



Check Point[®]
SOFTWARE TECHNOLOGIES LTD



CHECK POINT
INFINITY SOC

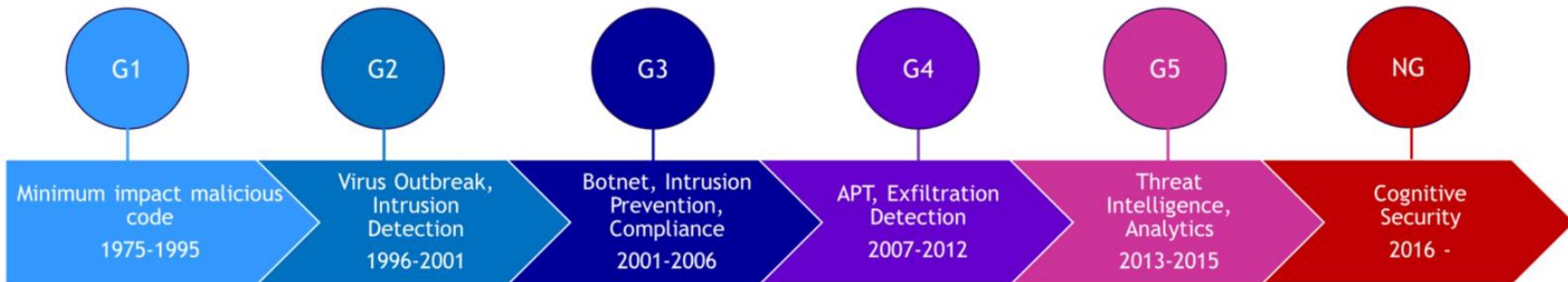
INFINITY SOC

TRUE XDR

Турков Никита | Security Engineer
nikitat@checkpoint.com

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

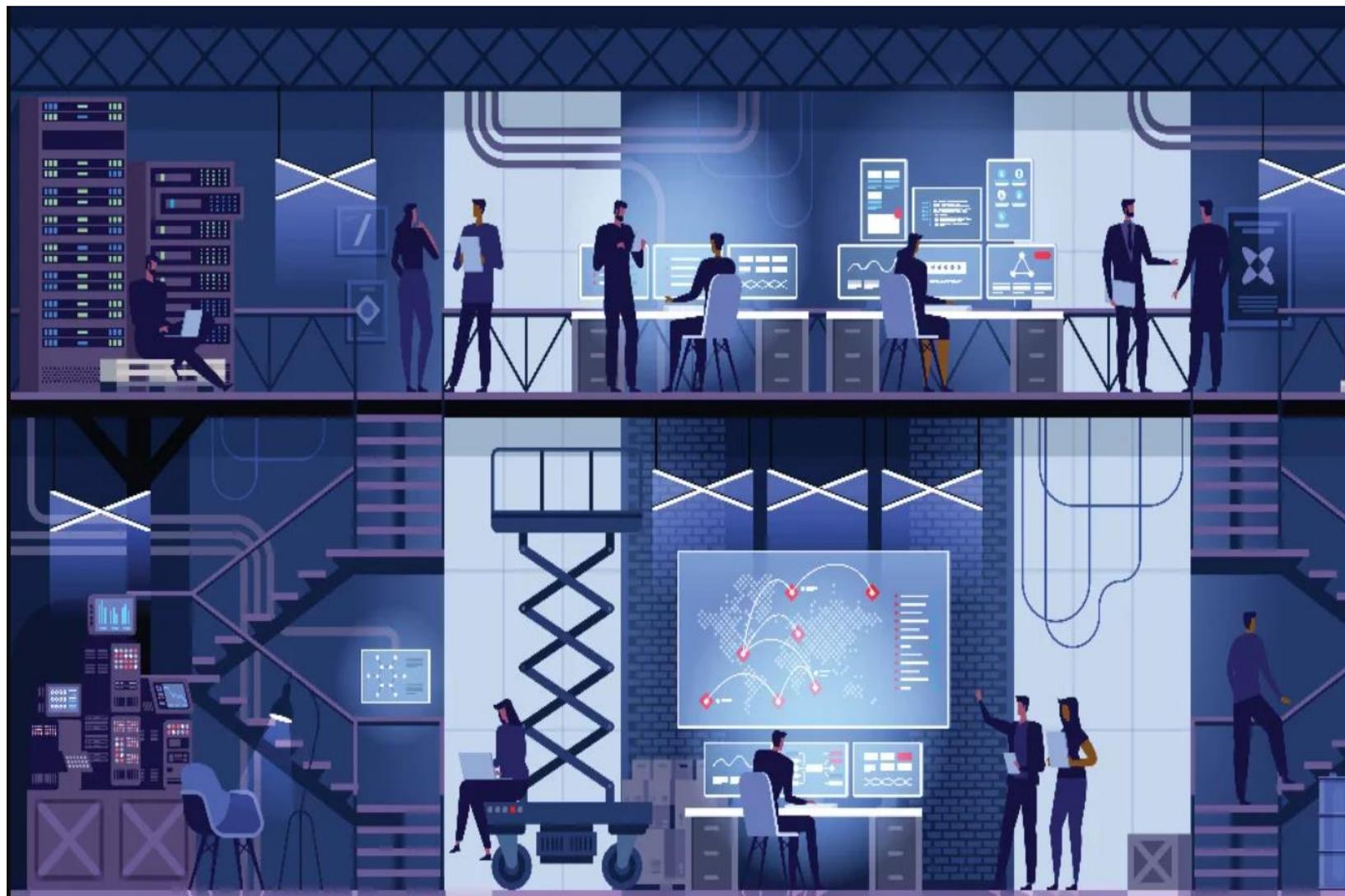
НЕМНОГО ИСТОРИИ



