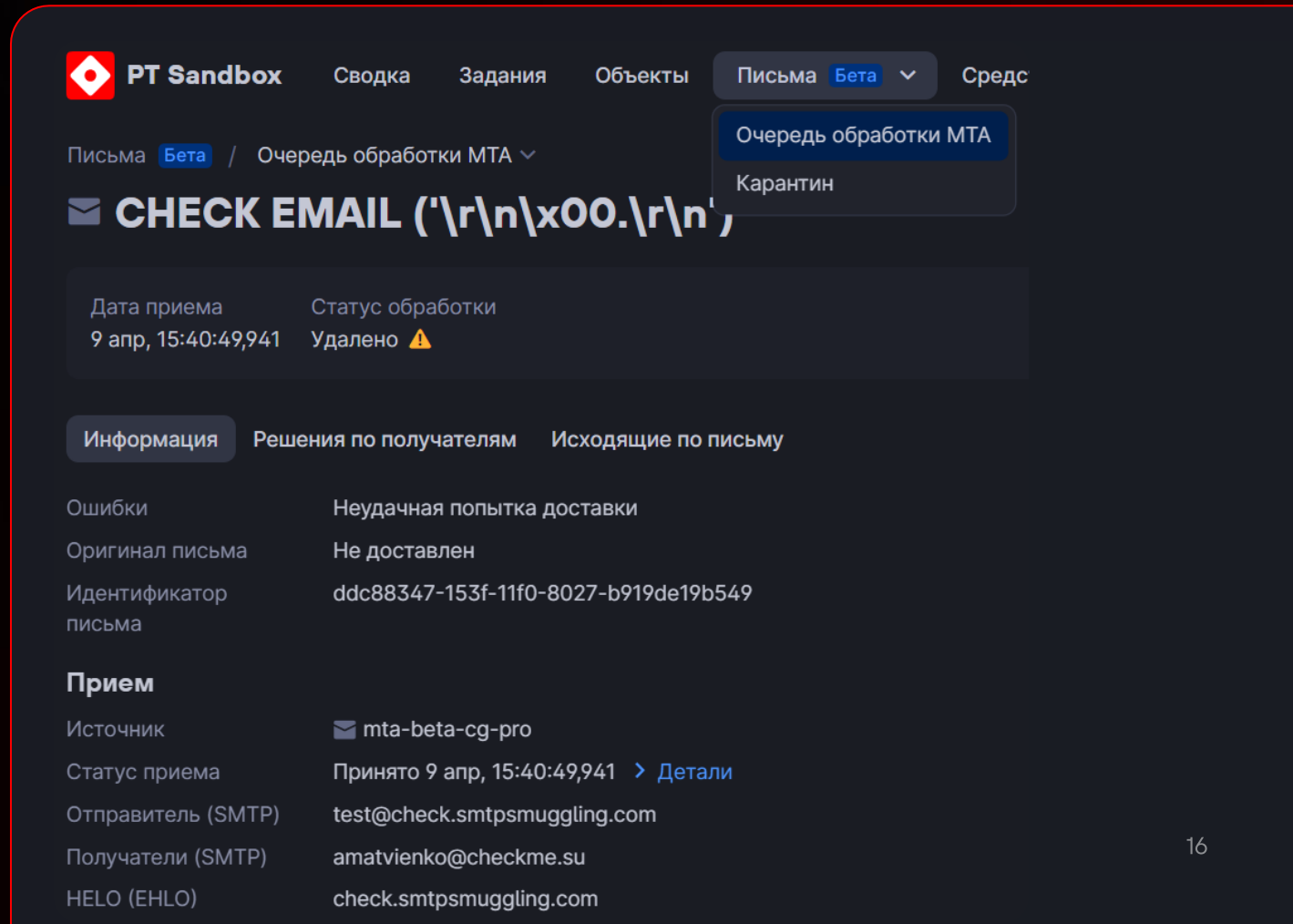
PT Email Security:

комплексная защита почты (бета-версия — в конце 2025 года)

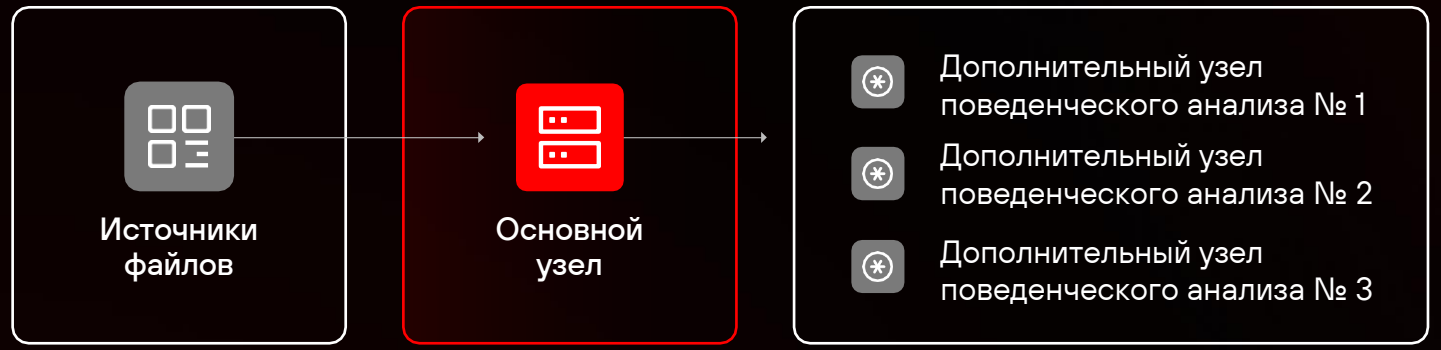
Расширение набора функций для обеспечения безопасности почты:

