Рудаков Константин
Лидер продуктовой практики PT Sandbox

Летаем с PT Sandbox

изучение, блокировки, производительность

О спикере

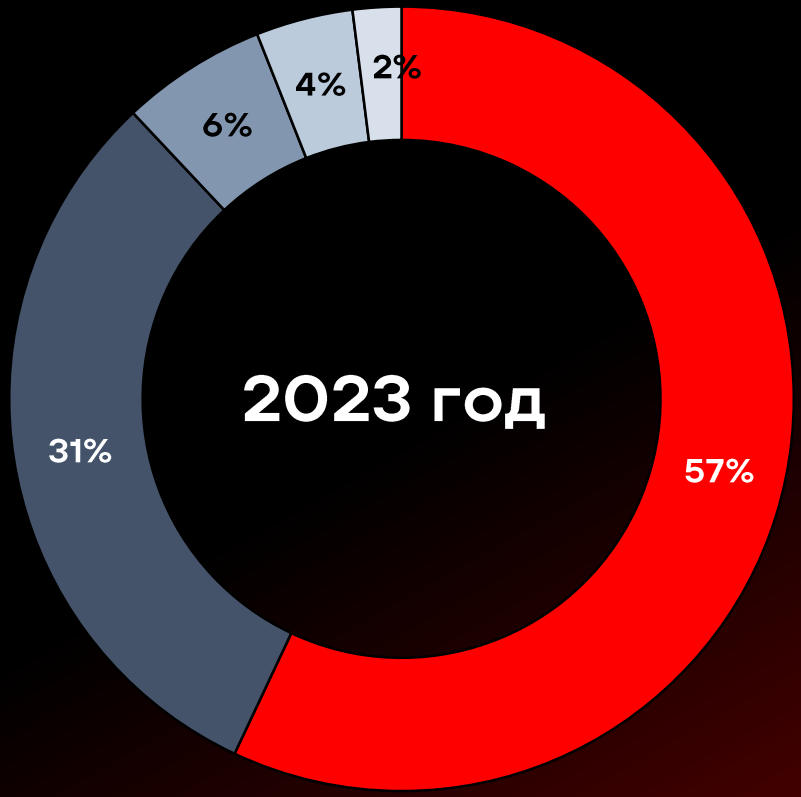
С 2019 года занимаюсь развитием технической экспертизы по применению решений в области сетевой безопасности

Непосредственно вношу свой вклад в улучшение качества внедрений и развитие практик применения таких продуктов, как PT Sandbox, PT NAD и PT MultiScanner

Каналы распространения ВПО

Три основных канала распространения ВПО:

- Электронная почта
- Узлы
- Веб-ресурсы



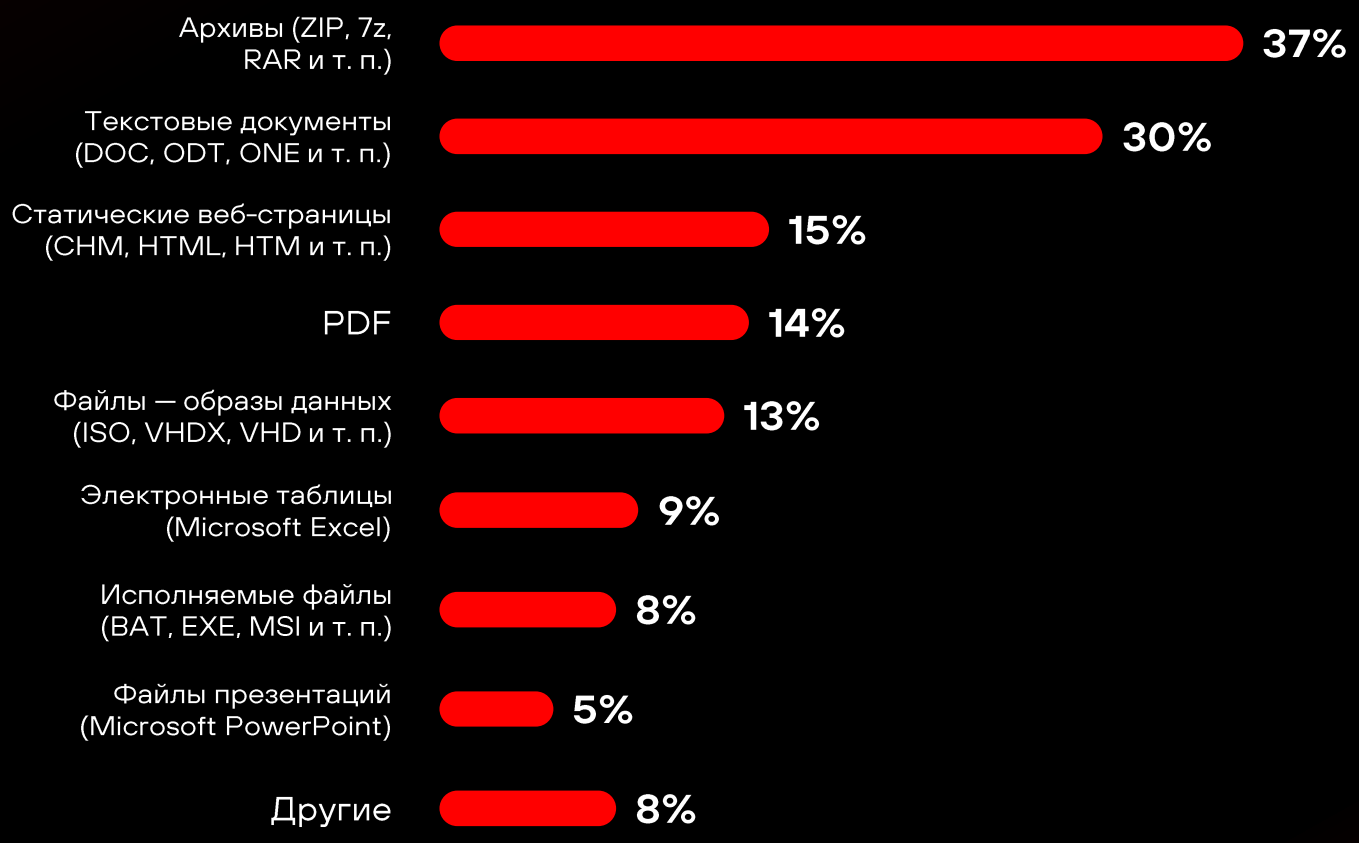
Вредоносное ПО: исследование поведения и каналов распространения

