



Check Point
SOFTWARE TECHNOLOGIES LTD

«Автономный» EDR на службе SOC

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



WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  CHECK POINT
INFINITY

CLOUD • MOBILE • THREAT PREVENTION

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

600

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,

\$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

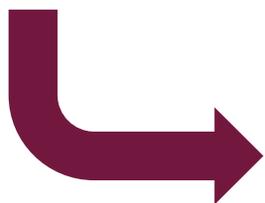
TRIPLE EXTORTION RANSOMWARE

ВСПЛЕСК АТАК ВЫМОГАТЕЛЕЙ В МИРЕ

Что происходит, когда событий в SOC слишком много

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

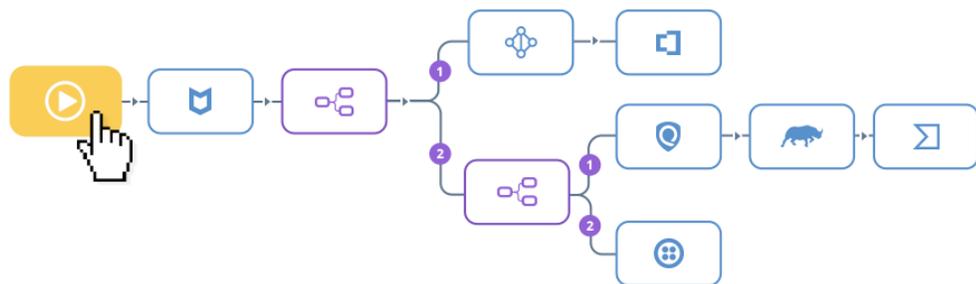
Элементы автоматизации в SOC

Снижение времени на проверку событий и реагирование



Check Point
SOFTWARE TECHNOLOGIES LTD

На макро-уровне



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

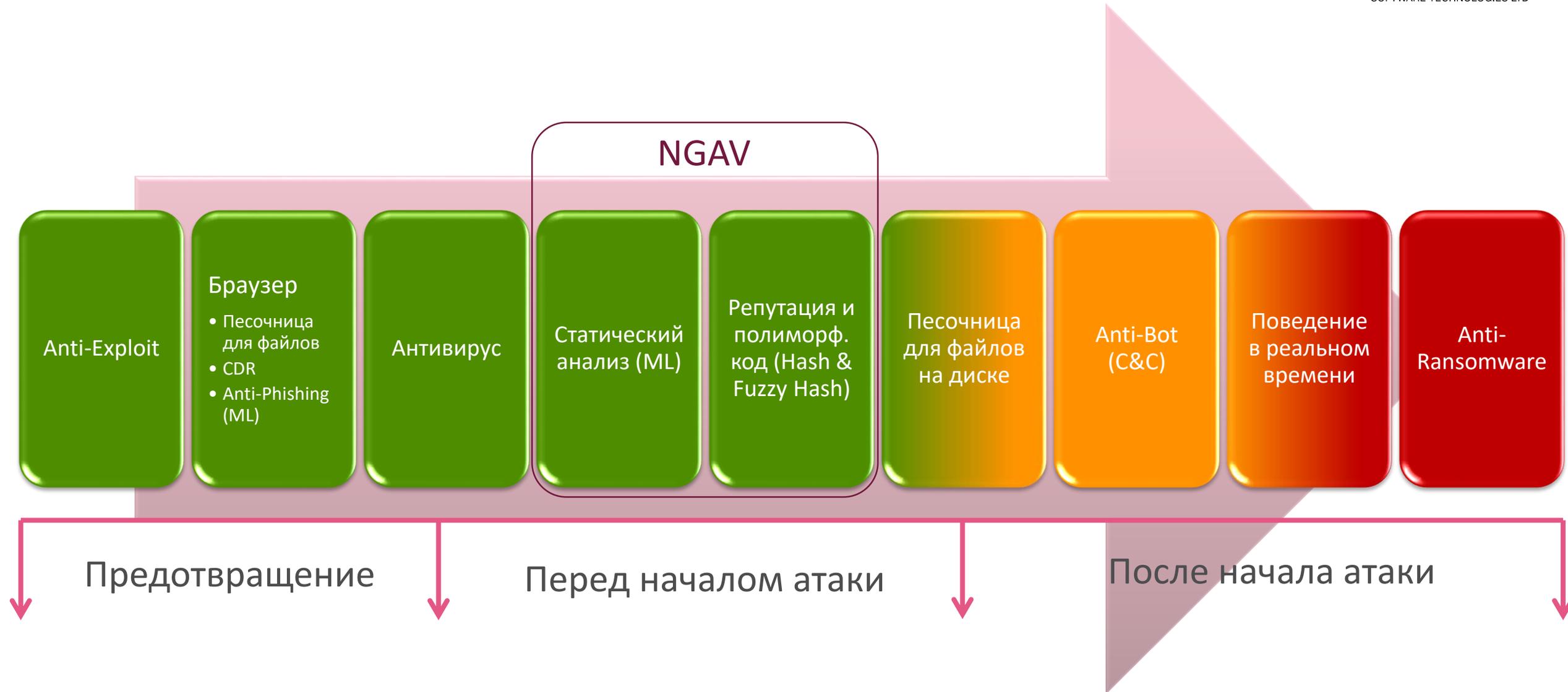
На микро-уровне



«Автономный» EDR:

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

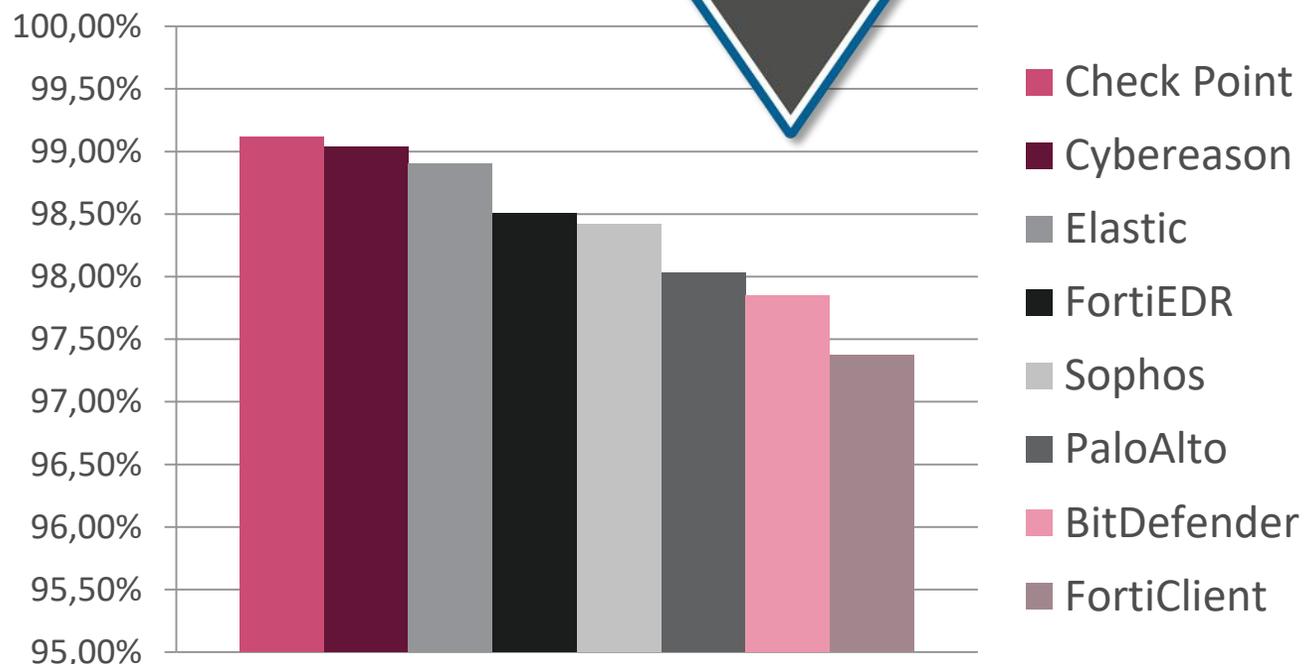
Эшелонированная защита конечных точек



NSS Labs Advanced Endpoint Protection Test 2020

Предотвращение 97-99% атак реально!

