Статистика и практика инцидентов ИБ

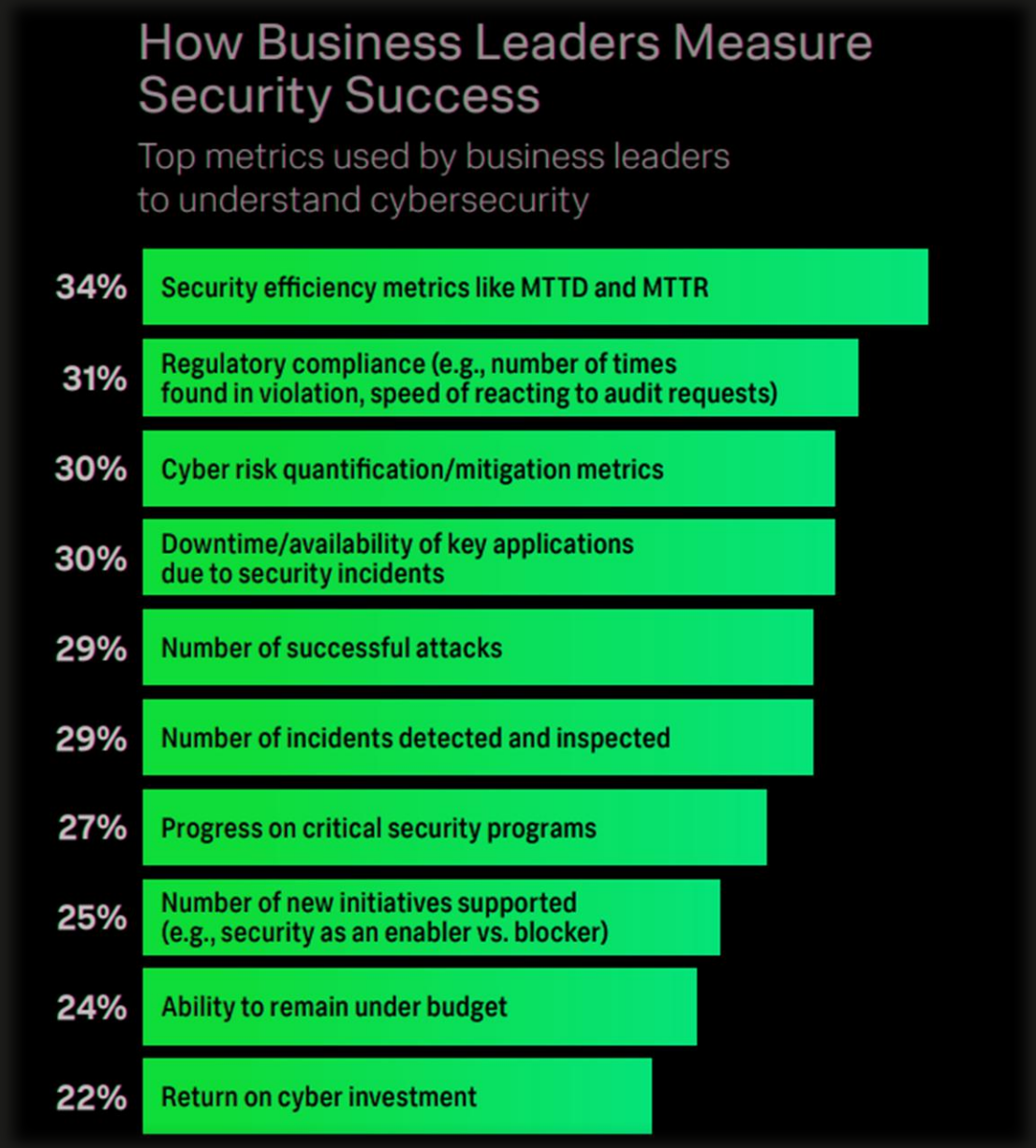
Борис Осепов,
старший инженер
предпродажной поддержки

kaspersky

Forbes. ТОП-200 наиболее "киберзащищенных" компаний США

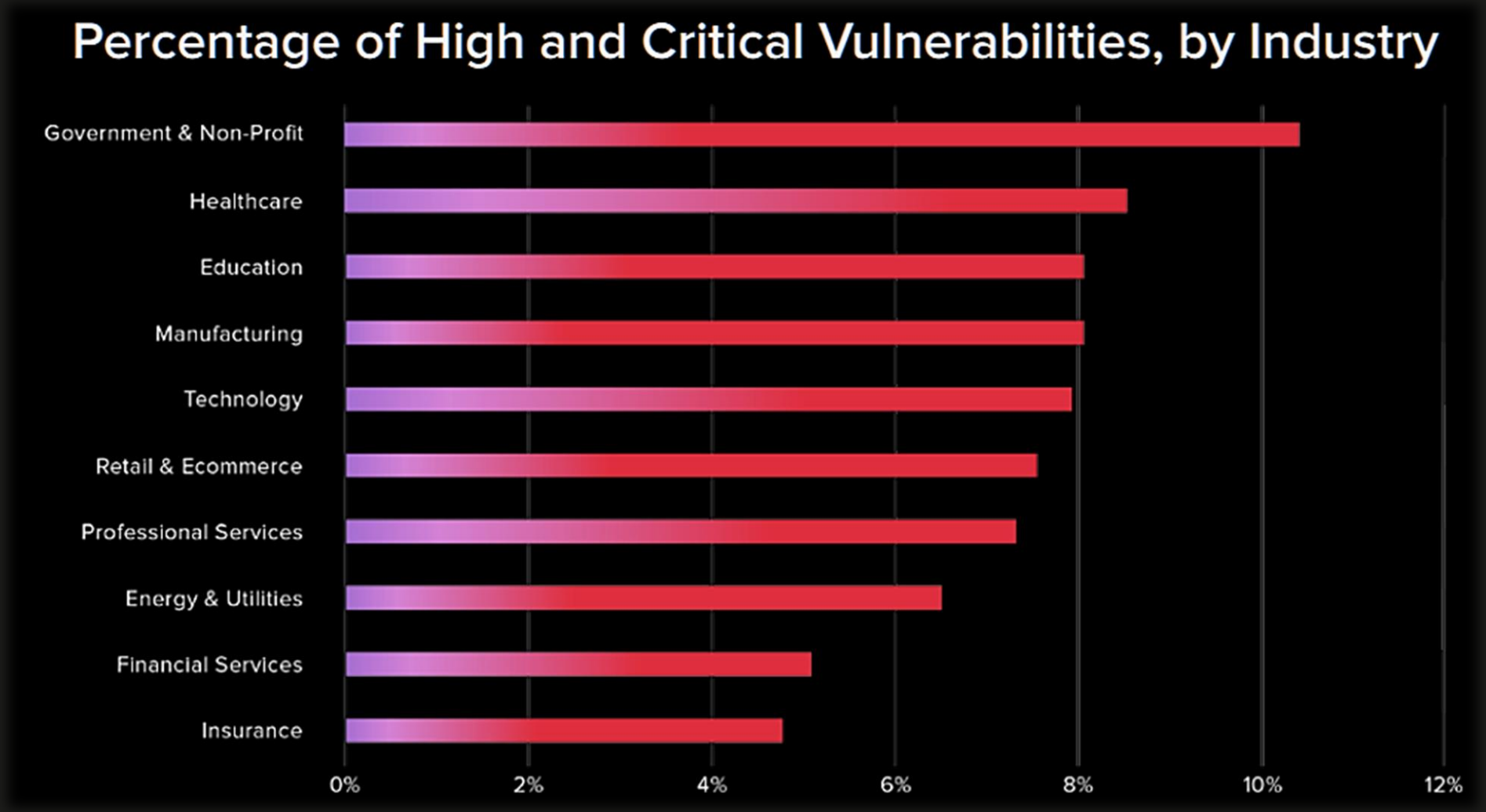
https://www.forbes.com/lists/most-cybersecure-companies/

