Эльман Бейбутов

Директор по развитию
продуктового бизнеса

От ЦПК до автопилота в мире кибербеза

Эволюция с Positive Technologies

О спикере

С 2011 года занимаюсь продвижением продуктов и проектов в области мониторинга событий ИБ для создания центров противодействия киберугрозам. Стартовал в Jet Infosystems, потом в Solar Security, 5 лет работал в IBM, а сейчас — с командой Positive Technologies

За 10 лет на моих глазах сменилось несколько лидеров рынка SIEM-систем, а также наработан огромный опыт продаж и продвижения решений и услуг на очень конкурентном рынке ЦПК (MSS)

01

Ты помнишь, как все начиналось?

Как устроен стандартный подход к ИБ

ИБ не говорит с руководством на одном языке

Поэтому нет диалога между службой ИБ и менеджментом

Бюджет на ИБ растет, но результат непрозрачен

Высшее руководство не видит выгоды от этих инвестиций

ИБ воспринимается как лишний барьер

Служба ИБ стремится все запретить или снять с себя ответственность

Служба ИБ стремится защитить все

Значит, потенциально не защищает ничего

Защита на бумаге — для регуляторов

Важно соответствие требованиям, а не реальная защита

Размытие ответственности за ИБ

Всегда найдутся тысячи причин, почему небезопасно

02

Как не проспать ожидания бизнеса

Предпосылки

Сформировавшееся отношение к информационной безопасности ставит ее далеко от приоритетных направлений развития организации

Из-за этого ключевые руководители и владельцы компаний не видят практической, понятной и измеримой пользы инвестиций в информационную безопасность

А что, если киберзащиту сделать такой, чтобы **недопустимые** с точки зрения руководства и владельцев компании **события и ущерб** стали практически **невозможными**?

Что делать в условиях парадигмы «всех уже давно взломали»?

Для чего мы внедряем технические средства защиты?

?

Как в результате получить не стопку бумаг, а реальную защиту бизнеса?

Чем измерить эффект от инвестиций в кибер-безопасность?

Почему мы говорим о недопустимых событиях

Современные условия, формирующие **значимость недопустимых событий**

Темп деятельности

Рост скорости принятия решений и выполнения деятельности сводит к минимуму время, доступное на реагирование в случае чрезвычайных ситуаций

Зависимость от технологий

Цифровизация деятельности вместе с повышением уровня автоматизации изменяет ландшафт угроз и формирует новые технологические риски

Централизация деятельности

Требования к устойчивости централизованных решений высоки из-за агрегации точек отказа и сокращения цепочки допустимых ошибок

Требования к качеству

Рост целевых показателей требует постоянного повышения эффективности деятельности и дополнительного контроля

Рост объема деятельности

Увеличение количества операций и объема информации усиливает негативные последствия от ошибок и сбоев

Что такое недопустимые события

Недопустимое событие —

возникающее в результате действий киберзлоумышленников событие, приводящее к продолжительному нарушению или полной остановке процессов компании и ставящее под угрозу **достижение операционных или стратегических целей бизнеса**

Кража денежных средств

Пример: незаконный вывод денег со счетов компании в размере 10–15% от чистой прибыли

Прерывание функционирования

Пример: сбои или остановка операционных процессов из-за недоступности поддерживающих информационных систем

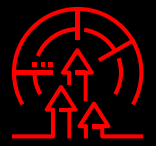
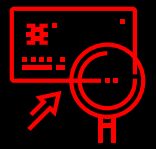
Искажение (утрата) рабочих данных

Пример: несанкционированные изменения, приводящие к некорректным результатам деятельности или к невозможности достижения целей

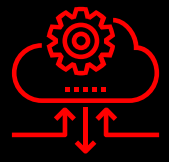
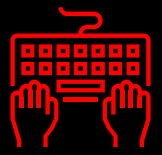
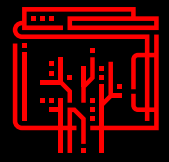
Утечка конфиденциальной информации

Пример: масштабная утечка персональных данных работников, клиентов и контрагентов или конфиденциальной информации, представляющей ценность для бизнеса