- Очередь обработки писем (MTA)
- Карантин для MTA
- Правила обработки писем для указанных отправителей и получателей

Экспертиза, заложенная в PT Sandbox, вместе с новой функциональностью почтовой защиты войдет в продукт для комплексной защиты почты от всех векторов атак — PT Email Security



Расширение возможностей развертывания



Каждый дополнительный узел обеспечивает прирост производительности до 20 000 файлов в сутки

Для основных узлов доступна функция отказоустойчивого кластера

1

Поддержка установки продукта на актуальные ОС: Debian 12, Astra Linux 1.8, «ОСнова» Onyx 2.0

2

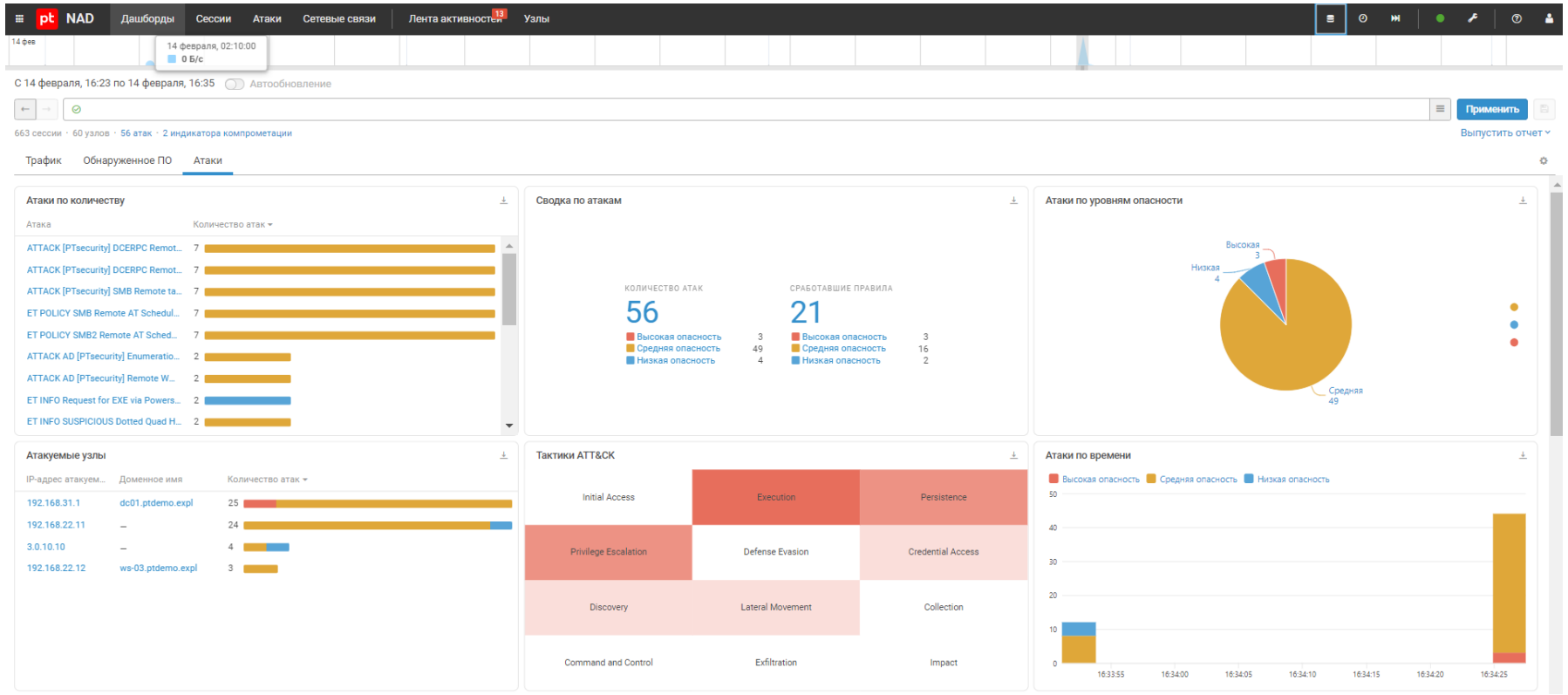
Бета-тестирование: установка узлов ПА поверх KVM-виртуализации

02

PT Network Attack Discovery

PT Network Attack Discovery

Эталонный источник данных о сети для контроля инфраструктуры и обнаружения действий злоумышленников в трафике



PT NAD знает, что искать

Быстро и точно определяет действия злоумышленников в сети на ранних этапах атаки

Видит точки проникновения в инфраструктуру и масштаб атаки в режиме, близком к реальному времени

Защищает георазпределенные инфраструктуры любого масштаба

Центральная консоль обеспечивает возможность централизации процесса анализа сетевого трафика, гарантируя надежную защиту в условиях нехватки кадров

Является незаменимым инструментом для ретроспективного анализа и расследований

- Технология DPI детально разбирает сетевой трафик на любых скоростях
- Данные используются для автоматического обнаружения аномалий и ручного анализа
- Позволяет выявлять угрозы, которых нет в базах данных сигнатур IDS, IPS и NGFW

