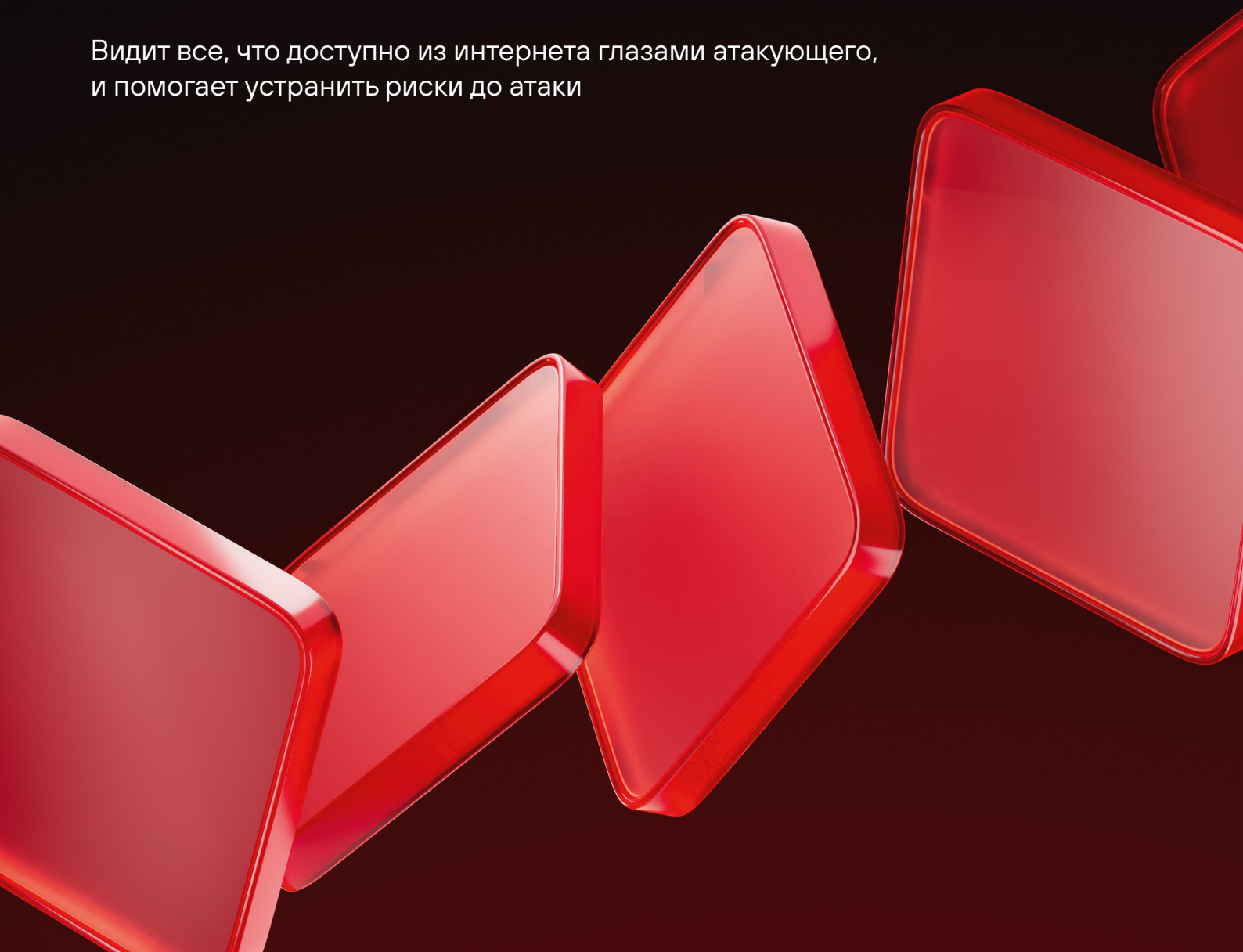




Умный радар внешнего периметра

Видит все, что доступно из интернета глазами атакующего,
и помогает устранить риски до атаки



Цифровые активы, с которыми клиенты, сотрудники или партнеры взаимодействуют, а также активы, доступные из интернета, — серверы, облачные сервисы или IoT-устройства, забытые лендинги и хостинги — все они и формируют вашу внешнюю поверхность атаки.