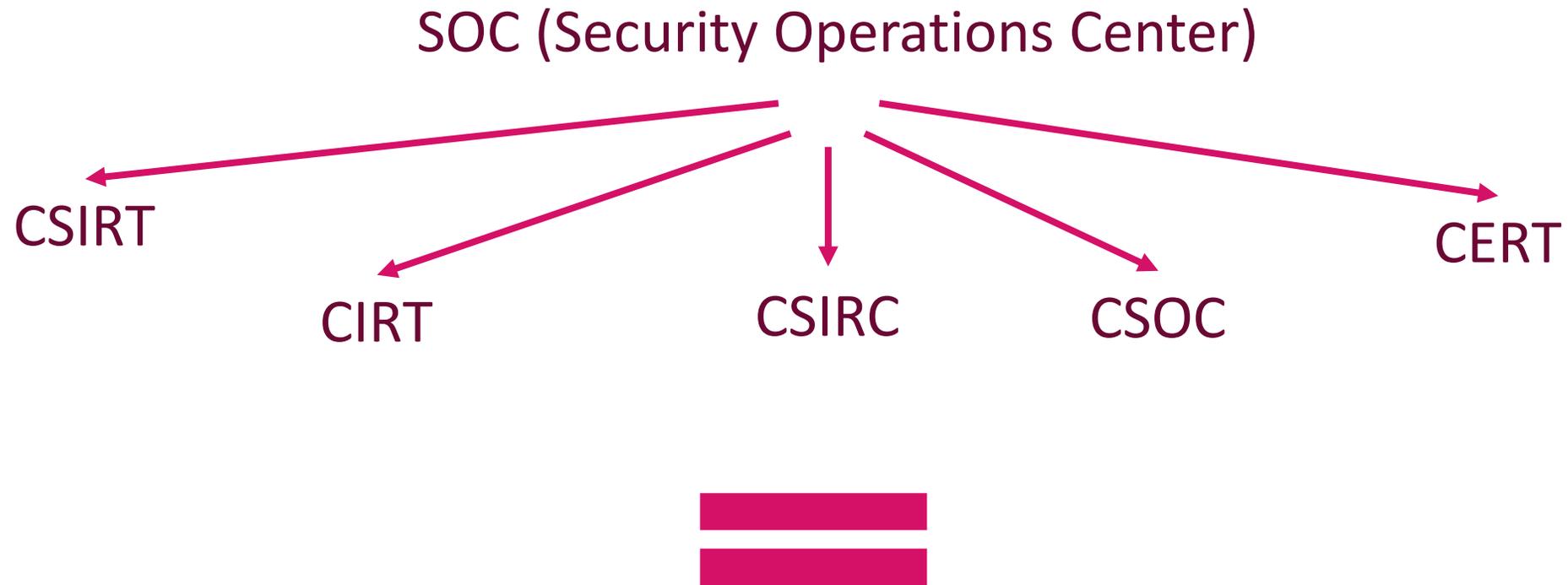
*Концепция создания SOC следующего поколения – Anti-malware

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

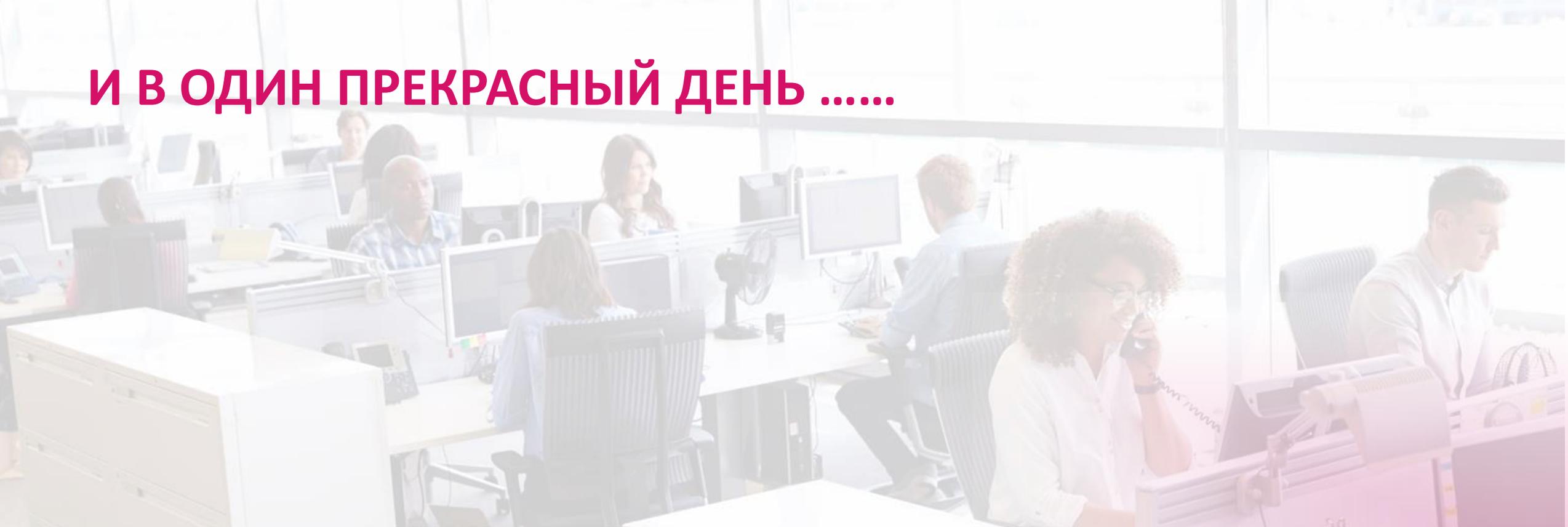
доход



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

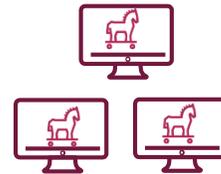
КАК ЭТО МОГЛО ПРОИЗОЙТИ?

