



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD



CHECK POINT  
**INFINITY SOC**

# INFINITY SOC

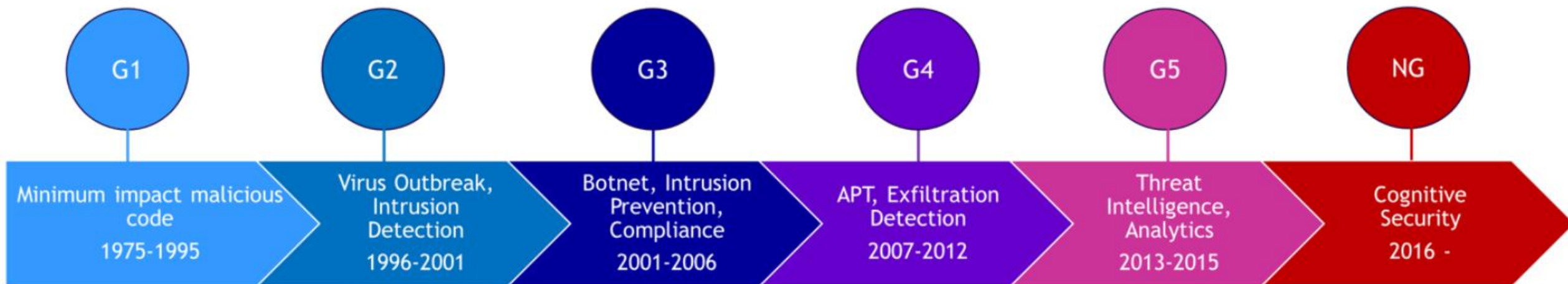
---

**TRUE XDR**

Турков Никита | Security Engineer  
[nikitat@checkpoint.com](mailto:nikitat@checkpoint.com)

Сергей Забула | Channel SE Team Lead  
[szabula@checkpoint.com](mailto:szabula@checkpoint.com)