Сравнение подходов. Стратегия

Результативная КБ		Классическая ИБ
Непосредственное участие руководства в постановке целей КБ, понимание того, что действительно значимо для бизнеса, и заинтересованность в исключении недопустимых событий	**Участие руководства**	**Формальное участие руководства** в утверждении стратегий и планов ИБ, в заседаниях коллегиального органа по направлению ИБ
Верификация сценариев, понятных бизнесу, и учет особенностей каждой компании и ее инфраструктуры	 **Управление рисками**	**Основа — ограниченная статистика** инцидентов, влияющая на вероятности реализации угроз и их потенциальный ущерб
Практическая проверка возможностей противодействия кибератакам и исключение недопустимых событий в формате кибериспытаний разного уровня сложности	 **Контроль результатов**	**Классические аудиты** информационной безопасности (преимущественно без проверки работоспособности мер защиты)

Сравнение подходов. Процессы

Результативная КБ		Классическая ИБ
Концентрация усилий на мониторинге целевых активов и безопасной конфигурации (харденинга) компонентов инфраструктуры	 Мониторинг	**Стремление к полному покрытию активов** средствами мониторинга и защиты
Понимание целей атакующего и атрибуция атак для адекватного и эффективного реагирования **Предотвращение** недопустимых событий с последующей автоматизацией рутинных процедур	 Реагирование	**Отсутствие четкого представления о целях атаки** и, как следствие, увеличение трудозатрат на реагирование **Обработка** инцидентов и реагирование по предзаготовленным скриптам (плейбукам)
Отработка практических навыков команды защиты на киберполигоне, а также выявление и устранение уязвимых мест в инфраструктуре и слепых зон мониторинга	 Обучение и тестирование	**Настольное тестирование** планов реагирования и обработки инцидентов, направленное на их актуализацию

Сравнение подходов. Процессы

Результативная КБ

Постоянная инвентаризация активов и их классификация

с учетом недопустимых для бизнеса событий и реальных способов развития кибератаки

Управление активами

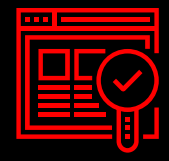
Классическая ИБ

Периодическая инвентаризация активов и их классификация

по принципу «конфиденциальность, целостность, доступность»

Приоритизация уязвимостей на основе информации о **возможных последствиях их эксплуатации и данных о недопустимых событиях в связке с целевыми и ключевыми системами**

Автоматизированный **контроль трендовых уязвимостей** и проверка наличия эксплойта, PoC



Управление активами

Приоритизация уязвимостей на основе **CVSS и качественной экспертной оценки значимости актива**

Рутинный **анализ уязвимостей,** получаемых от вендоров и из экспертного сообщества

Классический подход к построению SOC vs ЦПК

Классический подход к построению системы кибербезопасности неэффективен в стремительно меняющихся условиях

- Проектирование систем и разработка документации отнимает много времени, объем документации зачастую избыточный
- Пока длится проектирование, инфраструктура претерпевает значительные изменения, адаптировать проект под изменения среды затруднительно
- Внедряемые средства защищают все ресурсы без фокуса на самом главном
- Как правило, эффект от проекта ощутим только через год после старта, а полноценный результат виден заказчику только в конце проекта
- Сам факт внедрения средств защиты считается результатом, который обеспечивает надлежащую безопасность

Результативная кибербезопасность

1

Целеполагание

- Определение НС
- Декомпозиция НС
- Описание ландшафта ИТ, ИБ
- Определение условий, ограничений
- Формирование бизнес-требований

Цель определена и формализована

2

Целеполагание

- Харденинг (ИТ 2.0)
- Построение ЦПК
- Применение внешних сервисов (MSSP)
- Использование существующих решений