Анатомия атаки



Фишинговая рассылка привела к заражению **Trickbot Trojan**

Окт 2019



Trickbot горизонтальное распространение на 500 хостов

Дек 2019



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

Янв 2020

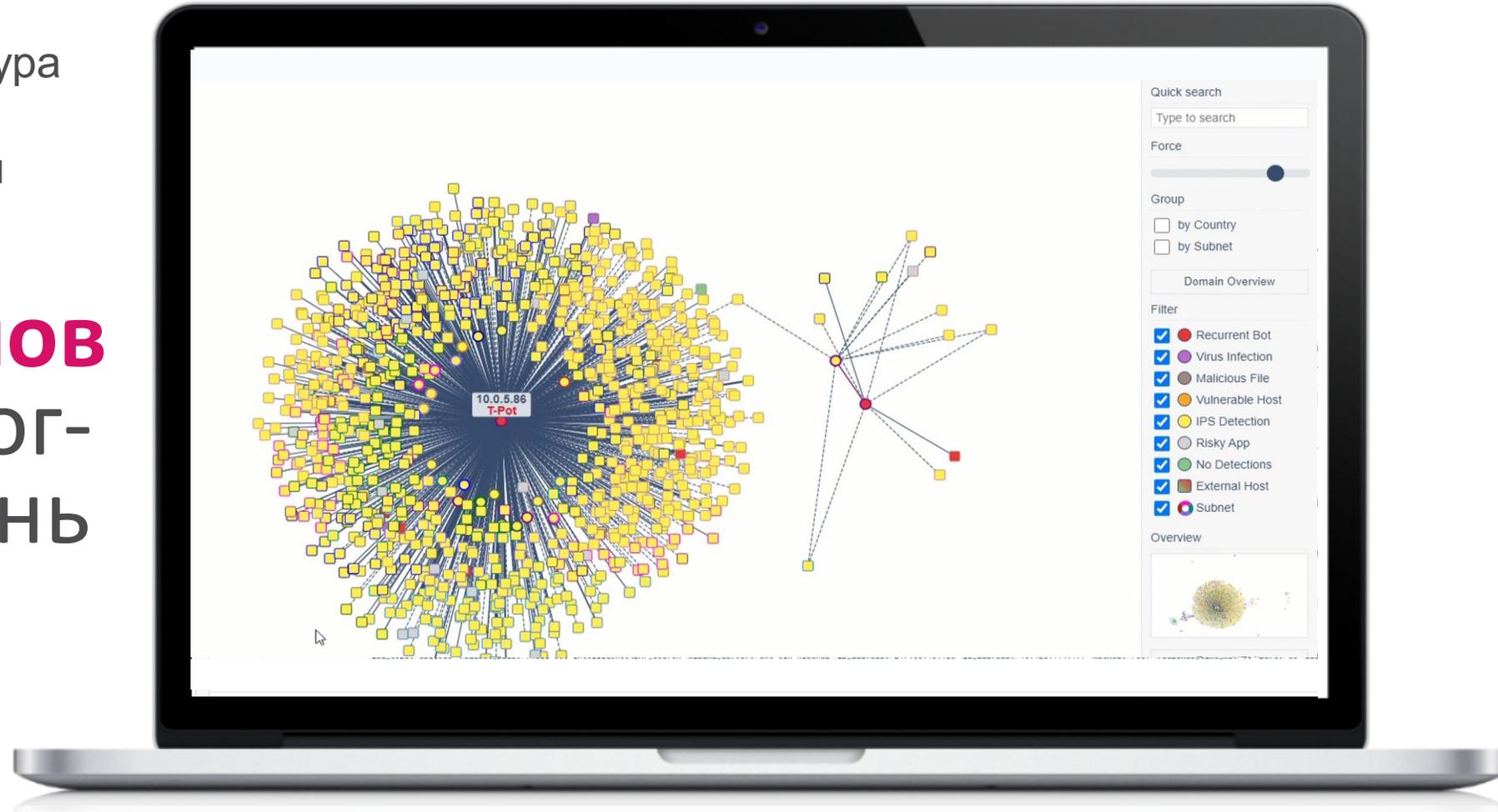
Фев 2020

