Check Point
SOFTWARE TECHNOLOGIES LTD

«Автономный» EDR на службе SOC

Алексей Белоглазов
Технический эксперт по защите от кибератак
abeloglazov@checkpoint.com

Американская трубопроводная компания Colonial Pipeline заплатила хакерам около $5 млн в криптовалюте через несколько часов после атаки, сообщает Bloomberg со ссылкой на информированные источники.

Известно, что взлом системы был осуществлён при помощи вируса-вымогателя и, по некоторым сведениям, группировкой DarkSide. Киберпреступники похитили 100 гигабайт данных и требовали за них выкуп, угрожая выложить информацию в Интернет. Телеканал CNN,

TRIPLE EXTORTION RANSOMWARE

ВСПЛЕСК АТАК ВЫМОГАТЕЛЕЙ В МИРЕ

$20 млрд.

ущерб от атак вымогательского ПО в мире в 2020

По сравнению с $11.5 млрд. в 2019

Более 50%

вымогателей угрожали опубликовать украденные данные, начиная с 3-го кв. 2020

$233 тыс.

средний размер выплаченного выкупа

На 30% выше, чем во 2-м кв. 2020

https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

Что происходит, когда событий в SOC слишком много

Check Point
SOFTWARE TECHNOLOGIES LTD

10...25+ тысяч алертов в день в среднем в 55% SOC

Более 4 дней – среднее время решения инцидента (MTTR) в 79% SOC

Результат:

10% – нанимают больше инженеров

57% – изменяют политики ИБ, чтобы уменьшить число алертов

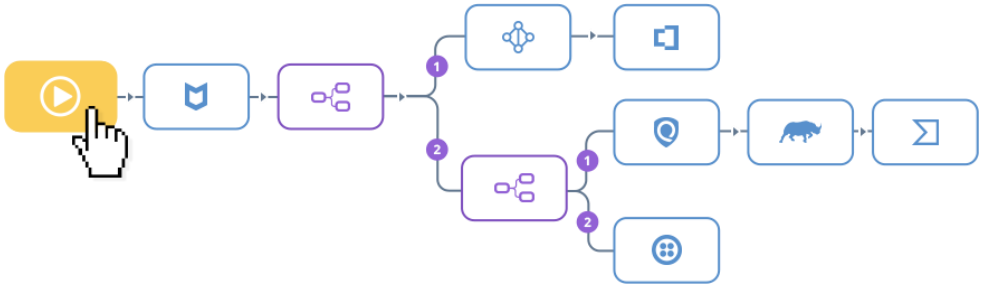
30% – игнорируют определенные категории алертов

Источники: https://www.infosecurity-magazine.com/news/174000-alerts-per-week-besiege/
https://www.imperva.com/blog/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/
https://www.helpnetsecurity.com/2019/08/29/soc-alert-overload/

Элементы автоматизации в SOC

Снижение времени на проверку событий и реагирование

На макро-уровне



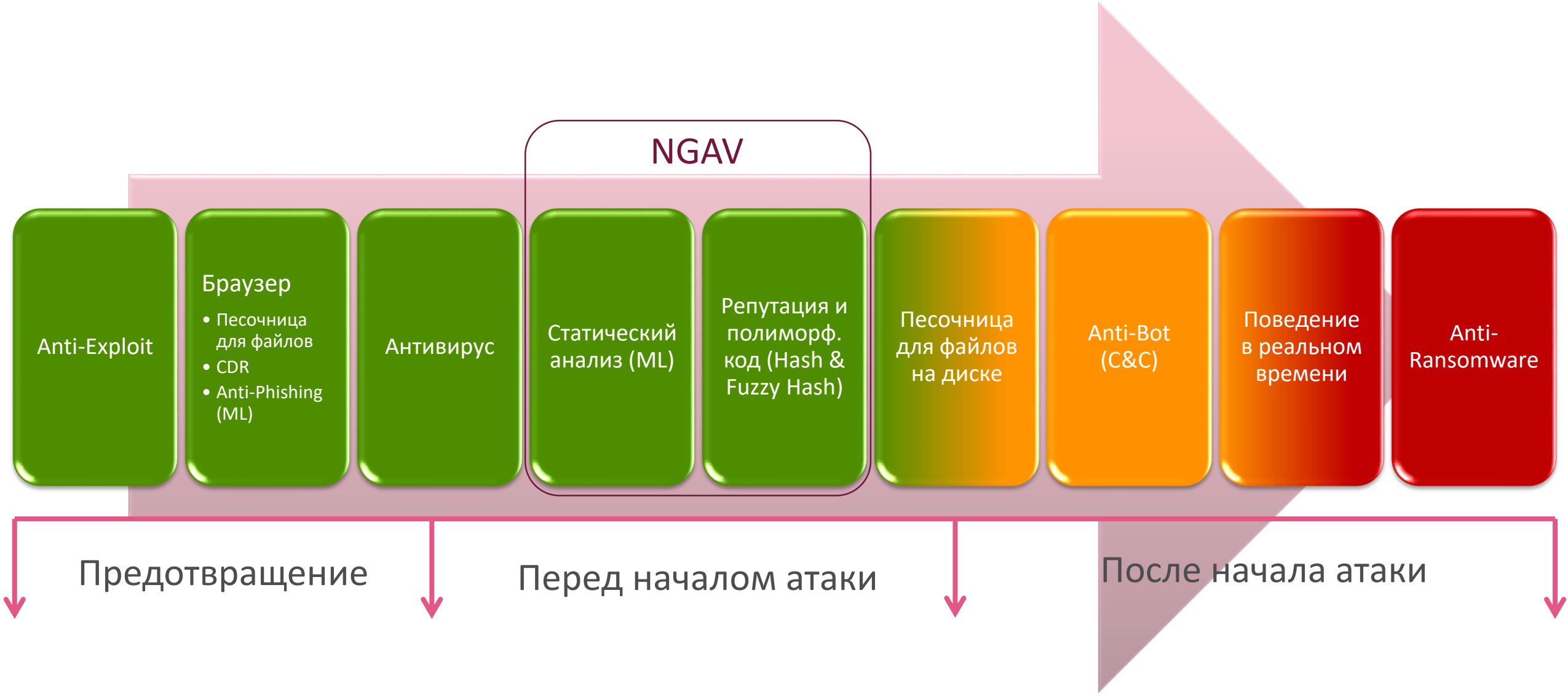
- ✓ Плэйбуки в SOAR
- ✓ Скрипты в SIEM
- ✓ Типовые реакции в XDR