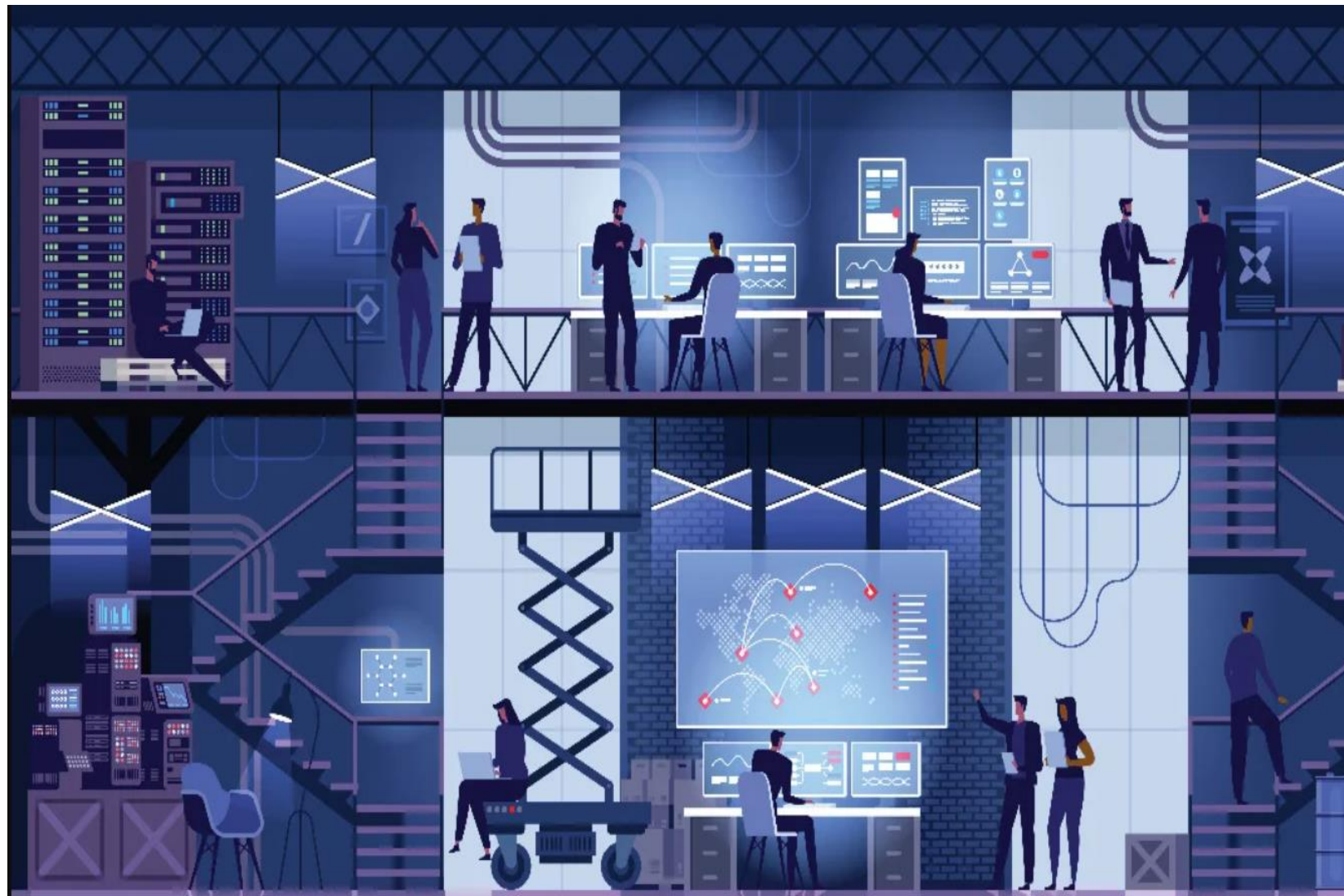
# НЕМНОГО ИСТОРИИ



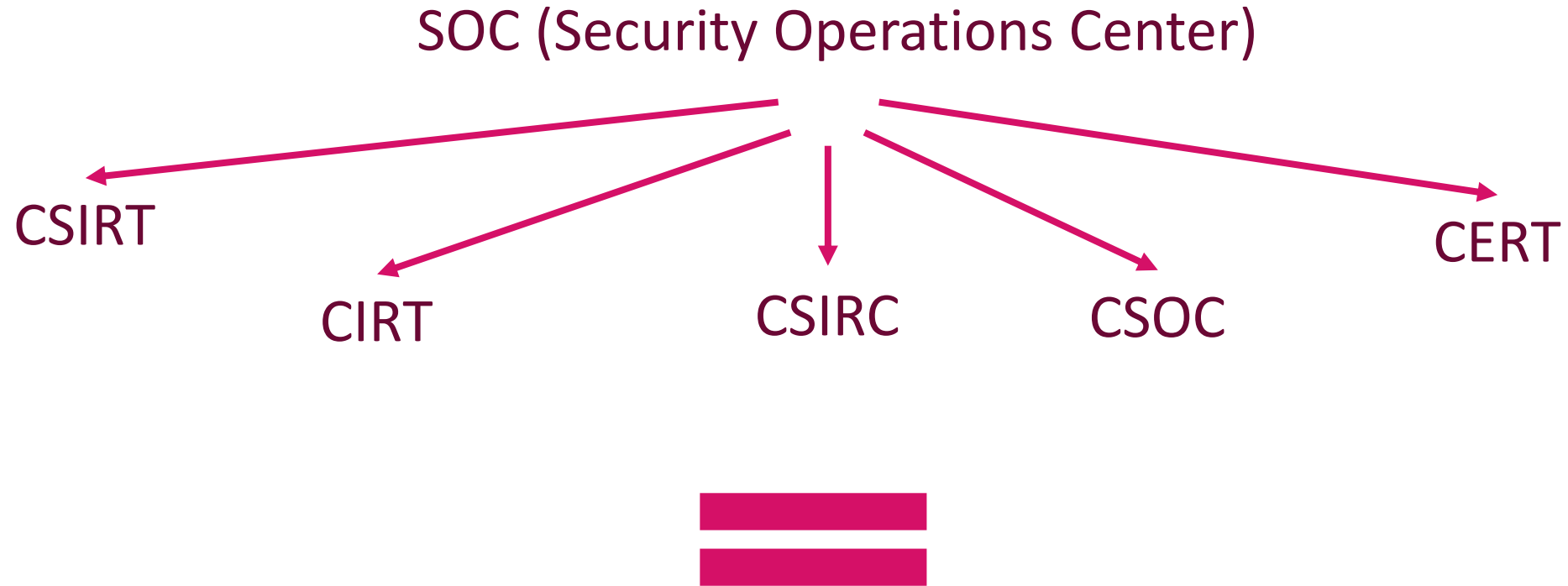
\*Концепция создания SOC следующего поколения – Anti-malware