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

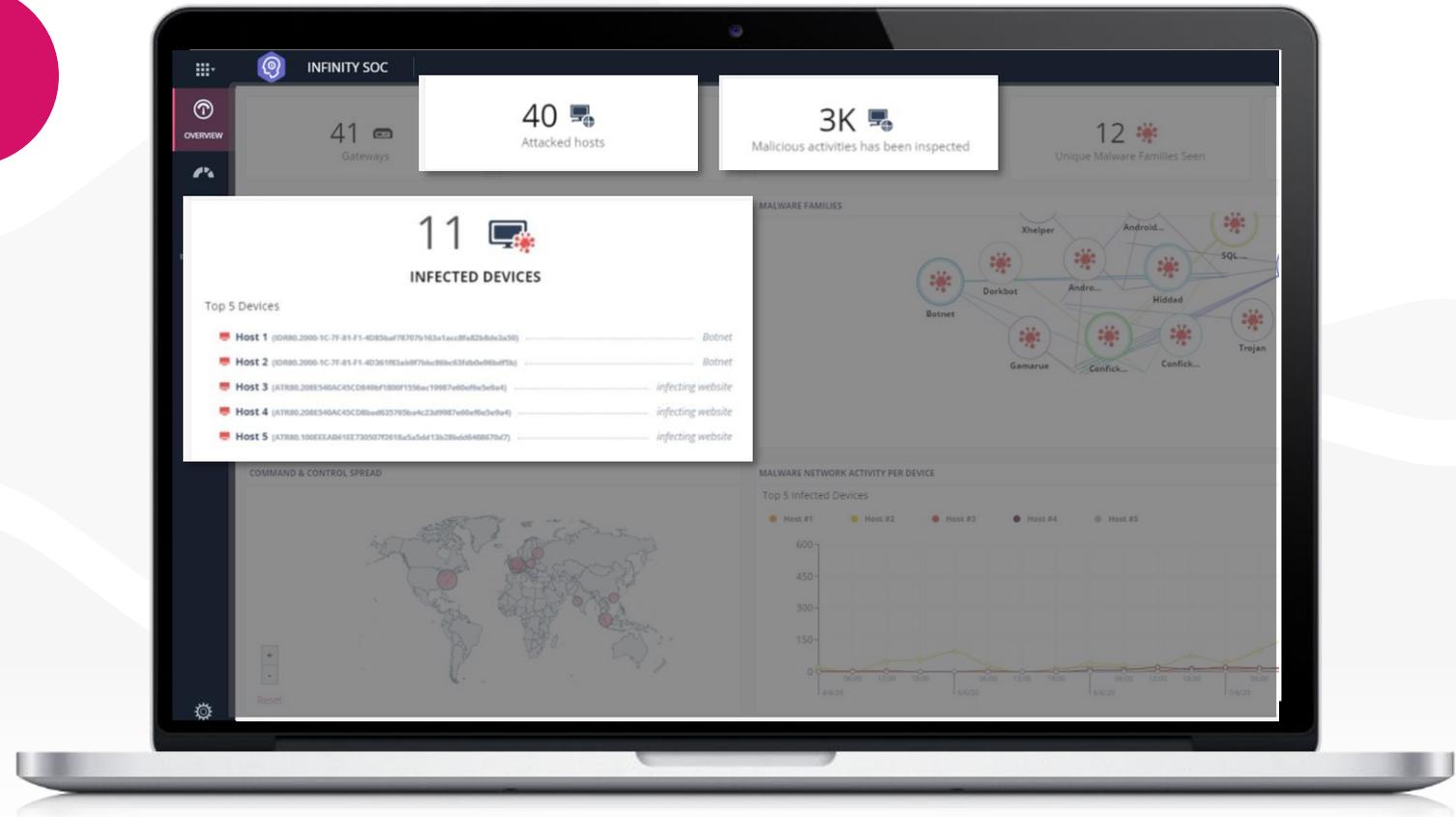
Вредоносных активностей

40

Затронутых
ХОСТОВ

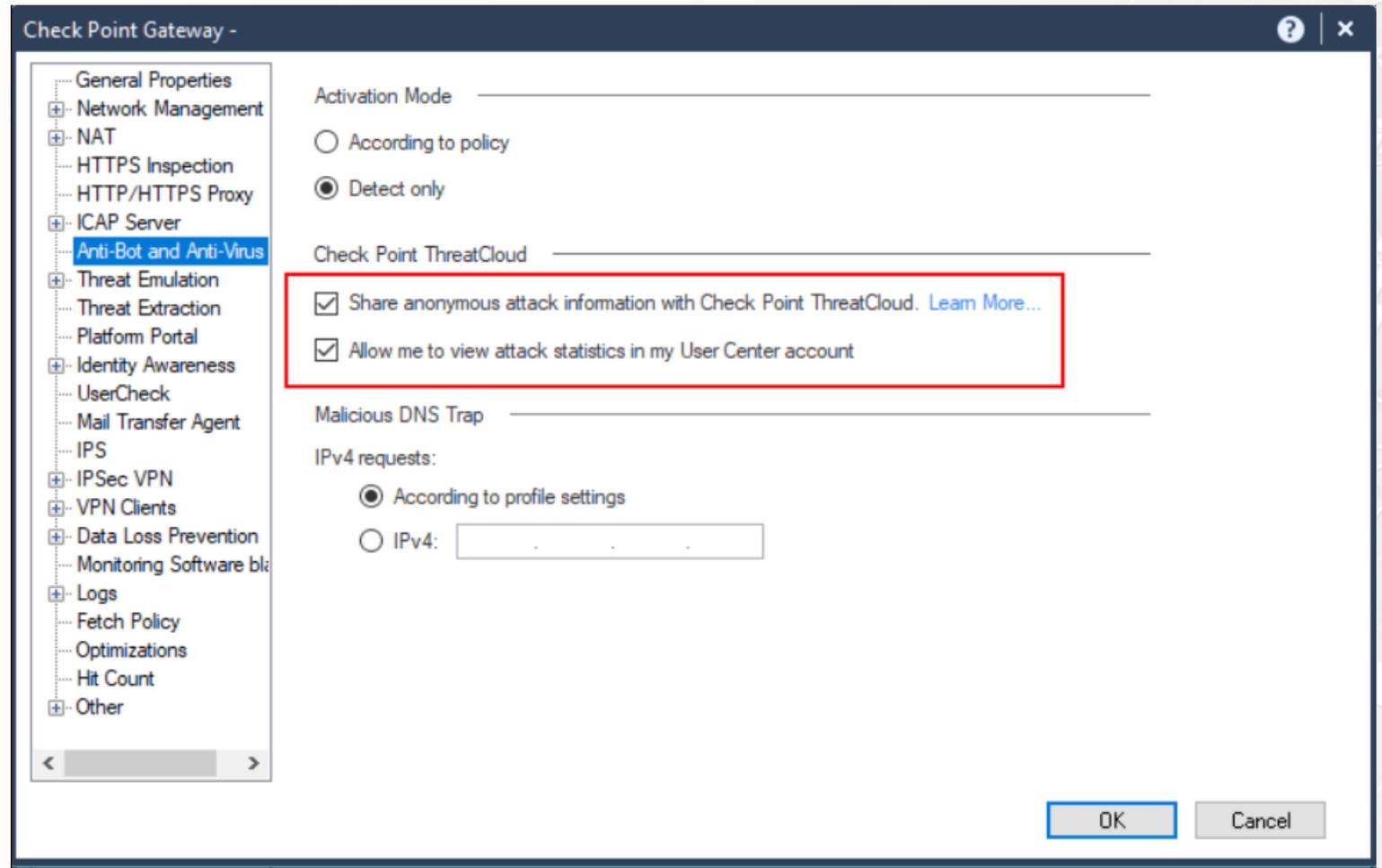
11

Зараженных
ХОСТОВ



ТЯЖЕЛО ЛИ НАСТРОИТЬ?

NGFW + 2 опции +
инсталляция политики, всё!