На микро-уровне

«Автономный» EDR:

- ✓ Предотвращение
- ✓ Обнаружение и расследование
- ✓ Аналитика и атрибуция
- ✓ Лечение и восстановление

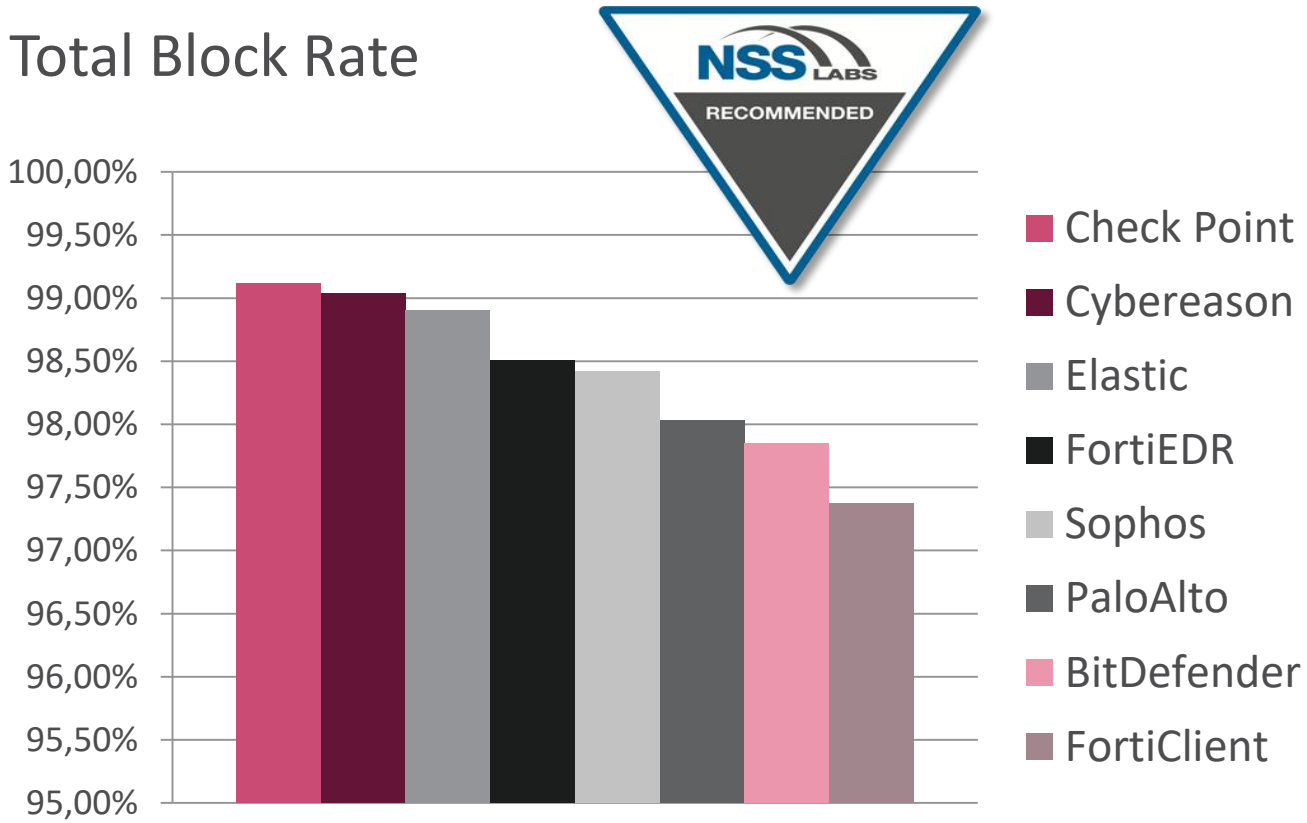
Эшелонированная защита конечных точек



NSS Labs Advanced Endpoint Protection Test 2020

Check Point
SOFTWARE TECHNOLOGIES LTD

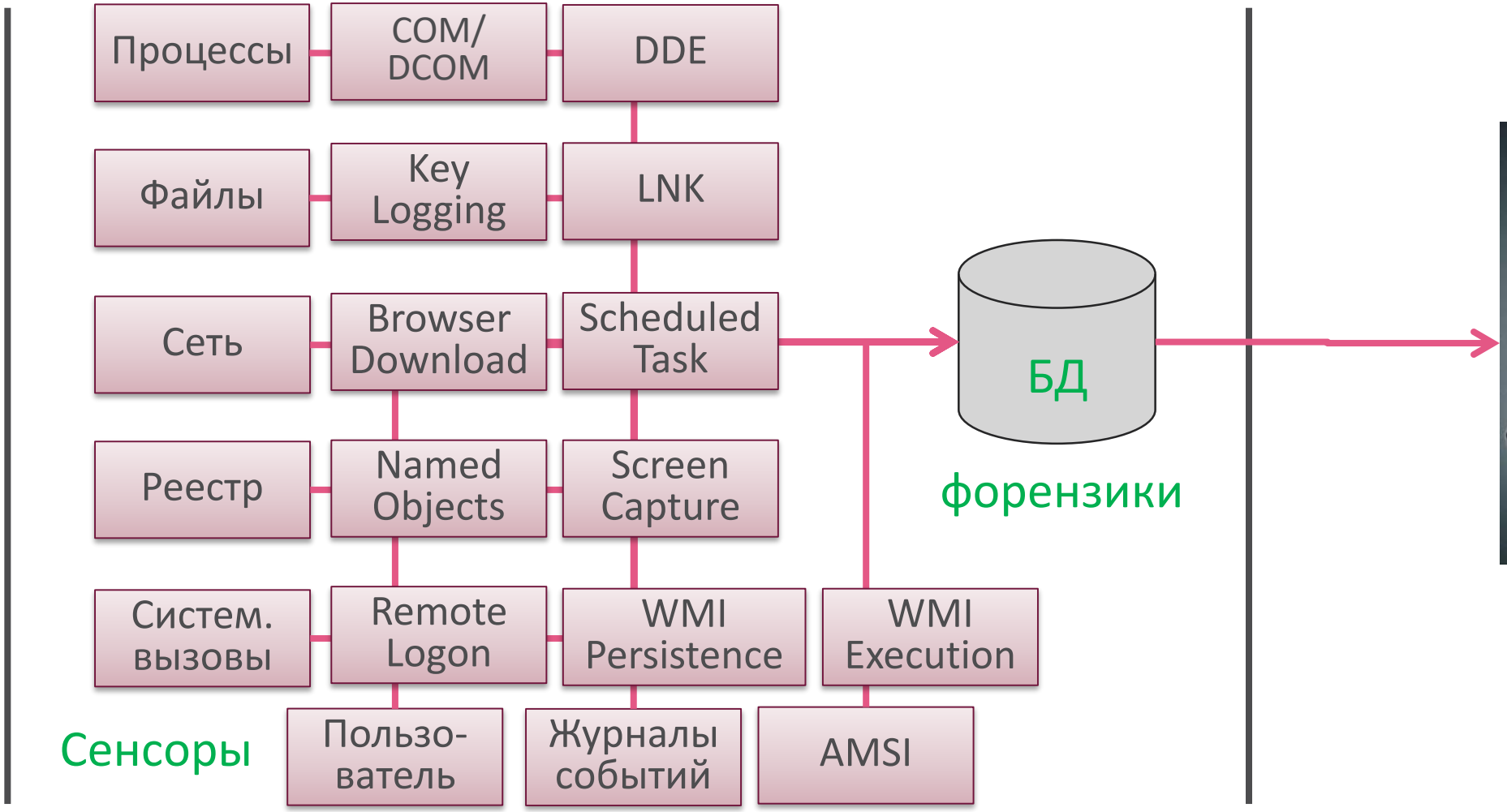
Предотвращение 97-99% атак реально!