Типы ВПО в успешных атаках

- Использование вымогательского ПО в атаках ознаменовало 2023 год
- Злоумышленники не только требовали выкуп за расшифровку данных, но и шантажировали жертв их публикацией (двойное вымогательство)

Вредоносное ПО: исследование поведения и каналов распространения

Типы файловых атак



- В архивах легко скрывать ВПО от средств проверки безопасности, маскируя его под безобидные документы или изображения
- В офисные таблицы и документы (DOC, PDF, XLS и PPTX) можно внедрить скрипты с вредоносной полезной нагрузкой, которые при активации в фоновом режиме загружают и разворачивают ВПО
- Использование PDF-файлов — тренд фишинговых атак

Тренды фишинговых атак на организации в 2022–2023 годах

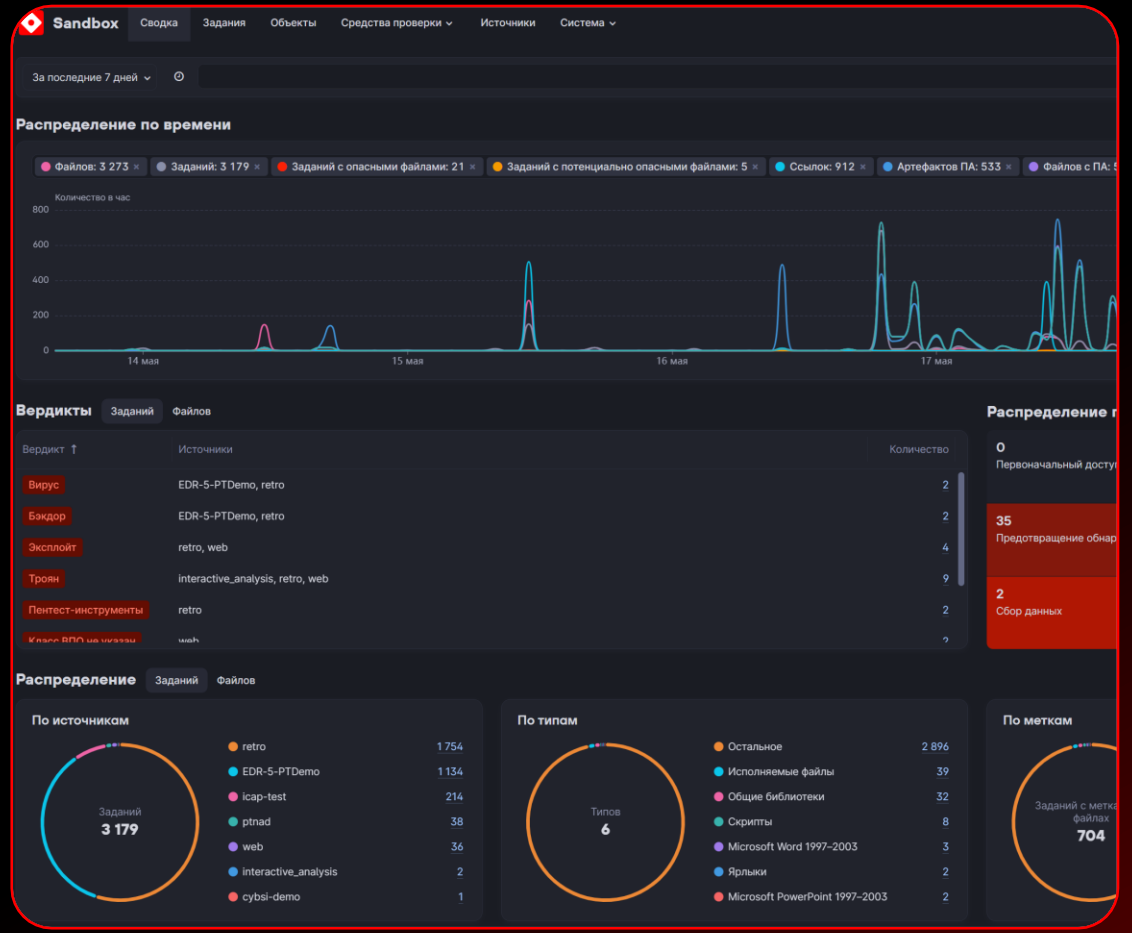
Последствия атак с использованием шифровальщиков в 2023 году