Оперативно выявляет угрозы, актуальные для российских компаний

Экспертный центр PT ESC поставляет индикаторы компрометации, правила, поведенческие и статистические модули, нацеленные на выявления атак, популярных на территории России

PT NAD для решения задач ИБ

Контроль активов

- Инвентаризирует узлы по сетевому отпечатку
- Обнаруживает нарушения регламентов ИБ

Нетипичное поведение узлов

- Находит аномалии в сетевом трафике
- Профилирует сетевые узлы и определяет приложения

180 техник и тактик атакующих

- Обнаруживает попытки эксплуатации уязвимостей и видит факты успешной эксплуатации
- Выявляет хакерские инструменты и перемещение атакующих внутри периметра
- Определяет угрозы в зашифрованном трафике
- Определяет зараженные узлы и подключения к C2-серверам

Как работает PT NAD

Захватывает и разбирает сетевой трафик на периметре и в инфраструктуре с помощью технологии DPI

Исходная копия сетевого трафика

Видимость сети

Обнаружение хакера в сети

Аномалии

Контроль регламентов ИБ

SOC

С помощью статистических и поведенческих модулей обнаруживает активность злоумышленника на самых ранних этапах проникновения в сеть, а также во время попыток закрепиться в ней и развить атаку

Методы анализа трафика

Классический	Глубокая экспертиза	ML
Сигнатурный анализ	Обнаружение новых активов	Пользовательские правила профилирования
Репутационные списки	Экспертные модули	Анализ шифрованного трафика
Интеграция с PT Sandbox	Детектирование приложений и сервисов	Поиск DGA-доменов

