Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT
INFINITY SOC

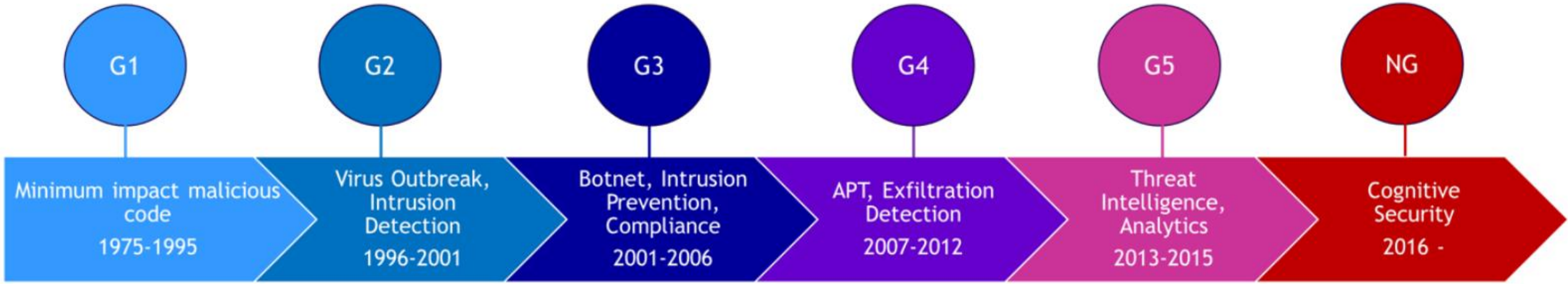
INFINITY SOC

TRUE XDR

Турков Никита | Security Engineer
nikitat@checkpoint.com

Сергей Забула | Channel SE Team Lead
szabula@checkpoint.com

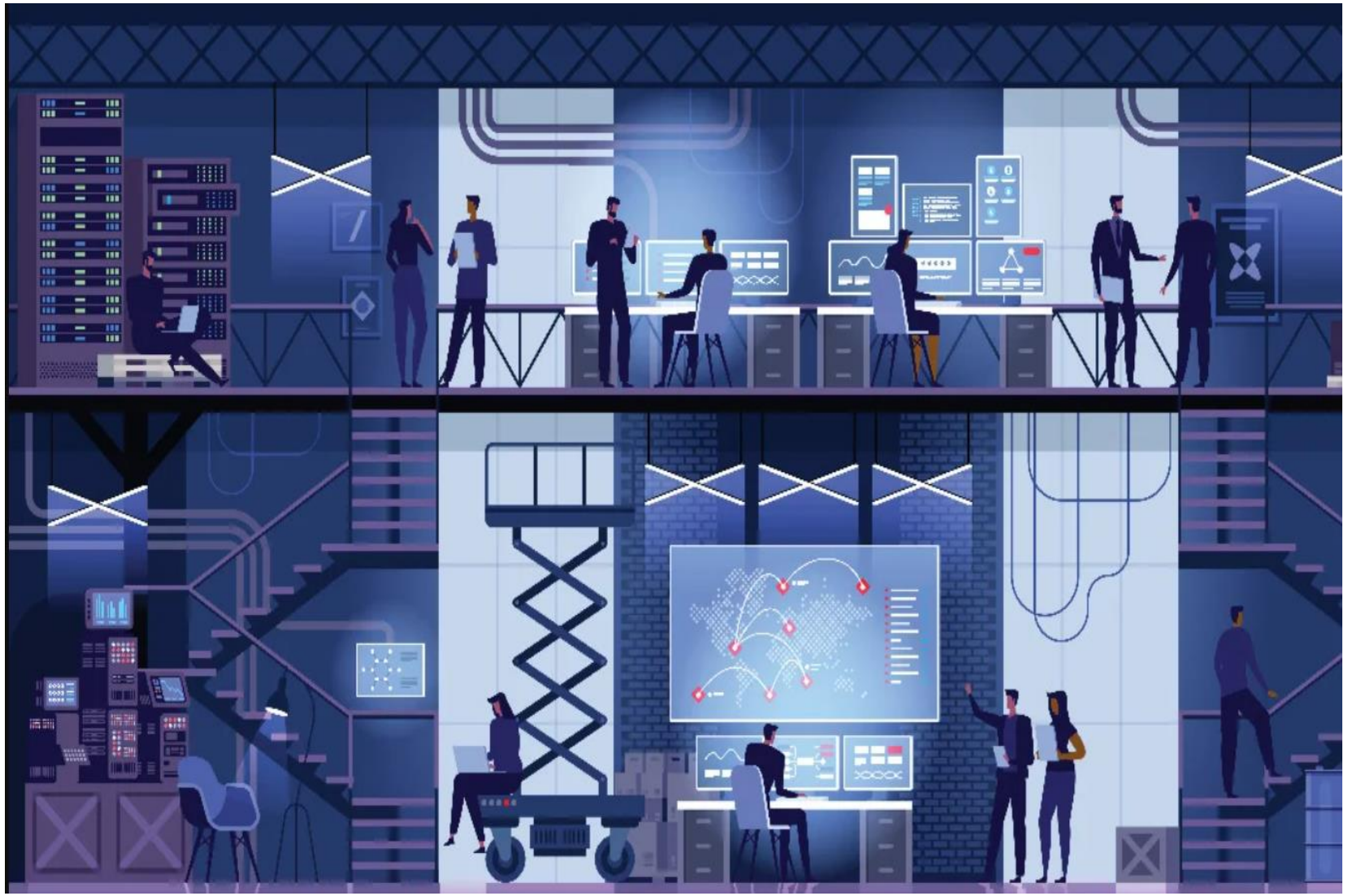
НЕМНОГО ИСТОРИИ



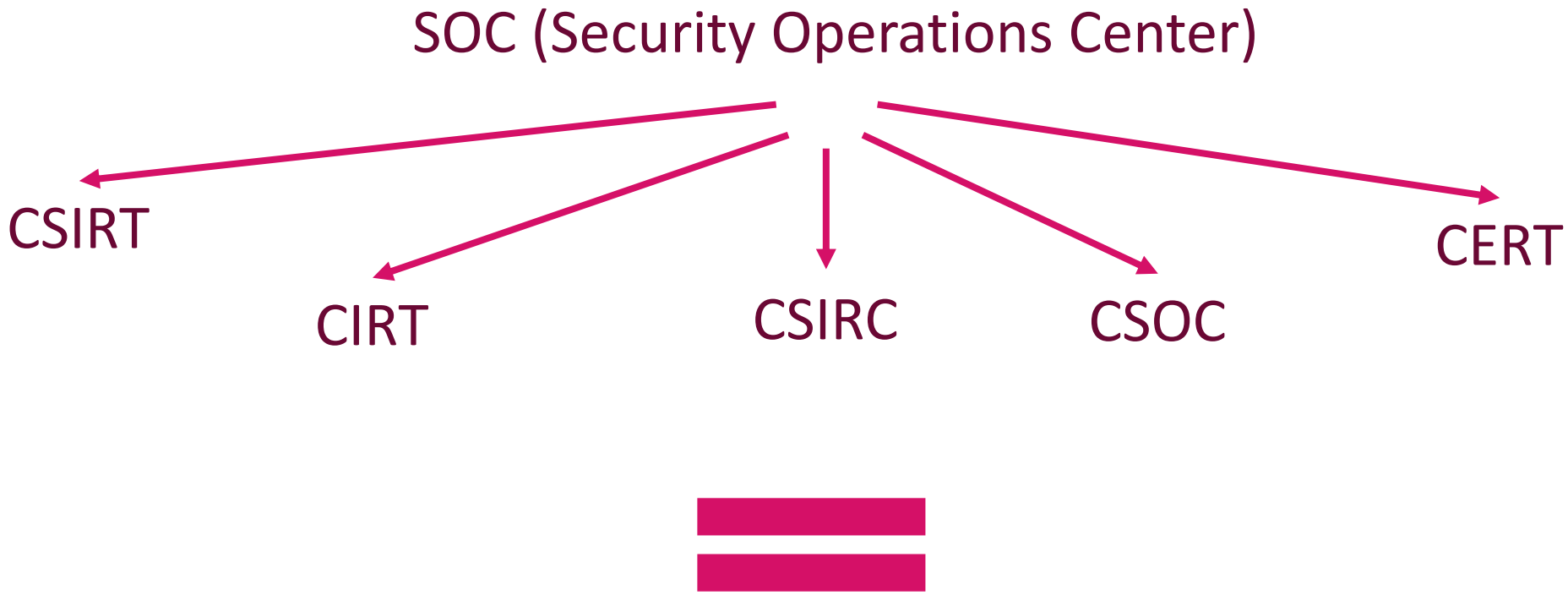
*Концепция создания SOC следующего поколения – Anti-malware