Наступление недопустимых событий невозможно

3

Целеполагание

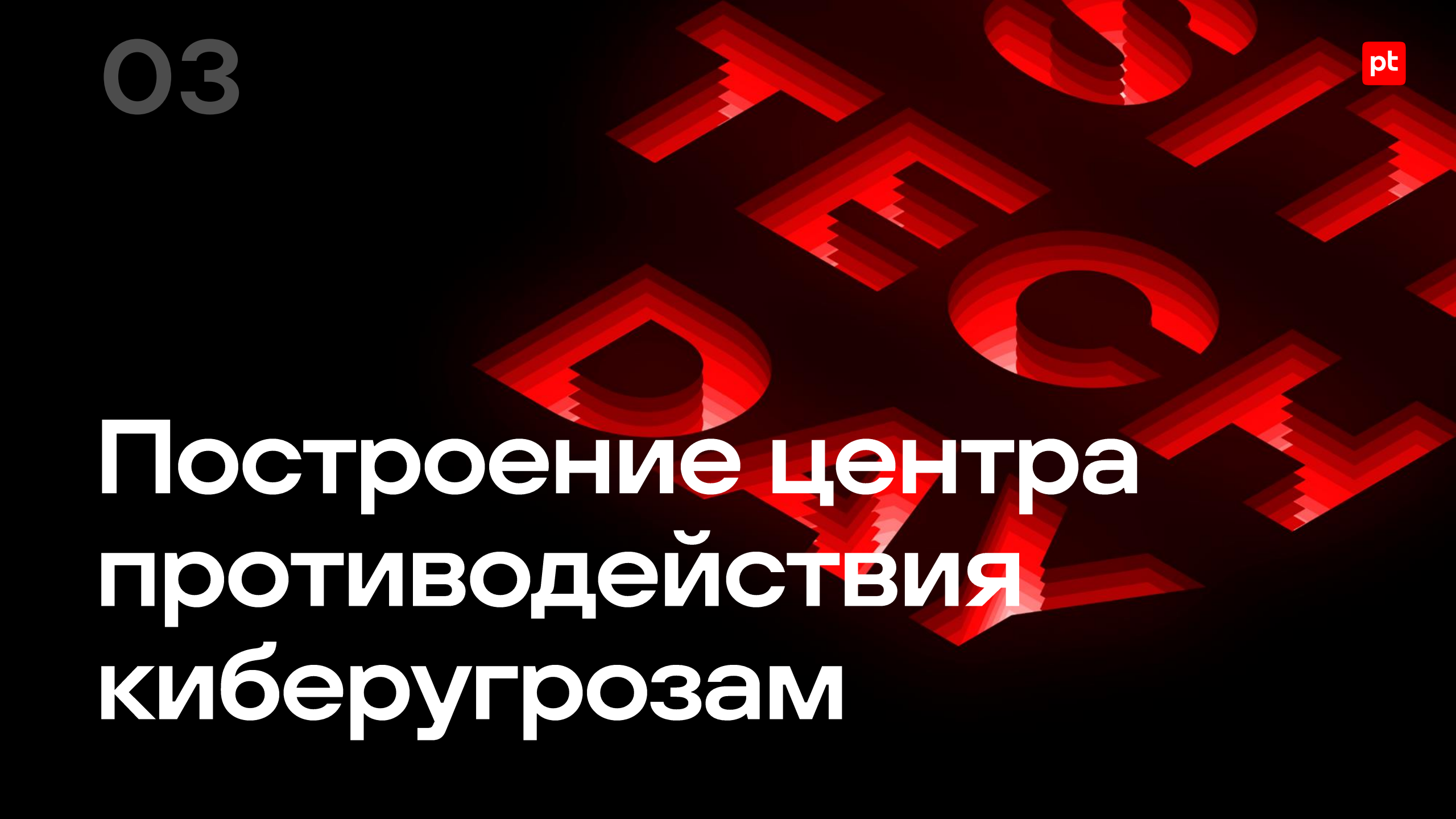
- Проведение внешних независимых кибериспытаний
- Регулярное участие в кибериспытаниях (bug bounty)

Достигнут значимый для бизнеса результат

Кибертрансформация

Гарантия результата

03



Построение центра противодействия киберугрозам

Что такое ЦПК

Центр противодействия киберугрозам (ЦПК)

Это выделенная структура, которая с помощью технологий, процессов и экспертов обеспечивает невозможность наступления **недопустимых для организации событий**

Внедренные операционные, аналитические, технологические процессы и соответствующие регламенты работ специалистов ЦПК

Средства защиты (для мониторинга, расследования инцидентов и т. п.)