Приоритезация важного

Реагируйте только на критичные события



Автоматическое ранжирование

99%
Вредонос TRICKBOT

99%  **Host #1** 6:58, 6/20/2020 
Host 1 might be infected with Trickbot (High probability)

99%
Рекламное ПО

99%  **Host #2** 6:58, 6/20/2020 
Host 2 might be infected with Adware (High probability)

30%
Внешняя угроза

30%  **Lookalike URL** 13:42, 6/8/2020 
Lookalike URL impersonating your website (Low probability)

10%
Мобильная угроза

10%  **Mobile Device** 6:57, 6/8/2020 
Mobile Device might be infected with Trojan Horse (Low probability)

Реакция

Минимизируйте последствия атаки с помощью восстановления одним кликом

1

Установите легковесный клиент на зараженный хост

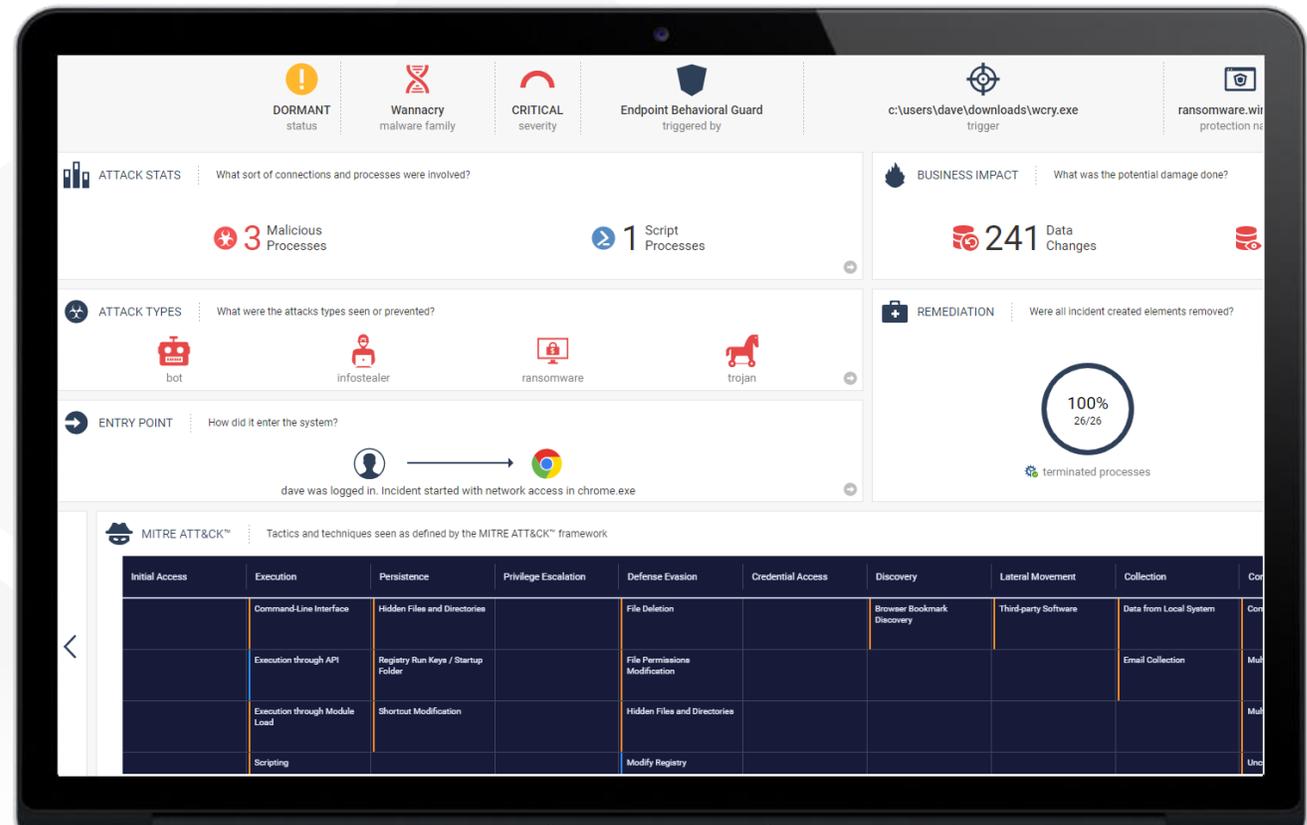
Идентифицируйте и остановите процессы

Заблокируйте C&C коммуникации

Удалите вредоносные файлы

2

Получите детальный отчет о форензике



Внешние угрозы

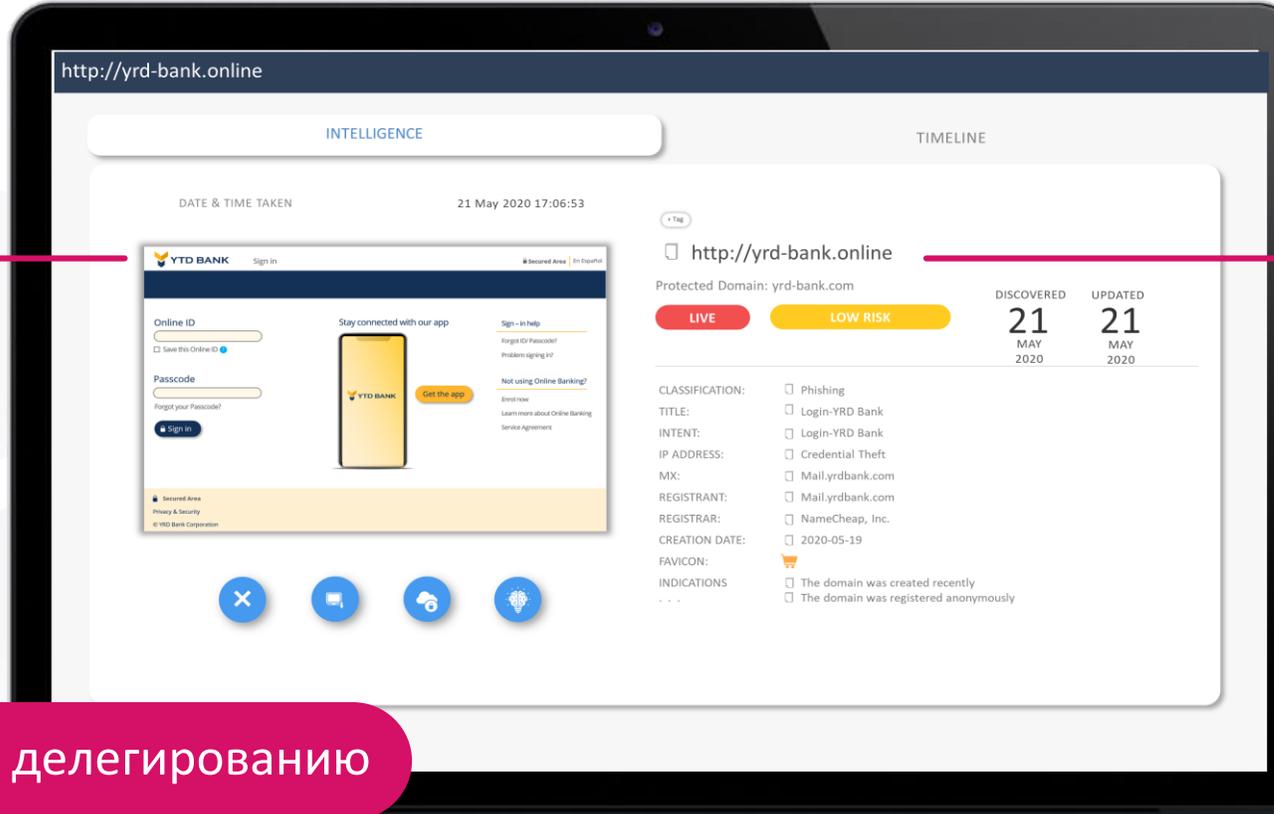
Предотвращайте фишинговые атаки на ваших сотрудников и заказчиков