Успешное ИБ, это что?



https://www.splunk.com/en_us/pdfs/gated/ebooks/state-of-security-2023.pdf

Статистика по уязвимостям на основе 300k пентестов



https://www.netspi.com/wp-content/uploads/netspi-offensive-security-vision-report-2023.pdf

Время закрытия критической уязвимости по регламенту

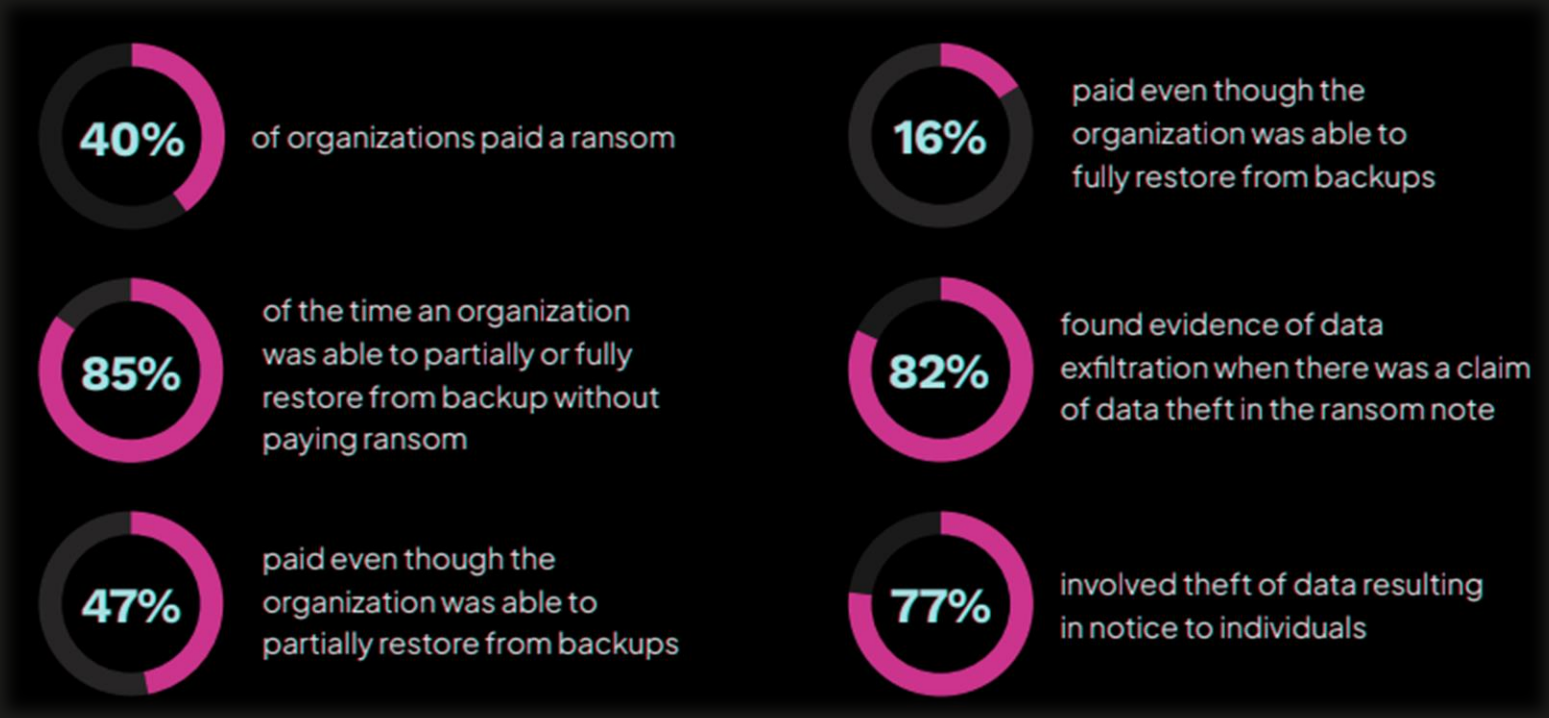
https://www.cisa.gov/news-events/directives/binding-operational-directive-19-02
https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-17-maya-2023-g

Цифры и статистика по шифровальщикам

Largest Ransom Demand in 2022:
$90+ million
($60+ million in 2021)

Largest Ransom Paid in 2022:
$8+ million
($5.5 million in 2021)

Average Ransom Paid in 2022:
$600,688
($511,957 in 2021)



