Игорь Протопопов

— Эксперт Центра Компетенций Positive Technologies

Подход к результативной кибербезопасности

О Positive Technologies

20 лет

опыта исследований
и разработок

1600 сотрудников

инженеров по ИБ,
разработчиков, аналитиков
и других специалистов

250 экспертов

в нашем
исследовательском
центре безопасности

200+

обнаруженных
уязвимостей
нулевого дня в год

200+

аудитов безопасности
корпоративных систем
делаем ежегодно

50%

всех уязвимостей
в промышленности и телекомах
обнаружили наши эксперты

Защищаем крупные информационные системы от киберугроз:

- Создаем продукты и решения
- Проводим аудиты безопасности
- Расследуем инциденты
- Исследуем угрозы

Типовой защиты недостаточно

Защиты периметра недостаточно

96%

компаний
не защищены
от внешних атак

**От часа
до пяти дней**

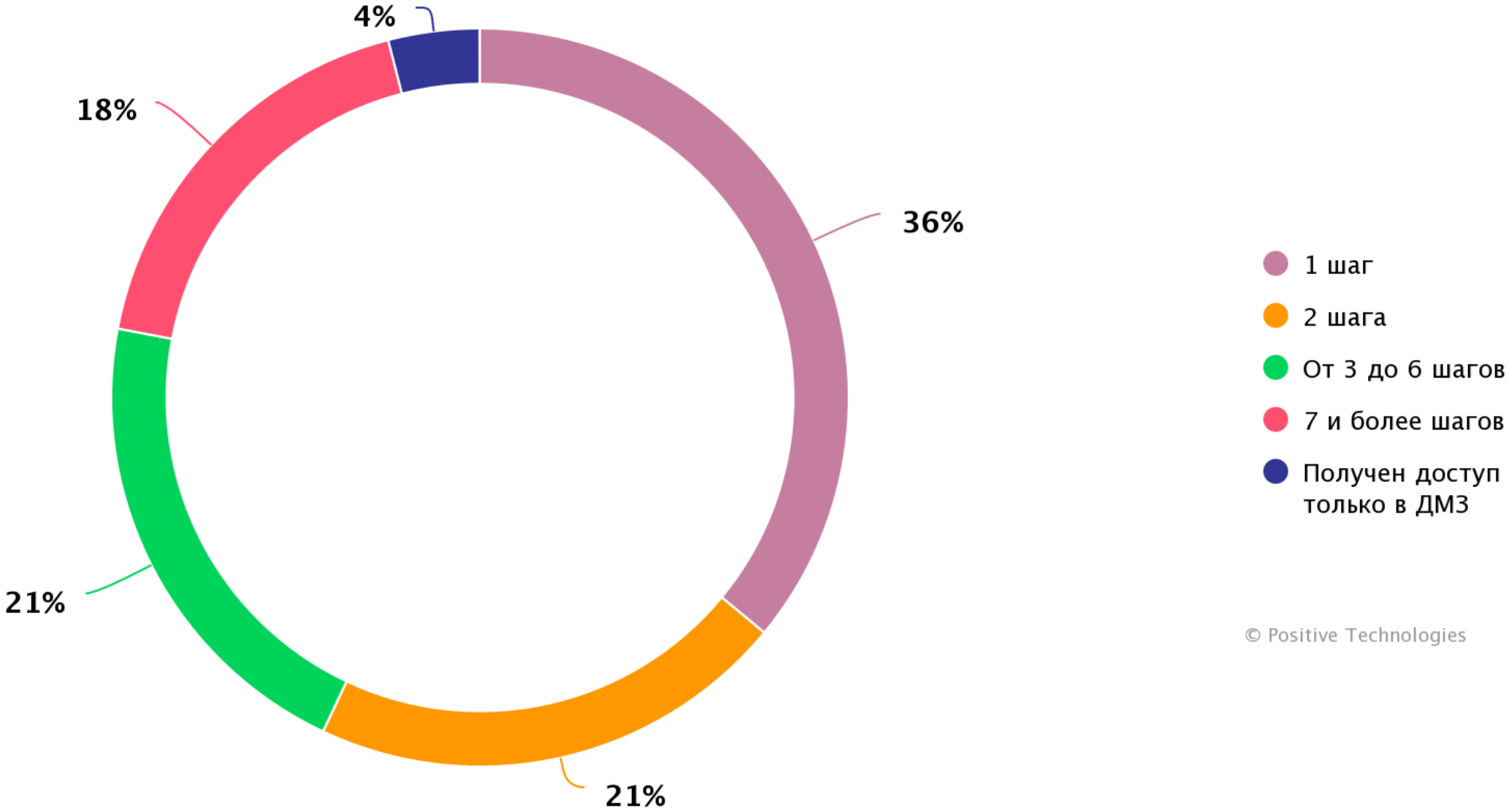
тратят злоумышленники
на проникновение
во внутреннюю сеть