Total Block Rate

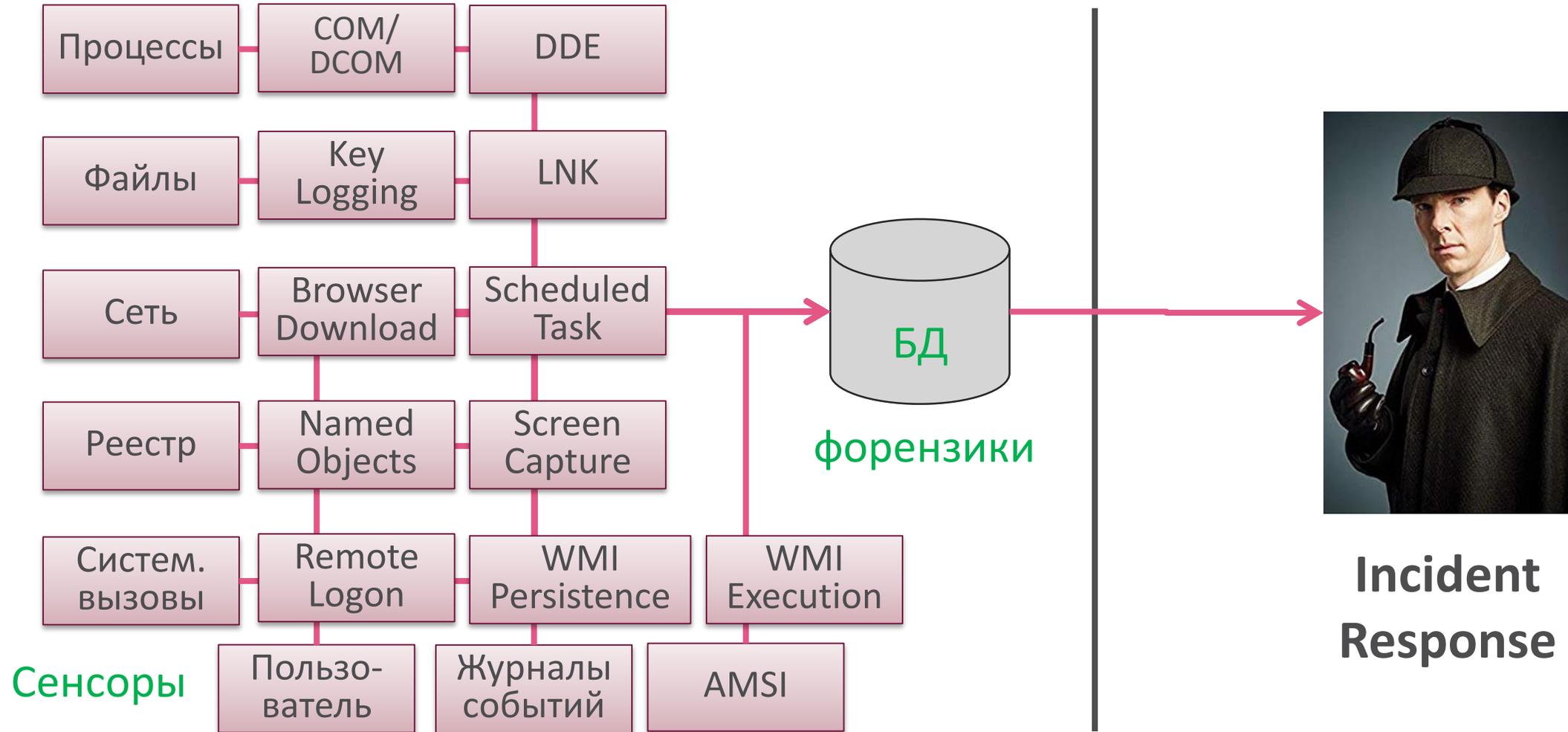


Полноценное расследование инцидентов потребуется лишь для **1-3% атак**





EDR/XDR – важный инструмент SOC и IR



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



WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  **CHECK POINT
INFINITY**

CLOUD • MOBILE • THREAT PREVENTION

ИИ для снижения числа ложных срабатываний

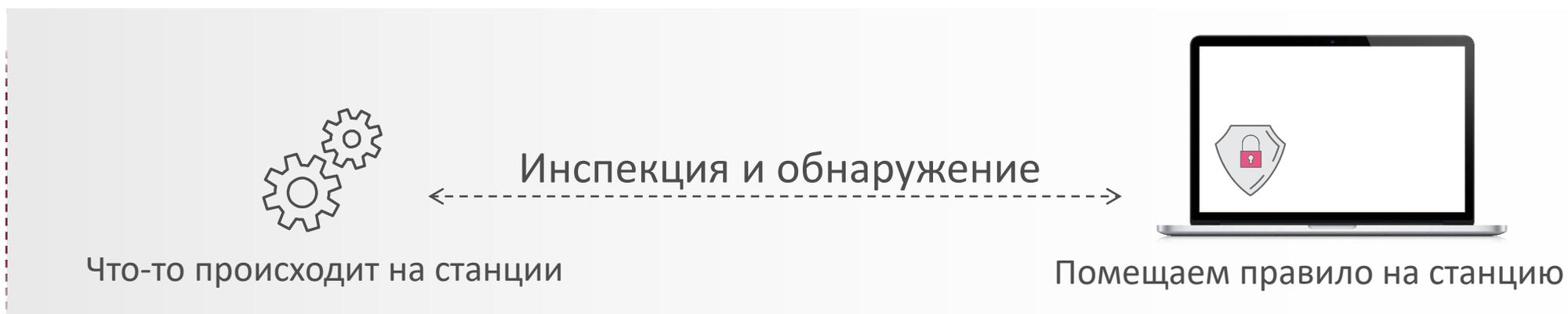


Check Point
SOFTWARE TECHNOLOGIES LTD

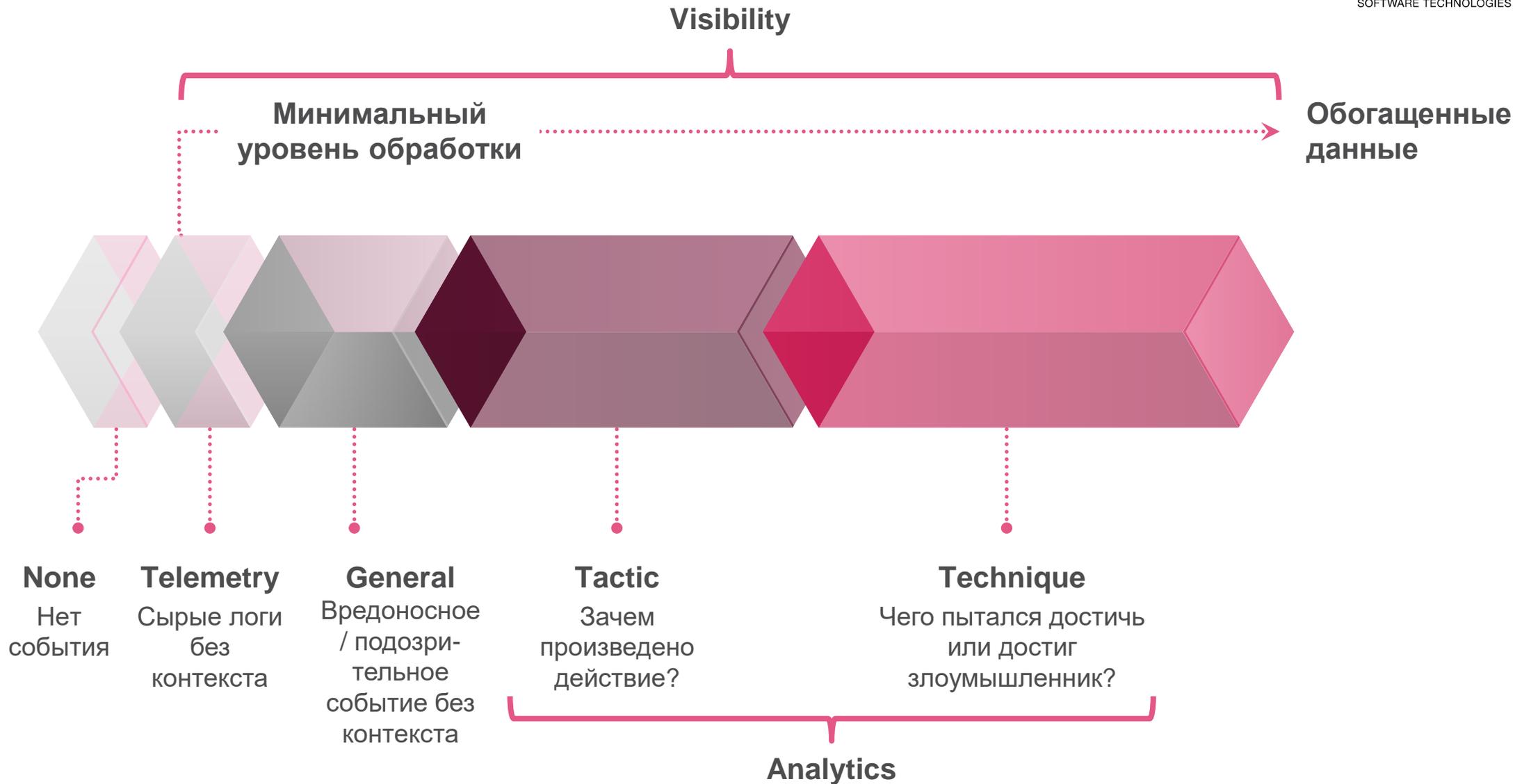
Этап 1
Обучение