https://www.bakerlaw.com/webfiles/2023%20DSIR%20Report.pdf

Цифры и статистика по шифровальщикам

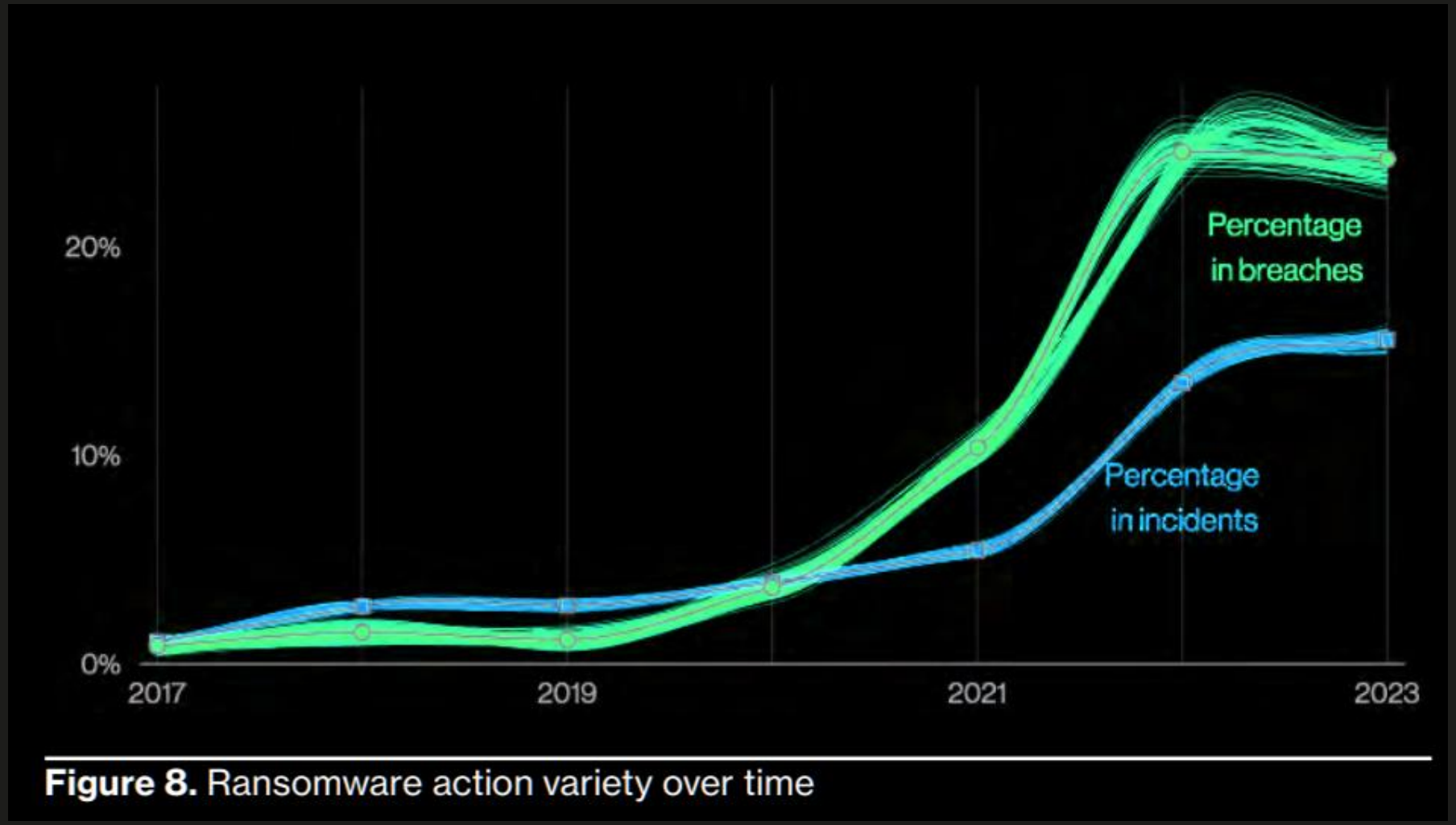
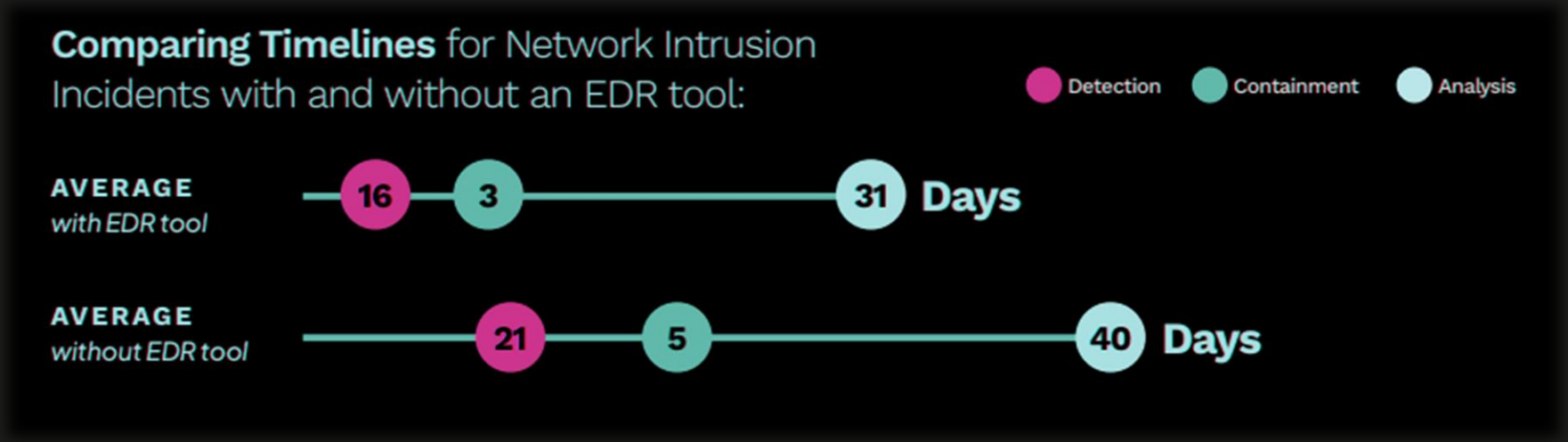