В 100%

компаний инсайдер может
контролировать
инфраструктуру

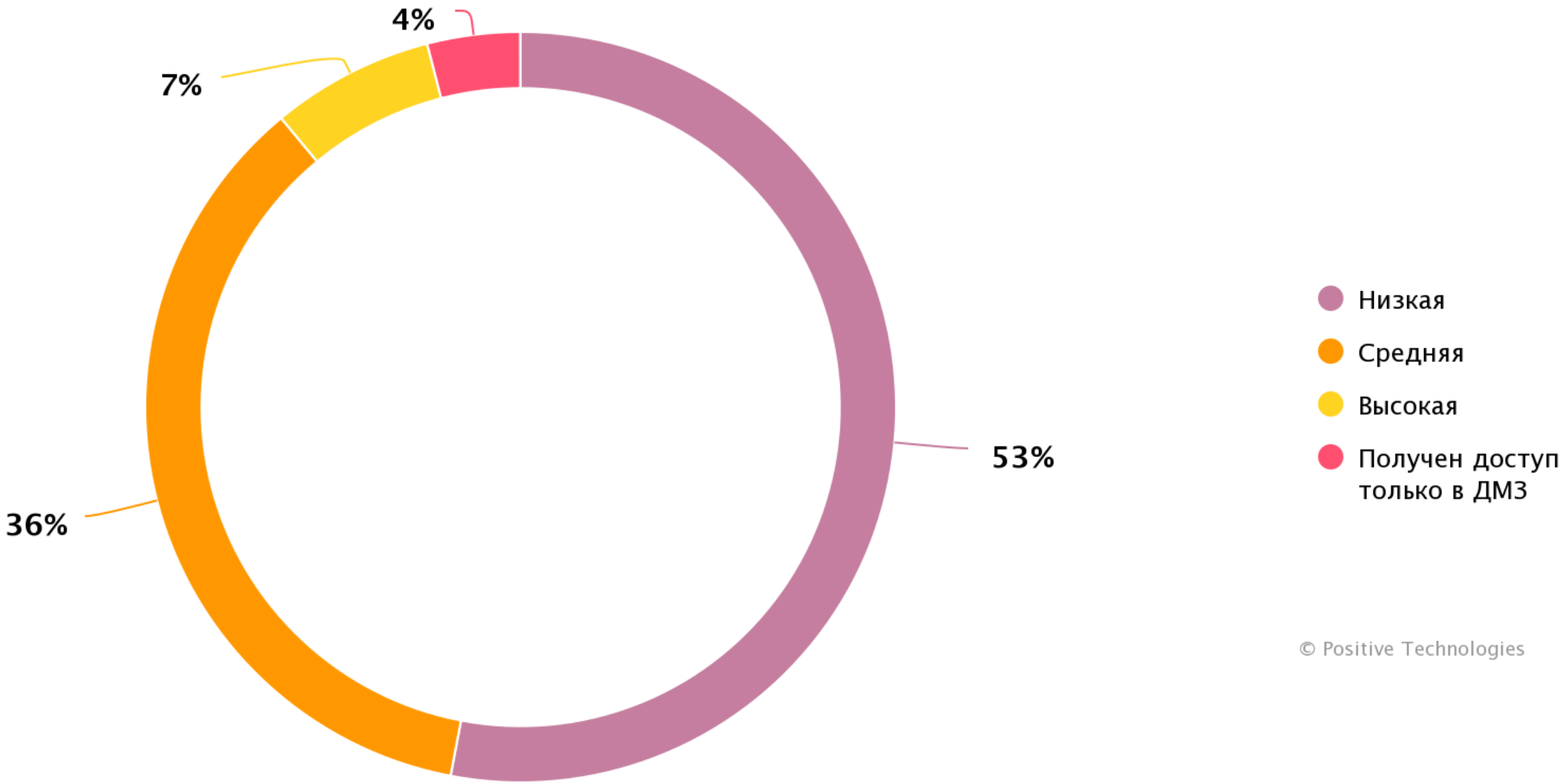
По данным исследования Positive Technologies «Итоги пентестов — 2022»

Минимальное число шагов для проникновения в локальную сеть



«Итоги пентестов — 2022», Positive Technologies

Минимальная сложность вектора проникновения во внутреннюю сеть



«Итоги пентестов — 2022», Positive Technologies

Классическая ИБ не защищает от целевых атак

Злоумышленники:

1. Инструменты автоматизации для проведения эффективных кибератак (AI и ML)
2. Сильное комьюнити для обмена практиками
3. Сервисная модель для заказных кампаний любого масштаба
4. Доступные бесплатные утилиты для взлома

Защитники:

1. Мониторинг для «галочки»
2. «Бумажная» безопасность
3. «Штабные» опросники вместо практических киберучений
4. Реализация типовых мер без реальной оценки актуальности угроз

Последствия:

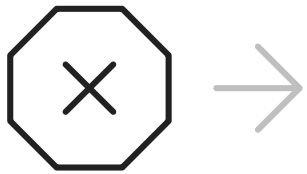
Реализация злоумышленниками недопустимых для организаций сценариев **незаметно и быстро**

Потребность:

Необходимы современные подходы и технологии, исключающие реализацию недопустимых сценариев

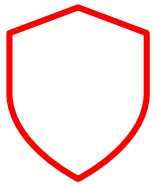
Нужна смена парадигмы

Основные элементы результативной кибербезопасности



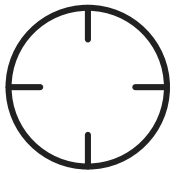
Недопустимые Событий

Выявляем, какие **события** действительно являются **недопустимыми** для компании, и проверяем их реализуемость на практике



Активное противодействие киберугрозам

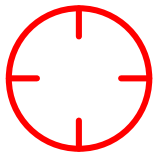
Проектируем и трансформируем кибербезопасность - создаем Центр противодействия киберугрозам, обеспечивая исключение недопустимых событий



Проведение киберучений

Проверяем достижение результата и невозможность реализации недопустимых событий путем киберучений

Шаги к исключению недопустимых событий

1. 

Определение недопустимых событий

Определение ключевых недопустимых событий, а также возможных сценариев их реализации

2. 

Анализ процессов ИБ и верификация

Определение причин, способствующих реализации недопустимых событий, и их проверка на практике

3. 

Формирование программы кибер-трансформации

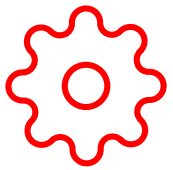
Разработка программы развития кибербезопасности

Шаги по построению центра противодействия киберугрозам

1. 

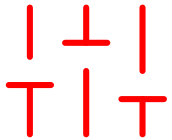
Адаптация ИТ инфраструктуры и бизнес-процессов

Перестроение инфраструктуры и подготовка к развертыванию ЦПК

2. 

Внедрение и настройка средств защиты

Развертывание необходимых решений для выявления кибератак

3. 

Тонкая настройка элементов ЦПК

Подключение целевых информационных систем и выстраивание процессов

Шаги по проведению киберучений

1. 

Подготовка к киберучениям

Планирование и согласование области работ, проведение предварительных киберучений

2. 