- Нарушение основной деятельности бизнеса
- Утечки конфиденциальной информации

Актуальные киберугрозы для организаций: итоги 2023 года

PT Sandbox

- Проверяет объекты (файлы и ссылки), поступающие из разнообразных независимых источников
- Выявляет как сложные вредоносные объекты, сокрытые от классических средств защиты, так и массовые угрозы
- Использует опыт и базу знаний PT ESC по обнаружению угроз, которые доставляются в продукт с публичными SLA в 2,5 часа



С чего начинаем

Обнаружение ВПО

Подключение песочницы к различным источникам, сбор файлов и ссылок для анализа и последующего уведомления об угрозах

Не влияет на бизнес-процессы

Решаемые задачи:

- Определение активности ВПО
- Выявление хакерских инструментов
- Обнаружение эксплуатации уязвимостей

Исследование угроз

Автоматизация труда специалистов SOC: продукт анализирует объекты, включая загруженные вручную. Предоставляет результаты с возможностью выгрузки нужных артефактов

Снижает время, затрачиваемое специалистами SOC на исследование угроз

Решаемые задачи:

- Получение безопасных обновлений ПО
- Автоматизация анализа объектов
- Ретроспективный анализ инцидентов

Изучаем с PT Sandbox

Получение объектов:

- от почтовых серверов
- ICAP-интеграций с системами анализа трафика
- API-интеграций
- файловых хранилищ
- загрузки вручную

Получение объектов:

- Наборы правил PT ESC
- PT Indicators of Compromise
- Категории URL PT Categorizer
- Содержимое ссылок PT Crawler
- Внешняя экспертиза
- Предфильтрация

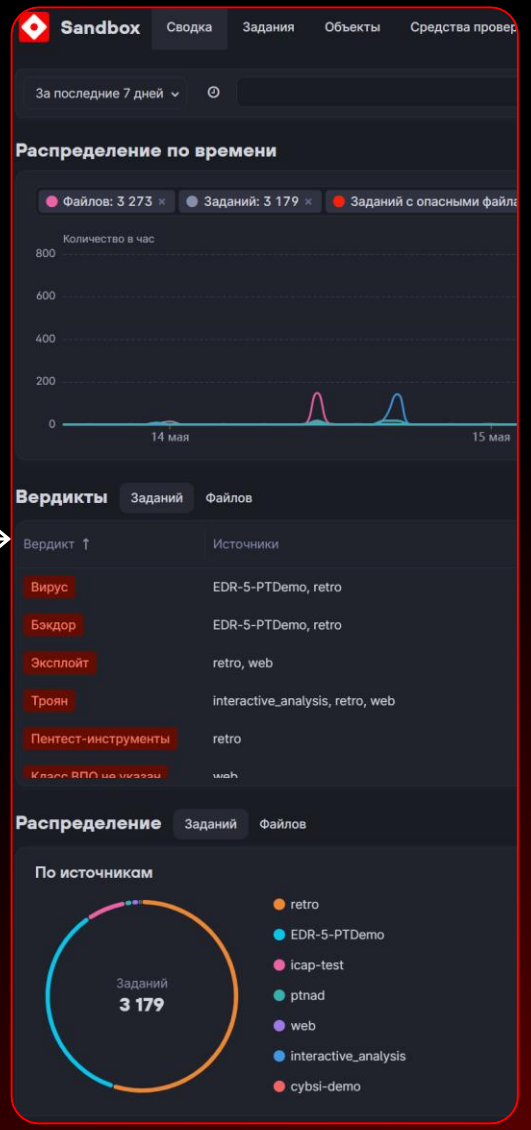
поведенческий

- Сетевой трафик и подключения объекта
- ML по признакам поведения*
- Снимки памяти и процессов
- Встроенные приманки