Figure 8. Ransomware action variety over time

https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

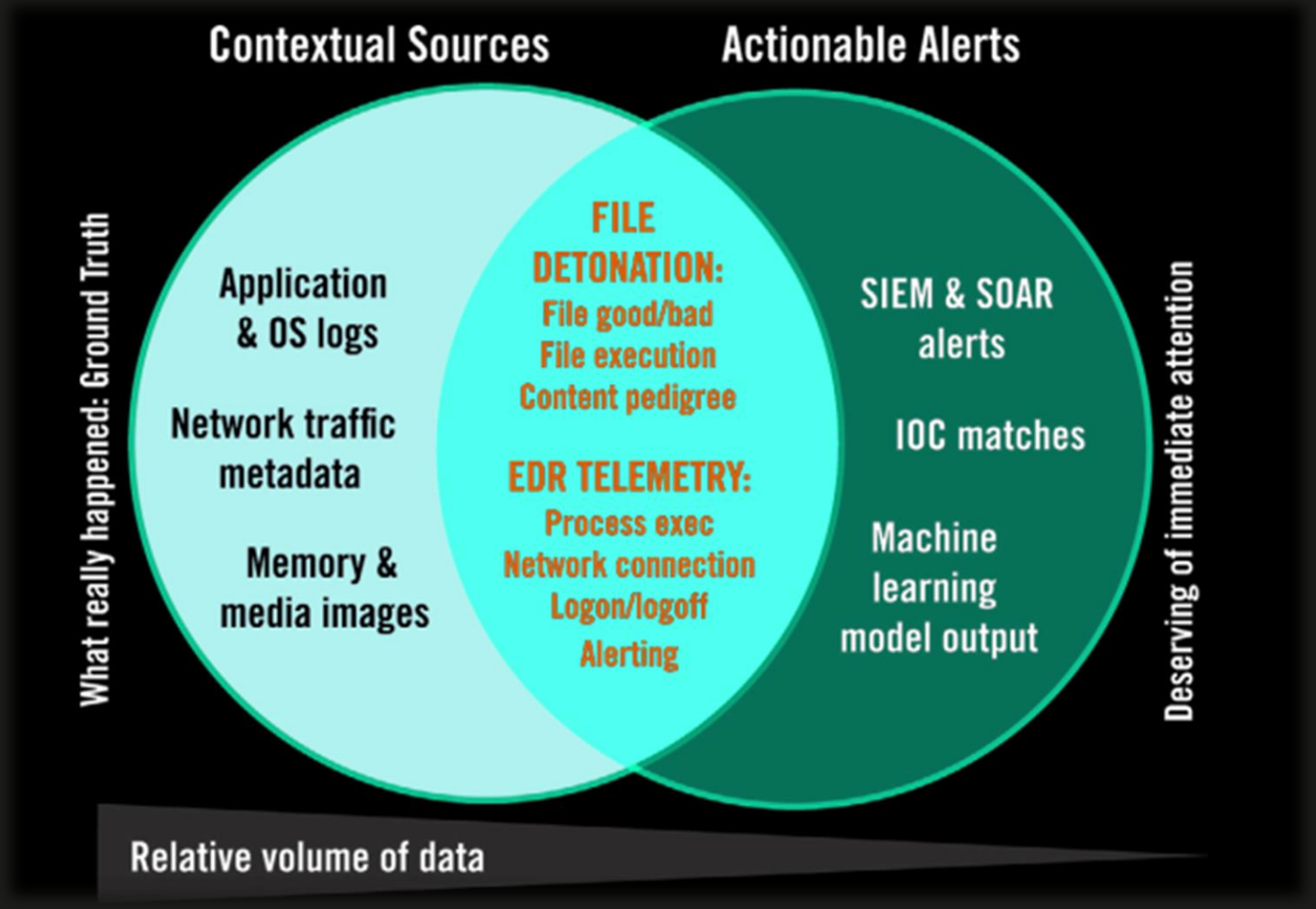
Что помогает?



Улучшение метрик на 22,5 %

https://www.bakerlaw.com/webfiles/2023%20DSIR%20Report.pdf

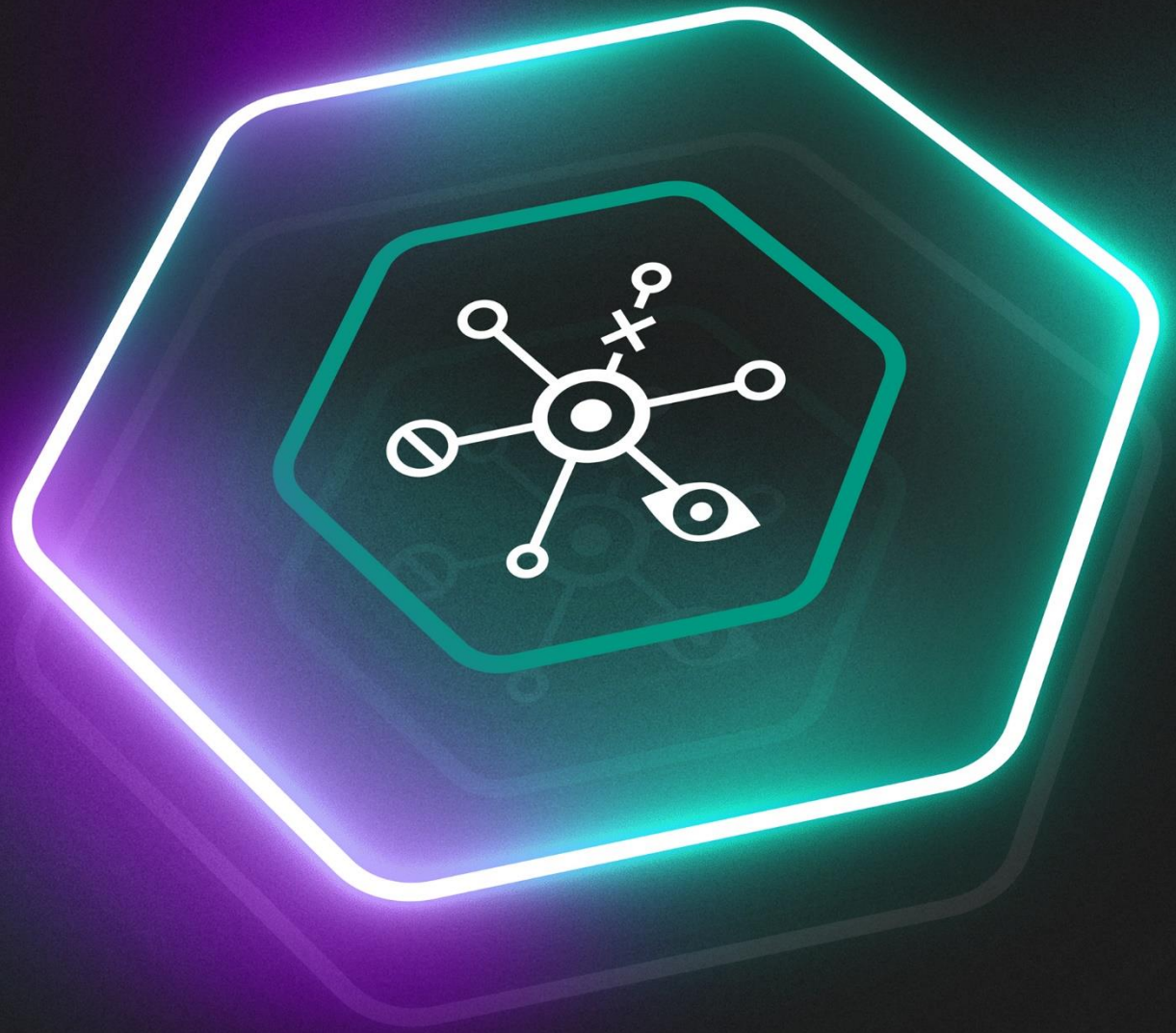
Что помогает?