Проверка качества ЦПК и невозможности реализации недопустимых событий

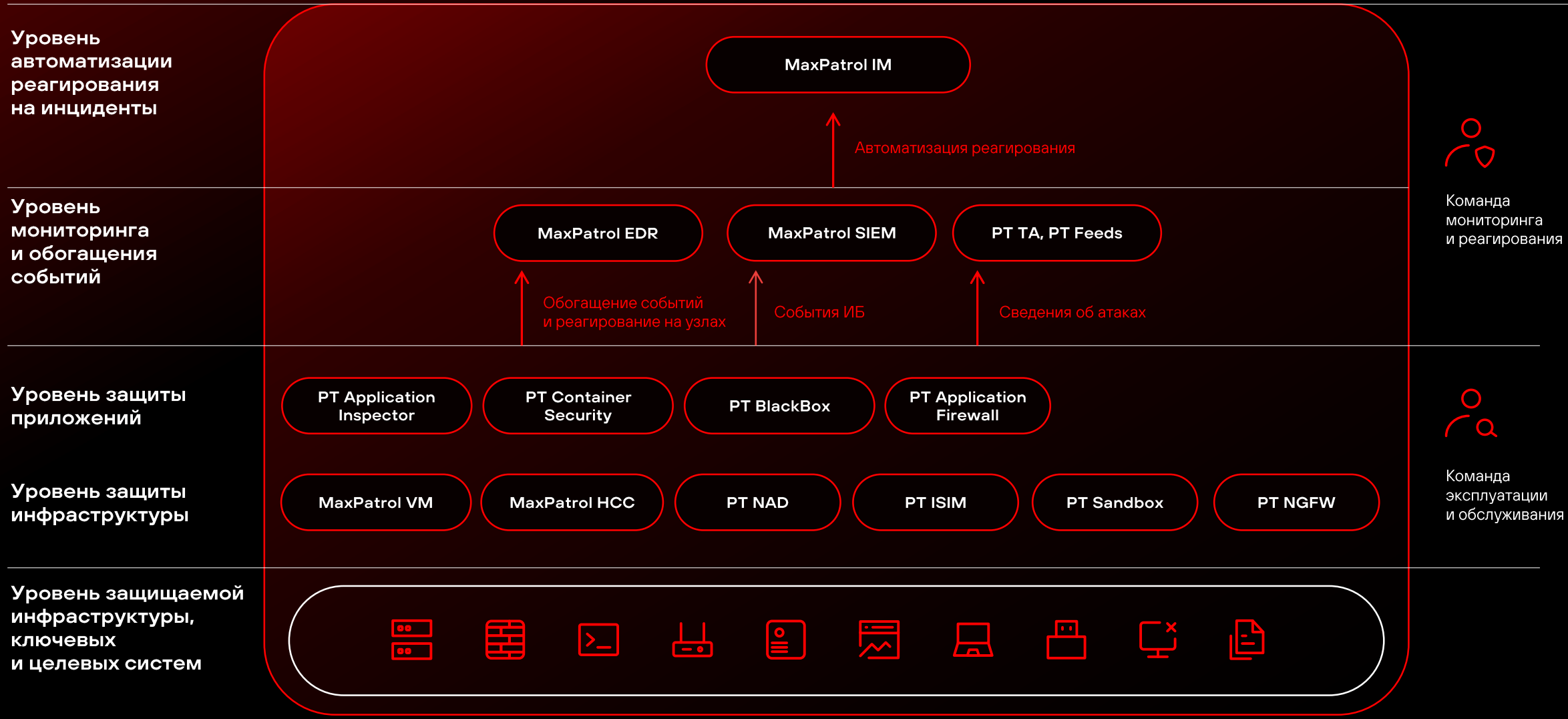
Специалисты, имеющие необходимые знания и опыт и постоянно повышающие квалификацию на кибериспытаниях (возможно привлечение экспертной поддержки Positive Technologies)

Результативный подход к построению ЦПК

Мы предлагаем результативный подход к трансформации кибербезопасности

- Для внедрения требуется минимальный объем документации
- Итерационный характер внедрения позволяет учесть изменения в инфраструктуре
- Фокус защиты направлен на целевые системы и связанные с ними недопустимые события
- Эффект становится виден сразу и усиливается ежегодно
- Выводы об эффективности внедренных средств защиты подтверждаются в ходе практических испытаний

Архитектура ЦПК



04

Вперед — к автопилоту в ИБ

Сколько специалистов по ИБ нужно для мониторинга

3000 активов, 10 000 EPS

Смотрит только наиболее критически опасные инциденты

Смотрят все инциденты

Смотрят все срабатывания СЗИ

Метапродукты

Решения Positive Technologies, которые работают поверх других продуктов PT и позволяют полностью выстроить мониторинг и реагирование в модели результативной кибербезопасности без участия (или с минимальным участием) человека

Архитектура метапродуктов

Ключевой результат

Злоумышленник не может реализовать недопустимые события

Результат 1

Формируем и контролируем выполнение требований к инфраструктуре, при которых злоумышленник не может достичь целевых активов менее чем за N шагов