Методы анализа SSL-, TLS-трафика

Анализ побочных каналов

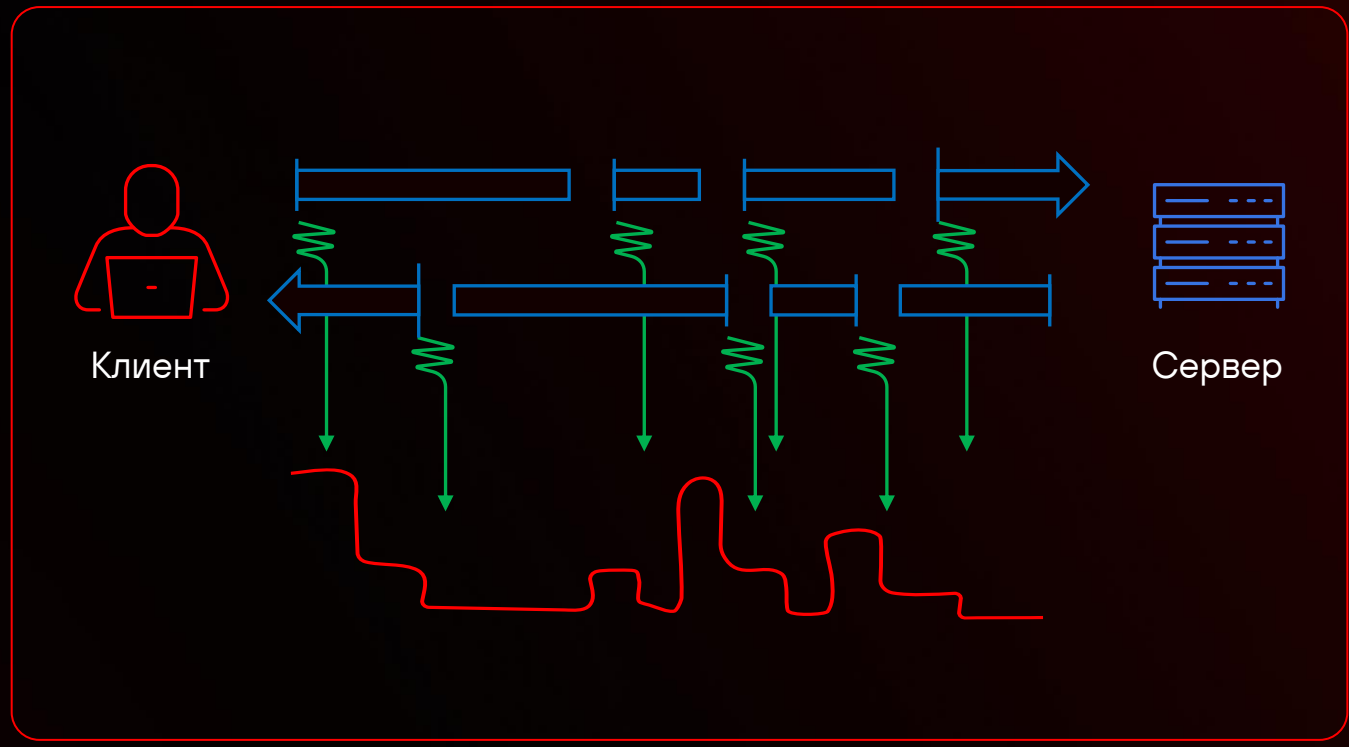
Поиск индикаторов компрометации

Детектирование аномалий

Детектирование приложений

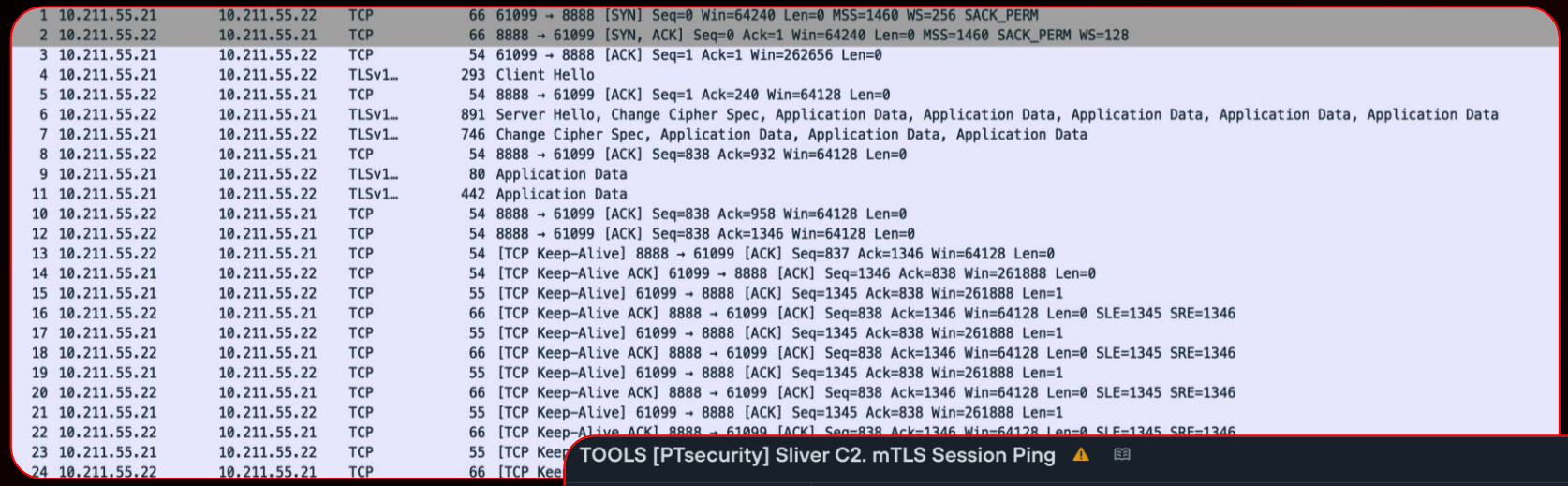
Анализ побочных каналов

- Шифрование не позволяет скрыть признаки функционирования хакерских инструментов
- Знание особенностей инструментов злоумышленников помогает обнаруживать их действия
- Распределение длин пакетов и интервалов между пакетами демаскирует хакеров