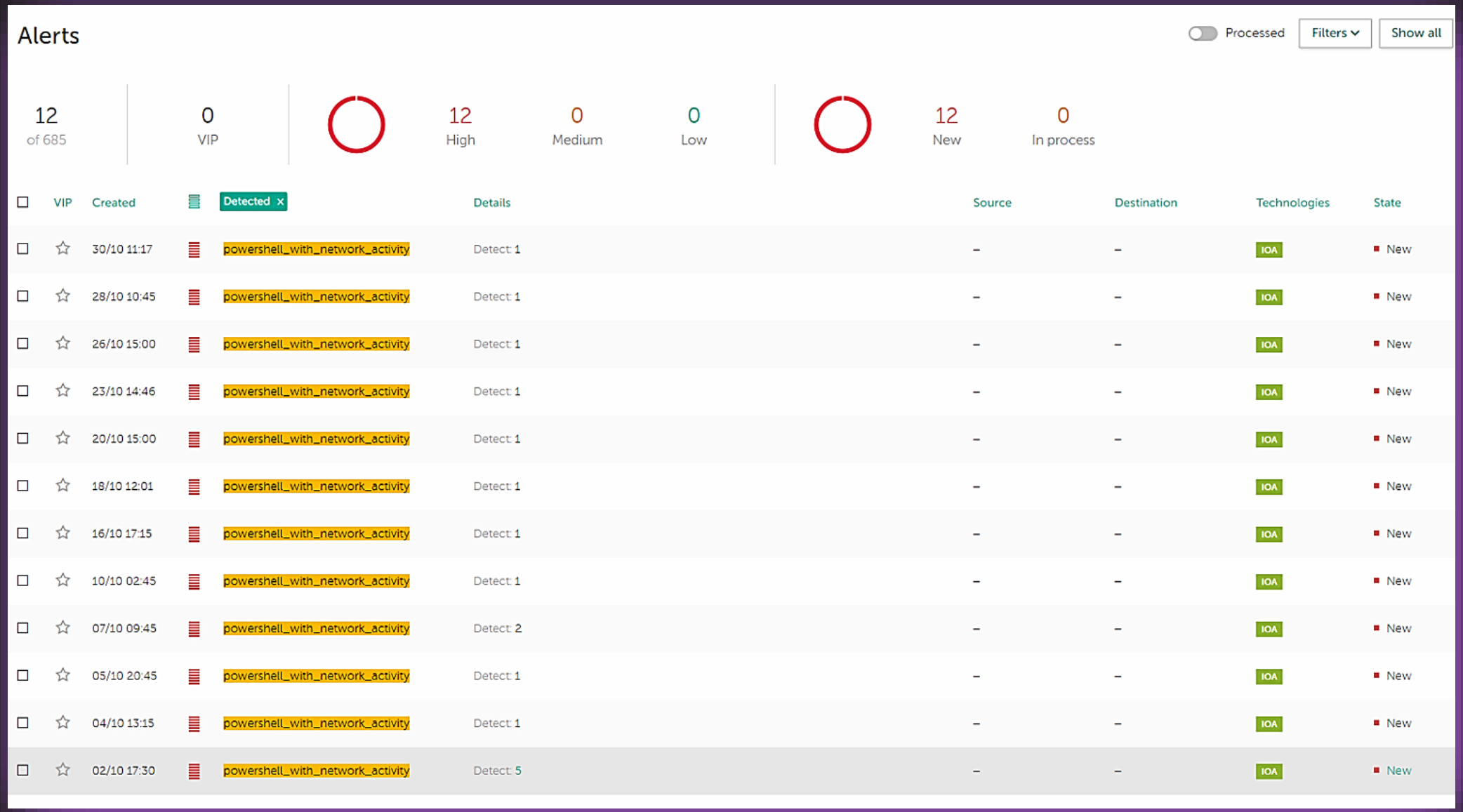
https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Больше тренировок!

Реальный кейс на пилоте (окт 2019)



Находим первое проявление PowerShell с сетевой активностью



Находим очень подозрительную проверку доступности ресурса

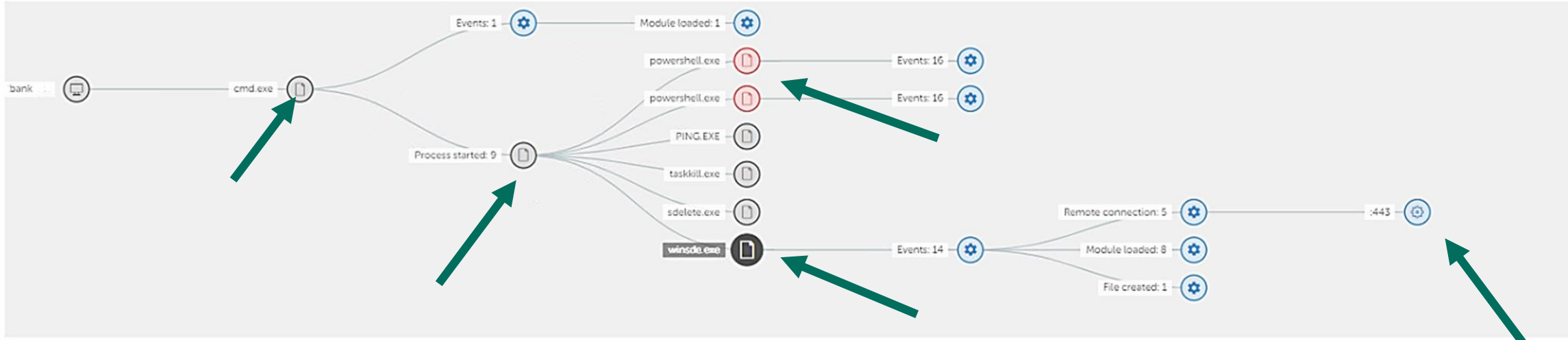
Process started

IOA tags	suspicious_powershell_cmdline_downloading, powershell_with_network_activity
Event time	03 October 2019 02:20
File	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Launch parameters	powershell try{$ip='216.58.213.142';$es=New-Object System.Net.Sockets.TcpClient($ip,443);Write-Host '[OK]';}catch{Write-Host '[FAIL]';}
MD5	92f44e405db16ac55d97e3bfe3b132fa
SHA256	6c05e11399b7e3c8ed31bae72014cf249c144a8f4a2c54a758eb2e6fad47aec7
Size	442 KB
Process ID	5012
Process end time	03 October 2019 02:20
Time created	14 July 2009 04:32

Parent process

File	C:\Windows\System32\cmd.exe
MD5	ad7b9c14083b52bc532fba5948342b98
SHA256	17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae
Process ID	9564