Видим внешние угрозы

Благодаря анализу интернет-трафика в реальном времени

Подражание
Вашему корпоративному веб-сайту или почтовому домену

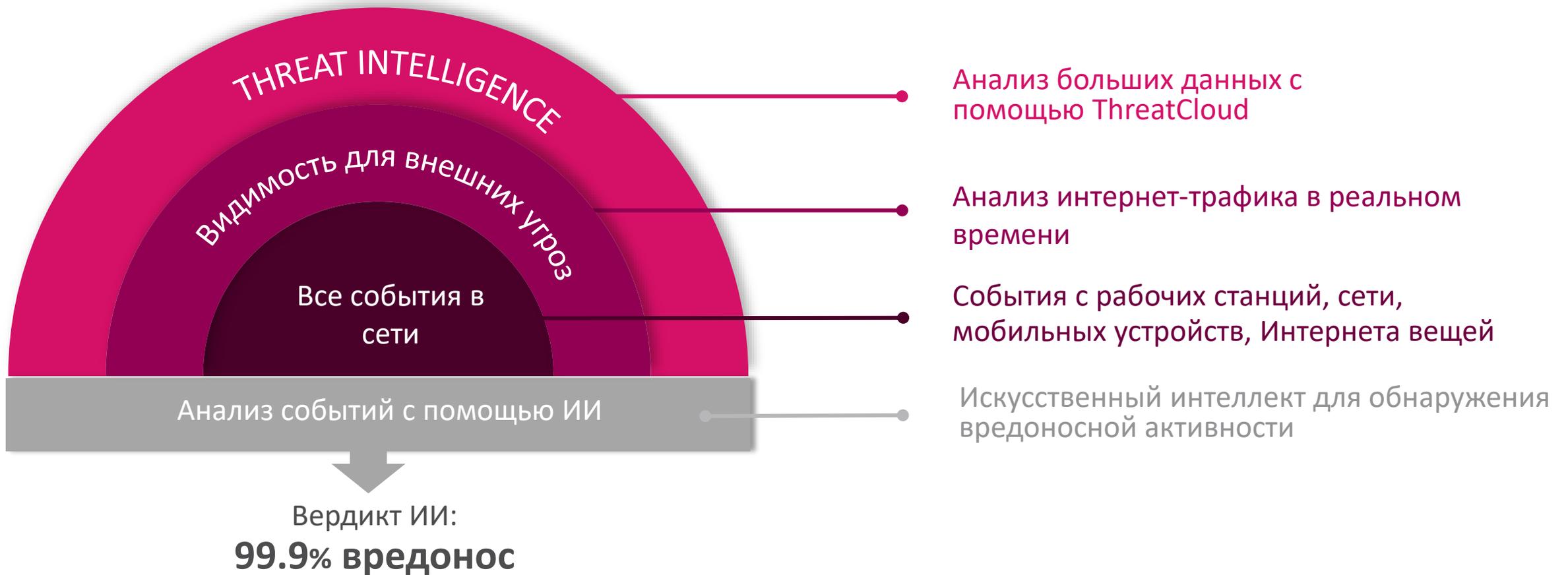
 Сервис по делегированию



The screenshot displays a security dashboard for the domain `http://yrd-bank.online`. The interface is divided into sections: 'INTELLIGENCE' and 'TIMELINE'. The main content area shows a 'DATE & TIME TAKEN' of '21 May 2020 17:06:53'. Below this is a thumbnail of the phishing site, which is a login page for 'YTD BANK' with fields for 'Online ID' and 'Passcode'. To the right of the thumbnail is a risk assessment section showing 'LIVE' and 'LOW RISK' status, with 'DISCOVERED' and 'UPDATED' dates both set to '21 MAY 2020'. Below the risk assessment is a 'CLASSIFICATION' section with a list of indicators, including 'Phishing', 'Login-YRD Bank', 'Credential Theft', and 'The domain was created recently'. The dashboard also features a 'Protected Domain' section for 'yrd-bank.com' and a 'FAVICON' section with a shopping cart icon.