Полноценное расследование инцидентов потребуется лишь для **1-3% атак**

EDR/XDR – важный инструмент SOC и IR

Check Point
SOFTWARE TECHNOLOGIES LTD



Incident Response

Нельзя так просто взять и расследовать инцидент

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

Особенности реагирования 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?

Check Point
SOFTWARE TECHNOLOGIES LTD

«Автономный» EDR спешит на помощь

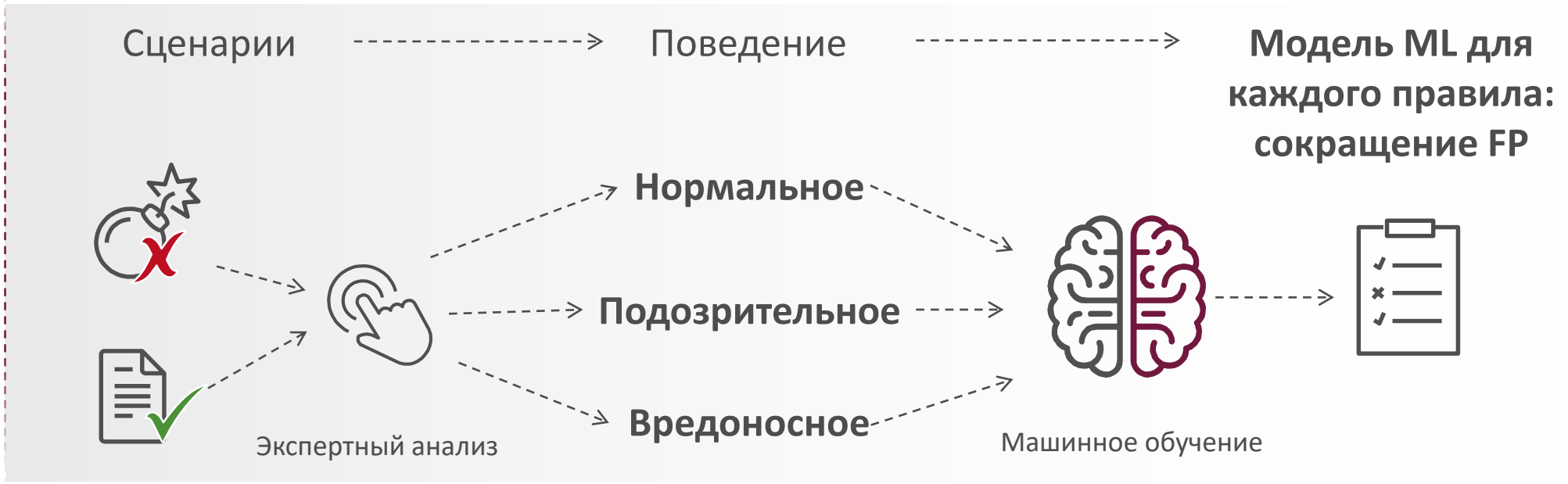
ИИ для снижения числа ложных срабатываний