ФАКТОРЫ

1. Персонал
2. Эксперты
3. Автоматизация
4. Интеграция
5. False / Positive



ТЕРМИНОЛОГИЯ



КОМАНДА, ОБНАРУЖЕНИЕ, АНАЛИЗ, РЕАКЦИЯ, ПРЕДОТВРАЩЕНИЕ, ЛОГИРОВАНИЕ

КЕЙС ПРО SOC

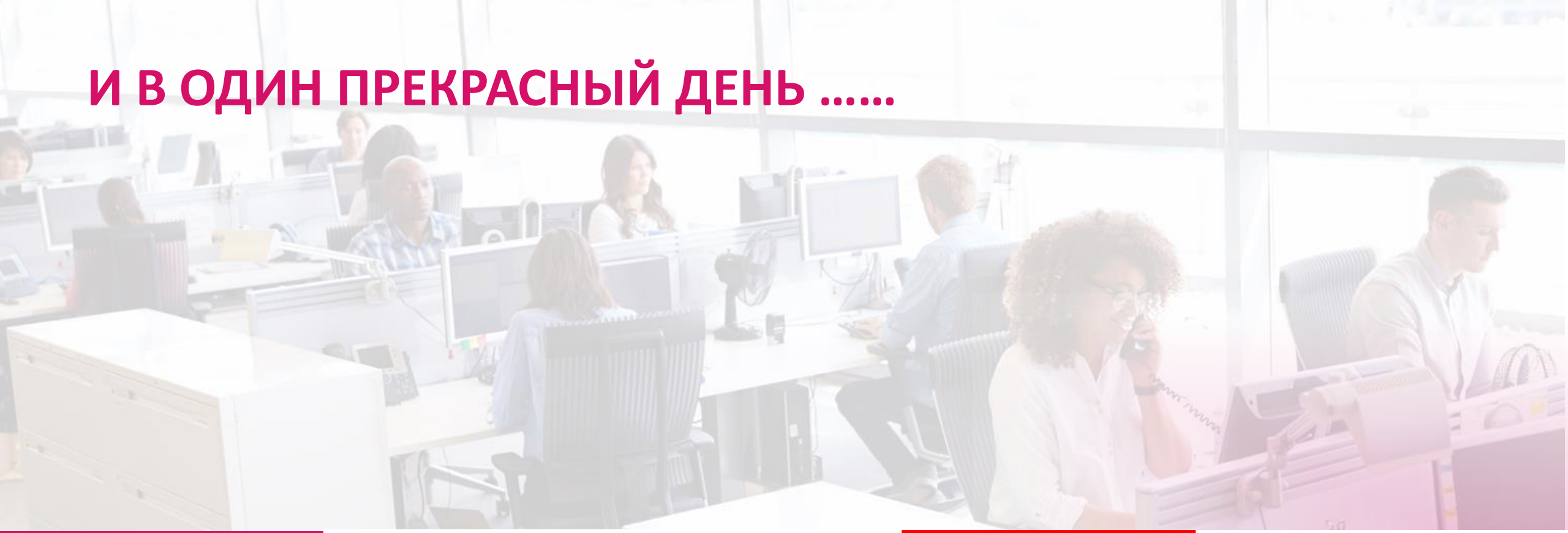
Европейский банк

5,000
сотрудников

€1.1 млрд
доход

2 сотрудника SOC
Рабочие часы: 8:00- 17:00

И В ОДИН ПРЕКРАСНЫЙ ДЕНЬ ……



23 февраля **2020**

- Атака шифровальщика Ryuk
- 500 критических систем затронуты
- 3 филиала парализованы

Экстренный звонок »»

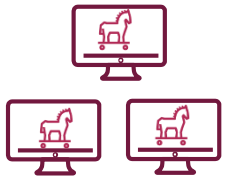
INCIDENT RESPONSE TEAM
CHECK POINT

КАК ЭТО МОГЛО ПРОИЗОЙТИ?