Похожий домен

Настоящий XDR: Обнаруживайте скрытые атаки с точностью 99.9%



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

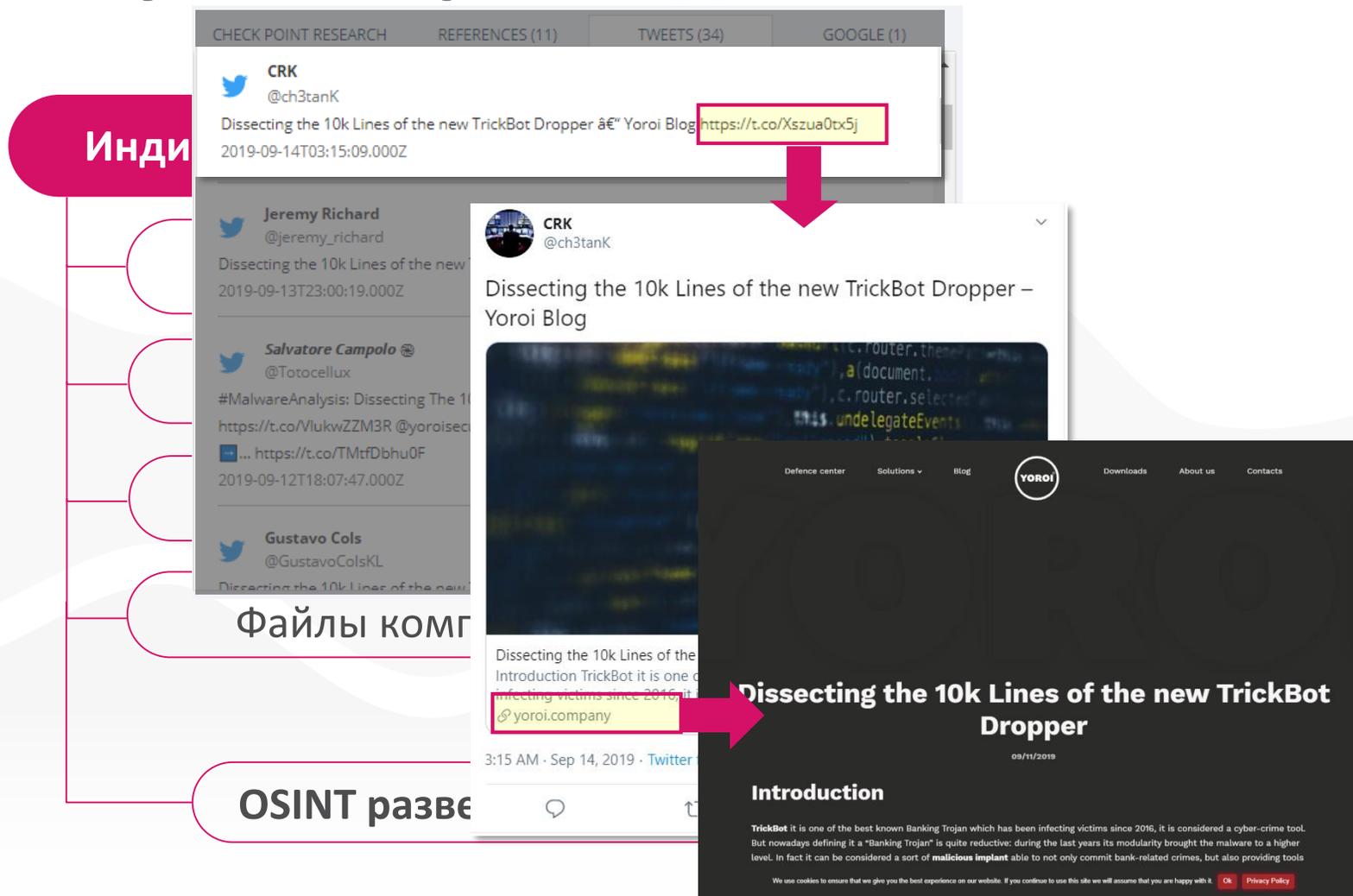
Данные по времени атаки

Аналитика исследователей

И другое...

The screenshot shows the ThreatCloud search interface. At the top, there is a search bar with the text 'Search...' and a magnifying glass icon. Below the search bar, it says 'Paste here any suspicious Domain URLs IPs or Hashes. Search for up to 20 indicators in a single search.' The search results are displayed in a grid layout. The first result is for the indicator 'MDS: 0bbf25412b4dc63e5bb1370ed782a93'. The 'INDICATOR INFORMATION' section shows the indicator's details, including its file type (XLSM), size (63 KB), and first/last seen dates. The 'RESEARCH' section shows a list of file names and their associated hashes. The 'GEOLOCATION' section shows a world map with red markers indicating the geographic distribution of the indicator. The 'TRICKBOT' section provides a detailed description of the malware family, including its capabilities and target sectors. The 'INDICATOR TIMELINE' section shows a line graph of the indicator's activity over time, and the 'DISTRIBUTION' section shows a donut chart indicating the delivery method (Email: 100%).

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!



Лучший CATCH RATE
по версии NSS LABS



Urgent PO Septemer.pdf.exe

SIZE: 1.33 MB | TYPE: EXE | HASH list

From: attacker@*****.com

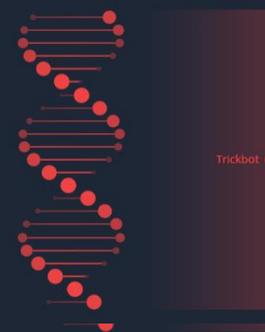
Subject: undefined

File Name:

To: customerservice@*****.com

Bevel Corp Intl Updated Statemen...

MALWARE FAMILY

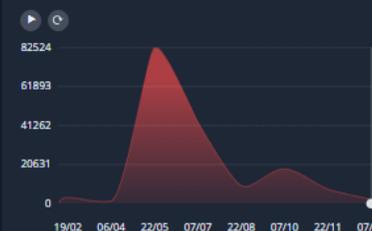


Trickbot

Trickbot is a modular Banking Trojan that targets the Windows platform, mostly delivered via spam campaigns or other malware families such as Emotet. Trickbot sends information about the infected system and can also download and execute arbitrary modules from a large array of available modules: from a VNC module for remote control, to an SMB module for spreading within a compromised network. Once a machine is infected, the Trickbot gang, the threat actors behind this malware, utilize this wide array of modules not only to steal banking credentials from the target PC but also for lateral movement and reconnaissance on the targeted organization itself, prior to delivering a company-wide targeted ransomware attack.