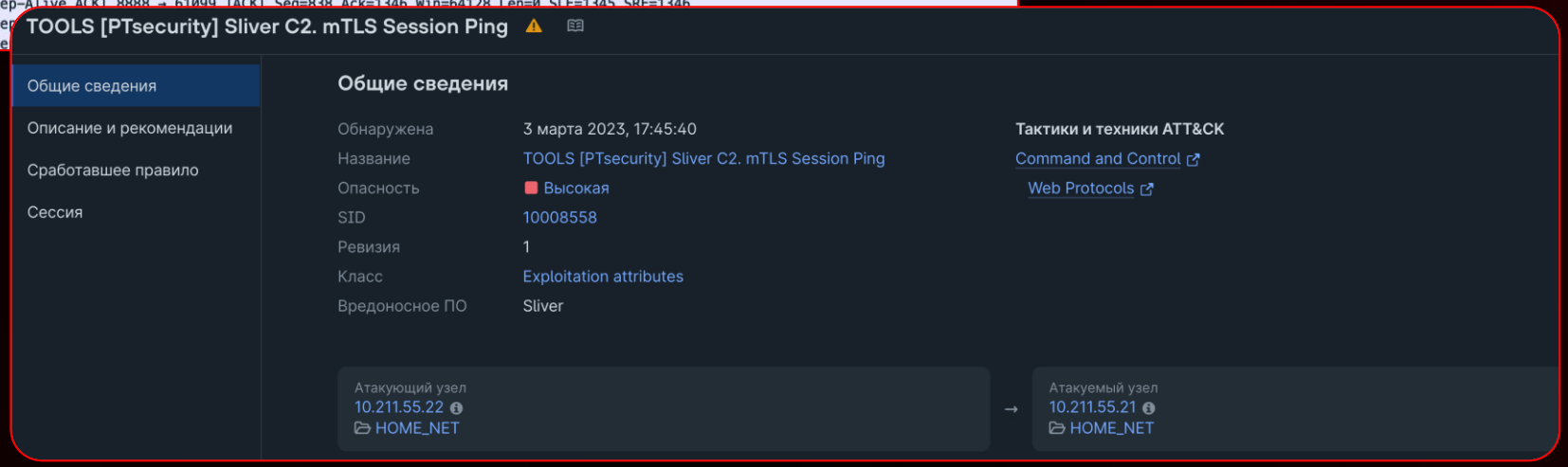


PT NAD выявляет признаки присутствия злоумышленника в шифрованном трафике

Анализ побочных каналов



1	10.211.55.21	10.211.55.22	TCP	66	61099 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	10.211.55.22	10.211.55.21	TCP	66	8888 → 61099 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	10.211.55.21	10.211.55.22	TCP	54	61099 → 8888 [ACK] Seq=1 Ack=1 Win=262656 Len=0
4	10.211.55.21	10.211.55.22	TLSv1…	293	Client Hello
5	10.211.55.22	10.211.55.21	TCP	54	8888 → 61099 [ACK] Seq=1 Ack=240 Win=64128 Len=0
6	10.211.55.22	10.211.55.21	TLSv1…	891	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data, Application Data
7	10.211.55.21	10.211.55.22	TLSv1…	746	Change Cipher Spec, Application Data, Application Data, Application Data
8	10.211.55.22	10.211.55.21	TCP	54	8888 → 61099 [ACK] Seq=838 Ack=932 Win=64128 Len=0
9	10.211.55.21	10.211.55.22	TLSv1…	80	Application Data
11	10.211.55.21	10.211.55.22	TLSv1…	442	Application Data
10	10.211.55.22	10.211.55.21	TCP	54	8888 → 61099 [ACK] Seq=838 Ack=958 Win=64128 Len=0
12	10.211.55.22	10.211.55.21	TCP	54	8888 → 61099 [ACK] Seq=838 Ack=1346 Win=64128 Len=0
13	10.211.55.22	10.211.55.21	TCP	54	[TCP Keep-Alive] 8888 → 61099 [ACK] Seq=837 Ack=1346 Win=64128 Len=0
14	10.211.55.21	10.211.55.22	TCP	54	[TCP Keep-Alive ACK] 61099 → 8888 [ACK] Seq=1346 Ack=838 Win=261888 Len=0
15	10.211.55.21	10.211.55.22	TCP	55	[TCP Keep-Alive] 61099 → 8888 [ACK] Seq=1345 Ack=838 Win=261888 Len=1
16	10.211.55.22	10.211.55.21	TCP	66	[TCP Keep-Alive ACK] 8888 → 61099 [ACK] Seq=838 Ack=1346 Win=64128 Len=0 SLE=1345 SRE=1346
17	10.211.55.21	10.211.55.22	TCP	55	[TCP Keep-Alive] 61099 → 8888 [ACK] Seq=1345 Ack=838 Win=261888 Len=1
18	10.211.55.22	10.211.55.21	TCP	66	[TCP Keep-Alive ACK] 8888 → 61099 [ACK] Seq=838 Ack=1346 Win=64128 Len=0 SLE=1345 SRE=1346
19	10.211.55.21	10.211.55.22	TCP	55	[TCP Keep-Alive] 61099 → 8888 [ACK] Seq=1345 Ack=838 Win=261888 Len=1
20	10.211.55.22	10.211.55.21	TCP	66	[TCP Keep-Alive ACK] 8888 → 61099 [ACK] Seq=838 Ack=1346 Win=64128 Len=0 SLE=1345 SRE=1346
21	10.211.55.21	10.211.55.22	TCP	55	[TCP Keep-Alive] 61099 → 8888 [ACK] Seq=1345 Ack=838 Win=261888 Len=1
22	10.211.55.22	10.211.55.21	TCP	66	[TCP Keep-Alive ACK] 8888 → 61099 [ACK] Seq=838 Ack=1346 Win=64128 Len=0 SLE=1345 SRE=1346
23	10.211.55.21	10.211.55.22	TCP	55	[TCP Kee
24	10.211.55.22	10.211.55.21	TCP	66	[TCP Kee



Используемые злоумышленниками утилиты имеют демаскирующие признаки, которые позволяют эффективно их детектировать

Анализ побочных каналов

C2-фреймворки

- Sliver
- Gsocket
- Mythic
- Cobalt Strike
- Meterpreter
- Brute Ratel

Утилиты туннелирования

- Localtonet
- Microsoft dev tunnels
- ngrok

Средства удаленного управления

- RMS
- MeshCentral
- Havoc
- Golang Reverse

Злоумышленник будет обнаружен даже при использовании самых эффективных инструментов

Особенности анализа трафика в PT NAD

Зашифрованный трафик

- Не извлекаются передаваемые файлы
- Сигнатурный анализ слабо применим
- Невозможно проверить файловые IoCs
- Невозможно автоматически проверить успешность эксплуатации уязвимости
- Поиск угроз по побочным каналам

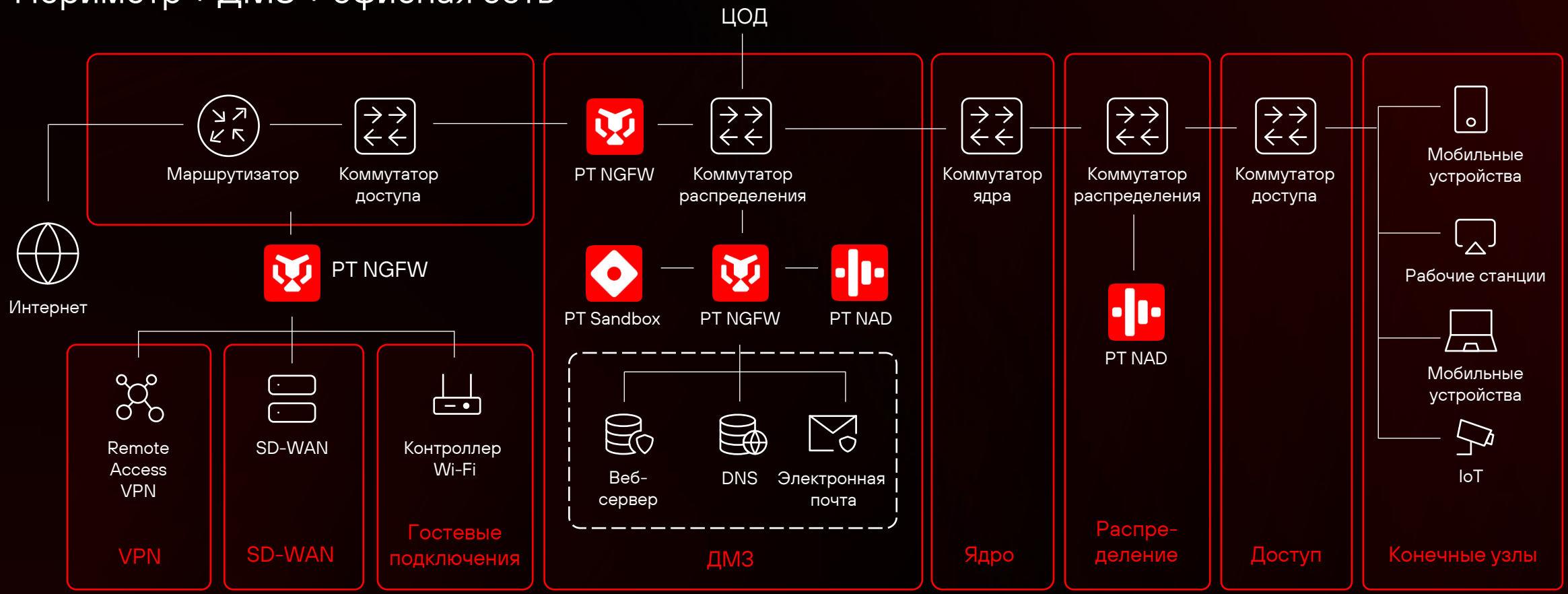
VS.