THREATCLOUD



Этап 2
Применение
Защищенная станция

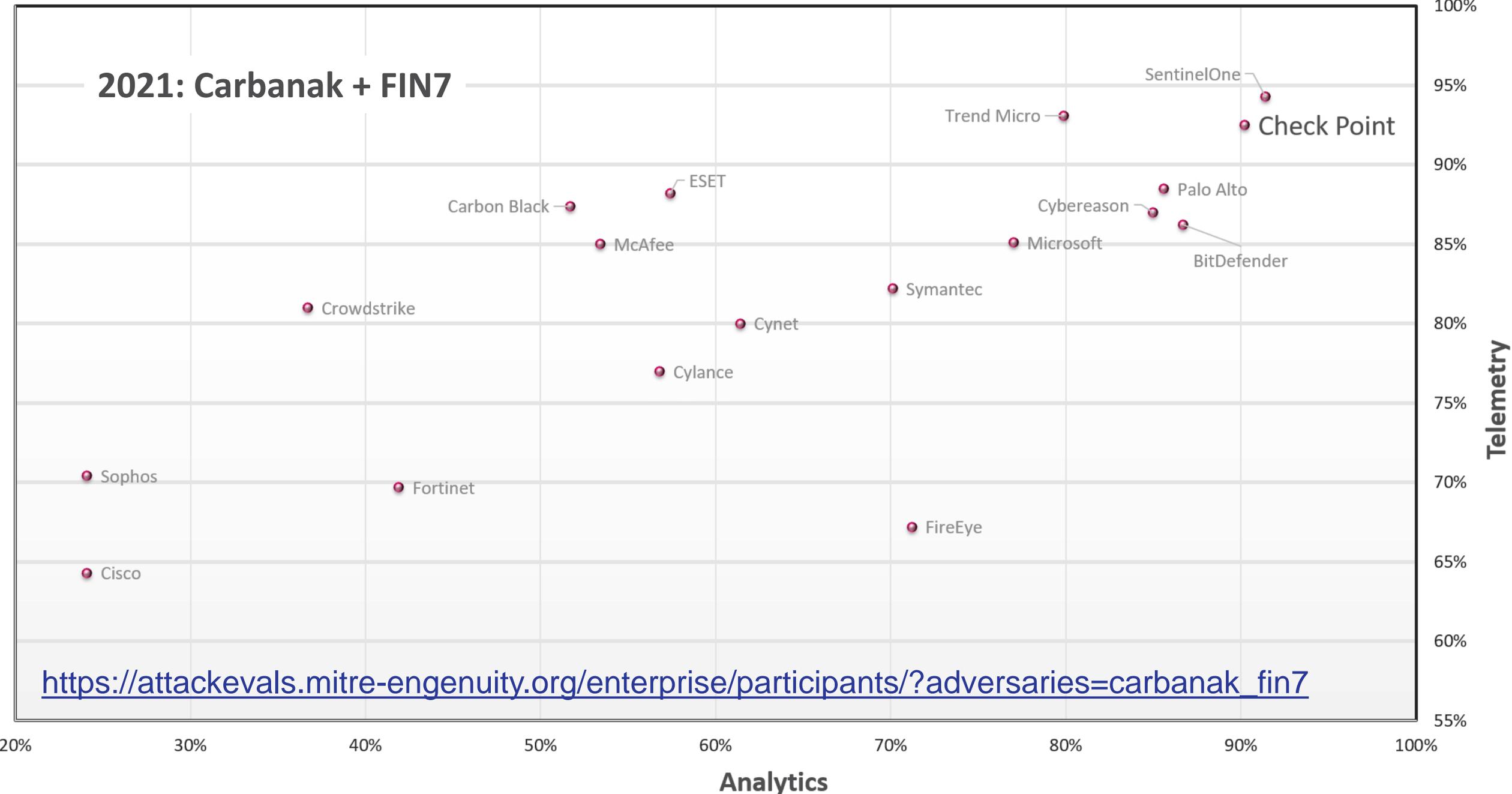


Параметры оценки EDR



MITRE ENGENUITY ATT&CK

2021: Carbanak + FIN7



https://attacker.mitre-engenuity.org/enterprise/participants/?adversaries=carbanak_fin7

Телеметрия:

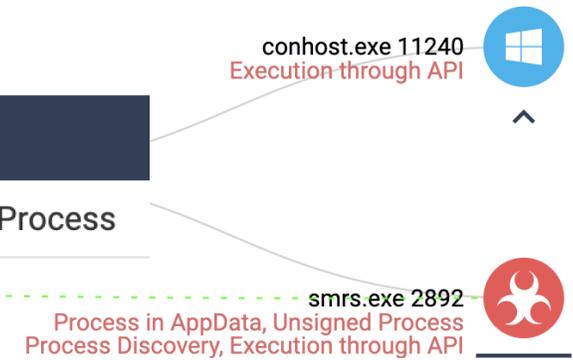
Description

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



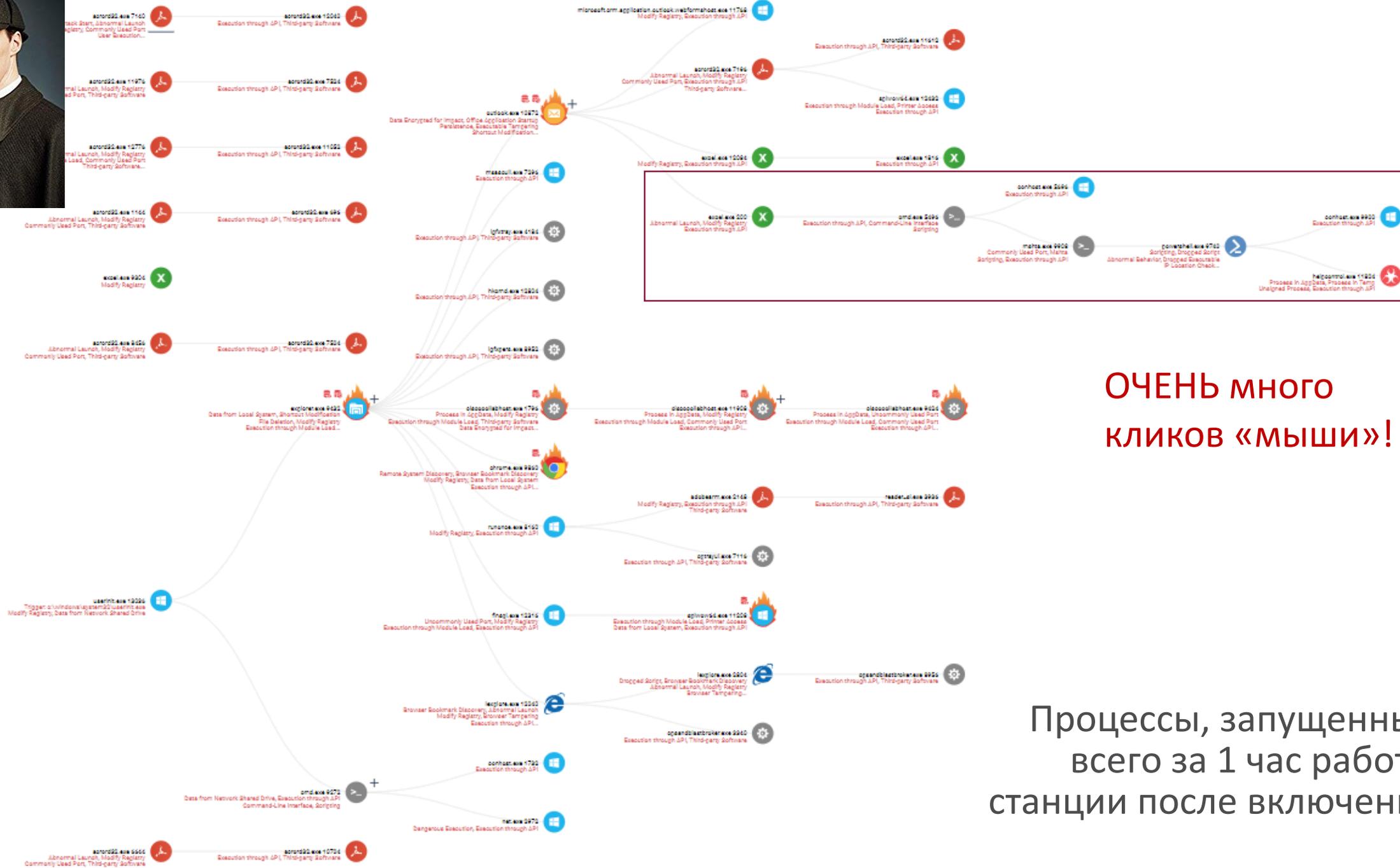
Аналитика (техники и тактики):



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



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.