[Read more on Check Point Threatcloud Intelligence](#)

Similarity Analysis



MITRE ATTACK

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND & CONTROL	IMPACT
	Windows Management Instrumentation	Registry Run Keys Startup Folder	Bypass User Account Control	Process Hollowing	Credentials In Files	Security Software Discovery		Email Collection			
	Execution Through API	Change Default File Association	Process Injection	Bypass User Account Control	Credentials from Web Browsers	System Information Discovery		Data from Local System			
	Regsvcs Regasm	AppCert DLLs	AppCert DLLs	Software Packing	Credentials In Registry	Application Window Discovery					
		Windows Management Instrumentation Event Subscription		Process Injection							
				Disabling Security Tools							
				Regsvcs Regasm							

Упрощение и уменьшение стоимости владения с единой централизованной SOC платформой

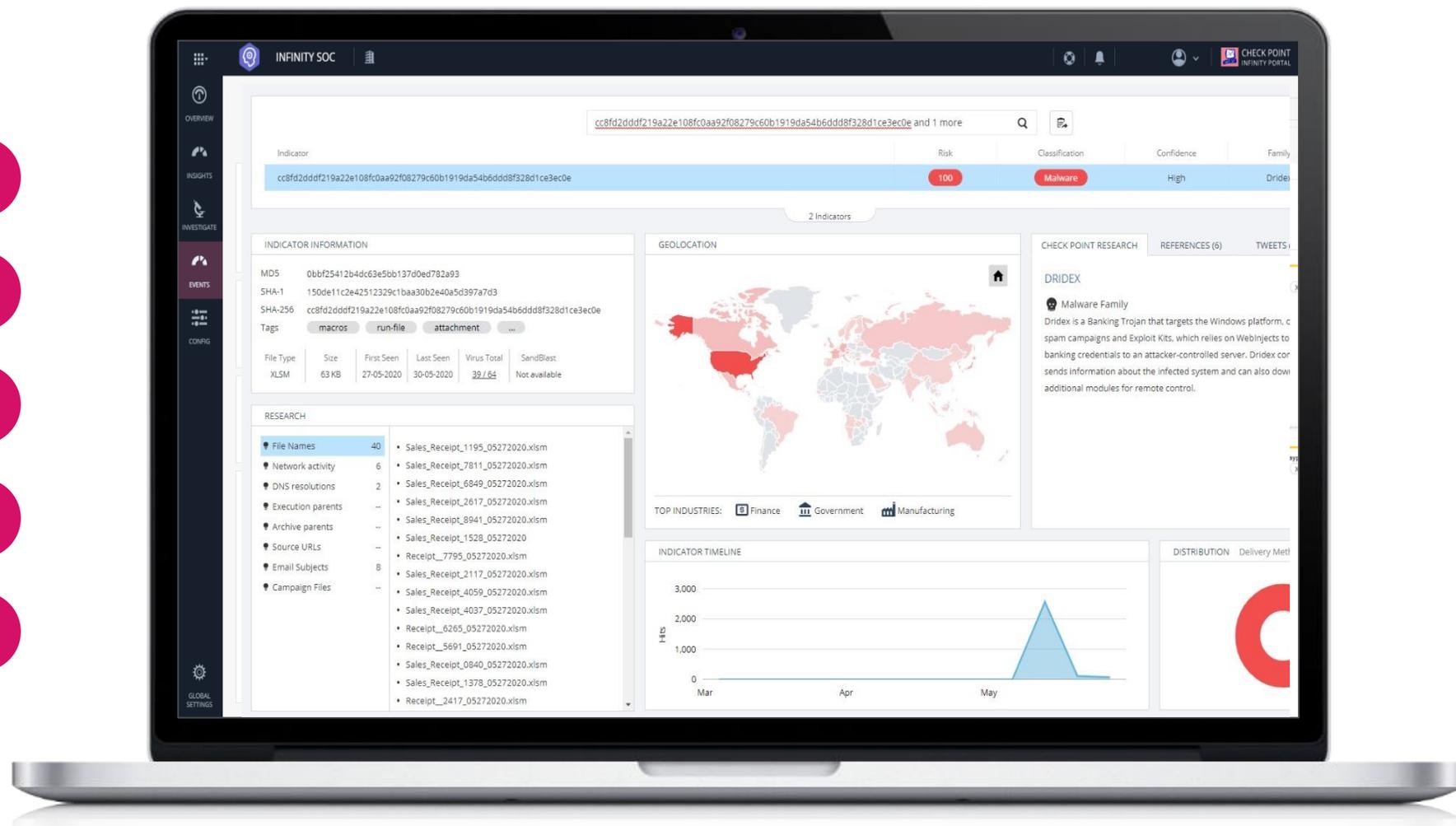
Внутренние угрозы

Внешние угрозы

Восстановление

Расследование

Управление



Можно начать пользоваться менее чем за 3 минуты

Легкое внедрение

Нет необходимости в дополнительных агентах

01

Зарегистрируйтесь на
Infinity Portal

02

Выберите шлюзы
(если они уже есть)

03

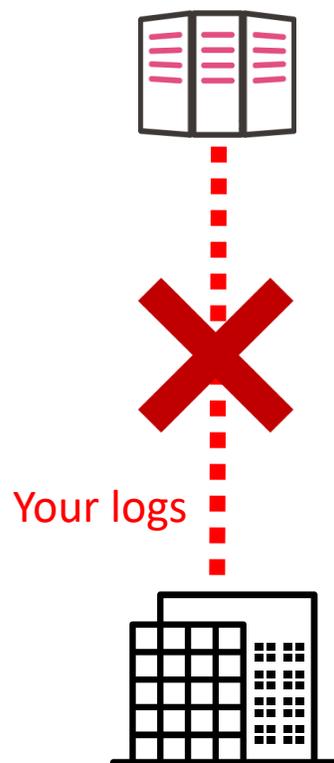
Подключитесь
к ThreatCloud

04

Начинайте

Приватность во главе угла

Ваши лог-файлы никуда не отправляются



**Защита
конфиденциальных
данных**



**Нет затрат на хранение
лог-файлов в облаке**

Готовы протестировать?



CHECK POINT

INFINITY SOC



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

ДЕМОНСТРАЦИЯ



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

СПАСИБО! ВОПРОСЫ?

Турков Никита | Security Engineer
nikitat@checkpoint.com

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