Хранение данных

Ретроспектива

Ручные средства перепроверки



* Программное обеспечение относится к сфере ИИ согласно единому реестру российских программ

Возможности анализа объектов в PT Sandbox

- Обнаружение вредоносного ПО с пользовательскими настройками и параллельно запускаемыми проверками

  Операционные системы:
  Windows (версий 7–10):
  Windows Server 2016 и
  Windows Server 2019

- Astra Linux Special Edition 1.7
- «РЕД ОС МУРОМ»
- Ubuntu Linux 22.04
- «Альт Рабочая станция» 10

- **Полное покрытие** тактик и техник угроз вредоносного ПО по MITRE ATT&CK в семействах операционных систем Linux и Windows
- Покрытие более 95% известных техник уклонения от проверок в песочнице
- Разбор сетевых подключений и копии трафика в образах
- Анализ и выявление угроз в дампах памяти и процессов

- Возможности **безагентной песочницы** — включая проверки загрузчика систем для выявления рут- и буткитов
- Приманки, имитирующие ценные для злоумышленника данные
- Машинное обучение, применяемое для поведенческого анализа
- Анализ и категоризация ссылок (URL)

Изучили — реактивно реагируем

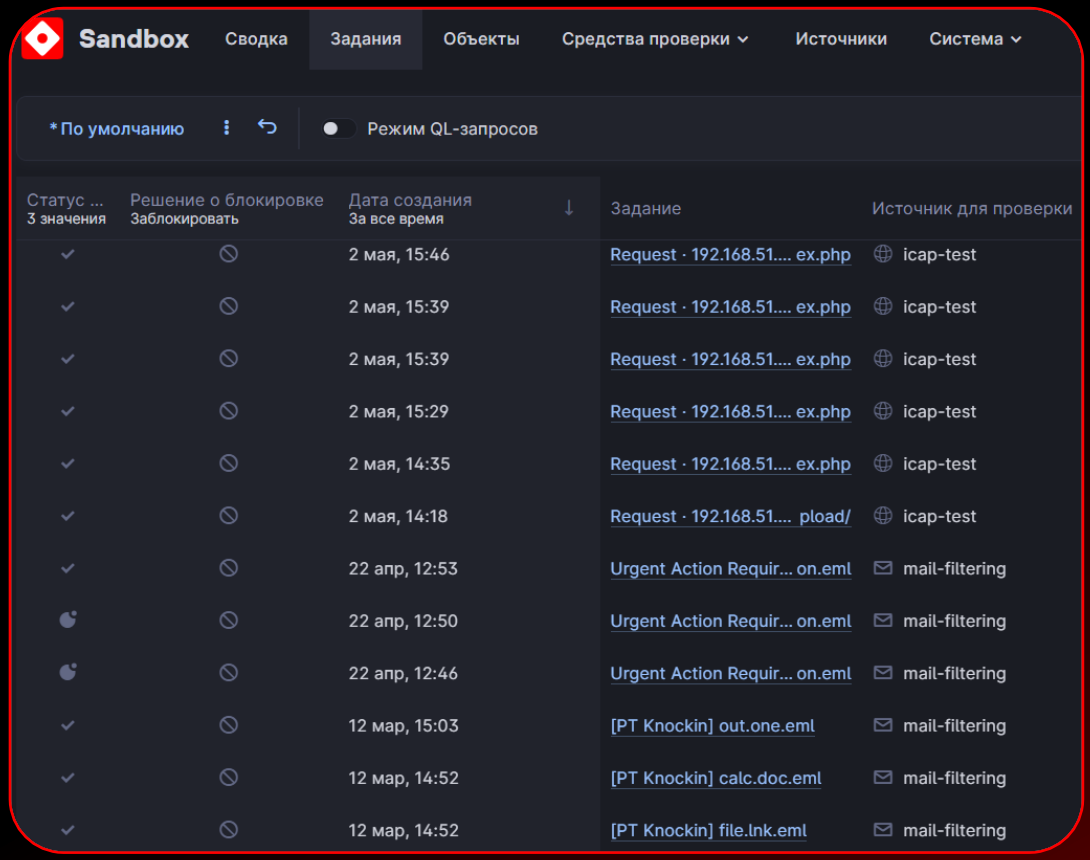
Блокировка ВПО

Защитное взаимодействие с почтовыми системами, системами контроля сетевого трафика и коннекторами API с целью недопуска вредоносного содержимого

Оказывает минимальное влияние на бизнес-процессы

Решаемые задачи:

- Блокировка ВПО, в том числе ранее неизвестного
- Защита от хакерских атак с применением различных инструментов
- Доставка пользователям сообщений безвредоносных вложений