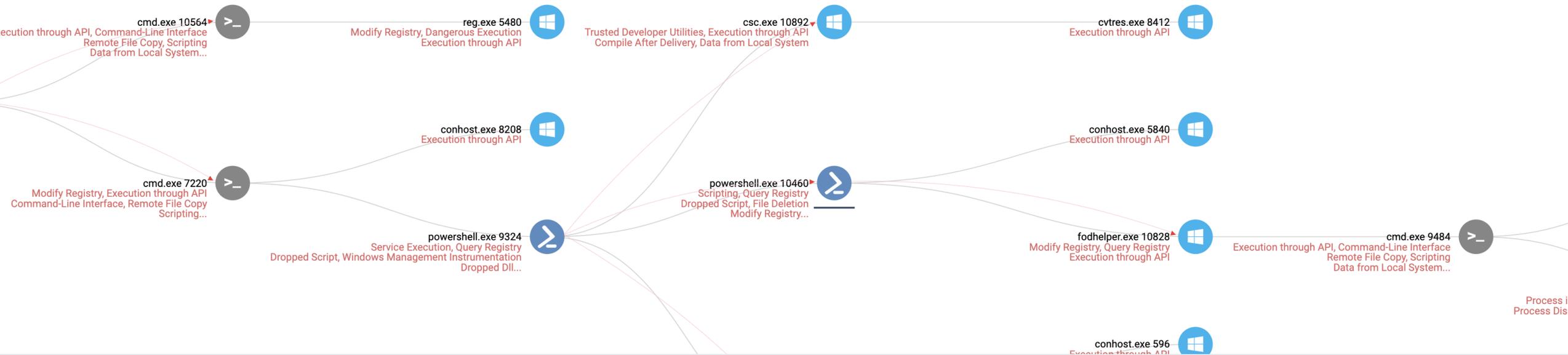


ОЧЕНЬ много
кликов «мыши»!

Процессы, запущенные
всего за 1 час работы
станции после включения



«Автономный» EDR: Полная цепочка кибератаки. Автоматически.



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.

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 ИОС в одном окне

MALICIOUS REPUTATION PASHAP-G4: analyzer1567881665849

All (10) Files (2) Domains (0) URLs (0) IPs (8)



93.184.220.29



Volatile
classification



IPv4
type



Coreinstaller
malware family



34
risk



Medium
severity



Low
confidence



Europe
country



N/A
city

► Additional Intelligence



c0202cf6aeab8437c638533d14563d35



Malware
classification



Win32 EXE
type



Ryuk
malware family



100
risk



High
severity



High
confidence



58/70 (82%)
virus total



8/17/2018, 12:47:40 PM
first seen on

► Additional Intelligence



dbe440017adef623761d55b58fbede35



Unknown
classification



N/A
type



N/A
malware family



50
risk



Medium
severity



High
confidence



N/A
virus total



N/A
first seen on

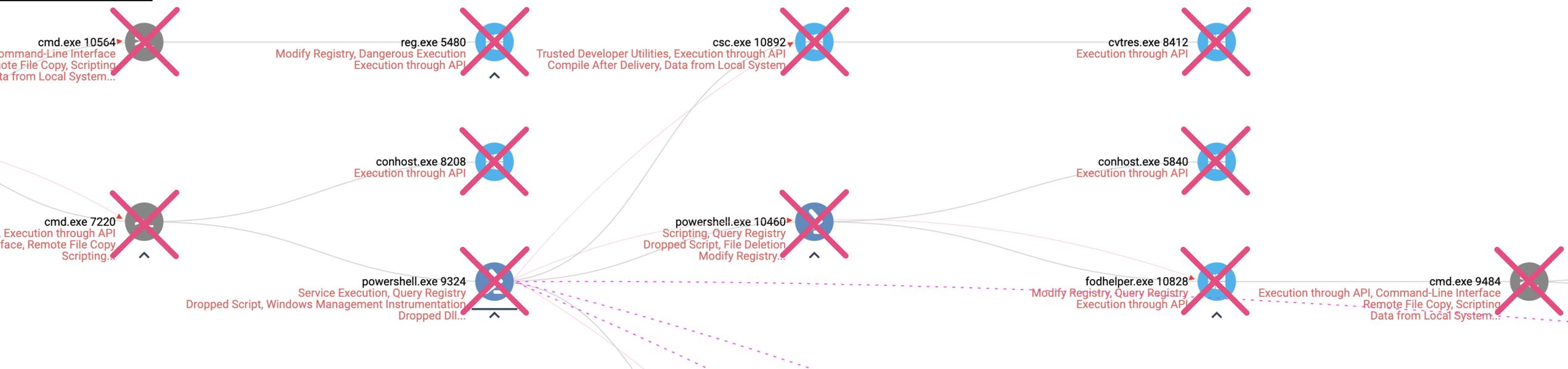
► Additional Intelligence



23.51.123.27



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



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\windows			22/09/2020, 16:33:21