Раскрываем ветки активности и смотрим проявление всей активности



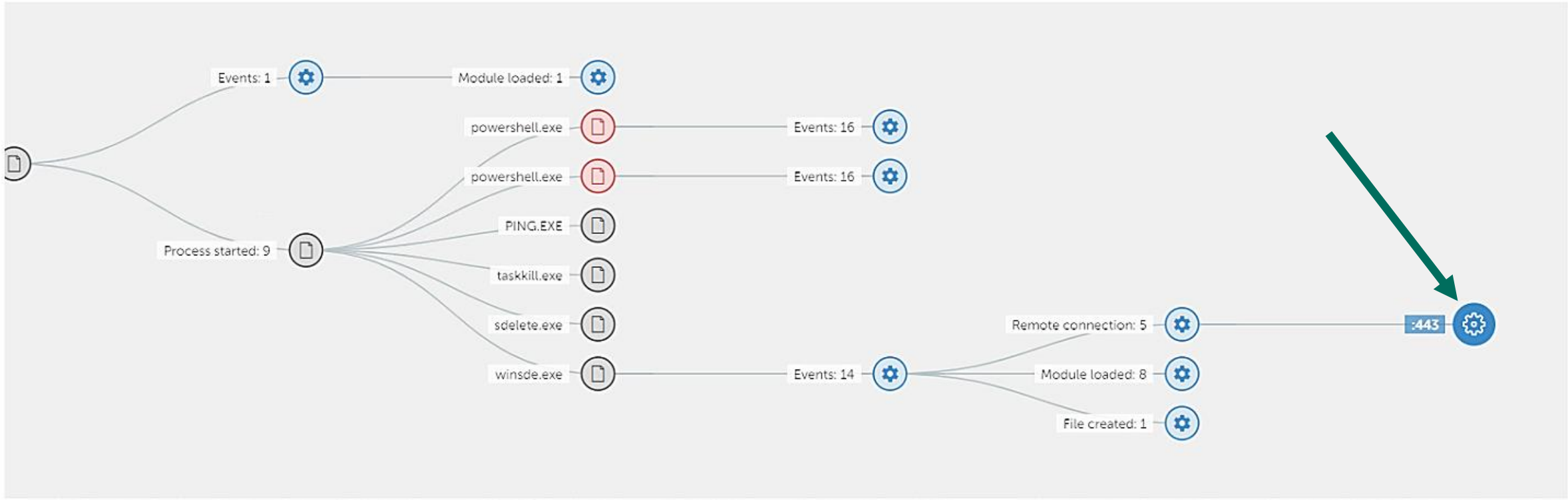
Process started

Event time	02 October 2019 17:08
File	C:\PerfLogs\winsde.exe
Launch parameters	ping 192.168.10.55 -n 1
MD5	6242e3d67787ccbf4e06ad2982853144
SHA256	4ca10dba7ff487fdb3f1362a3681d7d929f5aa1262cdfd31b04c30826983fb1d
Size	55 KB
Process ID	3796

Parent process

File	C:\Windows\System32\cmd.exe
MD5	ad7b9c14083b52bc532fba5948342b98
SHA256	17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae
Process ID	5132

Проверим сетевое обращение от winsde.exe



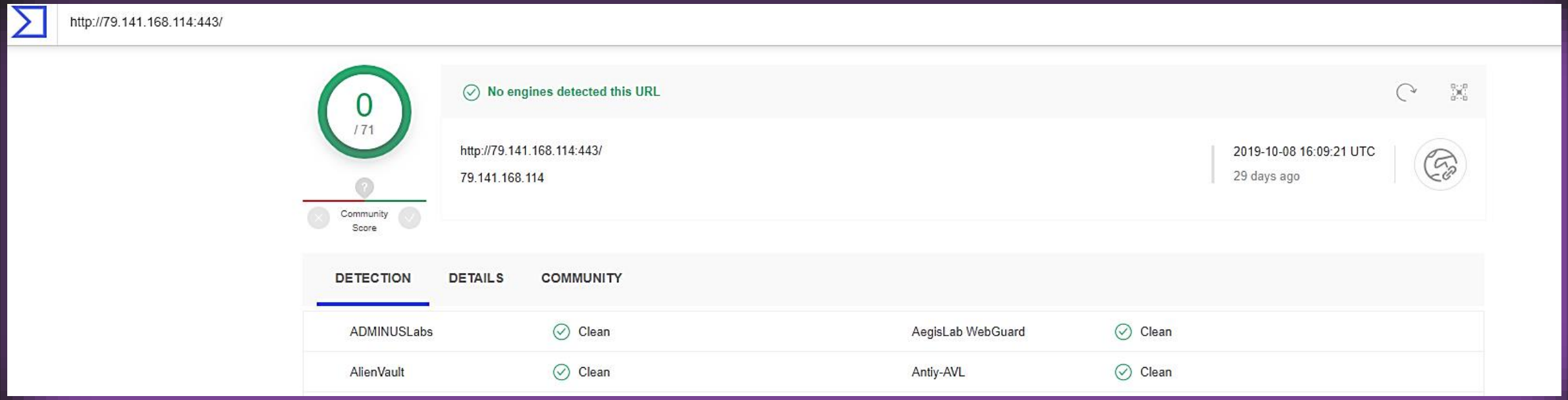
Remote connection

Event time	02 October 2019 17:09
Remote IP	79.141.168.114:443
Local IP	192.168.178.114
Host name	[redacted]
User name	NT AUTHORITY\SYSTEM