Расшифрованный трафик

- Все файлы проверяются в песочнице
- Сигнатурный анализ работает в полном объеме
- Полноценная проверка IoCs
- Можно автоматически проверить успешность эксплуатации уязвимости
- Поиск угроз классическими методами

Архитектура сетевой безопасности

Периметр + ДМЗ + офисная сеть

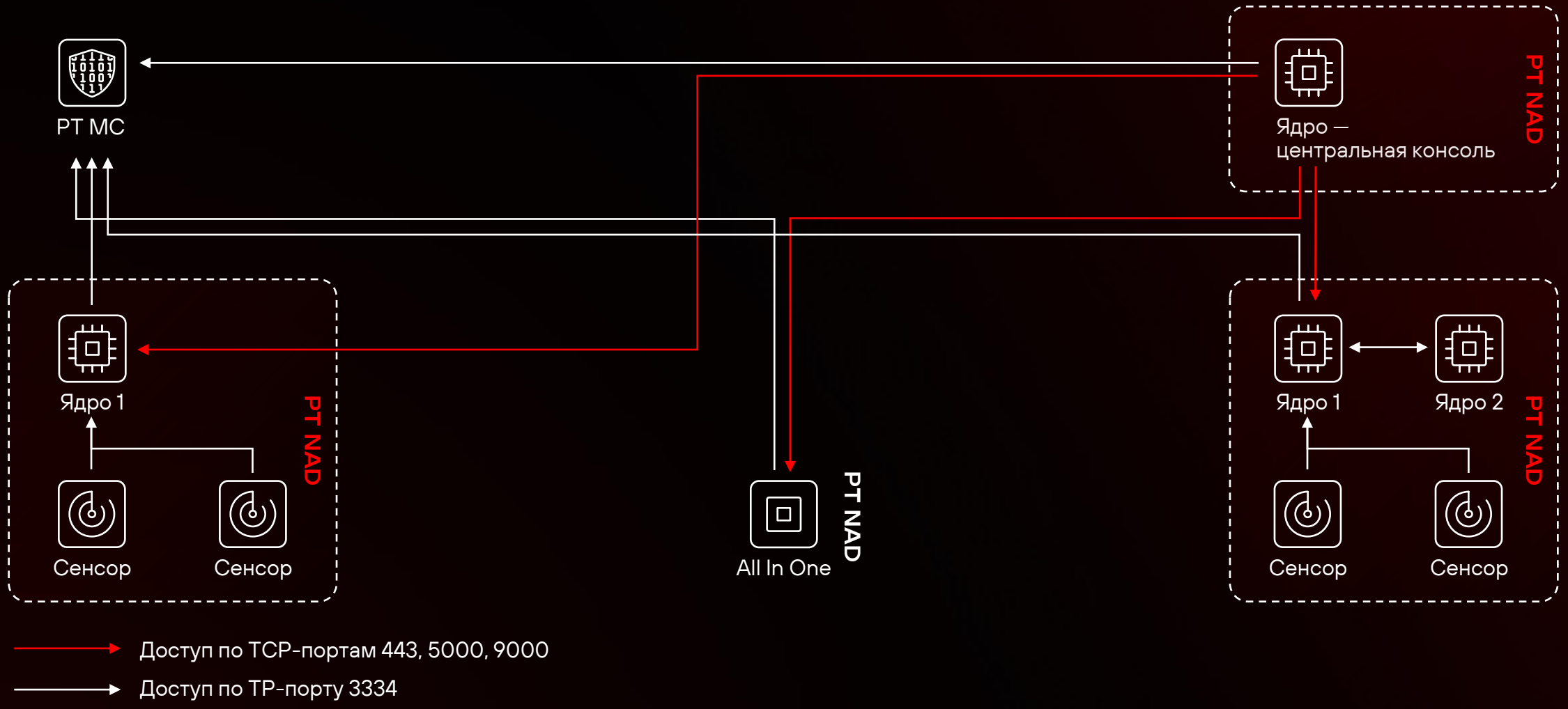


03

PT Network Attack Discovery

Новинки

Центральная консоль



Центральная консоль

Этапы развития

R12.2

- Получение информации о дочерних PT NAD
- Централизованный просмотр данных из дочерних систем