# 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**

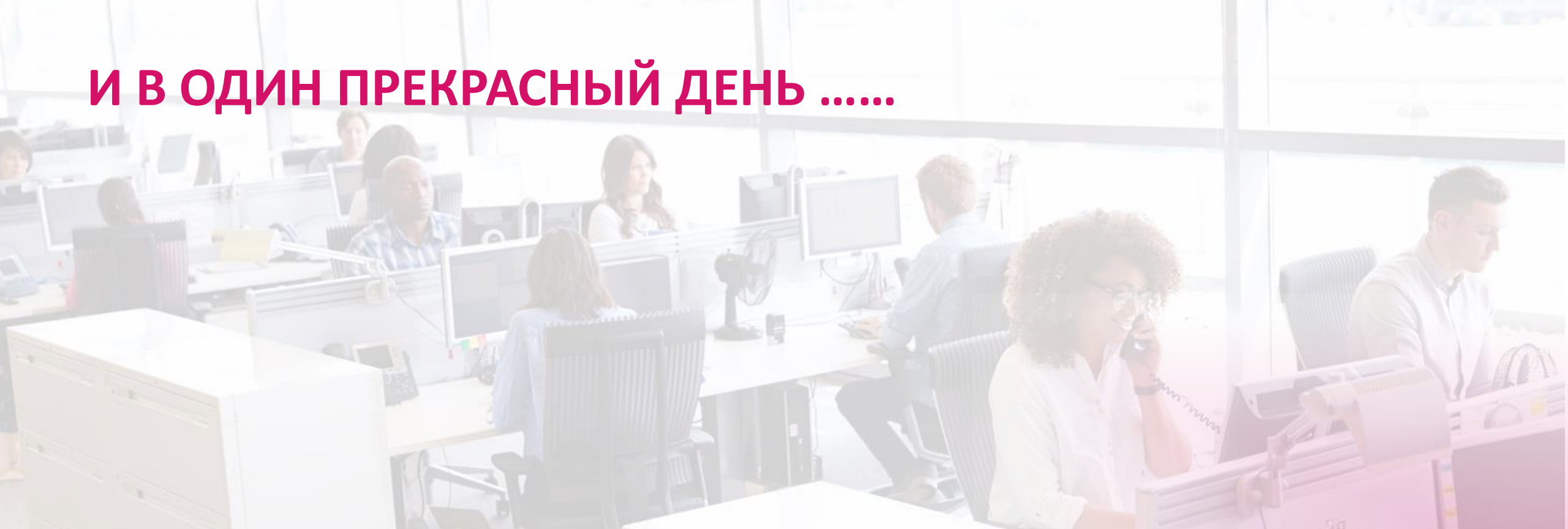
доход



**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** 

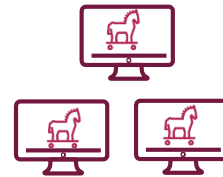


# КАК ЭТО МОГЛО ПРОИЗОЙТИ?

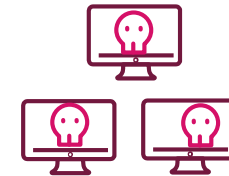
## Анатомия атаки



**Фишинговая** рассылка привела к заражению **Trickbot