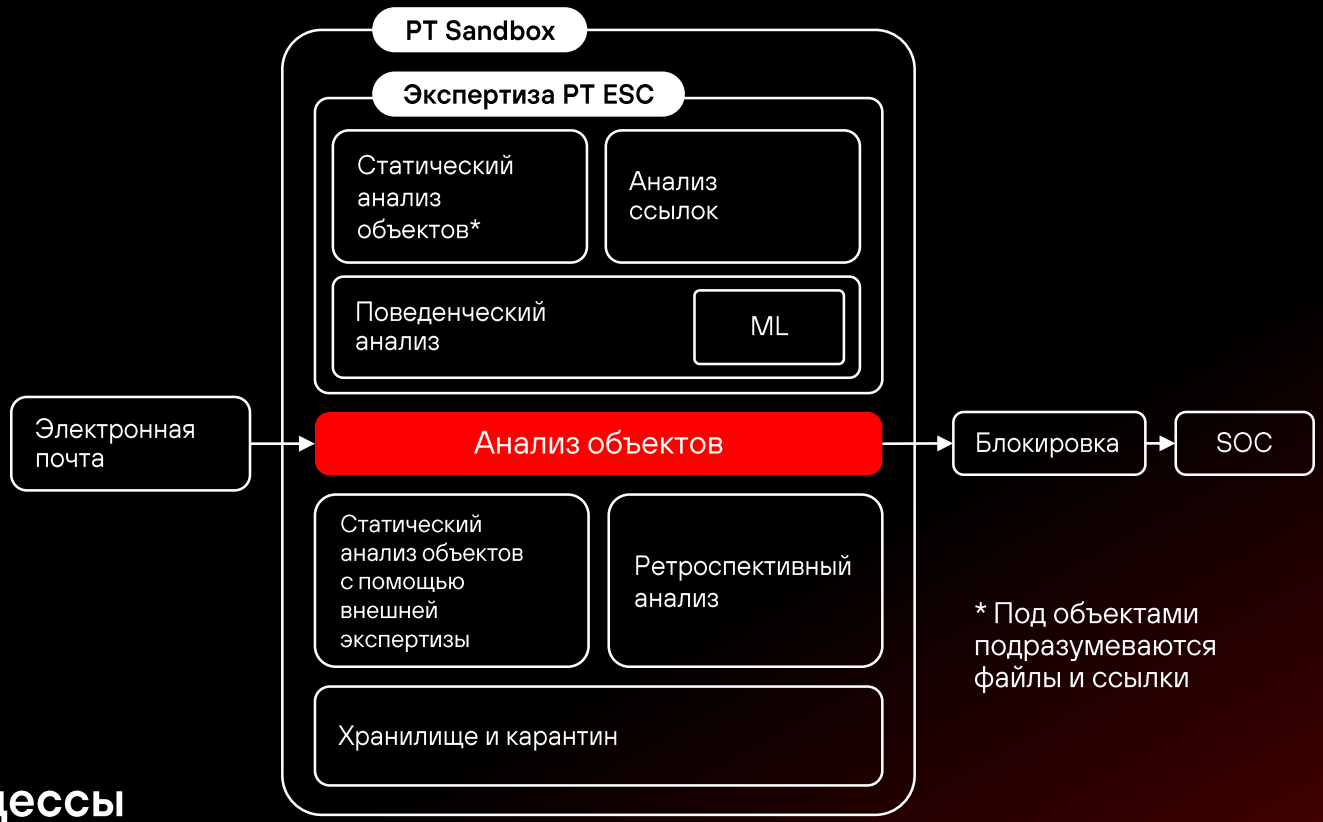
PT Sandbox

Блокировка ВПО в почтовом трафике

С 2019 года занимаюсь развитием технической экспертизы по применению решений в области сетевой безопасности

Непосредственно вношу свой вклад в улучшение качества внедрений и развитие практик применения таких продуктов, как PT Sandbox, PT NAD и PT MultiScanner