R12.3

- Централизованное выполнение операций с трафиком и файлами, полученными из дочерних систем
- Централизованное выполнение операций с сессиями, атаками, активностями и узлами дочерних систем
- Централизованный просмотр мониторинга дочерних систем

Q1 2025

Q2 2025

Преимущества

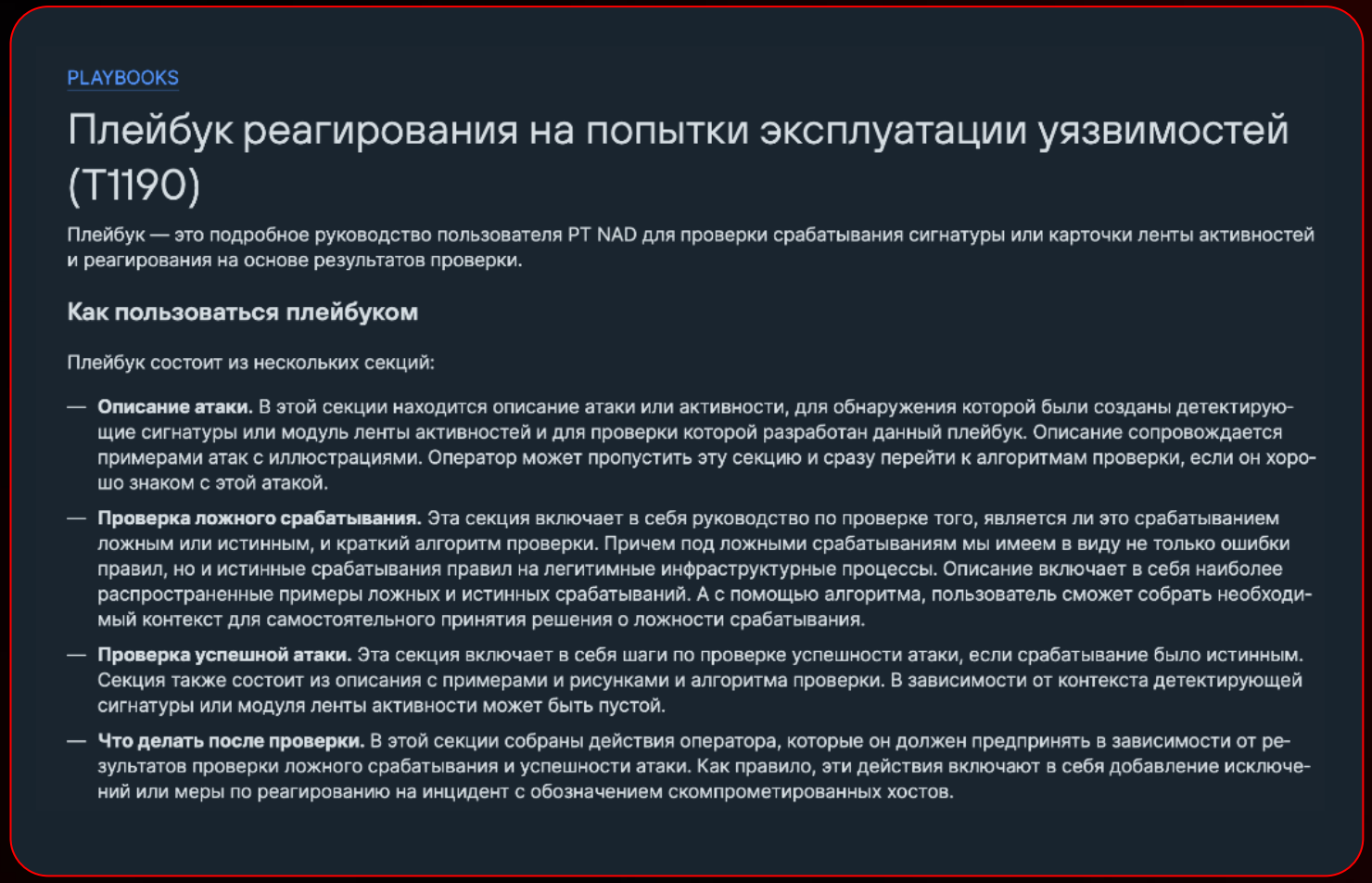
- Мониторинг распределенных информационных систем
- Число дочерних систем не ограничено
- Доступ к любой сущности любой дочерней инсталляции через механизм единого входа

Требования

- Регистрация всех PT NAD в PT MC
- Связность на уровне протокола IP между единой консолью и ядрами других PT NAD

Плейбуки

1. Инструкции по проверке срабатываний сигнатур и модулей ленты активностей
2. Решают задачу однозначной интерпретации результатов работы продуктов



PLAYBOOKS

Плейбук реагирования на попытки эксплуатации уязвимостей (T1190)

Плейбук — это подробное руководство пользователя PT NAD для проверки срабатывания сигнатуры или карточки ленты активностей и реагирования на основе результатов проверки.