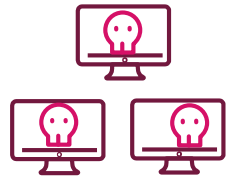
Анатомия атаки

INCIDENT RESPONSE TEAM
CHECK POINT

Фишинговая рассылка привела к заражению **Trickbot Trojan**



Trickbot горизонтальное распространение на 500 хостов



Злоумышленник использовал **Trickbot** для доставки **шифровальщика Ryuk**

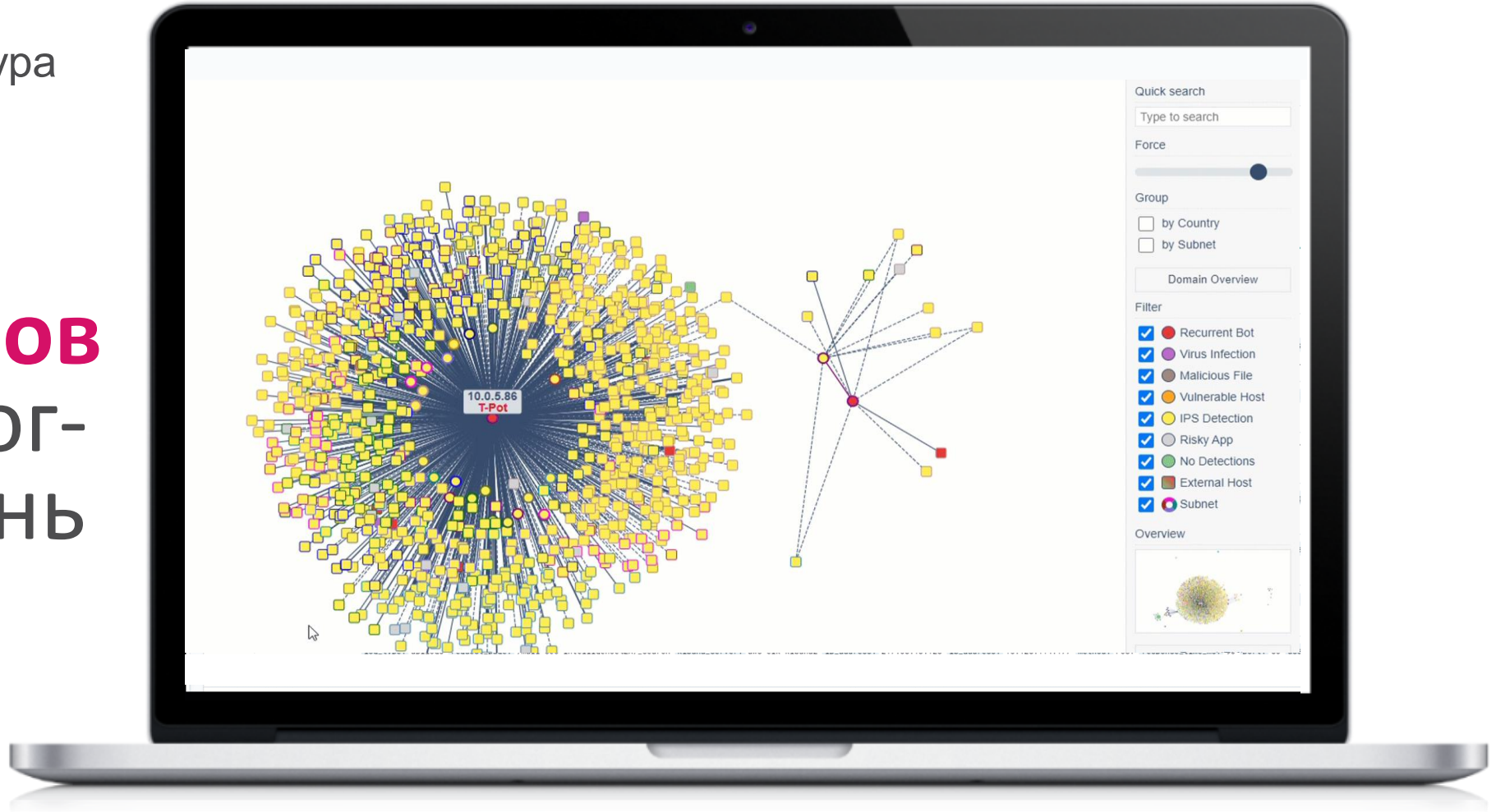
Окт 2019 — Ноя 2019 — Дек 2019 — Янв 2020 — Фев 2020

Работа SOC службы каждый день:
Ищем иголку в стоге сена

Типичная инфраструктура
среднего размера
2,000 пользователей

⬇

10 Миллионов
Записей в лог-файлах в день



CHECK POINT
INFINITY SOC

Добавляем уверенности SOC

99.9% ТОЧНОСТЬ

Обнаруживайте и останавливайте только реальные атаки, внутри и снаружи организации

Быстрое расследование

Самый продвинутый в индустрии threat intelligence

Минимум усилий

Простое внедрение и интеграция

ТОЧНОСТЬ

От миллионов записей – к реальным инцидентам

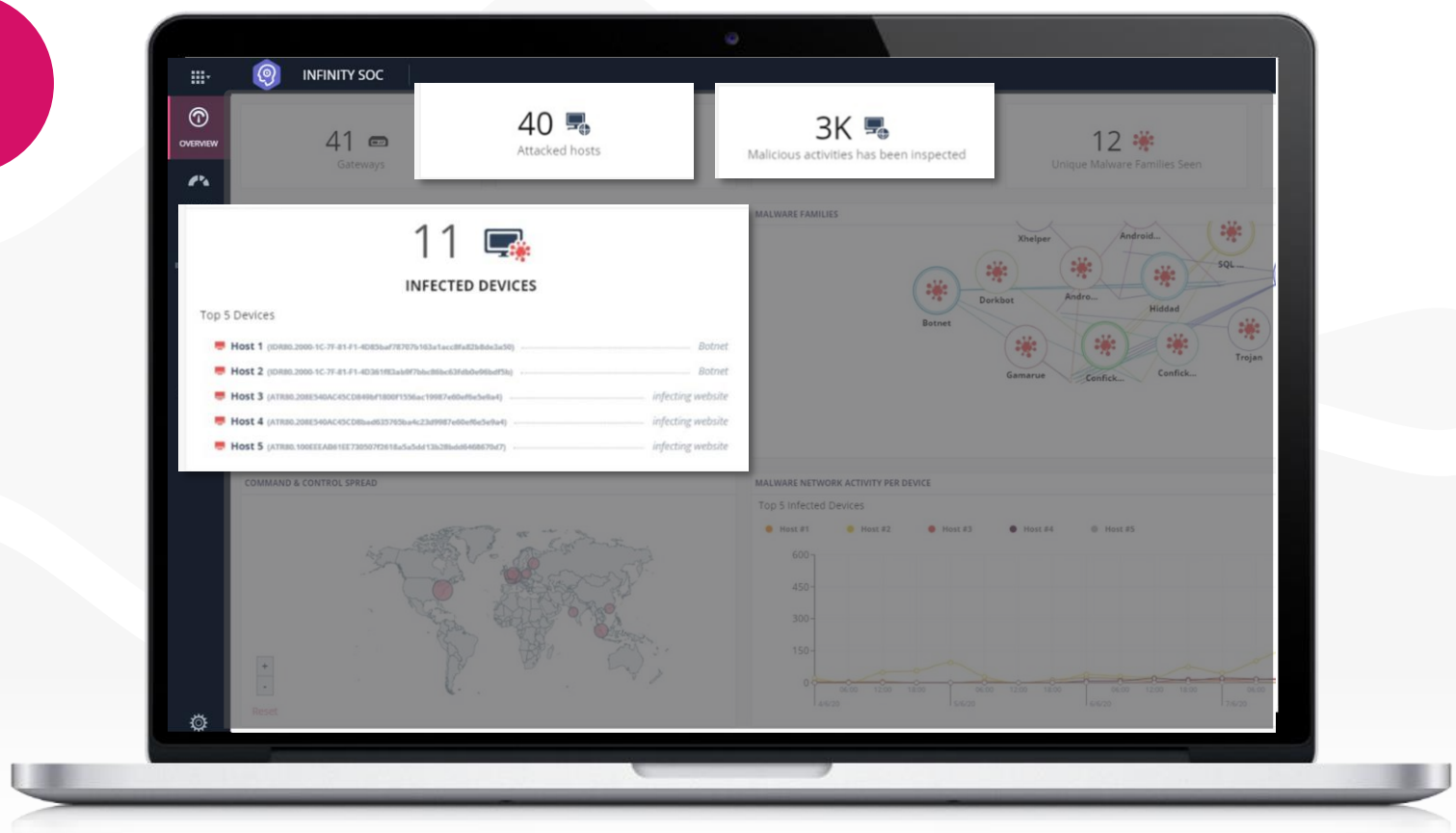
В среднем за неделю:

59,000,000
Записей в лог-файлах – рабочие станции, сеть, облака, мобильные устройства, Интернет вещей