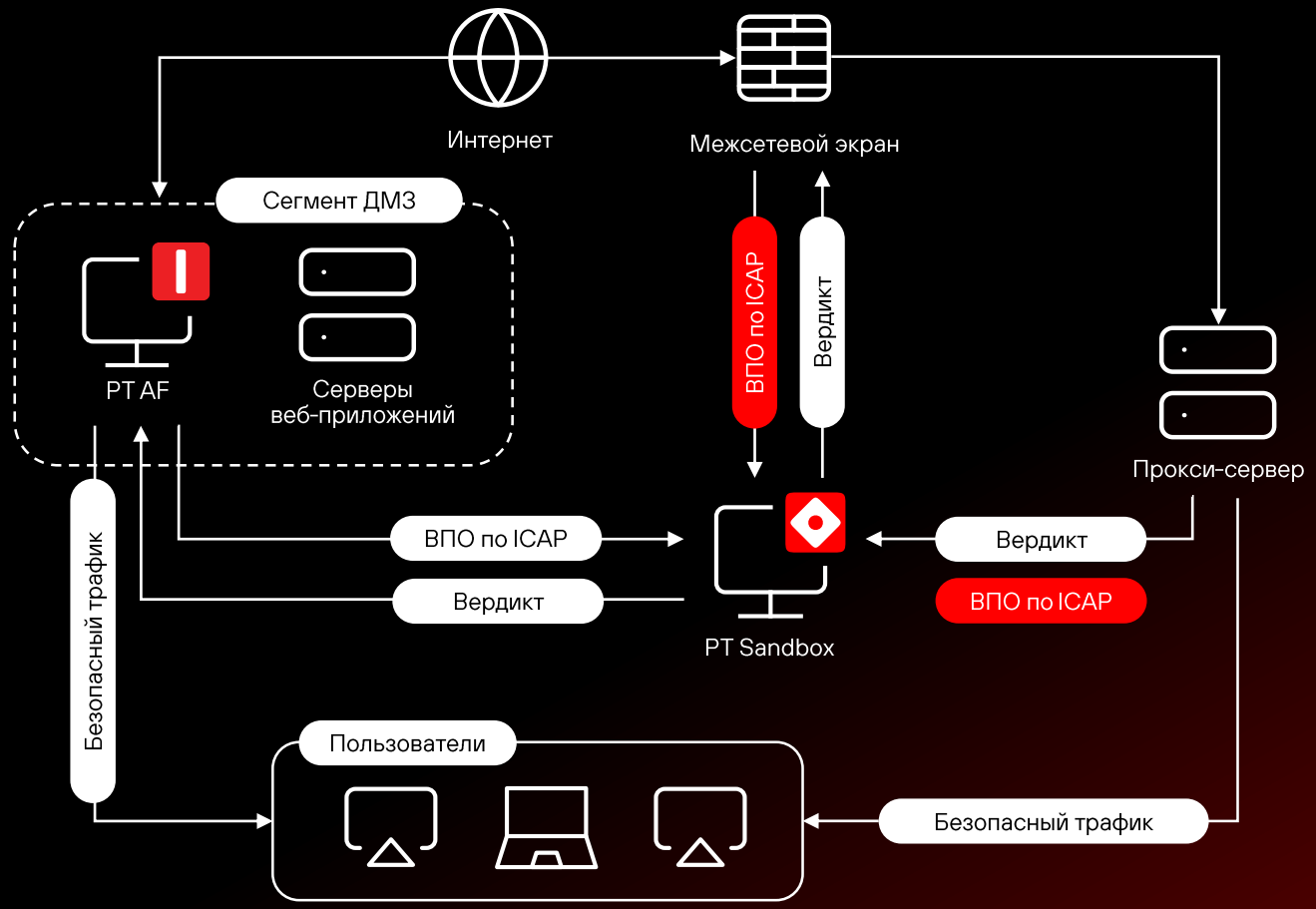
Минимальное влияние на бизнес-процессы



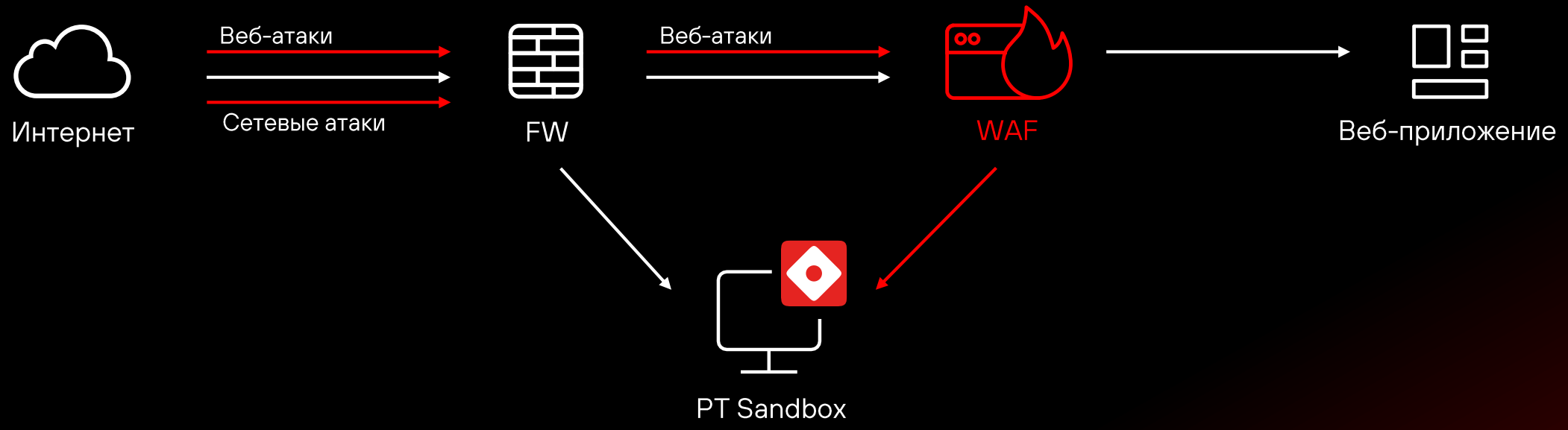
* Под объектами подразумеваются файлы и ссылки