Check Point
SOFTWARE TECHNOLOGIES LTD

Этап 1

Обучение

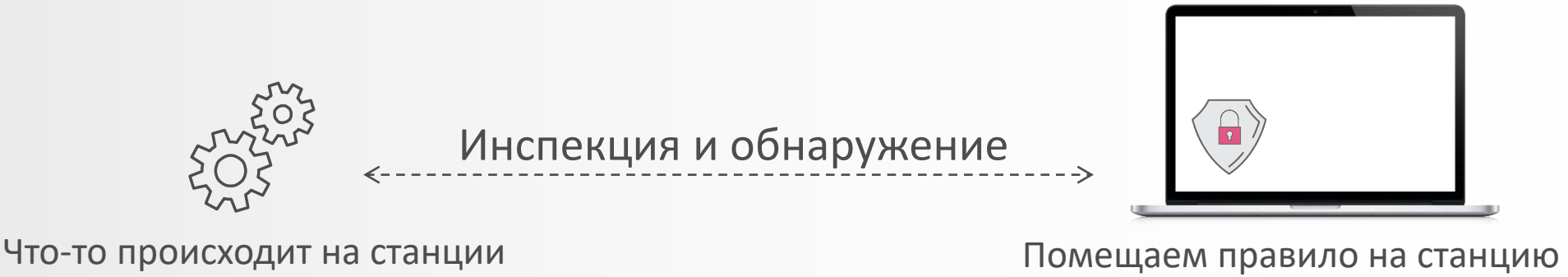
THREATCLOUD



Этап 2

Применение

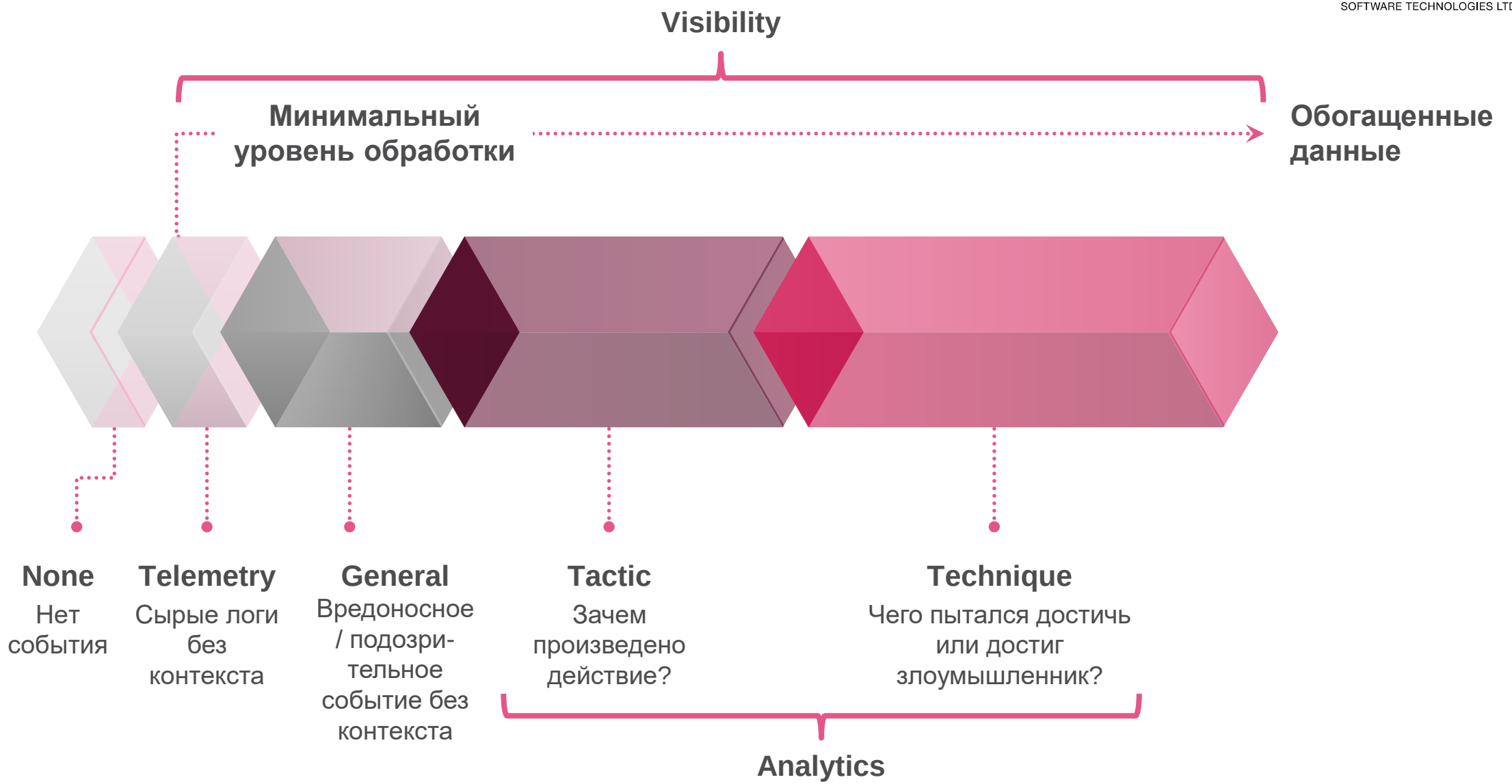
Защищенная станция

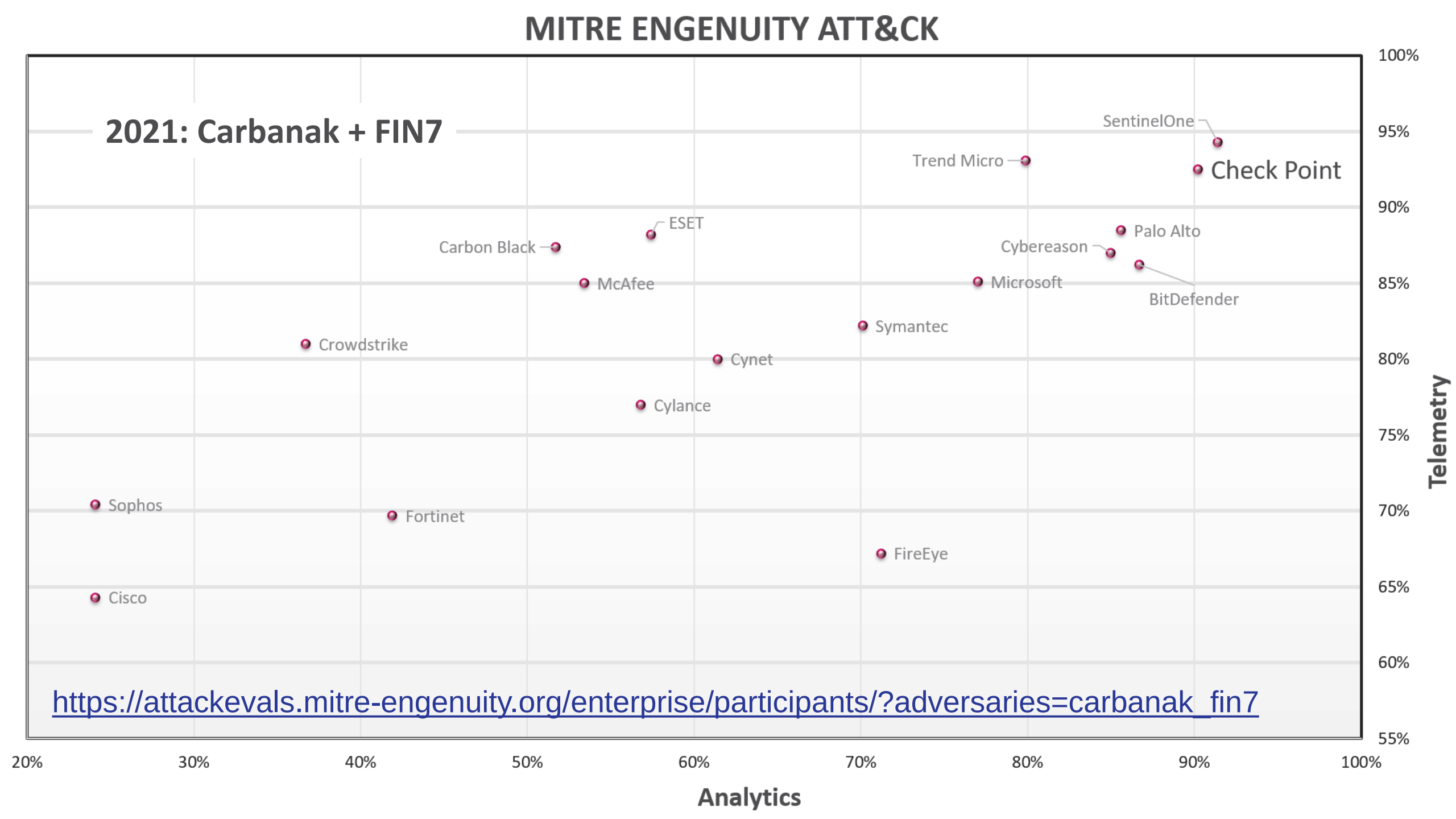


MITRE ENGENUITY | ATT&CK® Evaluations

Параметры оценки EDR

Check Point SOFTWARE TECHNOLOGIES LTD




MITRE ENGENUITY ATT&CK
2021: Carbanak + FIN7
SentinelOne
Trend Micro
Check Point
ESET
Palo Alto
Carbon Black
Cybereason
McAfee
Microsoft
BitDefender
Symantec
Crowdstrike
Cynet
Cylance
Sophos
Fortinet
FireEye
Cisco
https://attackevals.mitre-engenuity.org/enterprise/participants/?adversaries=carbanak_fin7
100%
95%
90%
85%
80%
75%
70%
65%
60%
55%
Telemetry
20%
30%
40%
50%
60%
70%
80%
90%
100%
Analytics

Примеры

Телеметрия:

Description
powershell.exe (PID: 6724) executed with arguments: C:\Users\kmitnick.financial\AppData\Roaming\TransbaseOdbcDriver\ API: BitBlt

Description
smrs.exe (PID: 2892) executed with arguments: : TYPE: External | Name: LsassOpenProcess

conhost.exe 11240
Execution through API

smrs.exe 2892
Process in AppData, Unsigned Process