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

- OVERVIEW
- POLICY
- COMPUTER MANAGEMENT
- LOGS
- PUSH OPERATIONS
- ENDPOINT SETTINGS
- SERVICE MANAGEMENT
- THREAT HUNTING
- GLOBAL SETTINGS
- APPROVERS

CUSTOM DATES | PROCESS | Process Name IS ONE OF 2 values | User Name IS IEUser | SEARCH

Graph counters represent the total number of events

26	20	6
----	----	---

Showing 50 out of 52 results (2020-09-02 16:19:11 ↔ 2020-09-03 01:26:23)

PREDEFINED

- Rare network ip addresses
- Rare unsigned processes by machines
- Rare unsigned processes
- Rare signed processes
- Powershell encoded commands
- Scripts launched through Outlook

PROCESS INFORMATION | HOST

Name	powershell.exe	User	IEUser
Dir	c:\windows\system32\windo...	Mac	Mac
Start Time	2020-09-02 18:24:19	OS	OS
Args		Host type	Windows
PID	3000	OS Version	10.0.17763.0
Signed By	Microsoft Windows	Product Version	83.20.3692
MD5	7353f60b1739074eb17c5f4d...	Domain Name	DomainNameNotFound
Invalid Signer	false	MD5	57aceb23c3e8f94fe0393aa2...
Process Account	BUILTIN\Administrators	Signed By	Microsoft Windows
Integrity Level	high	Classification	Benign
Classification	Benign	Detections	VirusTotal 0 out of 70

Зацепки для Threat Hunting и MDR



Check Point
SOFTWARE TECHNOLOGIES LTD

MITRE ATT&CK											
INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND AND CONTROL	IMPACT
Valid Accounts 2 ★ 2K	Software Deployment Tools	Accessibility Features 1 ★ 1	DLL Search Order Hijacking 3 ★ 878	File System Logical Offsets	Credential Dumping	System Service Discovery	Application Deployment Software	Data from Local System 3 ★ 300	Data Compressed 2 ★ 275	Commonly Used Port 4 ★ 7K	Data Destruction
Replication Through Removable Media	Windows Remote Management	Shortcut Modification	Process Injection	Obfuscated Files or Information 2 ★ 82	Input Capture	Query Registry 3 ★ 1K	Windows Remote Management	Input Capture	Data Encrypted	Application Layer Protocol 4 ★ 2K	Service Stop
External Remote Services	Service Execution 2 ★ 43	Modify Existing Service	Bypass User Access Control 1 ★ 1	DLL Search Order Hijacking 3 ★ 878	Brute Force 1 ★ 9	System Network Configuration Discovery 1 ★ 1	Remote Desktop Protocol 2 ★ 2K	Email Collection 1 ★ 14	Exfiltration Over Command and Control Channel 3 ★ 27	Multilayer Encryption	Inhibit System Recovery
Drive-by Compromise	Windows Management Instrumentation	Path Interception	Access Token Manipulation	Process Injection	Private Keys	Remote System Discovery 1 ★ 4	Windows Admin Shares 2 ★ 1K	Screen Capture		Remote File Copy 4 ★ 382	Resource Hijacking
Spearphishing Attachment	Scheduled Task/Job	Logon Scripts	Sudo	Indicator Removal on Host	Credentials in Registry	System Owner/User Discovery	Remote File Copy 4 ★ 382			Multi-hop Proxy	
Spearphishing Link	Command-Line Interface 2	DLL Search Order Hijacking		Rundll32 1 ★ 3	Credentials from Web Browsers	System Network Connections Discovery	Remote Services			Remote Access Tools	

Last Loaded 12:05:53 AM | LAST WEEK

- OVERVIEW
- POLICY
- COMPUTER MANAGEMENT
- LOGS
- PUSH OPERATIONS
- ENDPOINT SETTINGS
- SERVICE MANAGEMENT
- THREAT HUNTING
- GLOBAL SETTINGS

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



- ✓ 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

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  CHECK POINT
INFINITY

CLOUD • MOBILE • THREAT PREVENTION