Проведение киберучений

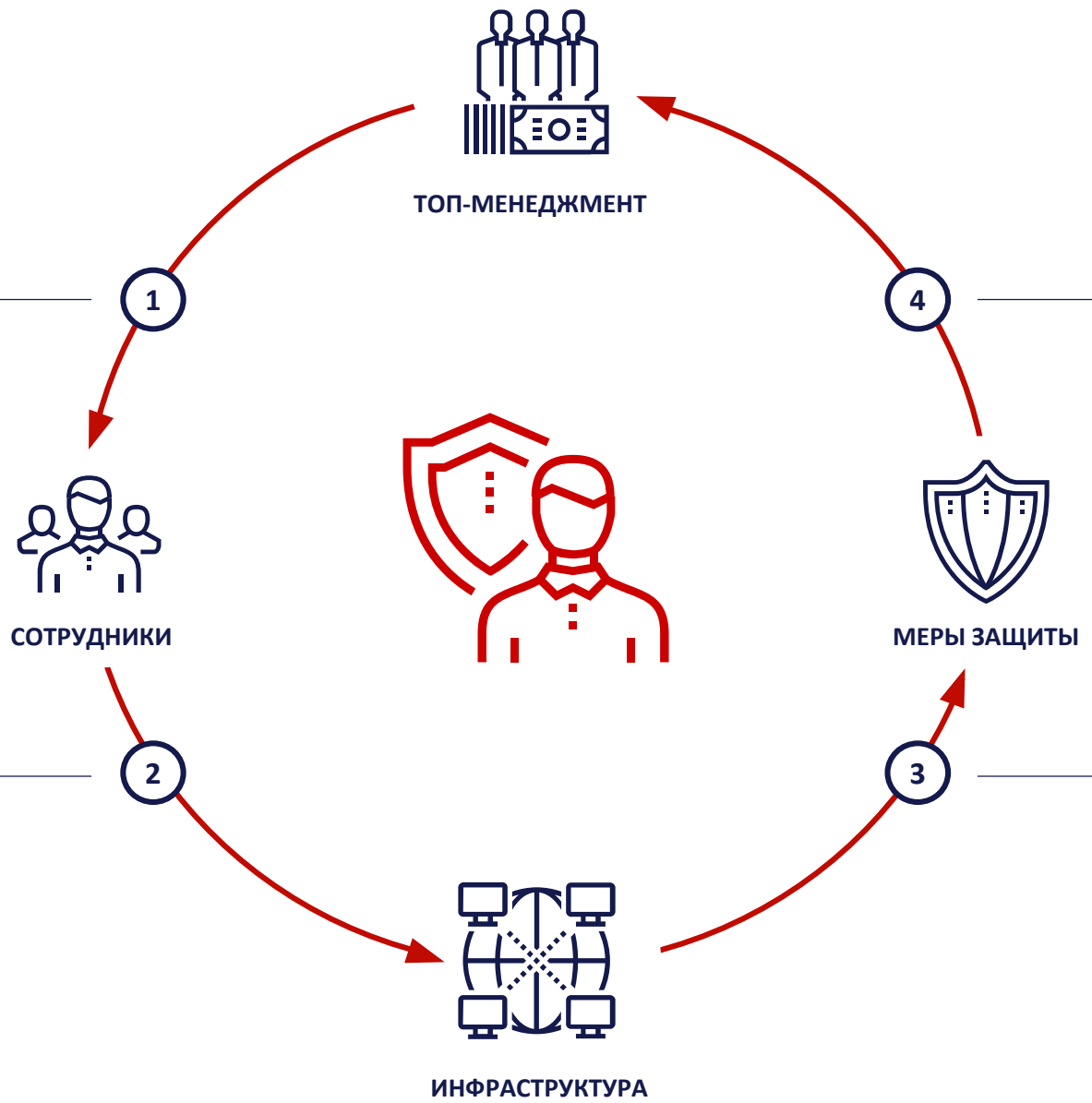
Активная стадия проверки эффективности работы ЦПК в процессе кибератаки

3. 