Process Discovery, Execution through API

Аналитика (техники и тактики):

COLLECTION > SCREEN CAPTURE > 1 EVENT > MEDIUM SEVERITY

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation.

CREDENTIAL ACCESS > CREDENTIAL DUMPING > 1 EVENT > MEDIUM SEVERITY

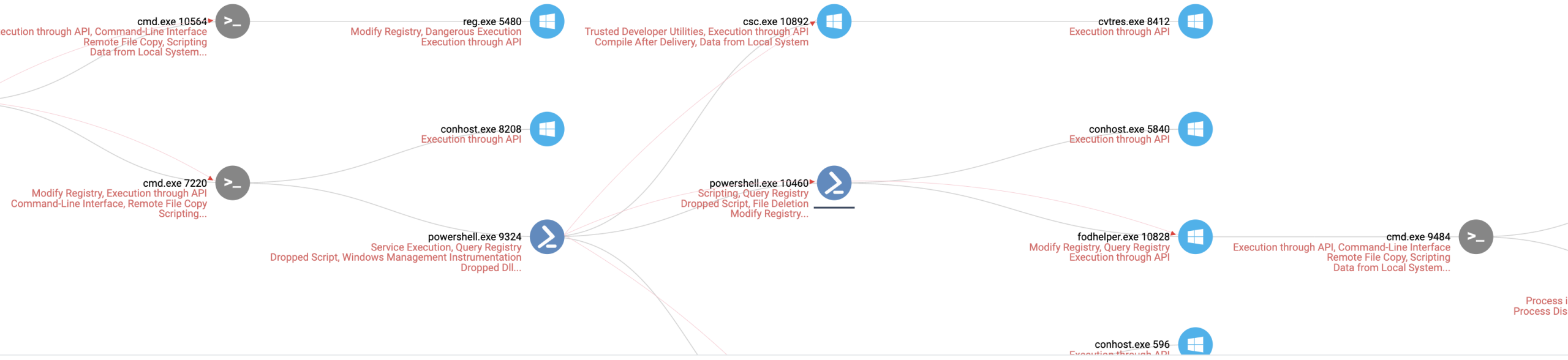
Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, then be used to perform Lateral Movement and access restricted information.

ОЧЕНЬ много кликов «мыши»!

Процессы, запущенные всего за 1 час работы станции после включения

«Автономный» EDR: Полная цепочка кибератаки. Автоматически.

Check Point
SOFTWARE TECHNOLOGIES LTD



Process | Security | Reputation | Content | File Ops (41) | Network Ops (0) | Registry Ops (6) | Injections/Objects (29) | Suspicious Events (30) | Damage (0)

Decoded Script:

```
# Example: .\uac-bypass -exe process-to-run-as-high-integrity (powershell by default)

param (
   $exe="cmd.exe /C C:\Users\kmitnick.FINANCIAL\AppData\Roaming\TransbaseOdbcDriver\smrs.exe > C:\Users\kmitnick.financial\AppData\Roaming\TransbaseOdbcDriver\MGsCOxPSNK.txt"
)

$high_integrity_binary="fodhelper.exe";
```