Trojan**



**Trickbot** горизонтальное распространение на 500 хостов



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

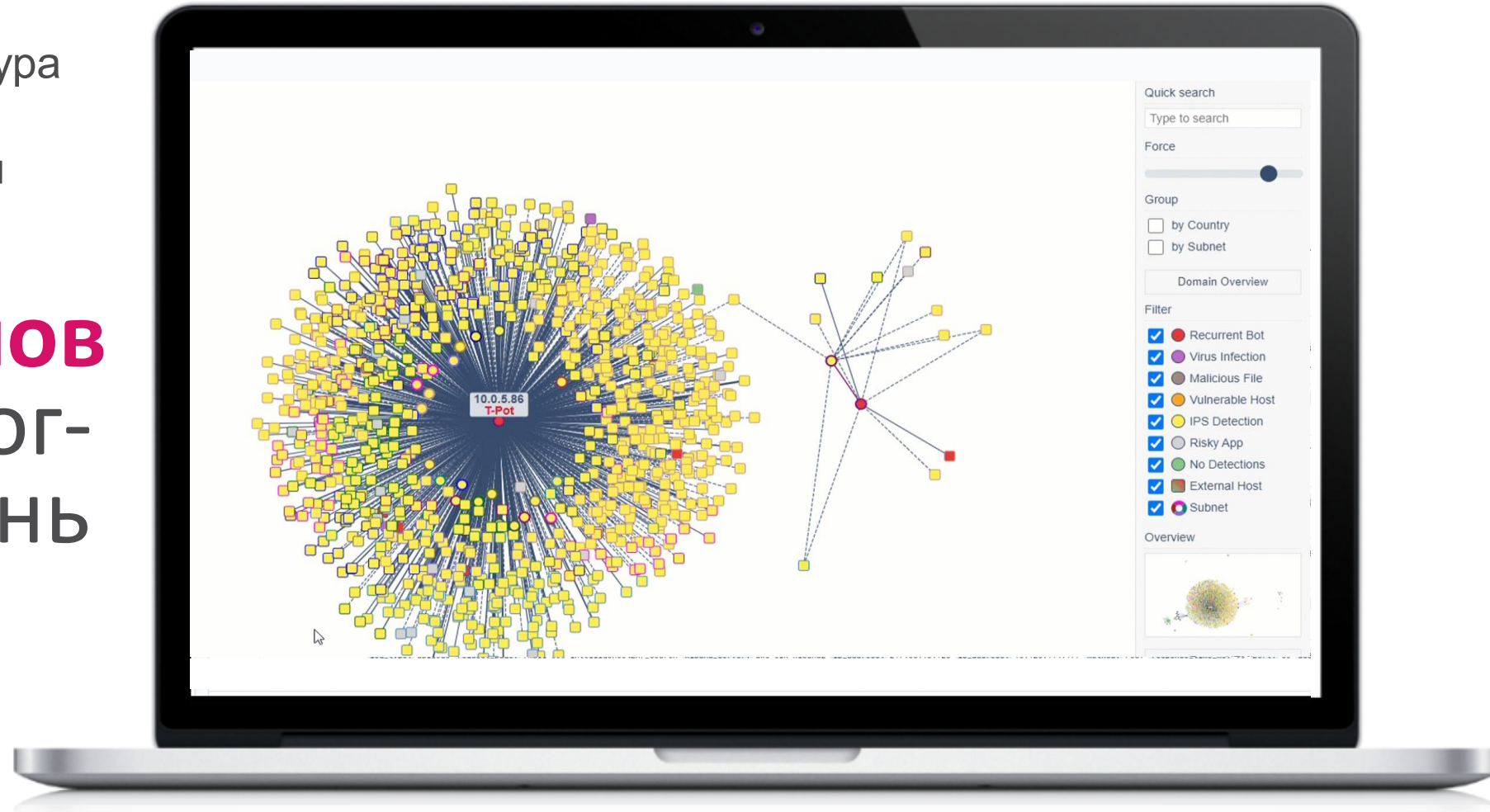


# Работа SOC службы каждый день: Ищем иголку в стоге сена

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**

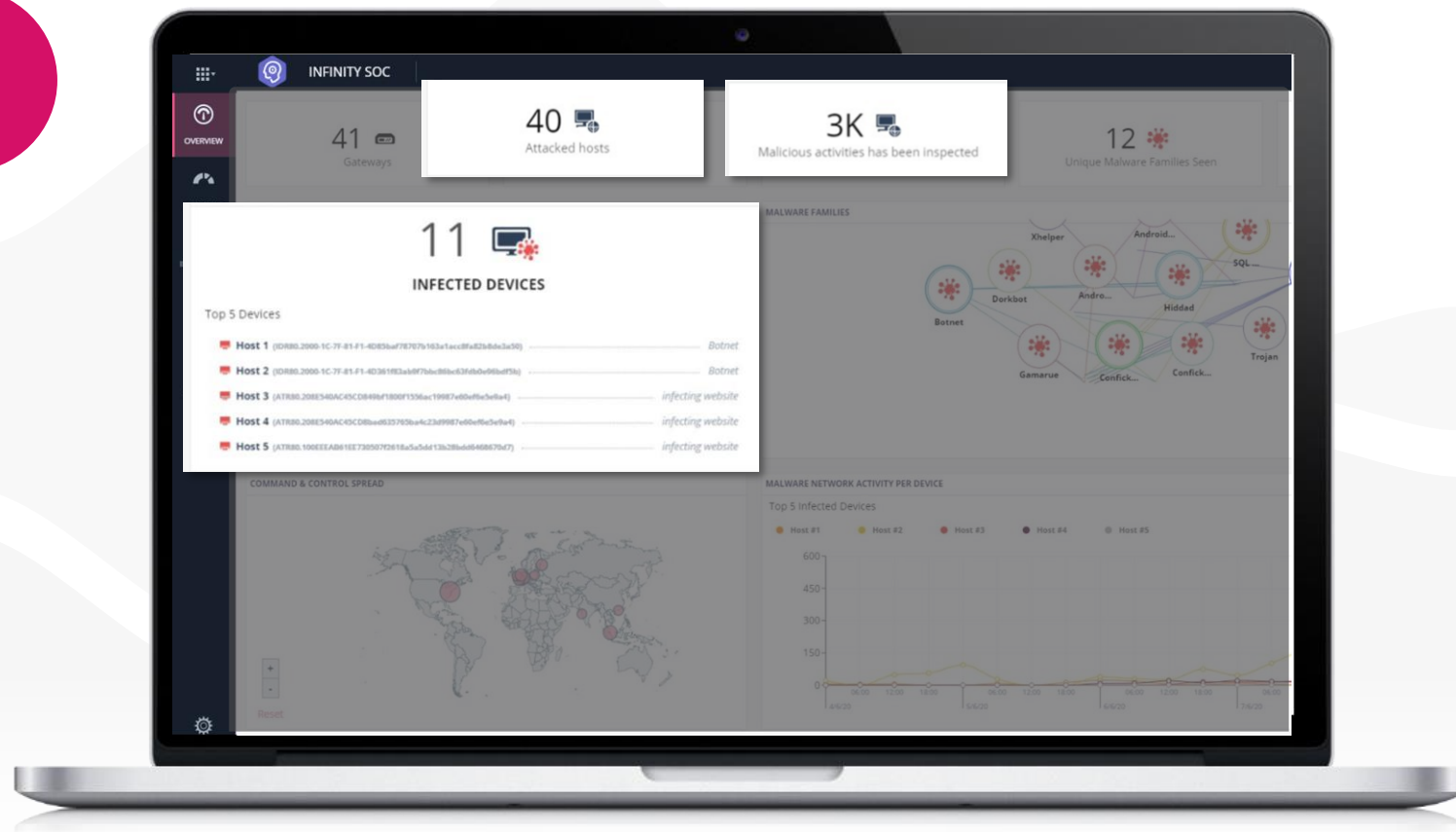
Вредоносных активностей

**40**

Затронутых  