Модернизация по результатам киберучений

Планирование мероприятий, направленных на повышение киберустойчивости компании

Позитивный подход к кибербезопасности



Технологии и автоматизация

Активное противодействие киберугрозам: процессы

инвентаризация

патч-менеджмент

управление уязвимостями

выявление целевых атак: трафик

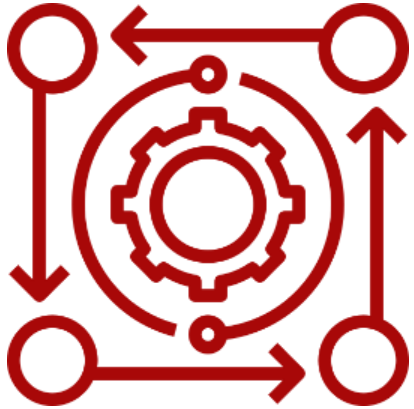
сбор и анализ событий ИБ

выявление целевых атак: вредоносное ПО

выявление инцидентов

реагирование на инциденты

расследование инцидентов

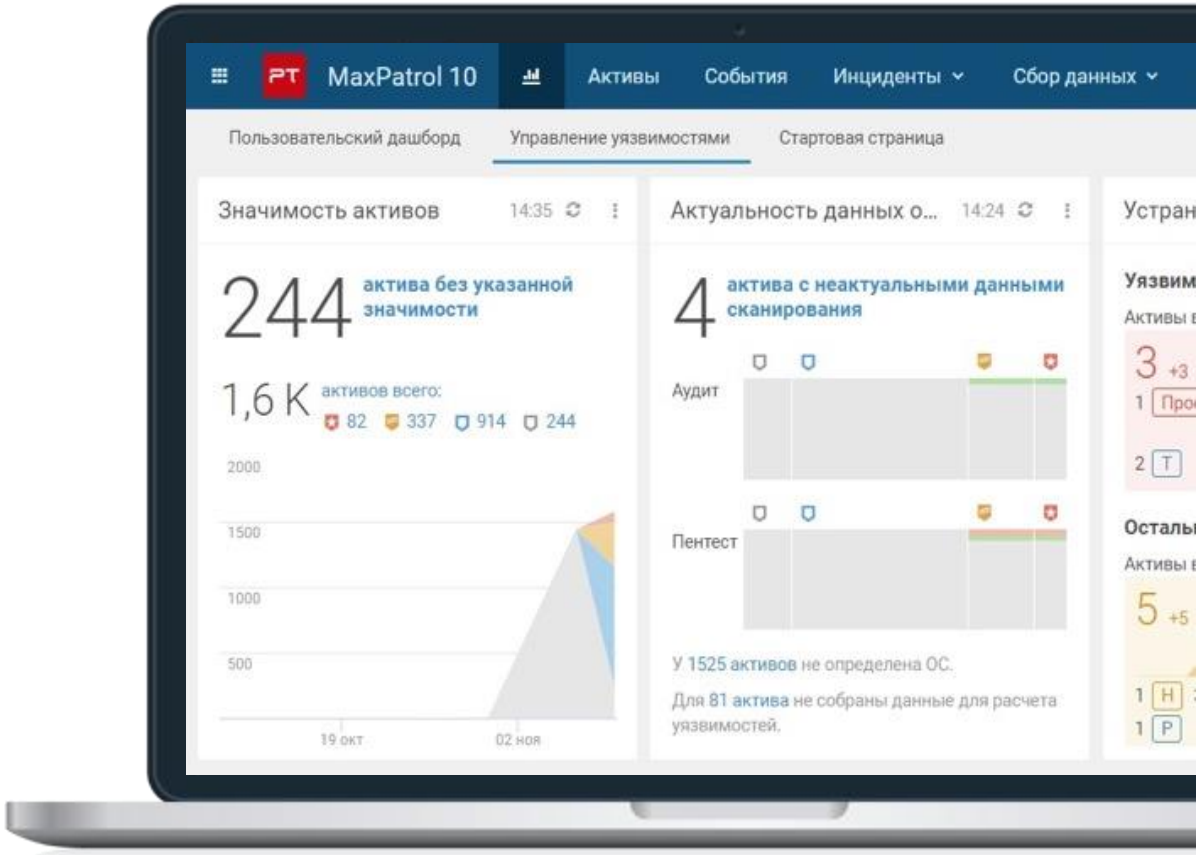


1. Управление уязвимостями - MaxPatrol VM

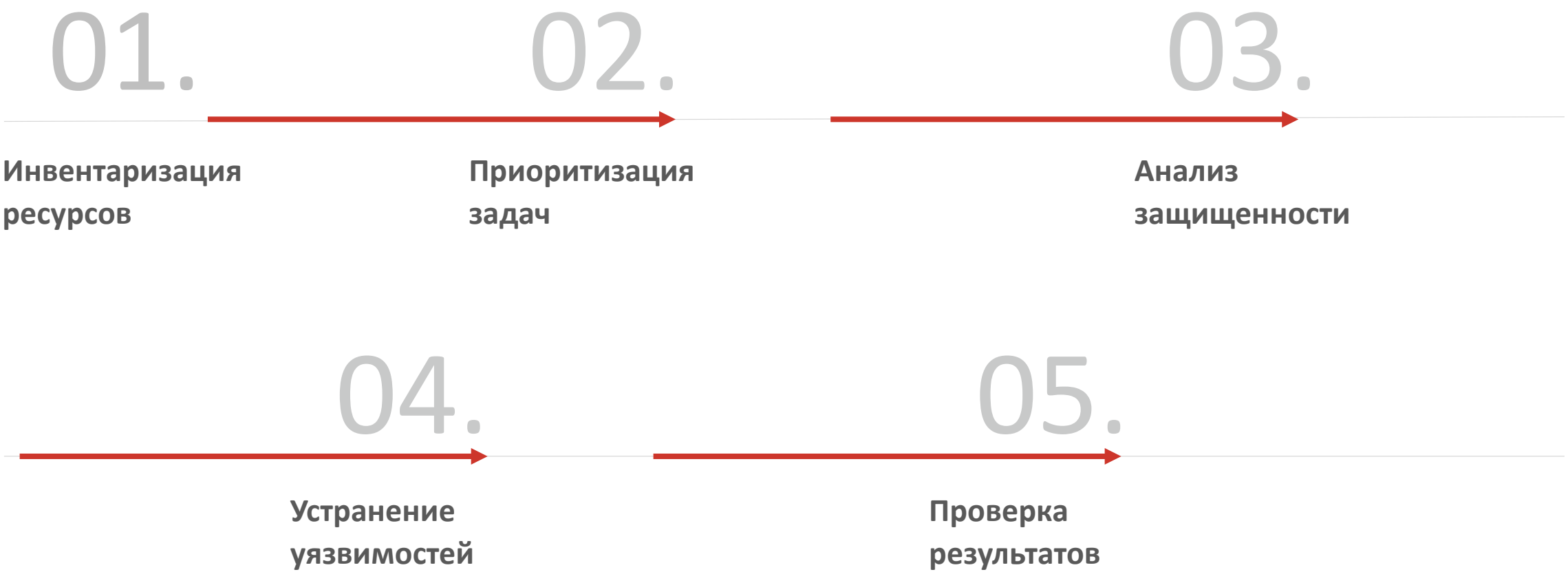
Система управления уязвимостями нового поколения

→ Помогает выстроить полноценный процесс управления уязвимостями, в который вовлечены как ИБ, так и IT-специалисты.

→ Контролирует защищенность IT-инфраструктуры в каждый момент времени и помогает правильно приоритизировать работу над уязвимостями.