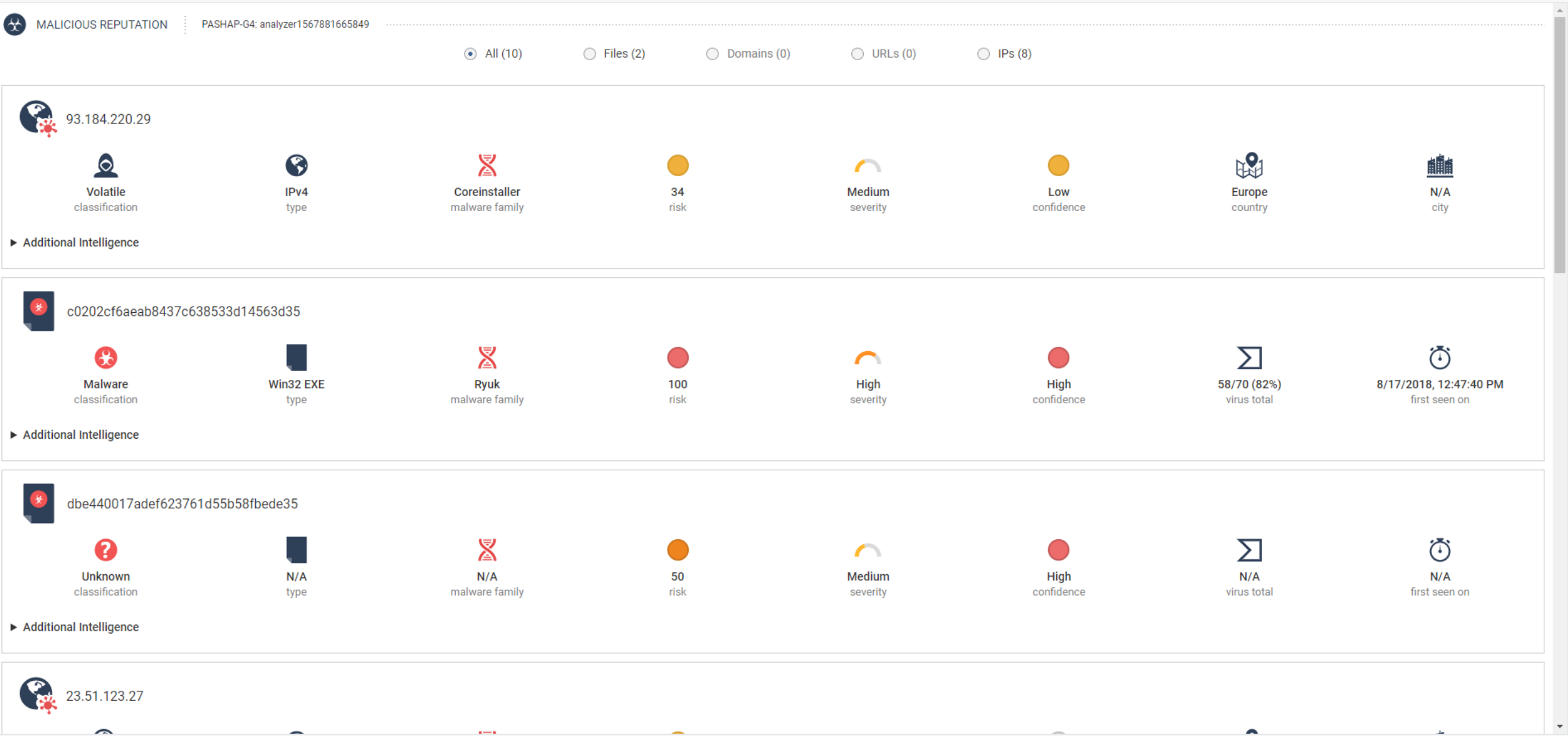
«Автономный» EDR: Полная матрица MITRE ATT&CK. Автоматически.

Check Point
SOFTWARE TECHNOLOGIES LTD

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Remote Logon Internal 1 event	Abnormal Launch 4 events	Office Application Startup 1 event	Process Injection 33 events	Code Signing 1 event	Credential Dumping 1 event	Application Window Discovery 4 events	Remote File Copy 42 events	Data from Local System 98 events	Commonly Used Port 169 events	Exfiltration Over Command and Control Channel 5 events	Process Termination 2 events
Valid Accounts 1 event	Command-Line Interface 8 events	Shortcut Modification 1 event	Valid Accounts 1 event	Compile After Delivery 1 event		File and Directory Discovery 1 event	Third-party Software 4 events	Data from Network Shared Drive 2 events	Remote File Copy 42 events		
	Execution through API 33 events	Valid Accounts 1 event		Deobfuscate/Decode Files or Information 10 events		Permission Groups Discovery 1 event		Screen Capture 1 event	Standard Application Layer Protocol 5 events		
	Execution through Module Load 25 events			Execution Guardrails 9 events		Process Discovery 8 events			Standard Cryptographic Protocol 7 events		
	PowerShell 3 events			File Deletion 4 events		Query Registry 17 events			Standard Non-Application Layer Protocol 10 events		

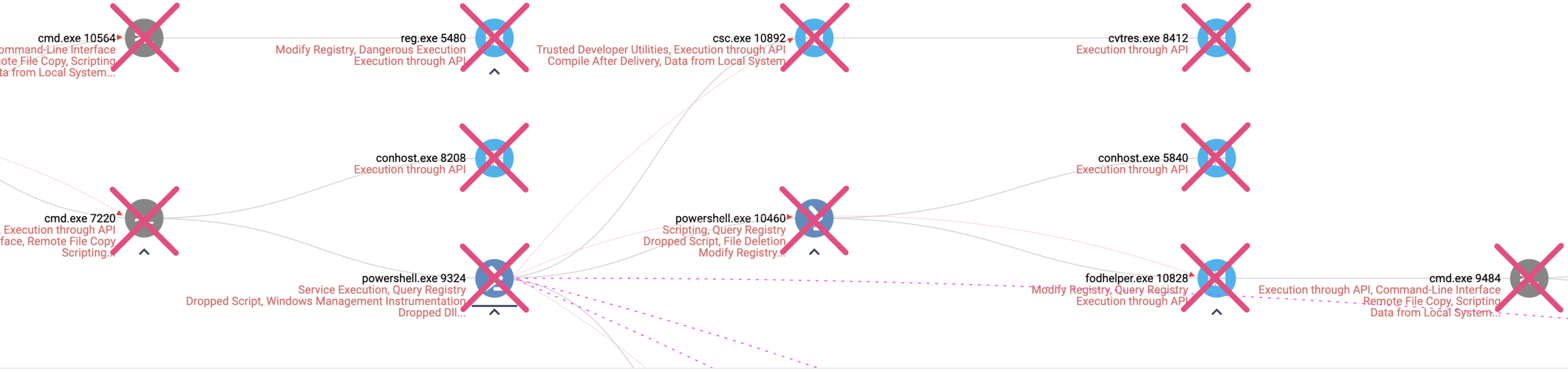
Сведения о репутации собранных IOC в одном окне

Check Point
SOFTWARE TECHNOLOGIES LTD



«Автономный» EDR: Лечение и восстановление данных. Автоматически.