ХОСТОВ

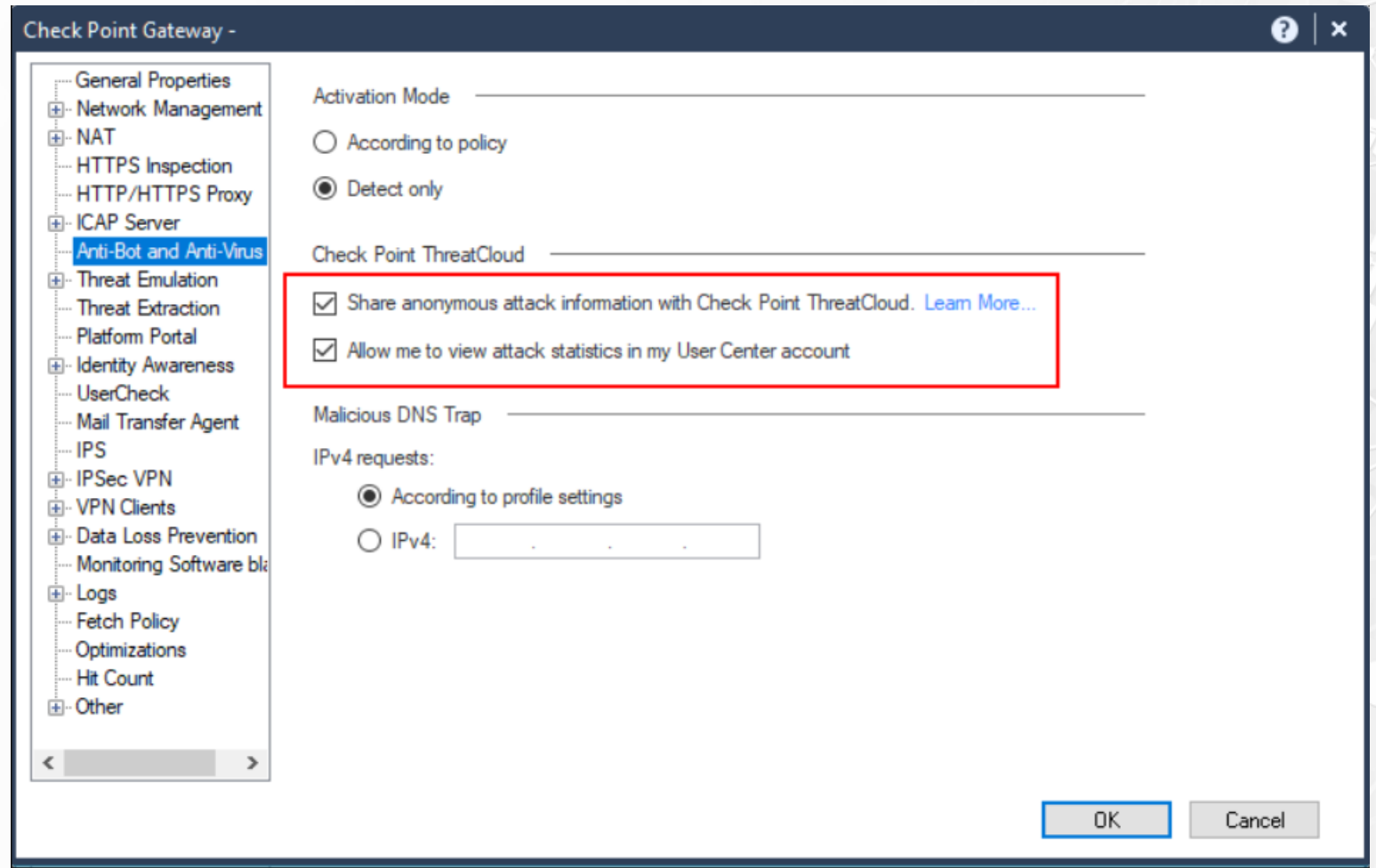
**11**

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

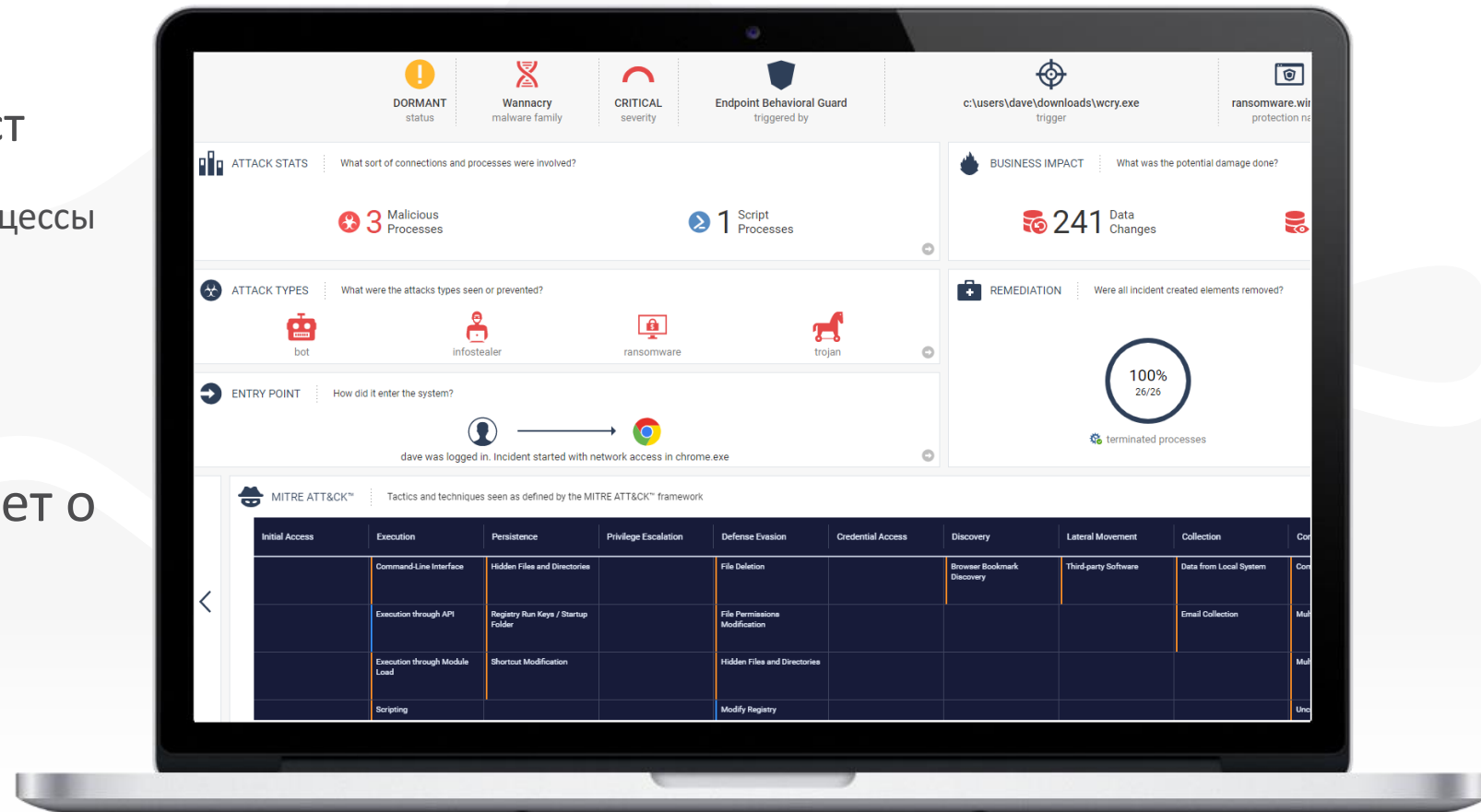
Идентифицируйте и остановите процессы

Заблокируйте C&C коммуникации

Удалите вредоносные файлы

2

Получите детальный отчет о форензике





# Внешние угрозы

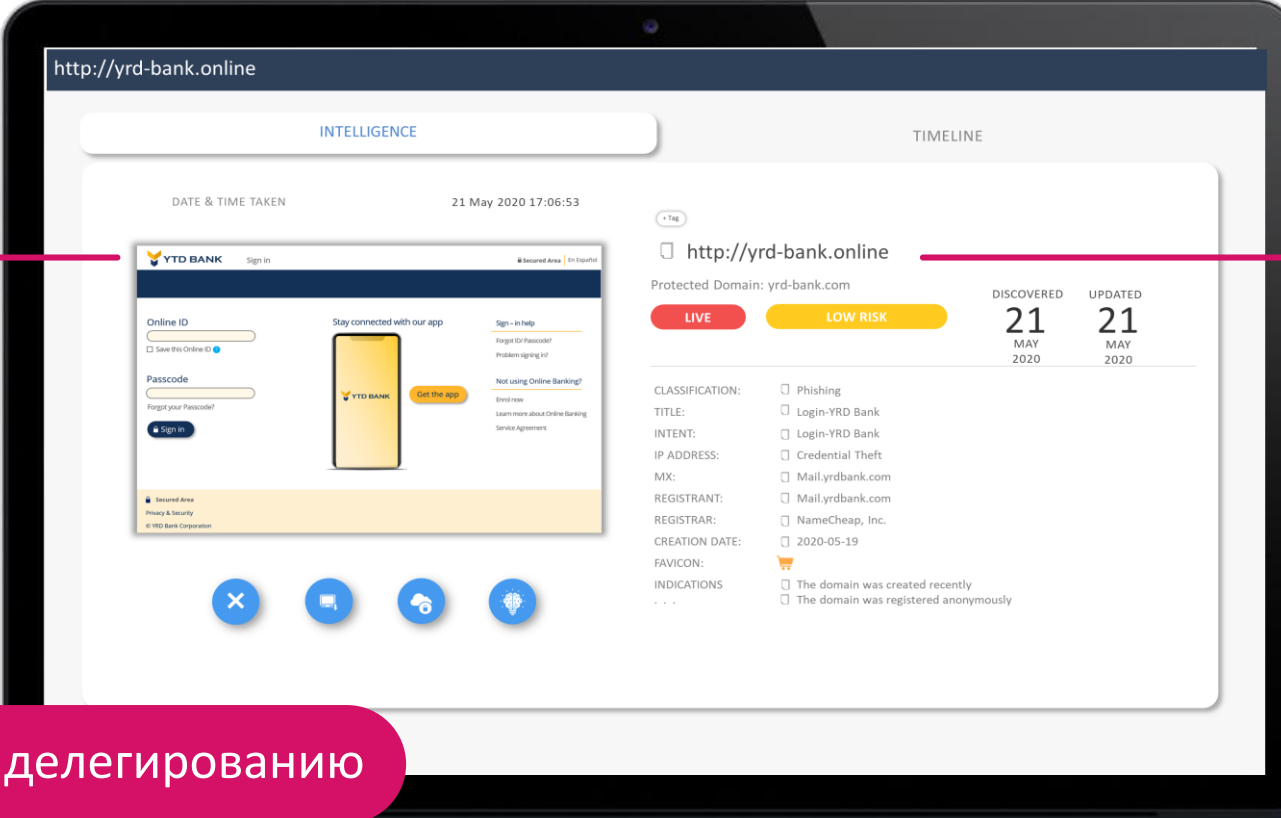