MaxPatrol VM:
Выстраиваем непрерывный процесс



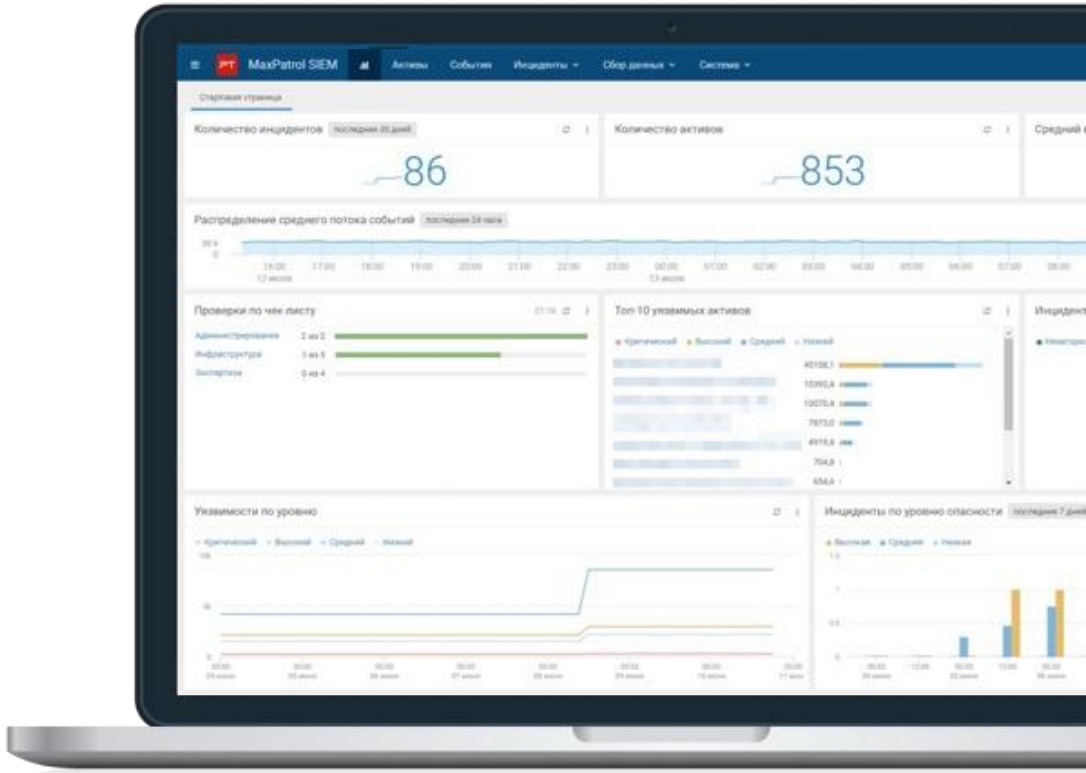
2. Сбор событий и выявление аномалии – MaxPatrol SIEM

Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз

→ Дает видимость IT-инфраструктуры

→ Позволяет выявлять самые актуальные угрозы

→ Снижает трудозатраты специалистов по ИБ на мониторинг состояния инфраструктуры и написание правил выявления атак



MaxPatrol SIEM:
Контролируем свою инфраструктуру

Лидирующее отечественное SIEM-решение

Продукт внедрен более чем в 200 промышленных, транспортных, финансовых компаниях, в частном и государственном секторе, в органах власти. Согласно исследованию IDC, MaxPatrol SIEM входит в тройку лидеров российского рынка SIEM. Другие отечественные SIEM-системы занимают не более 6% рынка

Регулярно получает экспертизу для обнаружения угроз

Раз в два месяца MaxPatrol SIEM пополняется пакетам экспертизы с новыми правилами корреляции, индикаторами компрометации и плейбуками

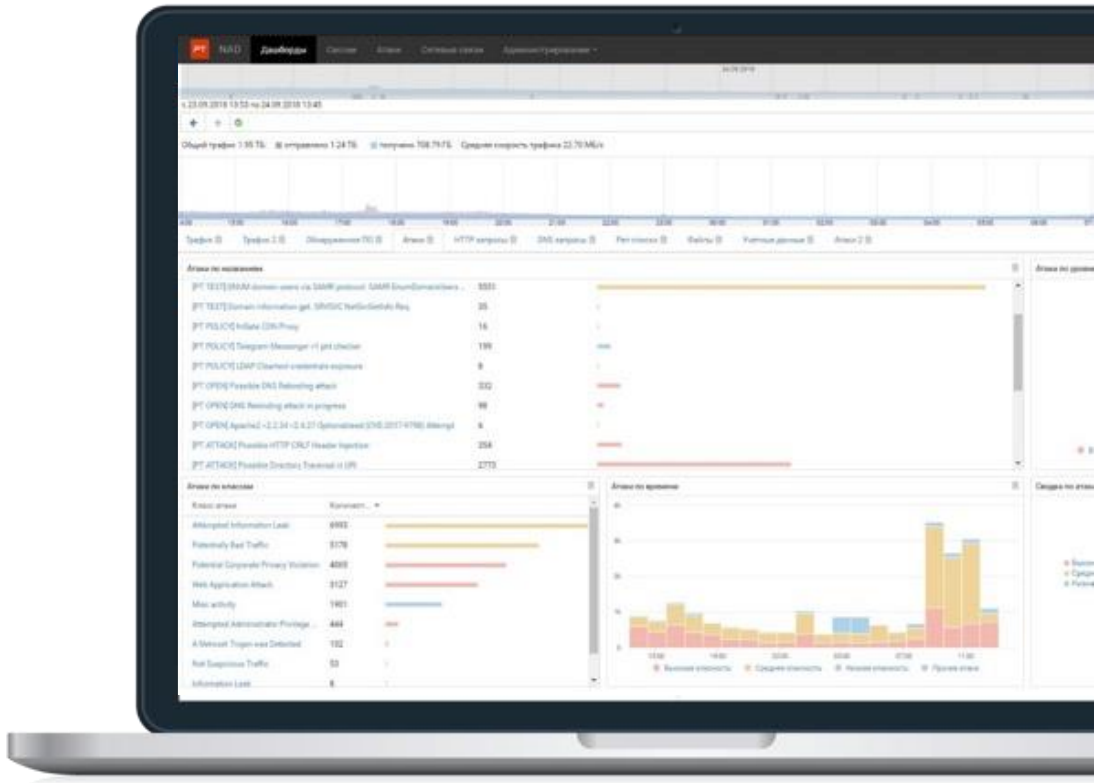
Быстро развивается и становится проще

Выпускаем два релиза в год, регулярно внедряем новые технологии и расширяем команду разработки продукта. Мы постоянно упрощаем продукт, чтобы развернуть MaxPatrol SIEM, работать с ним и выявлять угрозы мог даже новичок. Например, за последние два года в продукте появились регулярная поставка пакетов экспертизы, чек-лист настройки системы, конструктор правил корреляции и возможность быстрого снижения количества ложных срабатываний