3,000
Вредоносных активностей

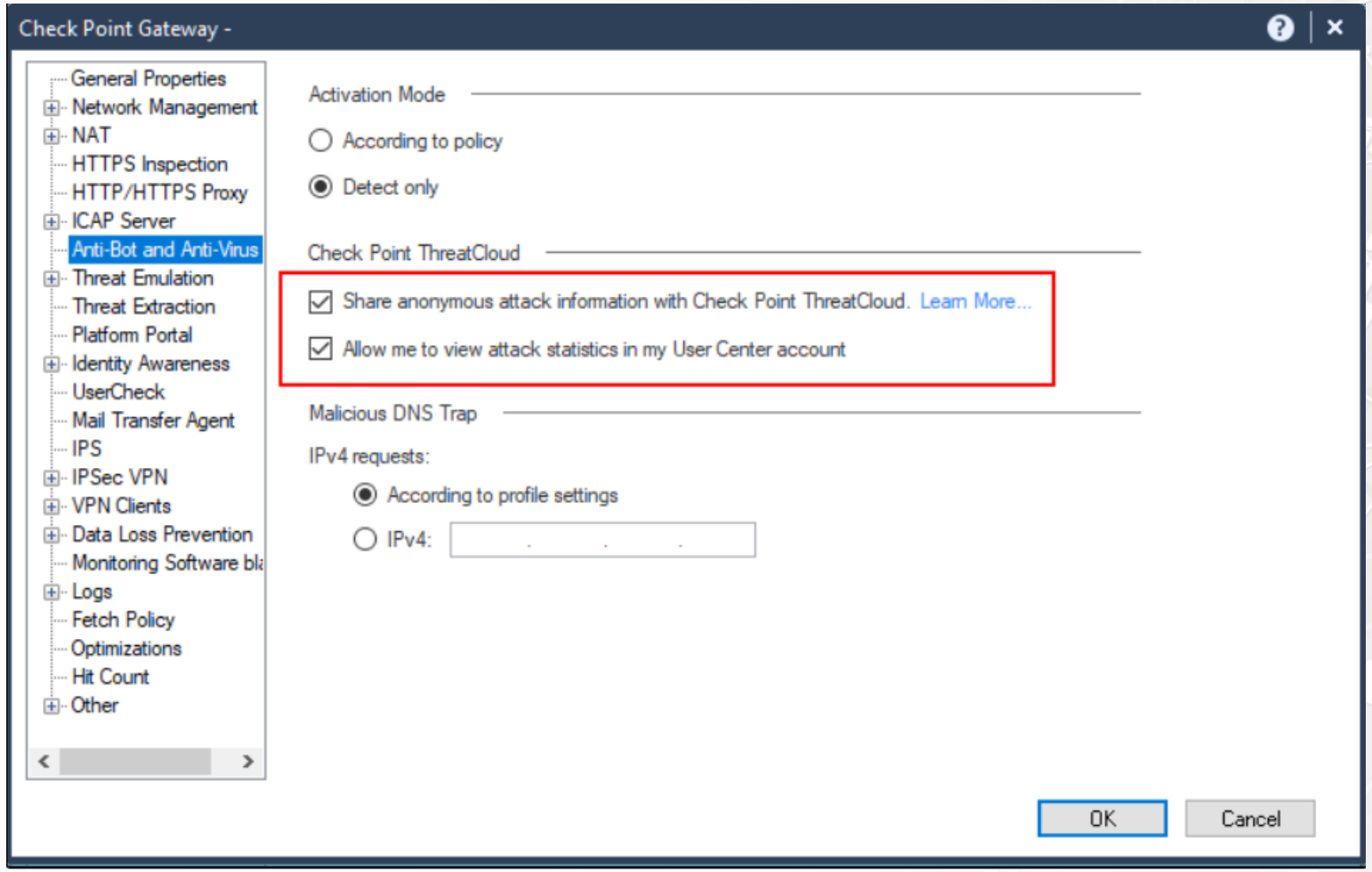
40
Затронутых хостов

11
Зараженных хостов

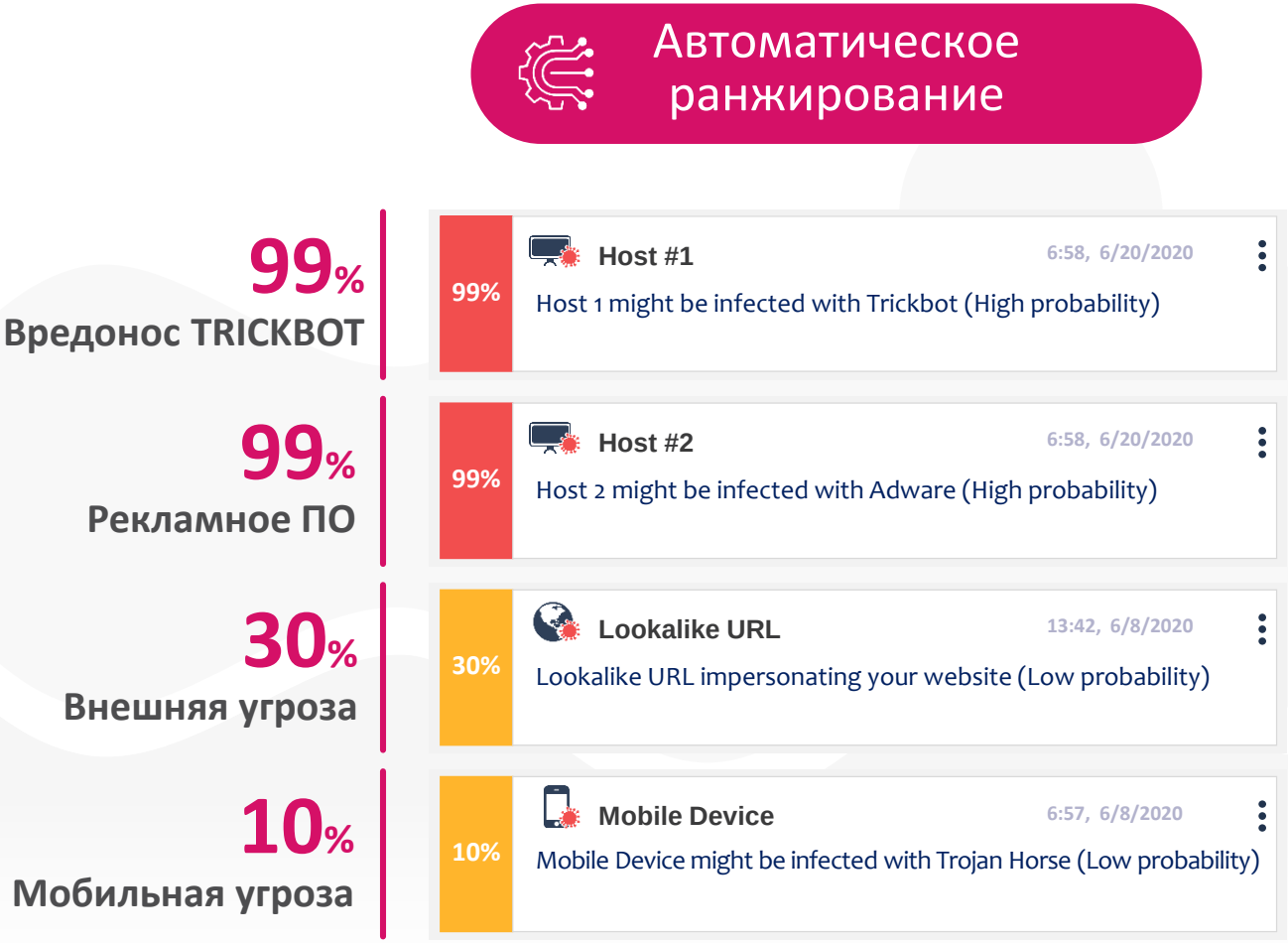


ТЯЖЕЛО ЛИ НАСТРОИТЬ?