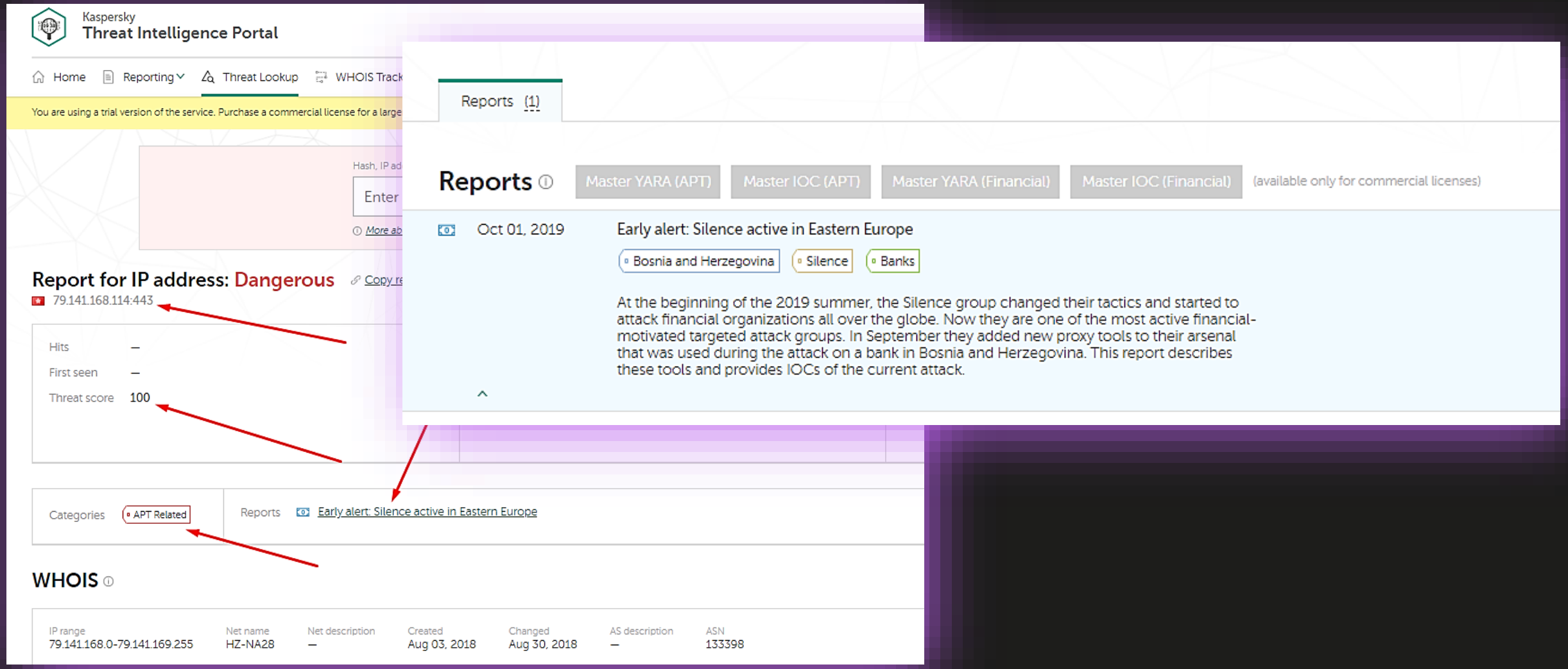
Parent process

File	C:\PerfLogs\winsde.exe
MD5	71fa6c1937eff70f619b5fb3ed5e9d37
SHA256	306dc58e4b023c9a72e1805341078736e4fd2138ad528ec3a57e99c89ac36fb2

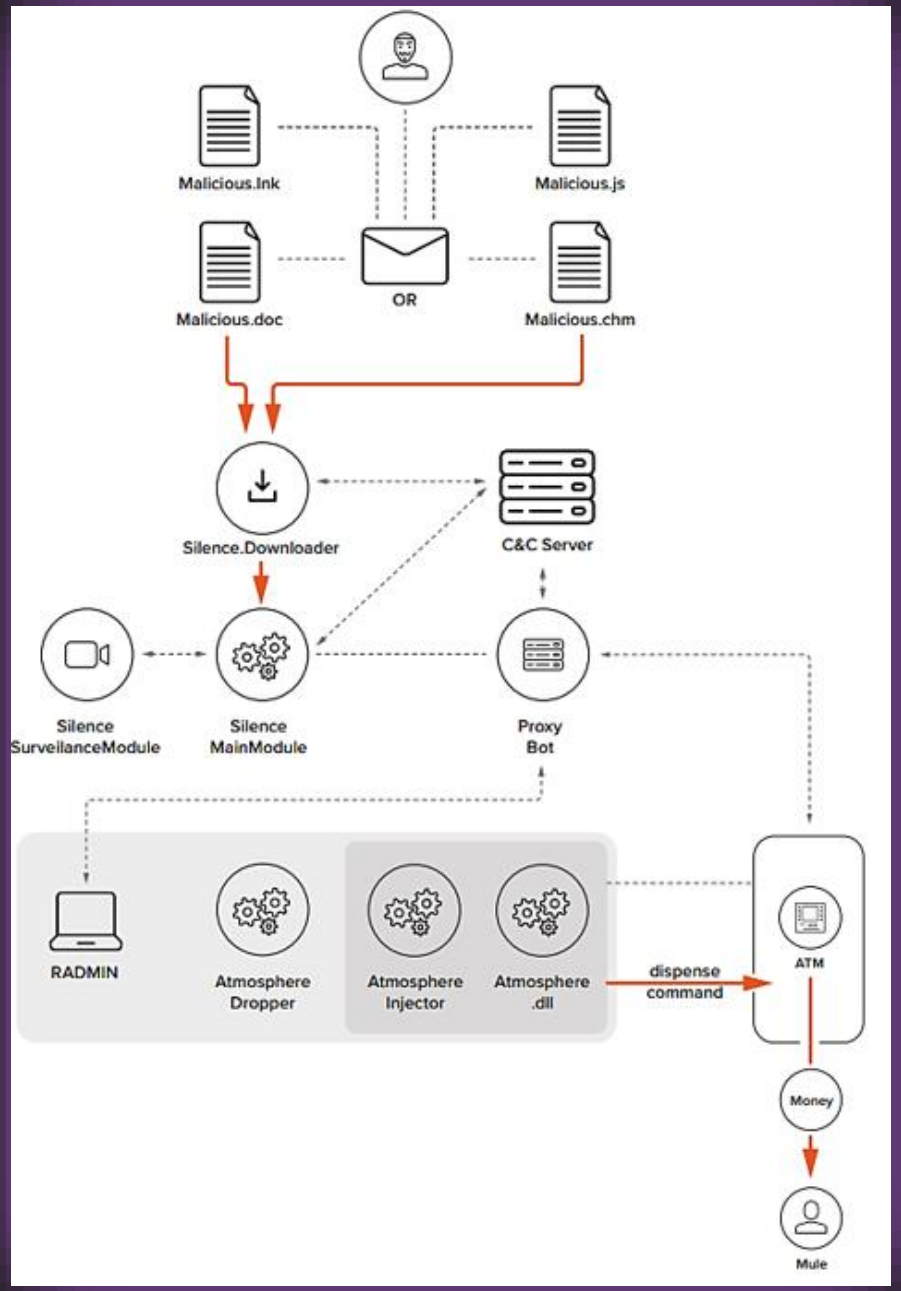
winsde.exe – Вредоносный?