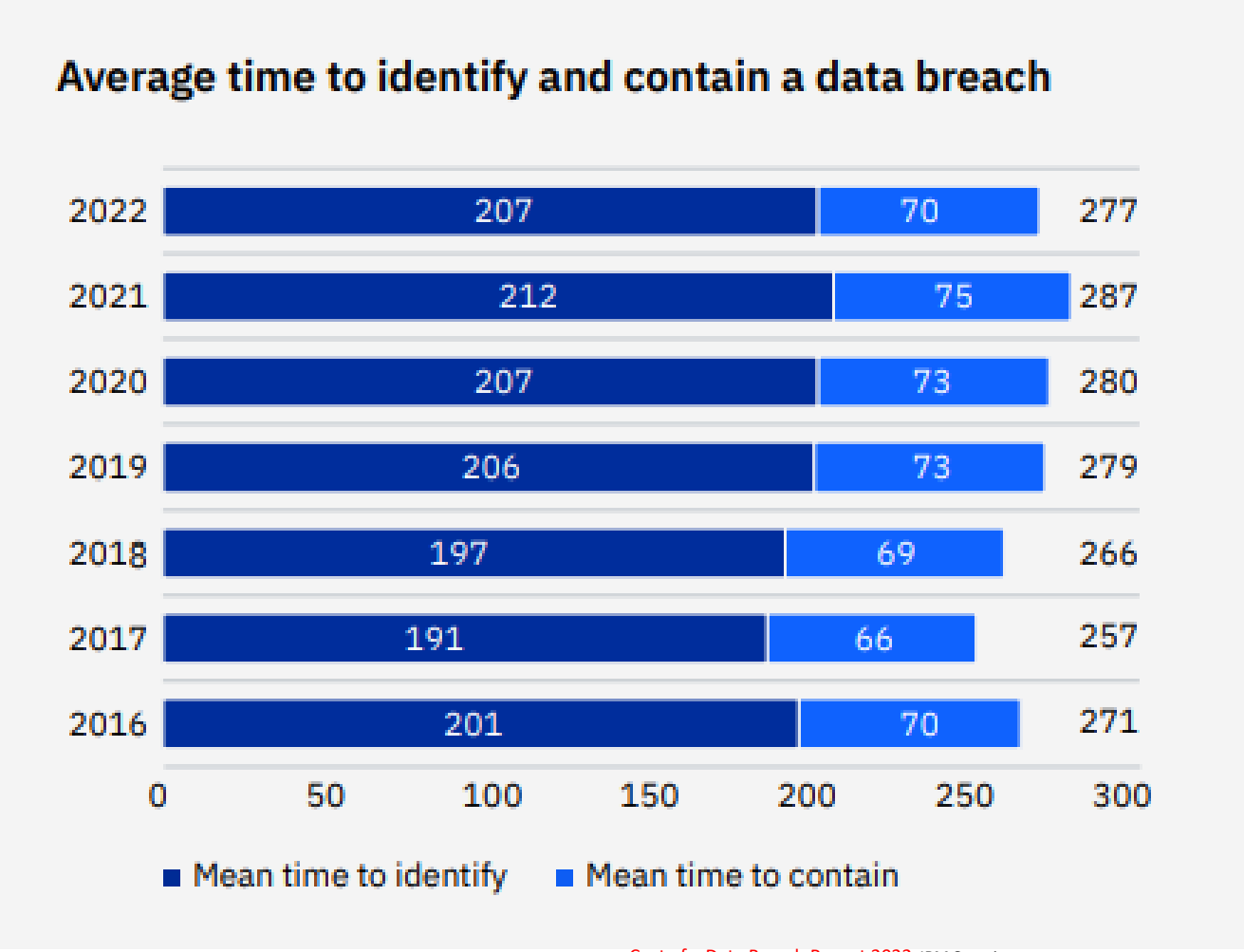
3. Обнаружение атакующего внутри сети - PT Network Attack Discovery

Система глубокого анализа сетевого трафика (NTA/NDR) для выявления атак на периметре и внутри сети

- Обнаруживает скрытые угрозы в сети по большому количеству признаков
- Дает понимание, что происходит в сети, и позволяет проконтролировать соблюдение регламентов ИБ
- Повышает эффективность работы SOC, помогает восстановить цепочку атаки и собрать доказательную базу



Нас никто не атакует…



Cost of a Data Breach Report 2022, IBM Security

Среднее время обнаружение и локализации взлома составляет 277 дней

PT Network Attack Discovery: знаем что происходит в сети

Видит активность злоумышленников как на периметре, так и внутри сети

PT NAD анализирует не только внешний, но и внутренний трафик, поэтому он детектирует горизонтальные перемещения злоумышленников, попытки эксплуатации уязвимостей, атаки на конечных пользователей в домене и на внутренние сервисы

Использует передовые технологии выявления угроз

Для выявления атак на ранних стадиях продукт использует технологии поведенческого анализа, глубокую аналитику, собственные правила детектирования угроз, индикаторы компрометации и ретроспективный анализ. PT NAD видит вредоносную активность даже в зашифрованном трафике