MaxPatrol Carbon

← До атаки

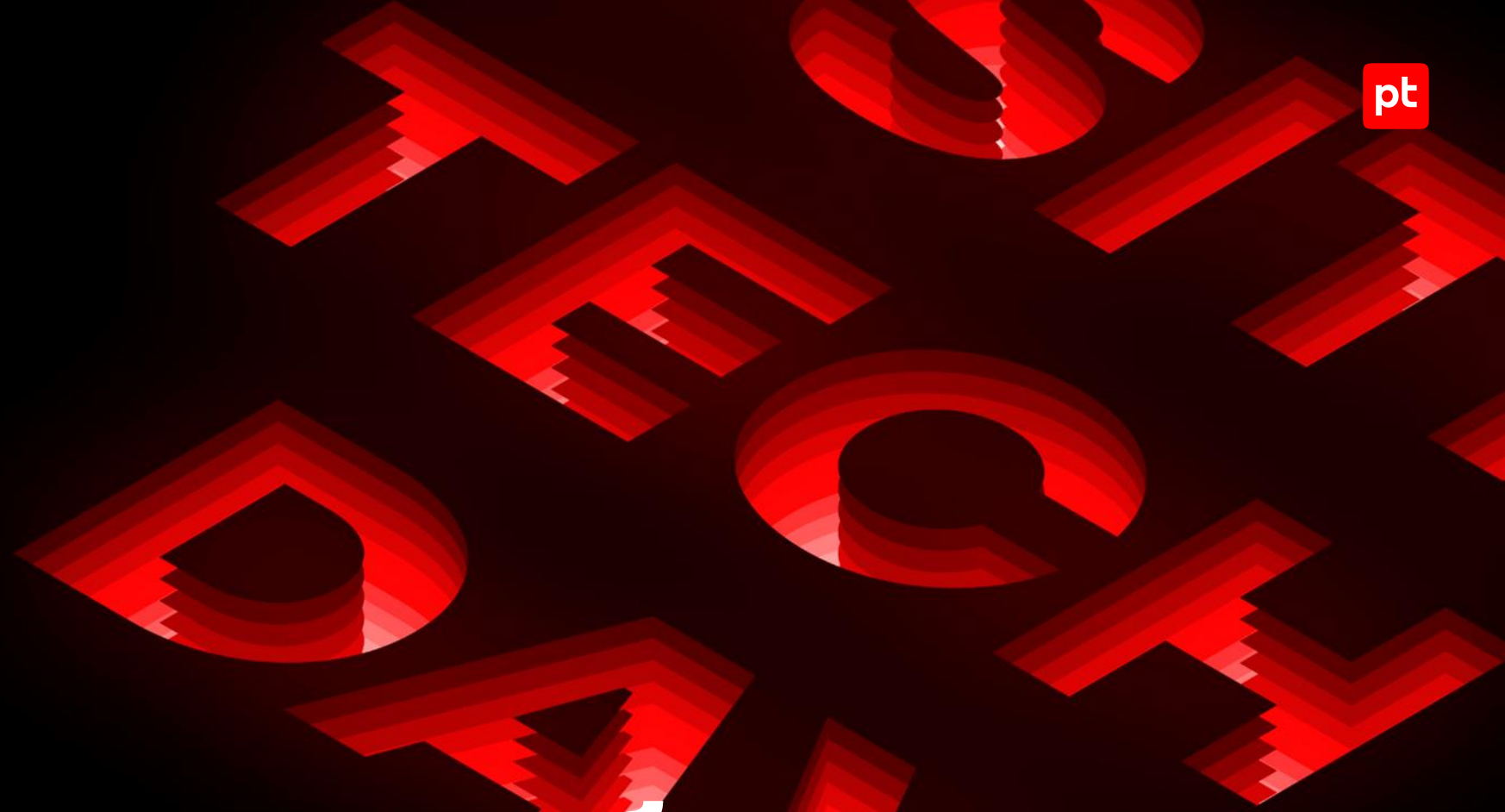
Результат 2

Обнаруживаем и останавливаем злоумышленника до реализации недопустимых событий

MaxPatrol O2

Во время атаки →

05



Поверить в себя и проверить себя...

Киберполигон и bug bounty

Когда киберполигон нужен

- Практическая оценка защищенности организации и отрасли (в том числе подтверждение безопасности системы для внешних контрагентов)
- Кибериспытания: обучение на большом потоке инцидентов, отладка взаимодействия команд
- Пилотирование средств защиты и мониторинга
- Все это — без ущерба для продуктивных систем

Когда он на самом деле работает

- Реальные бизнес-процессы, инфраструктура и СЗИ
- Актуальные угрозы и недопустимые события
- Главное — живые атаки квалифицированных этичных хакеров

Спасибо!