NGFW + 2 опции +
инсталяция политики, всё!



Приоритезация важного
Реагируйте только на критичные события



Реакция
Минимизируйте последствия атаки с помощью восстановления одним кликом

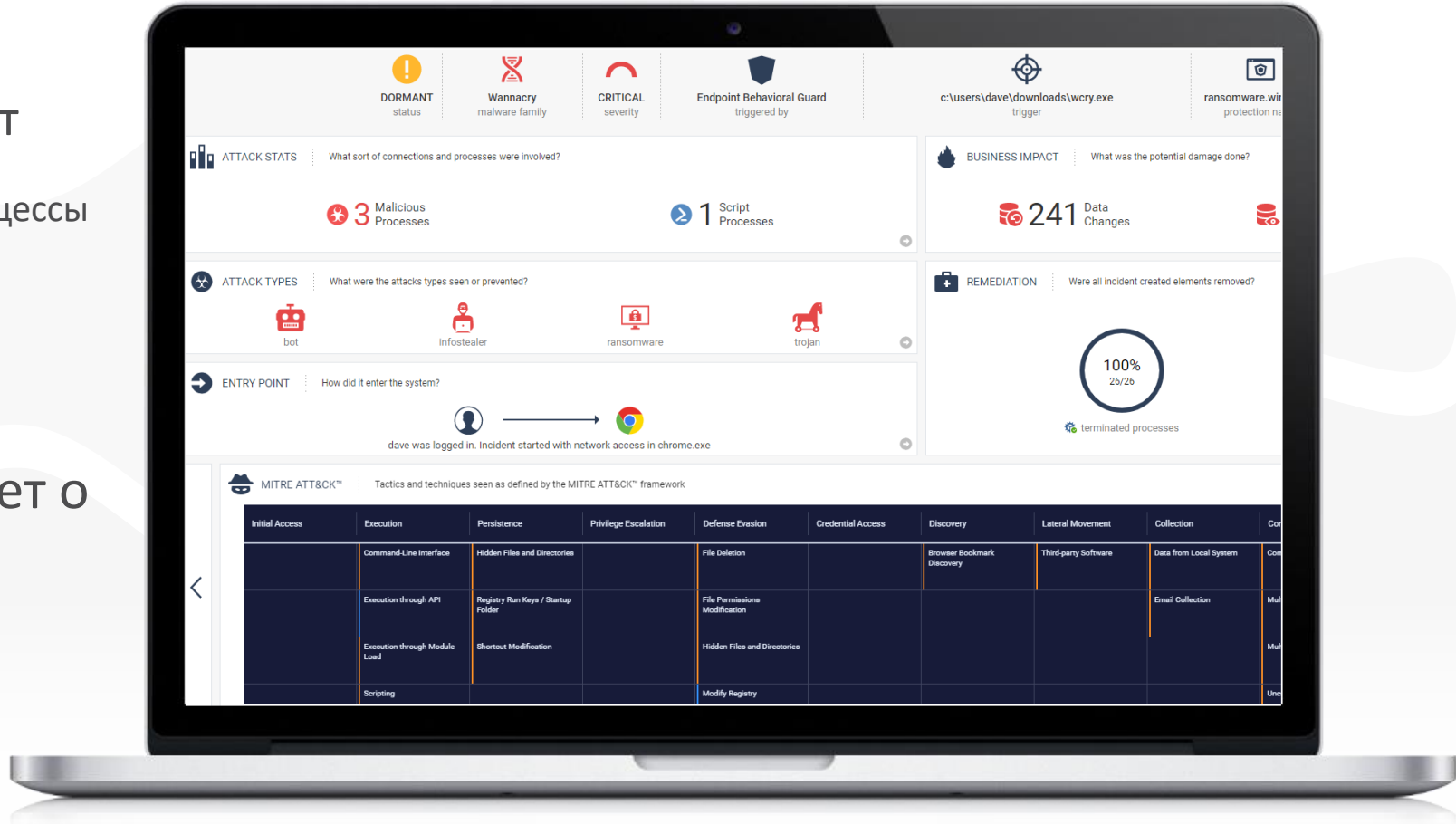
1 | Установите легковесный клиент на зараженный хост

Идентифицируйте и остановите процессы

Заблокируйте C&C коммуникации

Удалите вредоносные файлы

2 | Получите детальный отчет о форензике



Внешние угрозы

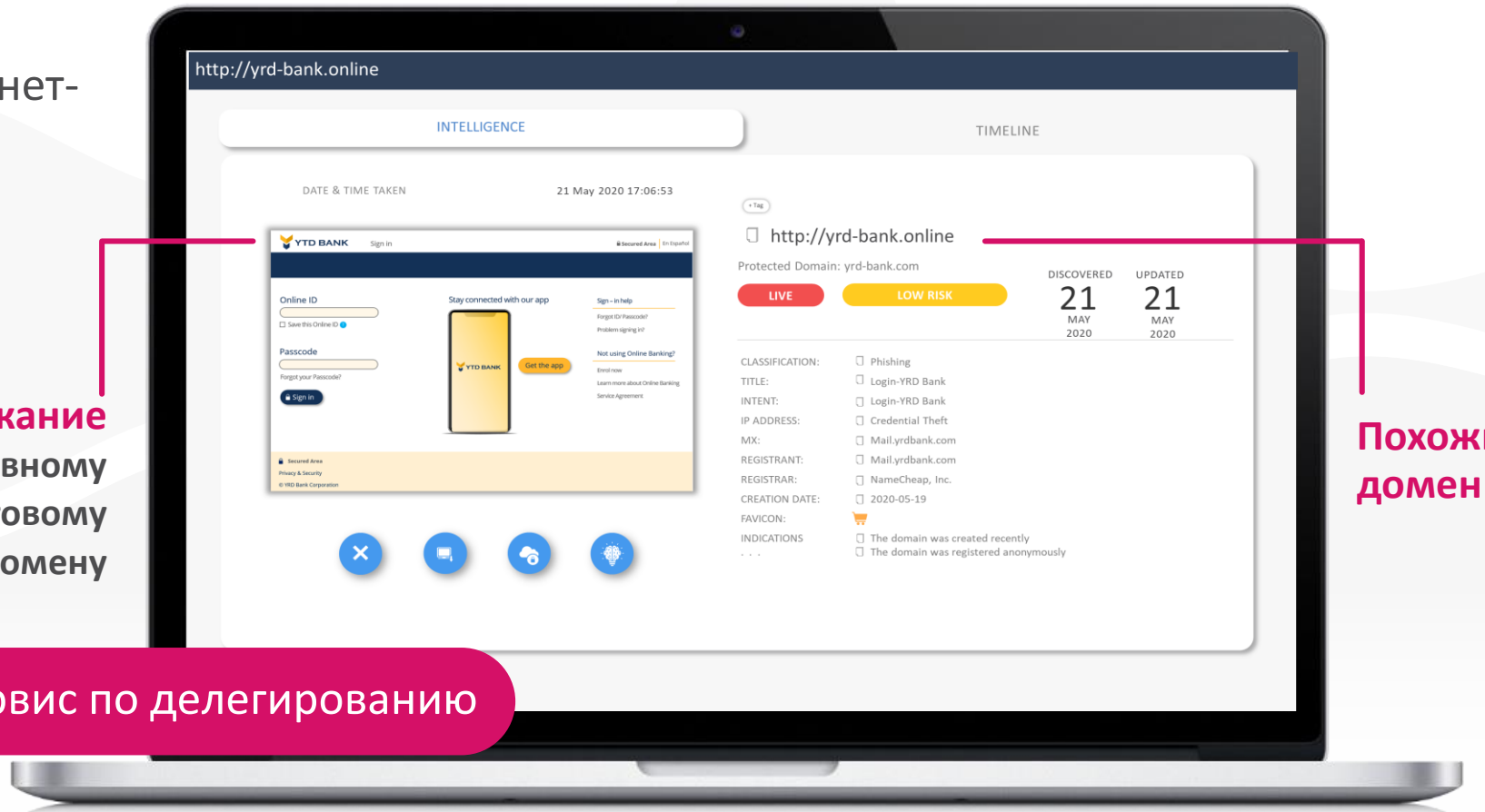
Предотвращайте фишинговые атаки на ваших сотрудников и заказчиков