Является основой для построения SOC и threat hunting

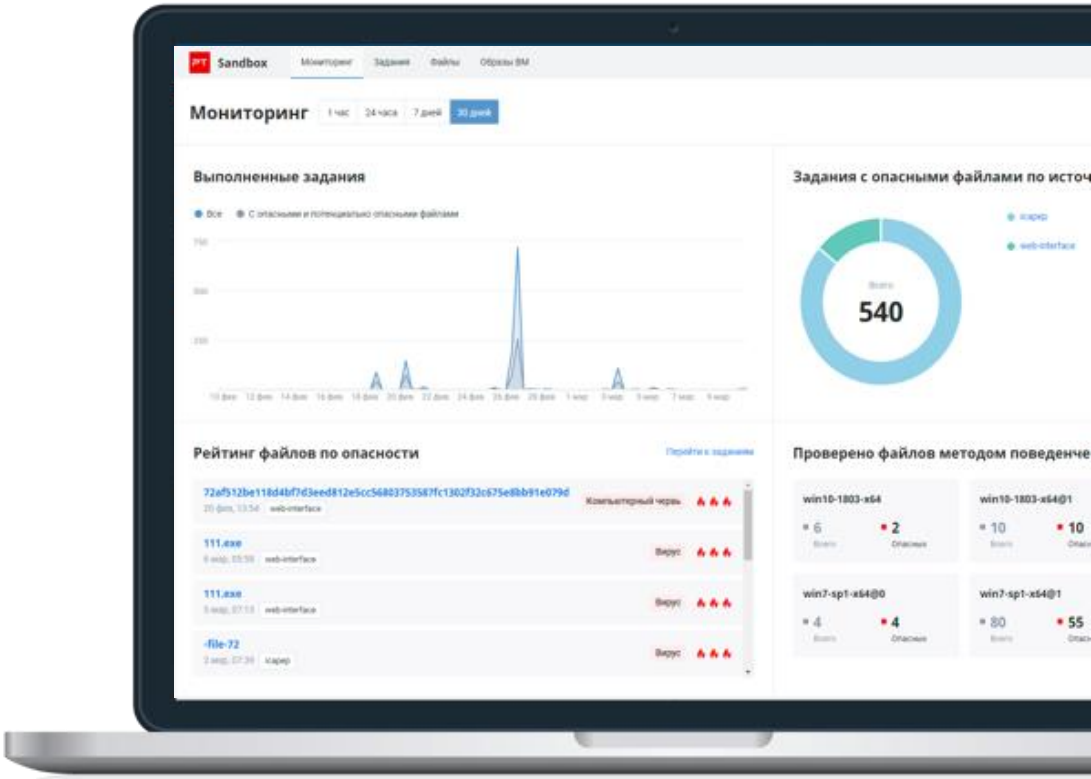
Продукт хранит 1200 параметров сессий и записи сырого трафика. Такие данные становятся полезными источниками знаний при раскрутке цепочки атаки и ее локализации, а также при проверке гипотез в рамках threat hunting

4. Блокирование вредоносного ПО - PT Sandbox

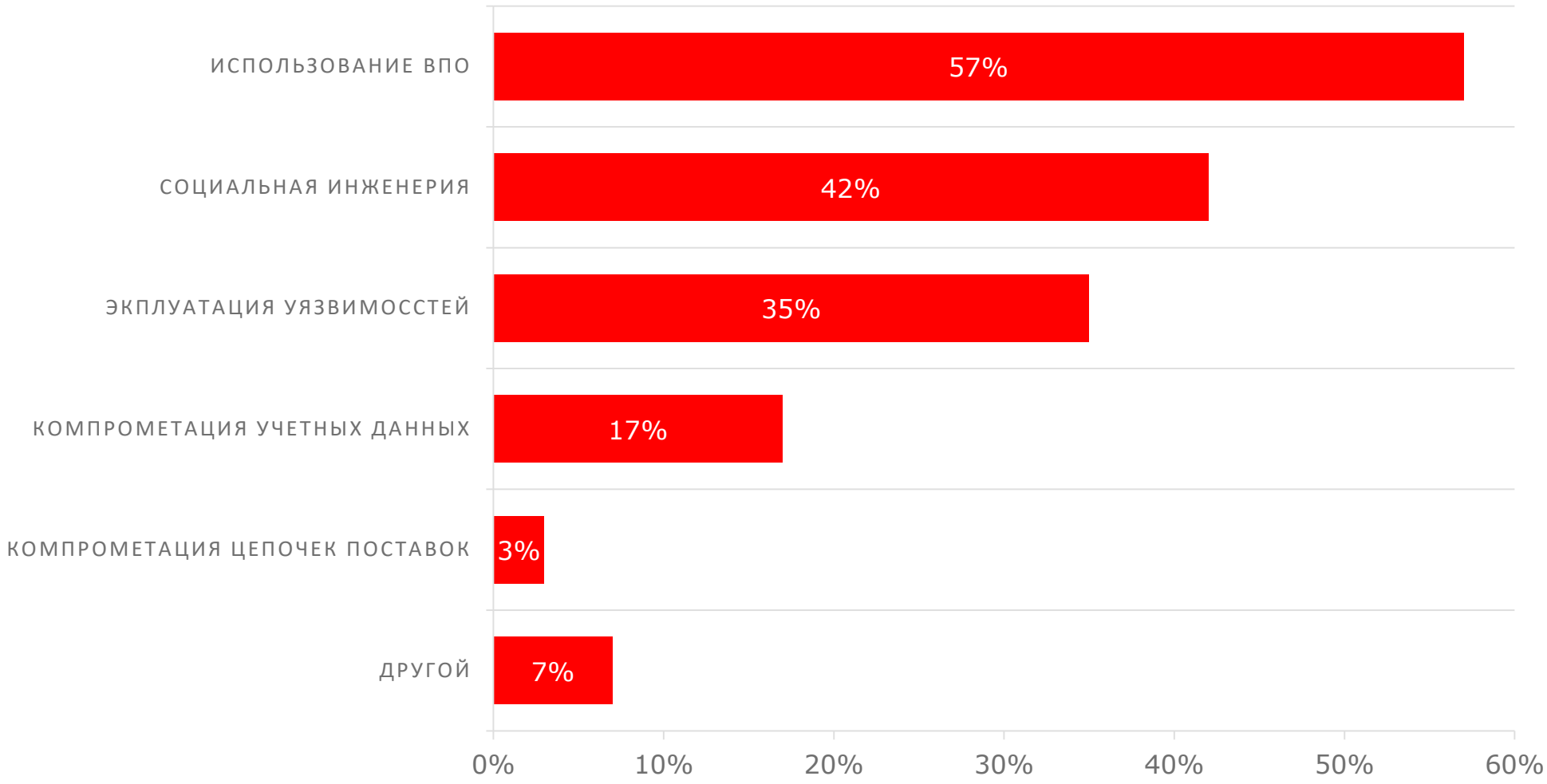
Риск-ориентированная песочница с возможностью кастомизации виртуальных сред

→ Защищает от целевых и массовых атак с применением неизвестного вредоносного ПО и угроз нулевого дня

→ Позволяет выявлять угрозы в почте, файловых хранилищах, веб-трафике пользователей, внутреннем сетевом трафике компании, корпоративных системах документооборота, а также на ручных порталах проверки файлов