Check Point
SOFTWARE TECHNOLOGIES LTD



Process | Security | Reputation | Content | File Ops (81) | Network Ops (14) | Registry Ops (4) | Injections/Objects (474) | Suspicious Events (196) | Damage (0)

Show 100 entries

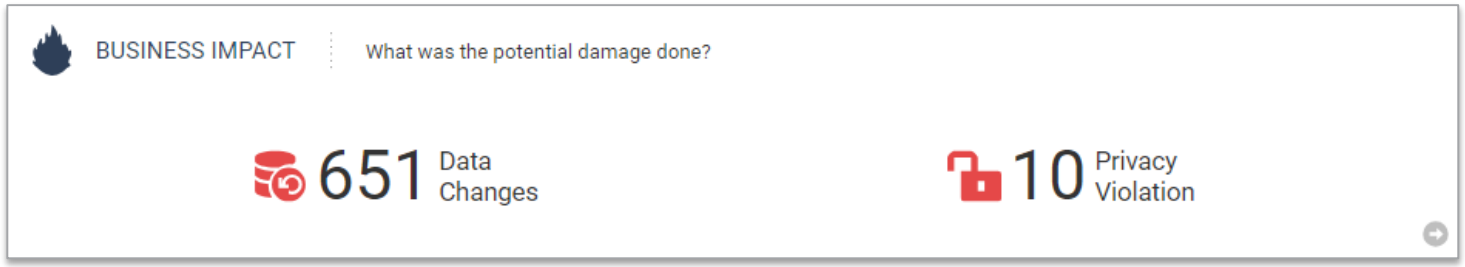
Search:

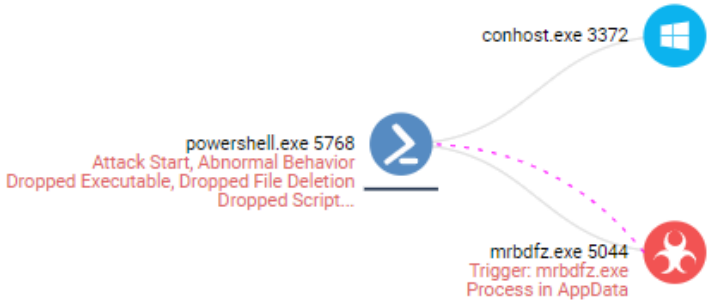
Registry Key	Action	Value	Data Old	Data New	Time
HKU\s-1-5-21-2979472553-3026127738-4227024803-500\software\microsoft\ads\providers\ldap\cn=aggregate,cn=schema,cn=configuration,dc=financial,dc=local	Delete Value Key, Query Value Key, Create Key	file			22/09/2020, 16:30:27
HKU\s-1-5-21-2979472553-3026127738-4227024803-500\software\microsoft\ads\providers\ldap\cn=aggregate,cn=schema,cn=configuration,dc=financial,dc=local	Set Value Key, Delete Value Key, Query Value Key, Create Key	file		%LOCALAPPDATA%\Microsoft\Windows\SchCache\financial.local.sch	22/09/2020, 16:30:27
HKLM\system\controlset001\services\bam\state\usersettings\s-1-5-21-2979472553-3026127738-4227024803-500	Set Value Key, Query Value Key	\device\harddiskvolume2\windows\system32\windowsp			22/09/2020, 16:33:21

Быстрое лечение – меньше ущерба

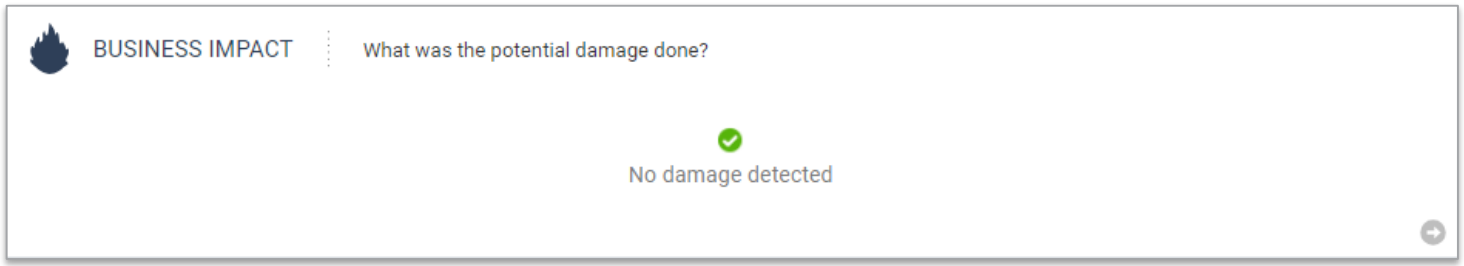
Check Point
SOFTWARE TECHNOLOGIES LTD

Классический EDR/XDR (реагирование вручную):





«Автономный» EDR:

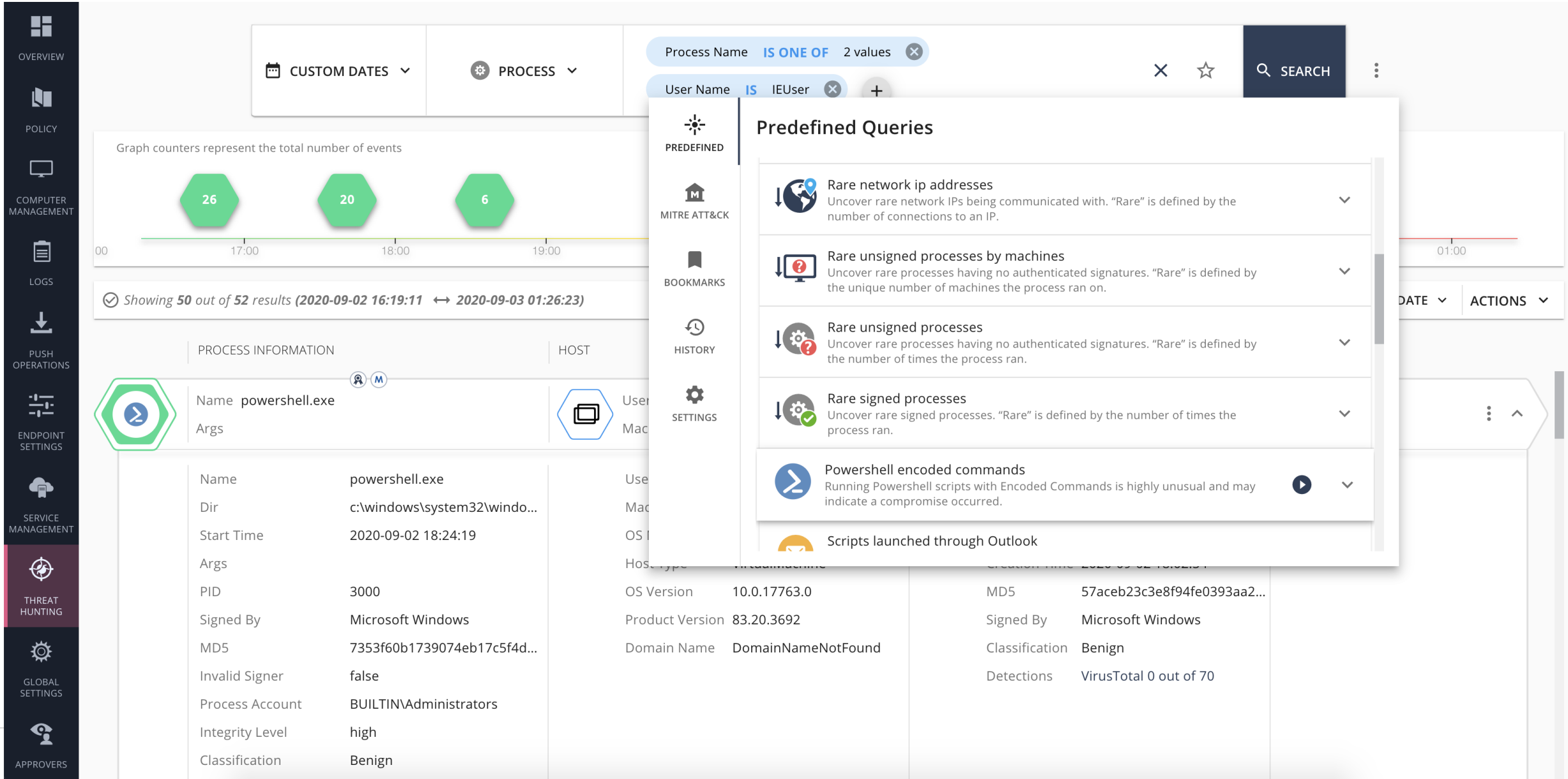


Можно так просто взять и расследовать инцидент

- 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)

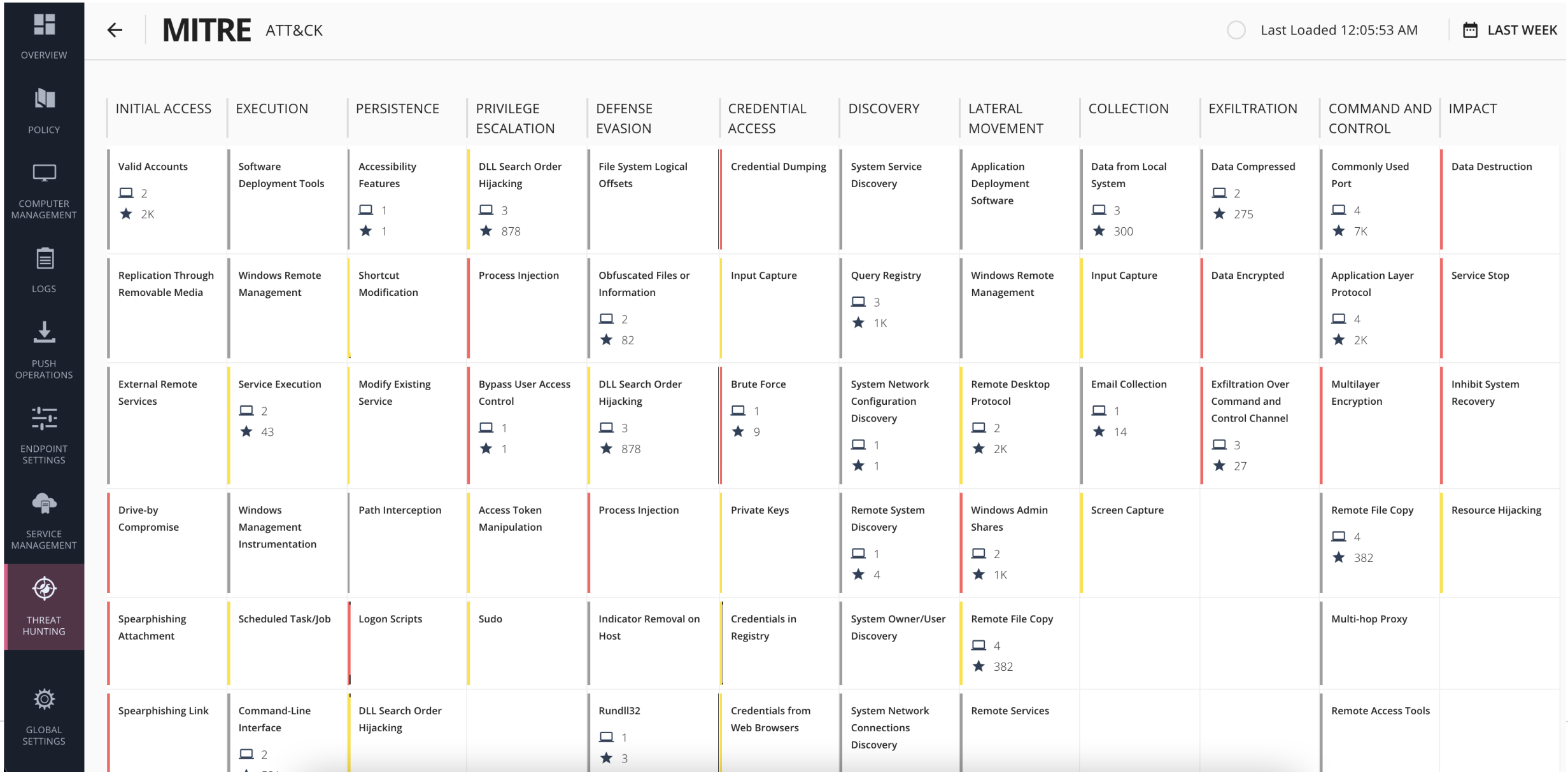
Зацепки для Threat Hunting и MDR

Check Point
SOFTWARE TECHNOLOGIES LTD



Зацепки для Threat Hunting и MDR

Check Point
SOFTWARE TECHNOLOGIES LTD



«Автономный» EDR снижает нагрузку на SOC и ускоряет решение инцидентов

Check Point
SOFTWARE TECHNOLOGIES LTD

Harmony
Endpoint

- ✓ Меньше ложных срабатываний
- ✓ Аналитика и атрибуция
- ✓ Определение всей цепочки атаки
- ✓ Лечение и восстановление данных
- ✓ Зацепки для хантинга и MDR

Пример:
2 крупных MSSP в Великобритании и Норвегии
~1 млн. рабочих станций и серверов у клиентов
На 50% ниже фин. затраты на предоставление сервисов

Check Point
SOFTWARE TECHNOLOGIES LTD

PREVENT
AI/ML
AUTOMATE

СПАСИБО

Алексей Белоглазов
Технический эксперт по защите от кибератак
abeloglazov@checkpoint.com