Схема подключения PT Sandbox к сетевым СЗИ в режиме блокировки

PT Sandbox устанавливается в инфраструктуре и подключается к сетевым устройствам по протоколу ICAP. Получает файл на анализ, проверяет его и отправляет обратно команду на блокировку, защищая пользователей от неизвестного ВПО



Защита от сетевых и веб-атак

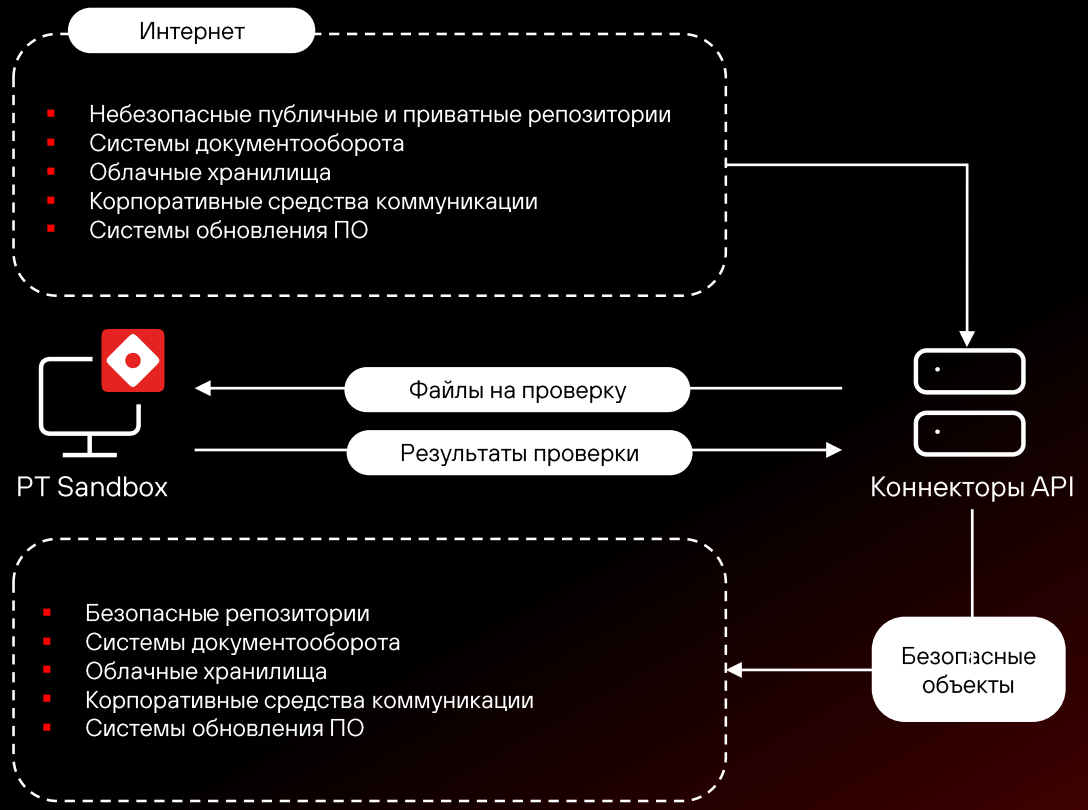


PT Sandbox анализирует файлы из трафика, защищаемого межсетевыми экранами и экранами уровня веб-приложений

PT Sandbox и сторонние системы

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

Развитие PT Sandbox

PT Sandbox 5.7
(декабрь 2023 года)

- Образ Ubuntu 22.04.1 Long-Term Support в поведенческом анализе
- Предфильтрация — признаки PDF-файлов для их проверки с помощью метода поведенческого анализа
- Распаковка ELF-файлов при проверке

PT Sandbox 5.8
(январь 2024 года)

- Переход для поиска на iocportal.ptsecurity.com
- Добавление пользовательских образов ВМ через веб-интерфейс
- Ввод команд для поведенческого анализа файлов

  Предфильтрация — признаки файлов офисных форматов для их проверки с помощью метода поведенческого анализа

PT Sandbox 5.9
(февраль 2024 года)

- PT Categorizer — отображение категоризации ссылок в результатах проверки
- Обновление вида пользовательского интерфейса