Видим внешние угрозы

Благодаря анализу интернет-трафика в реальном времени

Подражание

Вашему корпоративному веб-сайту или почтовому домену



Похожий домен

Сервис по делегированию

Настоящий XDR:
Обнаруживайте скрытые атаки с точностью 99.9%

Анализ больших данных с помощью ThreatCloud

Анализ интернет-трафика в реальном времени

События с рабочих станций, сети, мобильных устройств, Интернета вещей

Искусственный интеллект для обнаружения вредоносной активности

Обогащаем данные с помощью продвинутого Threat intelligence

Сила ThreatCloud

2,000 угроз нулевого дня в день

150,000 подключенных сетей

13 миллионов файлов эмулируется в день

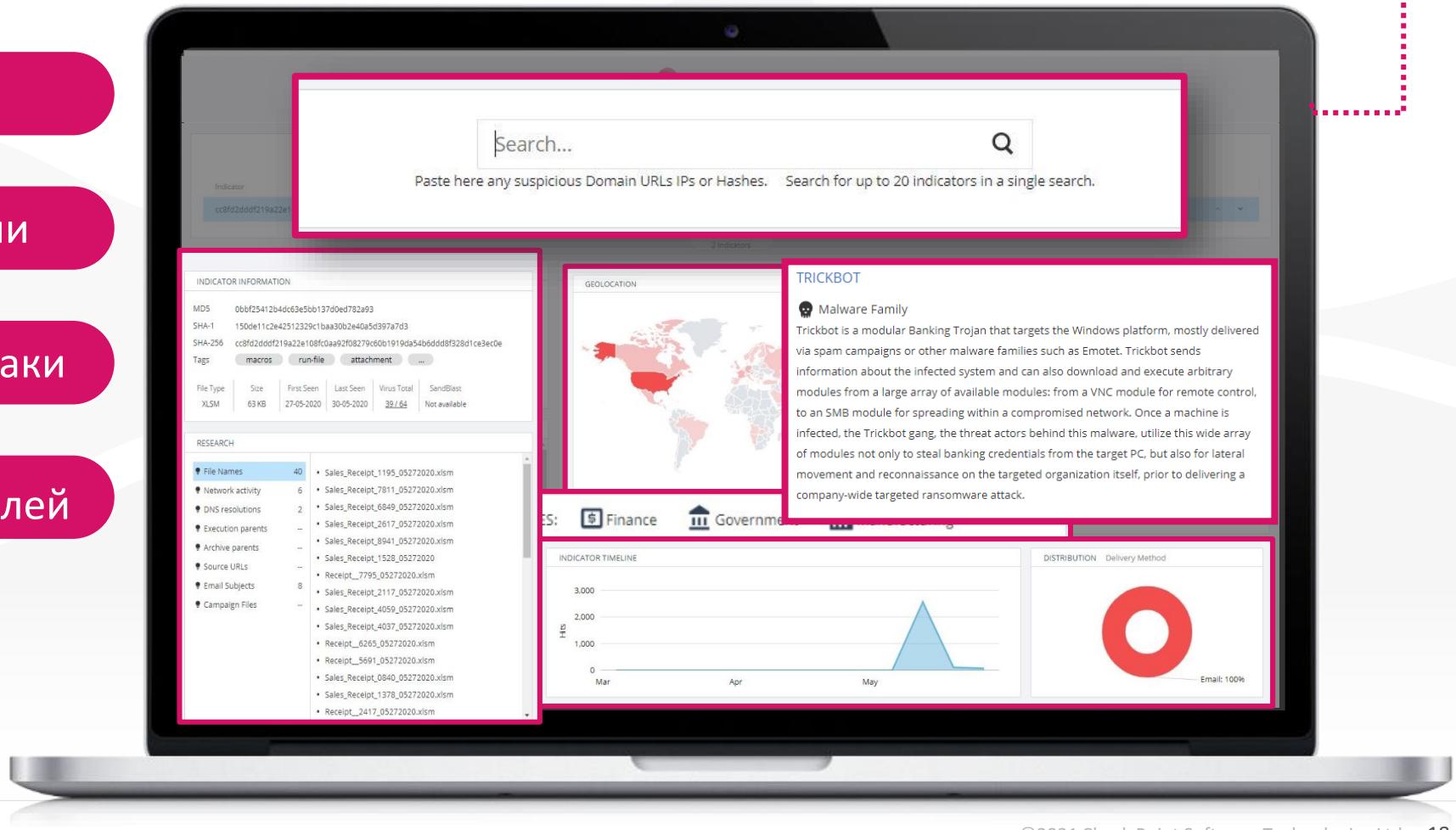
3 миллиарда Веб-сайтов и файлов обрабатывается в день