Классические сканеры уязвимостей и ежегодные пентесты показывают срез безопасности только в моменте. Тем временем, инфраструктура и ландшафт угроз меняются ежедневно.

Какие активы могут подвергнуть компанию рискам



Открытые серверы



Уязвимое стороннее ПО



Неверно настроенные облачные сервисы/службы

Знаете ли вы, что

1 из 3 атак*

реализуются через эксплуатацию уязвимостей на периметре

7 из 10 организаций**

подвергались атакам, которые начинались с использования теневых активов

О решении PT EASM

PT EASM — решение, которое обеспечивает постоянный контроль внешнего периметра: автоматическое обнаружение всех активов, доступных из внешних сетей, анализ уязвимостей внешних активов и ошибок конфигурации, а также приоритизация тех уязвимостей, которые способны привести к компрометации критичных систем.

PT EASM основан на платформе СКИПА разработчика ПО CyberOK, доказавшей свою эффективность в управлении безопасностью цифрового периметра на проектах национального уровня.

*Исследование Positive Technologies «Как организации подходят к процессу управления активами»

**Отчет Enterprise Strategy Group (ESG), Security Hygiene and Posture Management Report

PT EASM обеспечивает



Полную видимость внешних активов (Asset Discovery)

Находит теневую инфраструктуру (Shadow IT), забытые тестовые стенды и неучтенные ресурсы раньше, чем это сделают злоумышленники



Приоритизацию и оценку рисков

Оцениваем уязвимости не просто по CVSS, а по реальной вероятности их эксплуатации в Рунете и мире — исправляйте только то, что критично



Снижение стоимости ошибки

Контроль устранения уязвимостей не дает закрытым внешним «дырам» появиться вновь при следующем релизе или обновлении

Ключевые возможности

ТЕХНОЛОГИЯ

ЧТО ВЫ ПОЛУЧАЕТЕ

Глубокая киберразведка и инвентаризация
Система автоматически, без участия заказчика, собирает данные обо всех внешних активах. Используем собственную базу СКИПА, passive DNS, реестр Whois

Актуальную карту внешнего периметра, включающую домены, поддомены, IP, порты, сервисы

Активный анализ и поиск уязвимостей на внешнем периметре
Выявляем недостатки конфигураций и известные уязвимости на всех найденных ресурсах. Наиболее критичные системы профилируются для углубленного анализа

Автоматизированное выявление брешей без влияния на работоспособность бизнес-систем

Обогащение, скоринг и верификация
Все найденные результаты агрегируются и проходят проверку. Это исключает ложные срабатывания (False Positives)

Экспертный контроль — аналитики верифицируют данные автоматикой. Для критичных ресурсов подключаются эксперты, проводящие ручные проверки сложной бизнес-логики, которые недоступны сканерам

Отчетность и контроль устранения
Мы не просто отдаем многостраничный отчет, а консультируем команду заказчика по каждой угрозе

Отслеживание динамики исправлений и оценку реальной эффективности процессов управления уязвимостями (Vulnerability Management) на внешнем периметре компании

Почему PT EASM

Динамическая база знаний

Учитываем не только новые CVE, но и наличие реальных эксплойтов под них прямо сейчас



Лучшее от двух миров

Гибридный подход — скорость и покрытие автоматизированной ИИ-платформы СКИПА, дополненные экспертизой и креативностью этичных хакеров



Готовность к масштабированию

Процесс легко адаптируется под рост ИТ-инфраструктуры заказчика



Защитите ваш периметр и находите теневые активы в реальном времени