PT Sandbox 5.10
(апрель 2024 года)

- Образ «Альт Рабочая станция» 10 в поведенческом анализе
- Снятие дампов памяти процессов при поведенческом анализе в ОС семейства Linux
- Поведенческий анализ файлов APPX, APPXBUNDLE, MSIX, MSIXBUNDLE в образах виртуальных машин Windows 10
- Определение потенциально опасных файлов OpenDocument
- Поддержка распаковки архивов LZH

PT Sandbox 5.11
(май 2024 года)

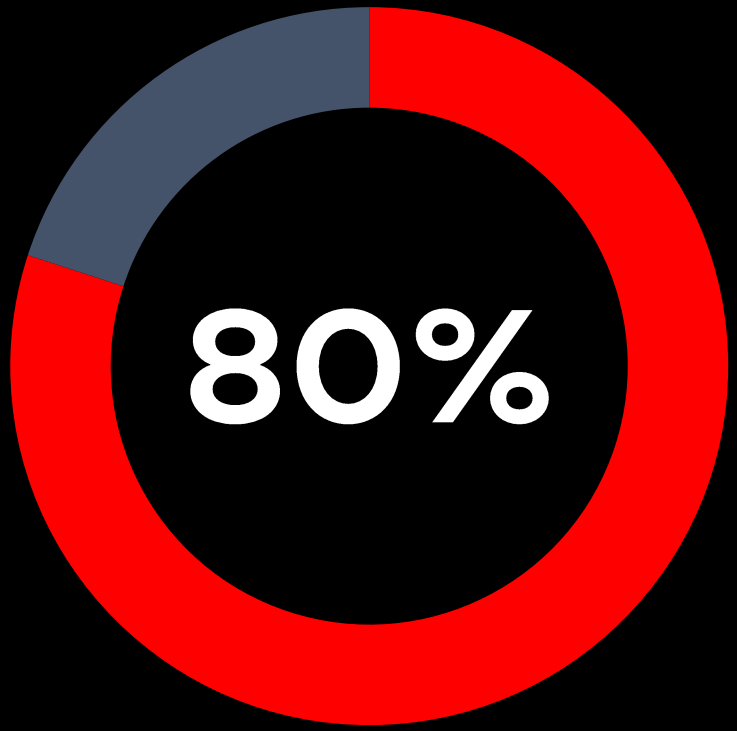
- Изменена страница «Сводка»
- Добавлена страница «Конфигурация» с информацией об узлах PT Sandbox и их ролях
- Дополнены признаки файлов Microsoft Office 97-2003, добавлены критерии вердикта и проверок

PT Sandbox 5.12
(июнь 2024 года)

- Доработка определения типов файлов перед отправкой на поведенческий анализ
- Поведенческий анализ файлов Microsoft Access
- Проверка цифровых подписей файлов CAB, DLL, EXE, MSI при поведенческом анализе

На крыльях

Новые возможности с функциями производительности



Снижение первоначальной нагрузки на поведенческий анализ с помощью возможностей настраиваемой фильтрации

Альфа-тестирование:

удвоение лимита виртуальных машин на сервер

Модель поставок и лицензирования

Поставка

На аппаратной платформе

Все узлы PT Sandbox разворачиваются на аппаратной платформе

Совмещенное размещение

Основной узел разворачивается на виртуальной машине, а узлы поведенческого анализа — на аппаратной платформе

Лицензирование

Инфраструктурные лицензии

- лицензия основного серверного узла
- лицензии узлов для отказоустойчивого кластера и горизонтального масштабирования узлов без поведенческого анализа

Лицензии на источники анализа:

- электронных писем (по числу почтовых ящиков)
- файлов из сетевого трафика (по нагрузке на канал)
- файлов, поступающих через API
- файлов из файловых хранилищ
- файлов из промышленного сетевого трафика (по нагрузке на канал обработки)

Также доступны опции: объединенная лицензия (all-in-one), PT Sandbox для небольших инфраструктур (SME)

Возможности интеграции PT Sandbox

MaxPatrol SIEM
Выявление инцидентов ИБ

PT NAD
Анализ сетевого трафика

PT Application Firewall
Защита веб-приложений

MaxPatrol EDR
Выявление киберугроз и реагирование на них

PT ISIM
Защита промышленных сетей

PT Threat Analyzer
Накопление и использование знаний об угрозах

PT Sandbox интегрируется с продуктами и решениями Positive Technologies, что позволяет создать экосистему кибербезопасности на базе единого технологического стека

Опробуйте песочницу PT Sandbox:

Запишитесь на демонстрацию
https://www.ptsecurity.com/ru-ru/products/sandbox/#materials

Задайте интересующие вопросы:

Телеграм-чат по PT Sandbox
https://t.me/ptsandbox

Спасибо!