‘GOOGLE ПОИСК’ любого индикатора на портале

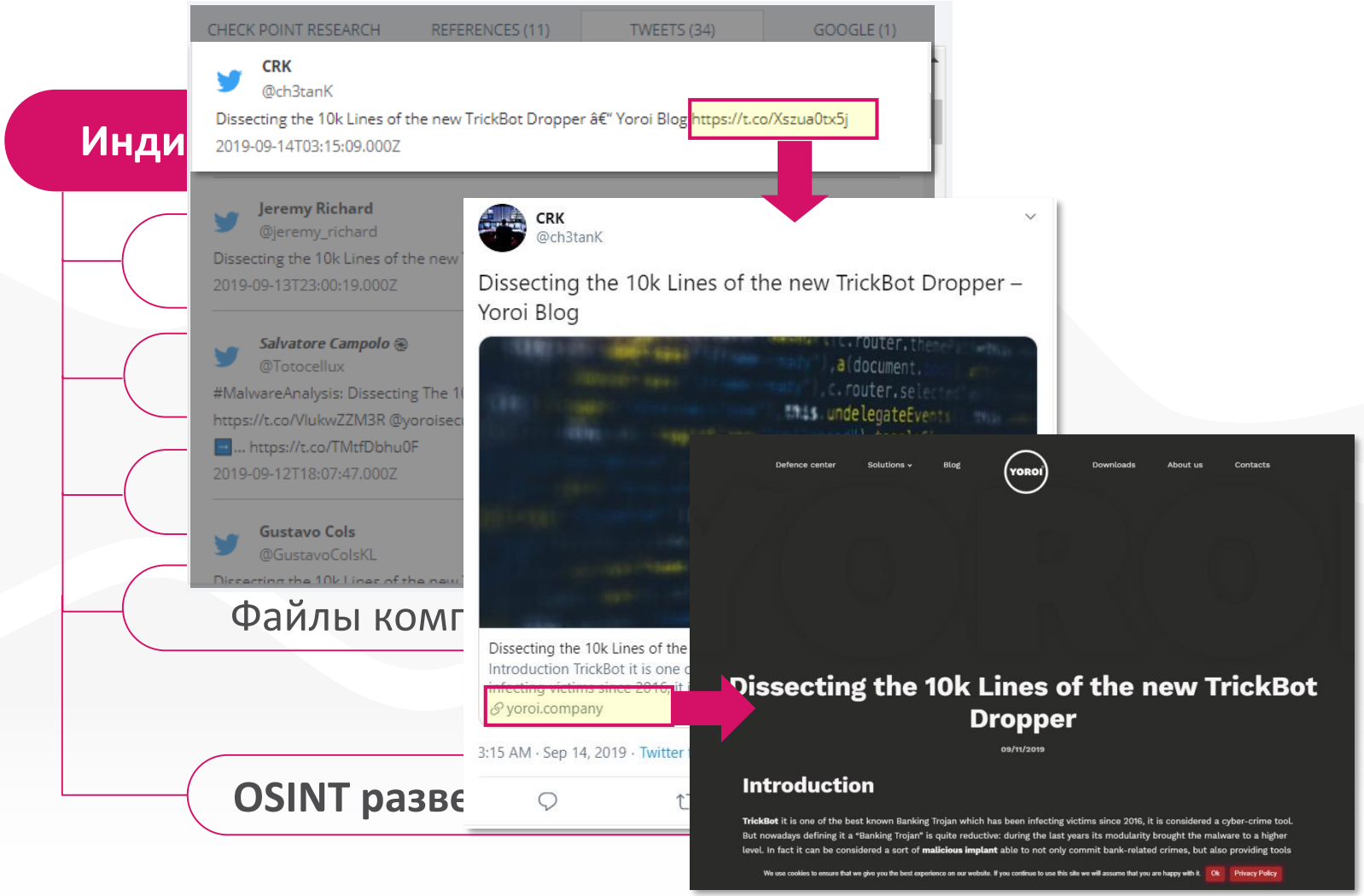
Получите быструю и предельно точную информацию

- География атаки
- Затронутые вертикали
- Данные по времени атаки
- Аналитика исследователей

И другое…



Аналитические данные
для глубокого расследования

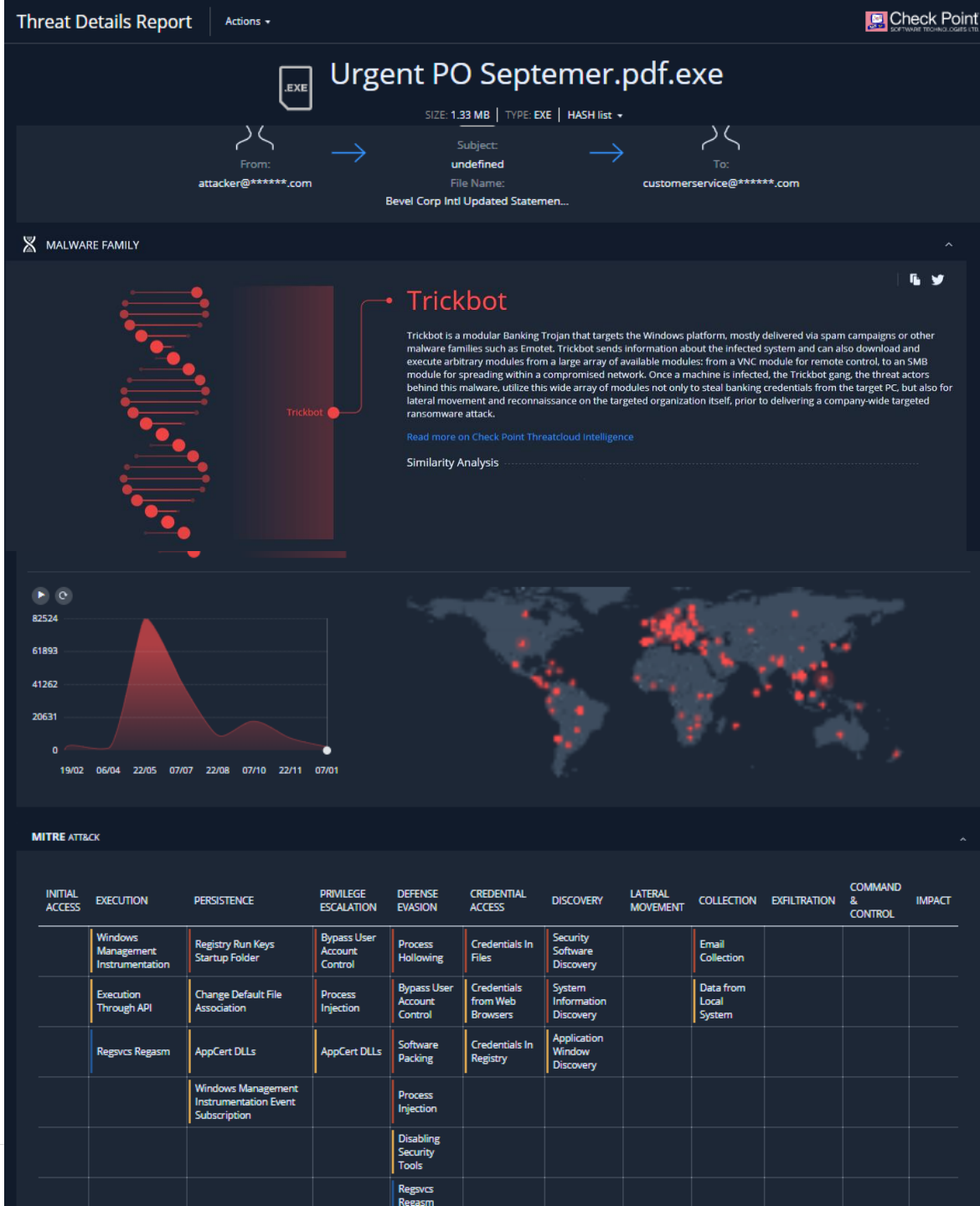


И многое другое…

Быстрая проверка подозрительного файла на вредоносное содержимое

С помощью сервиса SANDBLAST'S THREAT EMULATION

- Семейство вредоноса
- География
- MITRE ATT&CK матрица
- Видео эмуляции
- Файлы, которые были докачаны
- URL центров управления
- И другое!