Как пользоваться плейбуком

Плейбук состоит из нескольких секций:

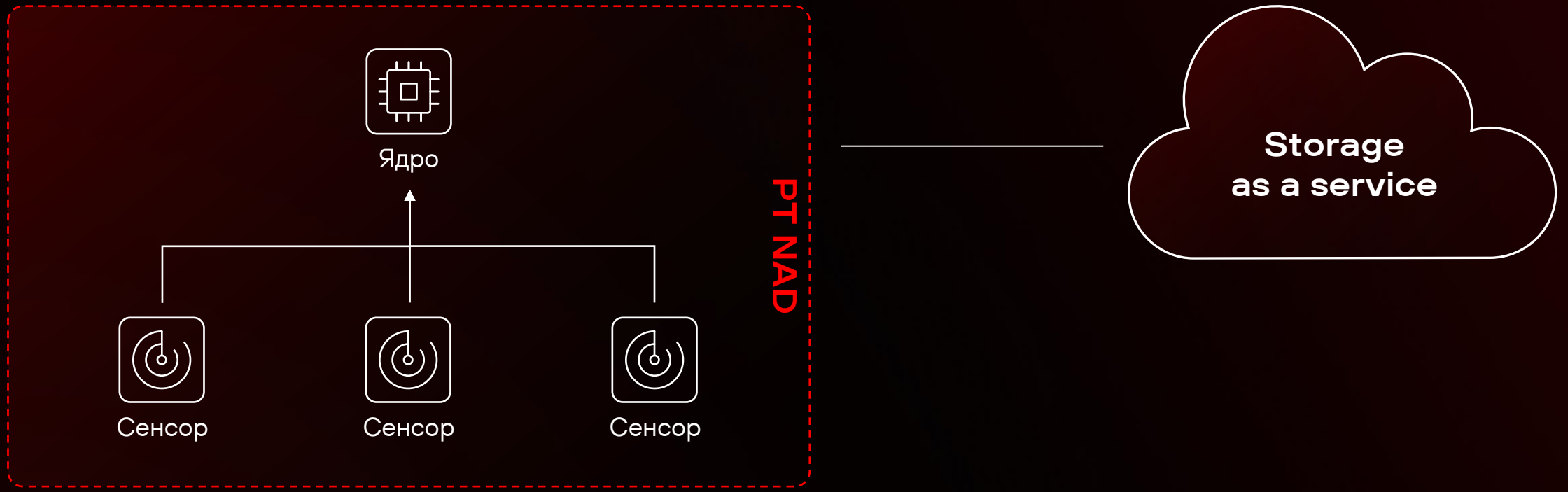
— **Описание атаки.** В этой секции находится описание атаки или активности, для обнаружения которой были созданы детектирующие сигнатуры или модуль ленты активностей и для проверки которой разработан данный плейбук. Описание сопровождается примерами атак с иллюстрациями. Оператор может пропустить эту секцию и сразу перейти к алгоритмам проверки, если он хорошо знаком с этой атакой.

— **Проверка ложного срабатывания.** Эта секция включает в себя руководство по проверке того, является ли это срабатыванием ложным или истинным, и краткий алгоритм проверки. Причем под ложными срабатываниям мы имеем в виду не только ошибки правил, но и истинные срабатывания правил на легитимные инфраструктурные процессы. Описание включает в себя наиболее распространенные примеры ложных и истинных срабатываний. А с помощью алгоритма, пользователь сможет собрать необходимый контекст для самостоятельного принятия решения о ложности срабатывания.

— **Проверка успешной атаки.** Эта секция включает в себя шаги по проверке успешности атаки, если срабатывание было истинным. Секция также состоит из описания с примерами и рисунками и алгоритма проверки. В зависимости от контекста детектирующей сигнатуры или модуля ленты активности может быть пустой.

— **Что делать после проверки.** В этой секции собраны действия оператора, которые он должен предпринять в зависимости от результатов проверки ложного срабатывания и успешности атаки. Как правило, эти действия включают в себя добавление исключений или меры по реагированию на инцидент с обозначением скомпрометированных хостов.

Хранение метаданных в «облаке»



Релиз Q1 2025

Оповещение об угрозах

PT NAD

Информация
об угрозах

4 New Alerts (3 Unique):

ATTACK AD [PTsecurity] WINREG dump LSA. OpenKey (2 occurrences)
Source: `10.144.0.101`
Destination: `10.144.0.111:445`
Classification: Active Directory exploitation attributes
Protocol: `tcp` (`smb`)
SID: `10003933`
Timestamp: 2024-09-05 19:03:17 (MSK) - 2024-09-05 19:05:37 (MSK)
View All Alerts in NAD

ATTACK AD [PTsecurity] WINREG dump SAM. CreateKey
Source: `10.144.0.101:47164`
Destination: `10.144.0.111:445`
Classification: Active Directory exploitation attributes
Protocol: `tcp` (`smb`)
SID: `10003936`
Timestamp: 2024-09-05 19:03:29 (MSK)
View All Alerts in NAD

ATTACK AD [PTsecurity] WINREG dump SECURITY. CreateKey
Source: `10.144.0.101:55974`
Destination: `10.144.0.111:445`
Classification: Active Directory exploitation attributes
Protocol: `tcp` (`smb`)
SID: `10003935`
Timestamp: 2024-09-05 19:05:48 (MSK)
View All Alerts in NAD

54 19:08

Ссылка на бот

Полезные ссылки

habrahabr.ru/
company/pt

t.me/
positive_technologies

vk.com/
ptsecurity

t.me/
positive_investing

Задать вопрос по теме выступления

Спасибо!