## Предотвращайте фишинговые атаки на ваших сотрудников и заказчиков

### Видим внешние угрозы


Благодаря анализу интернет-трафика в реальном времени

**Подражание**  
Вашему корпоративному веб-сайту или почтовому домену

 Сервис по делегированию

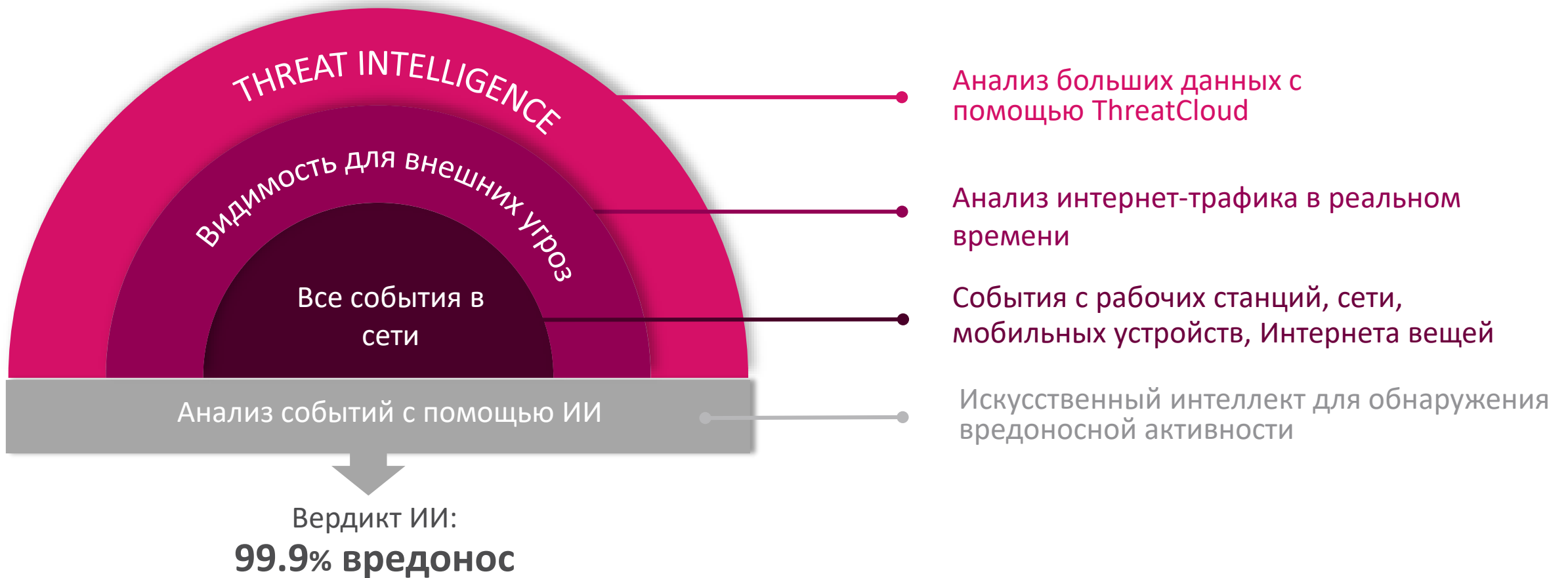


The screenshot displays a security interface with the following details:

- URL: <http://yrd-bank.online>
- Protected Domain: yrd-bank.com
- Risk Level: **LOW RISK**
- Discovery Date: 21 MAY 2020
- Update Date: 21 MAY 2020
- Classification: Phishing
- Intent: Login-YRD Bank
- IP Address: Credential Theft
- MX: Mail.yrdbank.com
- Registrant: Mail.yrdbank.com
- Registrar: NameCheap, Inc.
- Creation Date: 2020-05-19
- Favicon: 
- Indications:
  - The domain was created recently
  - The domain was registered anonymously

**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

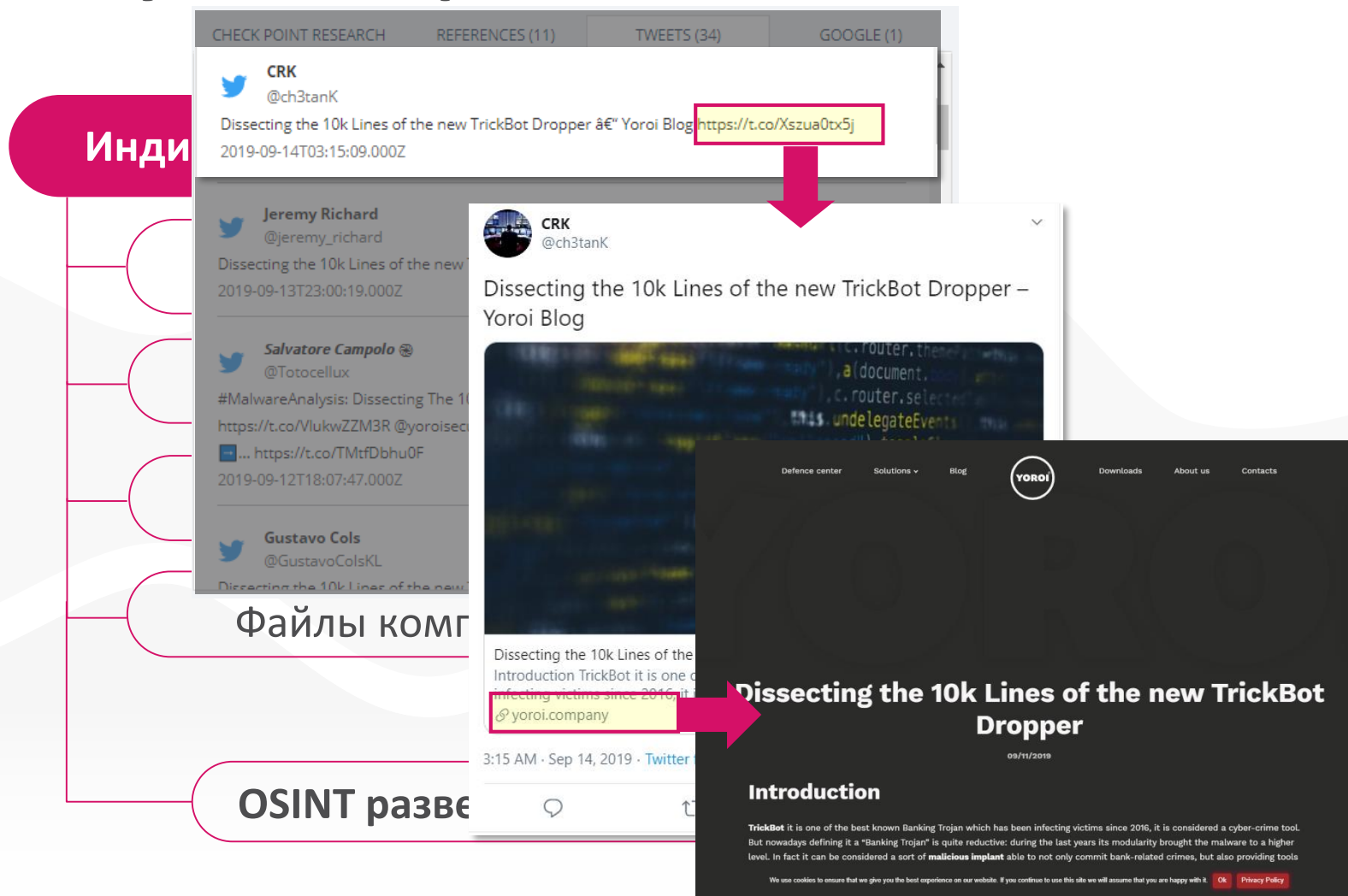
Данные по времени атаки

Аналитика исследователей

И другое...

The screenshot shows the ThreatCloud search interface on a laptop. At the top, there is a search bar with the placeholder 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 main content area is divided into several sections: 'INDICATOR INFORMATION' with fields for MD5, SHA-1, and SHA-256; 'GEOLOCATION' with a world map showing attack locations; 'TRICKBOT' with a description of the malware family; 'RESEARCH' with a list of file names and their details; 'INDICATOR TIMELINE' with a line graph showing activity over time; and 'DISTRIBUTION Delivery Method' with a donut chart showing the percentage of attacks by 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

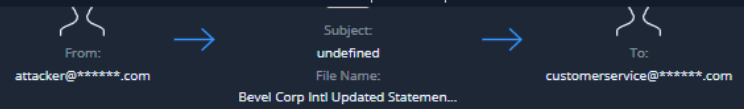
- Семейство вредоноса
- География
- MITRE ATT&CK матрица
- Видео эмуляции
- Файлы, которые были докачаны
- URL центров управления
- И другое!