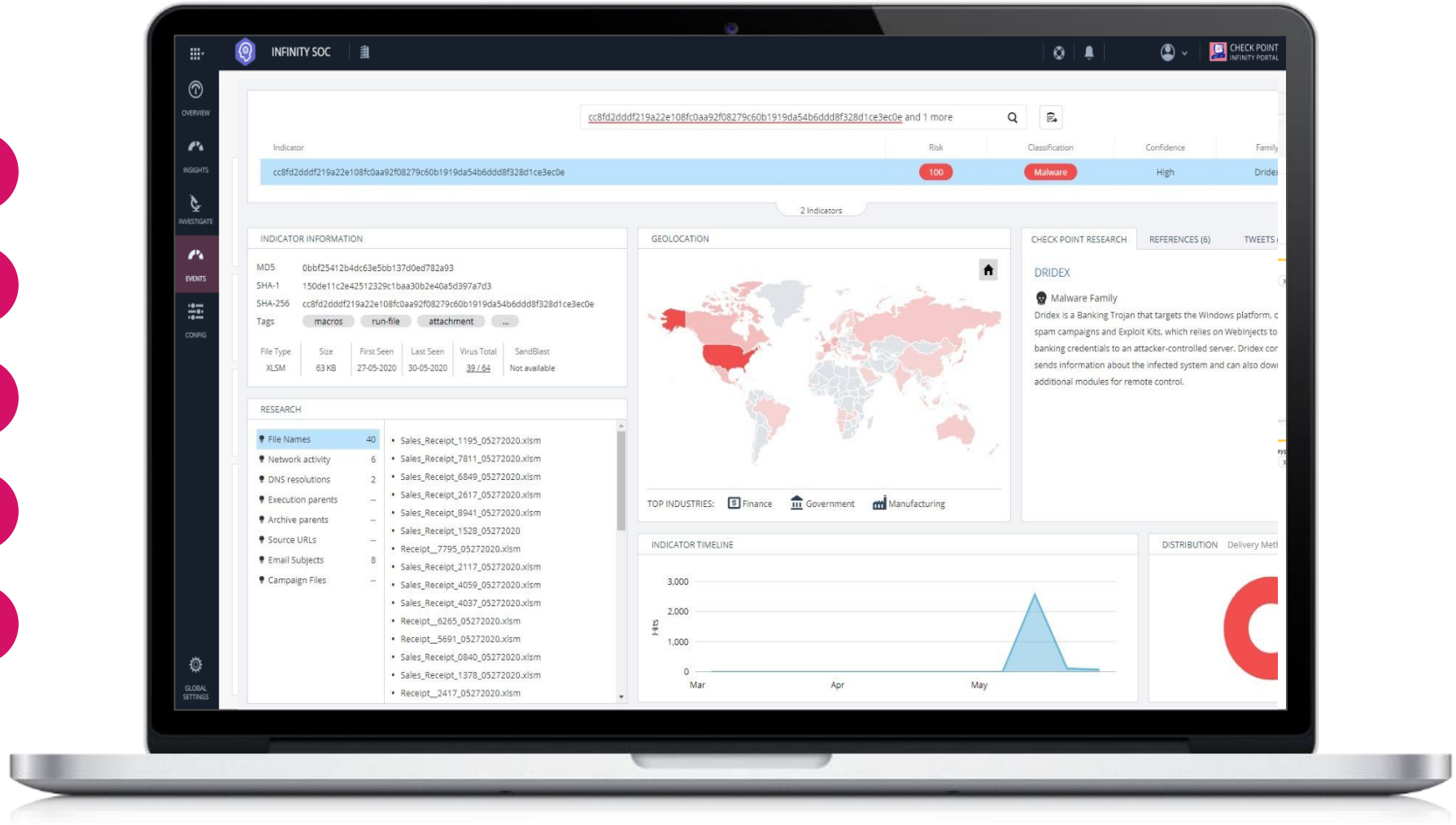
CHECK POINT
BREACH PREVENTION SYSTEMS 2.0
NSS LABS
RECOMMENDED
AUGUST 2019

Лучший CATCH RATE
по версии NSS LABS

Check Point
SOFTWARE TECHNOLOGIES

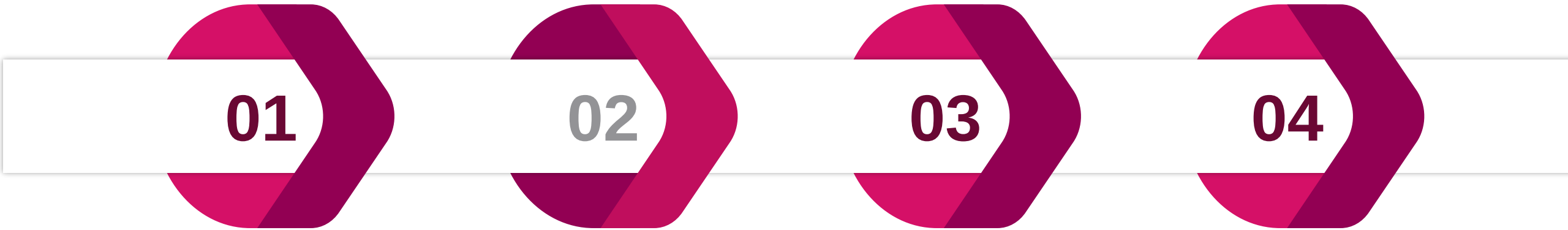
Упрощение и уменьшение стоимости владения с единой централизованной SOC платформой

- Внутренние угрозы
- Внешние угрозы
- Восстановление
- Расследование
- Управление



Можно начать пользоваться менее чем за 3 минуты

Легкое внедрение
Нет необходимости в дополнительных агентах



Зарегистрируйтесь на Infinity Portal

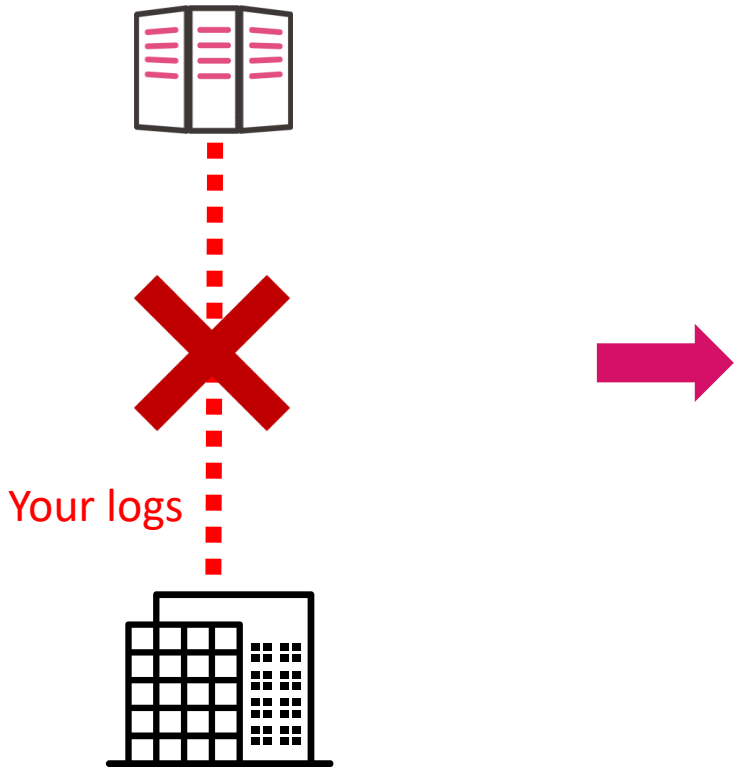
Выберите шлюзы
(если они уже есть)

Подключитесь к ThreatCloud

Начинайте

Приватность во главе угла

Ваши лог-файлы никуда не отправляются



Защита конфиденциальных данных

Нет затрат на хранение лог-файлов в облаке

Готовы протестировать?

В России:

Крупная страховая компания

200 филиалов, ЦОД
Отсутствие SOC, SIEM

Решение: Infinity SOC для старта!

Запросите **1:1 ДЕМО** с экспертом OCS или Check Point

Начните бесплатный **INFINITY SOC** триал

Больше информации:
www.checkpoint.com/products/Infinity-SOC

Check Point
SOFTWARE TECHNOLOGIES LTD

СПАСИБО!
ВОПРОСЫ?

Турков Никита | Security Engineer
nikitat@checkpoint.com

Сергей Забула | Channel SE Team Lead
szabula@checkpoint.com