ВПО это не страшно…



В 6 из 10 атак применяется **вредоносное ПО**

МЕТОДЫ АТАК НА ОРГАНИЗАЦИИ

«Актуальные киберугрозы: IV квартал 2022 года», Positive Technologies

PT Sandbox – защита от современного вредоносного ПО

Позволяет персонализировать защиту компании

PT Sandbox позволяет добавлять в виртуальные среды специфический софт и его версии, которые используются в компании и могут стать целью злоумышленников. Также в продукте реализованы deception-технологии: «приманки» в виде фейковых файлов, процессов и данных, которые провоцируют вредоносное ПО совершить активные действия и выдать себя

Обнаруживает угрозы не только в файлах, но и в трафике

Помимо файлов PT Sandbox проверяет трафик, который генерируется в процессе их анализа, а также выявляет вредоносную активность, скрытую под TLS. Это существенно повышает эффективность детектирования атак — даже в шифрованном трафике

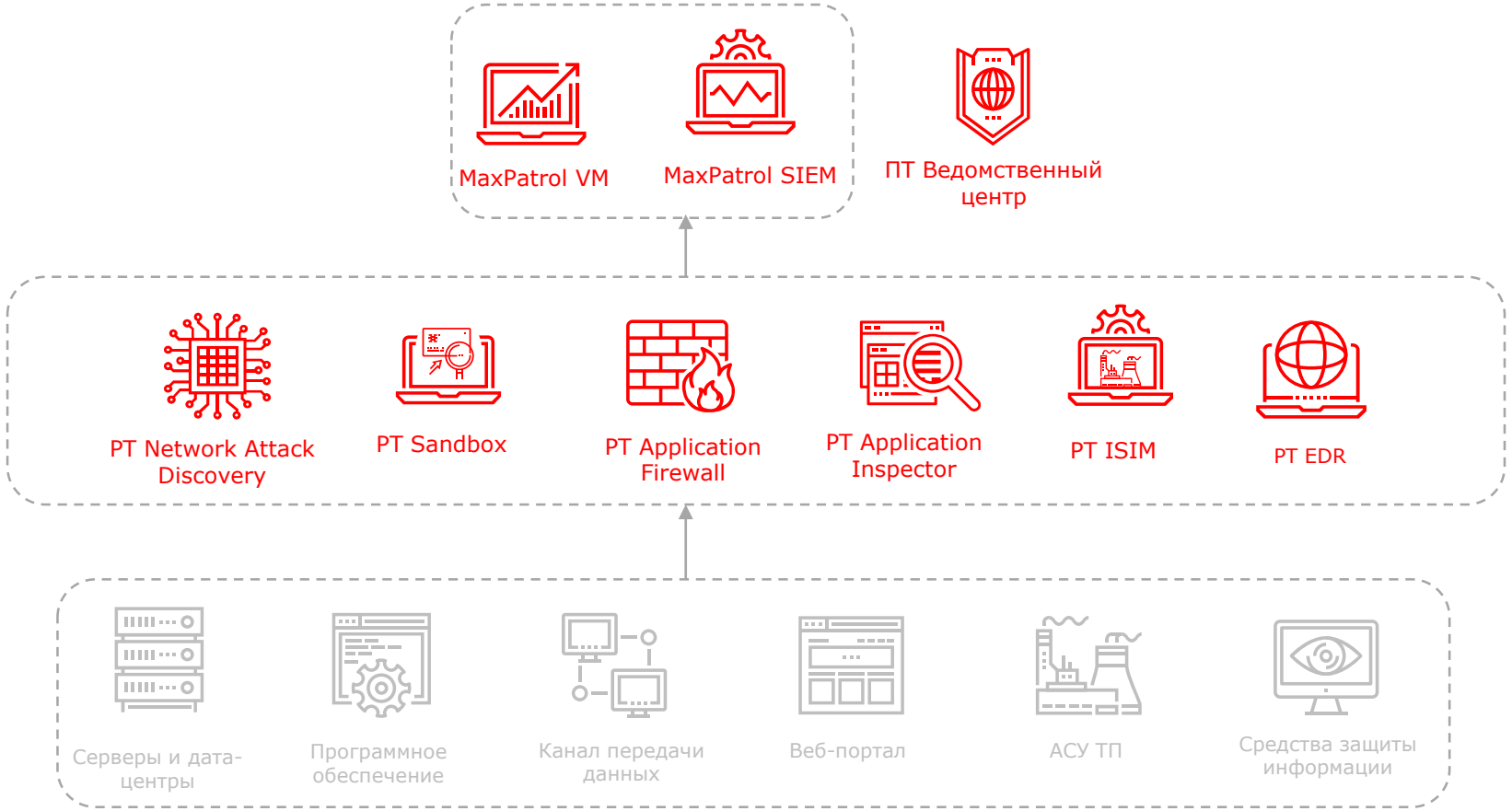
Выявляет атаки, не обнаруженные ранее

PT Sandbox запускает автоматическую перепроверку уже проанализированных файлов после обновления базы знаний. Так продукт максимально быстро обнаруживает скрытые в инфраструктуре угрозы

Не только для корпоративного сегмента: наличие промышленной версии

Промышленный PT Sandbox обнаруживает угрозы, нацеленные на компоненты АСУ ТП (SCADA), и позволяет кастомизировать среду эмуляции и «приманки» с учетом специфики сети промышленного предприятия

Комплексный подход для выявления сложных угроз



С чего начать?

Ознакомление с функционалом решений на демо-стенде PT

Сообщаете партнеру о необходимости демонстрации

Согласовываем дату и время. Обсуждаем желаемый сценарий демо

Проводим демонстрации в специально подготовленной инфраструктуре, приближенной к реальным условиям

Пилот: тестирования в реальной инфраструктуре

Заявка
Оставьте заявку через партнера или на нашем сайте

Подписание NDA, заполнение анкеты, составление плана

Развертывание
установка, настройка

Пилотный проект, мониторинг специалистами Positive Technologies

Отчет о результатах

≈ 6 недель

ИСКЛЮЧИТЬ НЕДОПУСТИМОЕ РЕАЛЬНО!

Игорь Протопопов

Менеджер по продвижению продуктов