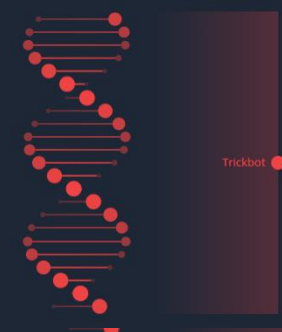
Лучший CATCH RATE  
по версии NSS LABS

### Urgent PO Septemer.pdf.exe

SIZE: 1.33 MB | TYPE: EXE | HASH list



#### MALWARE FAMILY

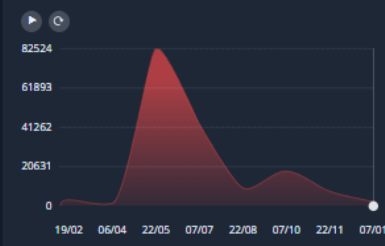


#### Trickbot

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

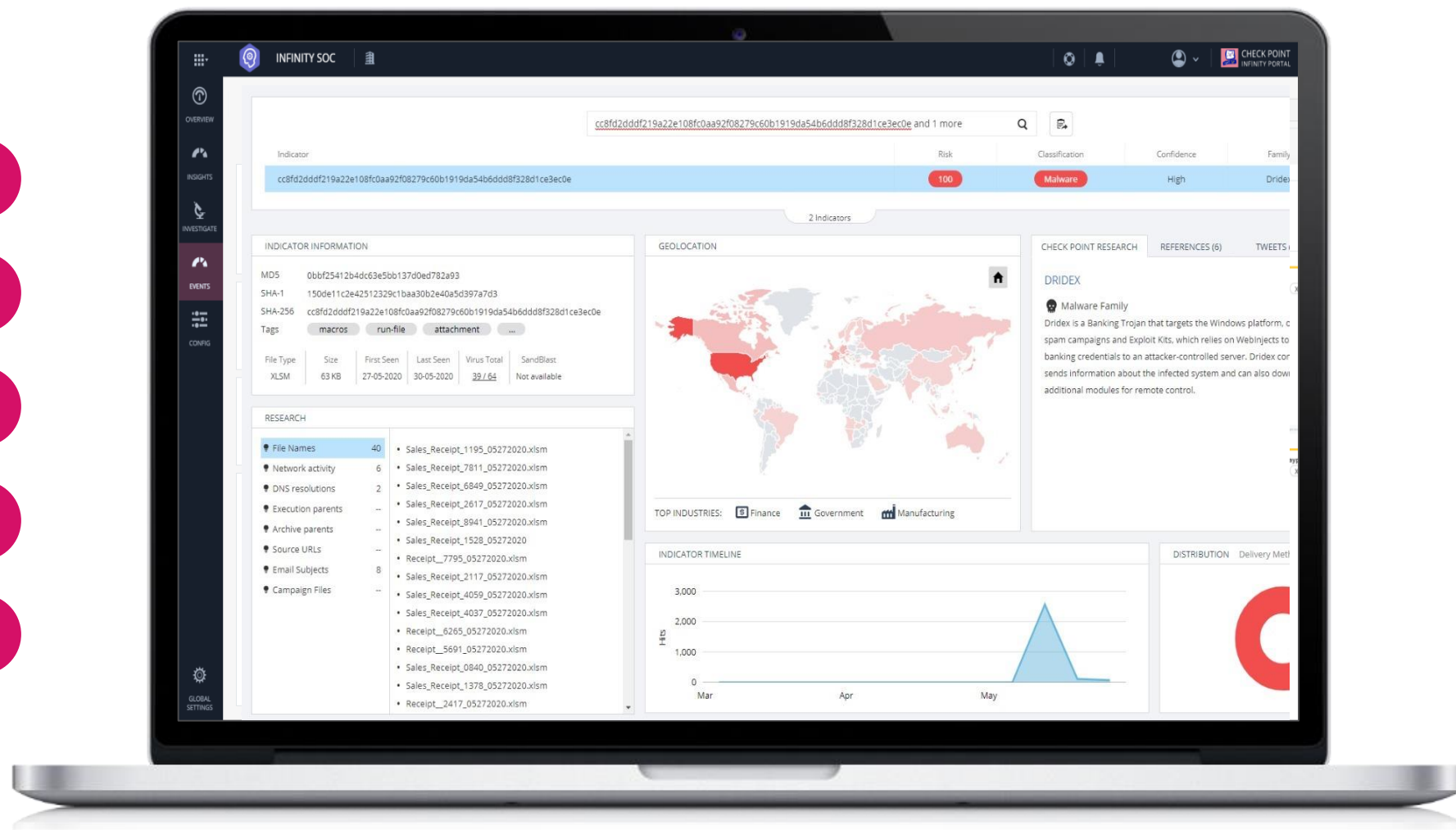
Внутренние угрозы

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](http://www.checkpoint.com/products/Infinity-SOC)



# ДЕМОНСТРАЦИЯ



**Check Point**<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD

# СПАСИБО! ВОПРОСЫ?

Турков Никита | Security Engineer  
[nikitat@checkpoint.com](mailto:nikitat@checkpoint.com)

Сергей Забула | Channel SE Team Lead  
[szabula@checkpoint.com](mailto:szabula@checkpoint.com)