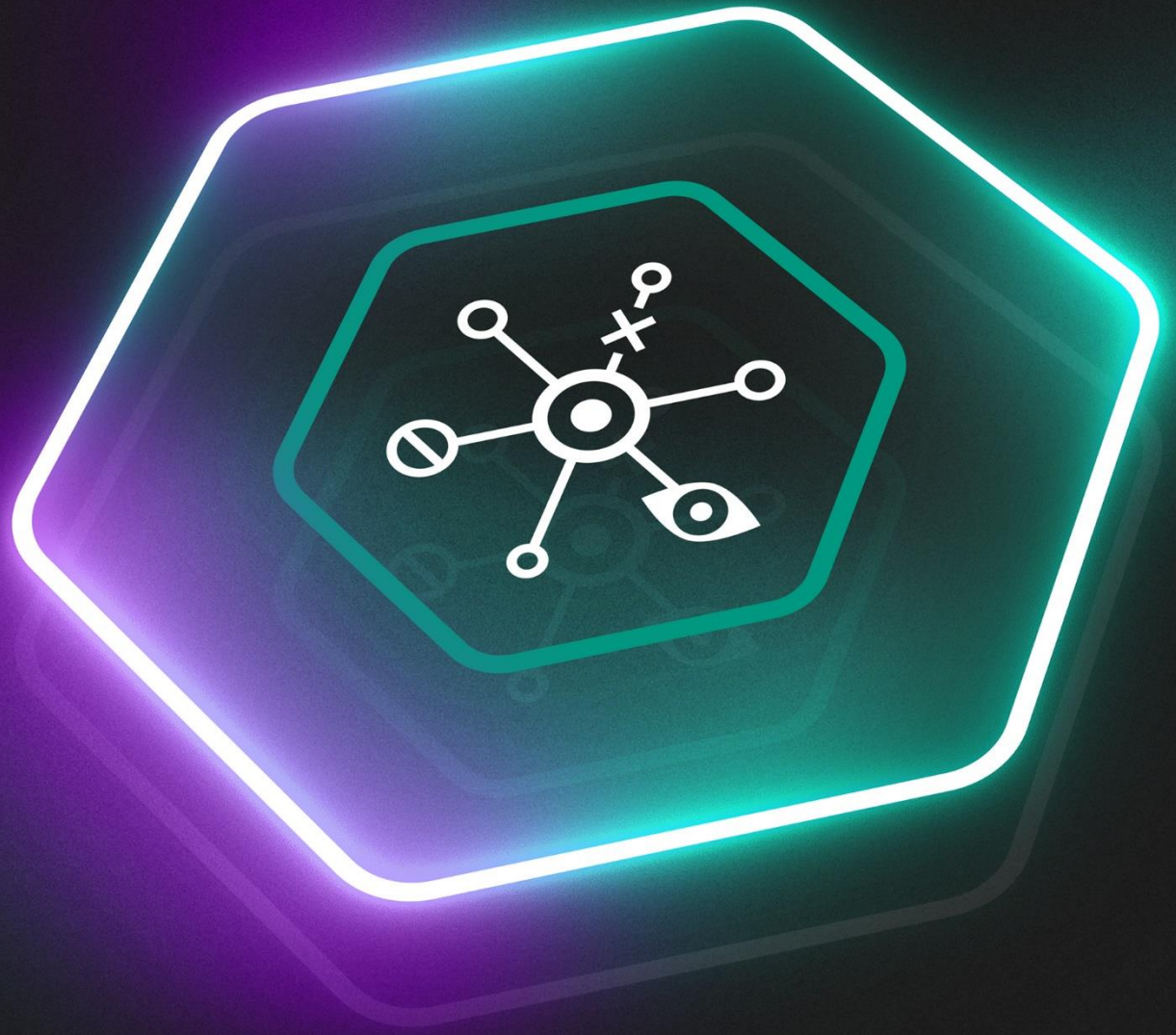
winsde.exe – Вредоносный !!!



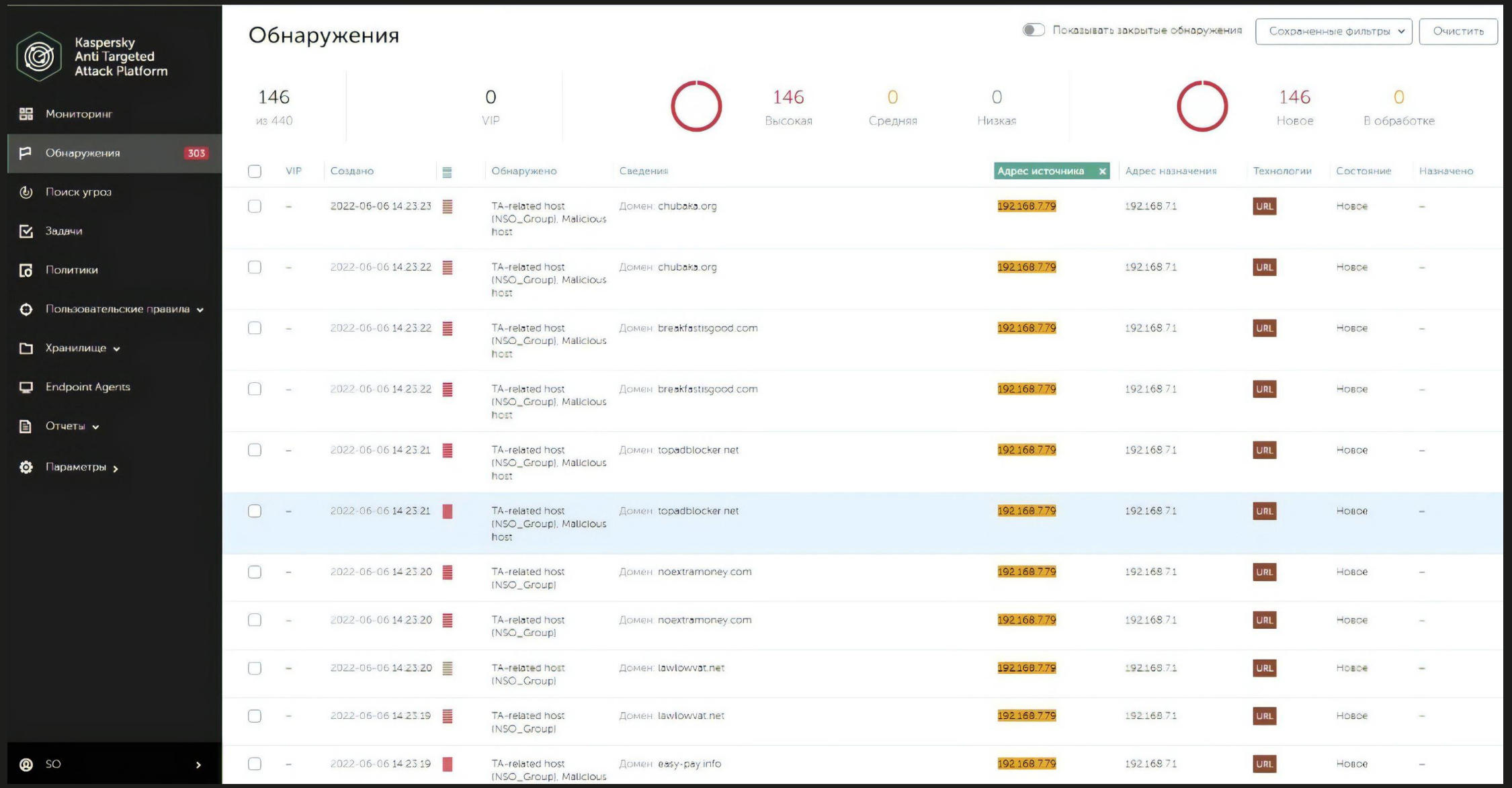
APT – Silence


Malicious.lnk
Malicious.js
Malicious.doc
OR
Malicious.chm
Silence.Downloader
C&C Server
Silence
SurveilanceModule
Silence
MainModule
Proxy
Bot
RADMIN
Atmosphere
Dropper
Atmosphere
Injector
Atmosphere
.dll
dispense
command
ATM
Money
Mule

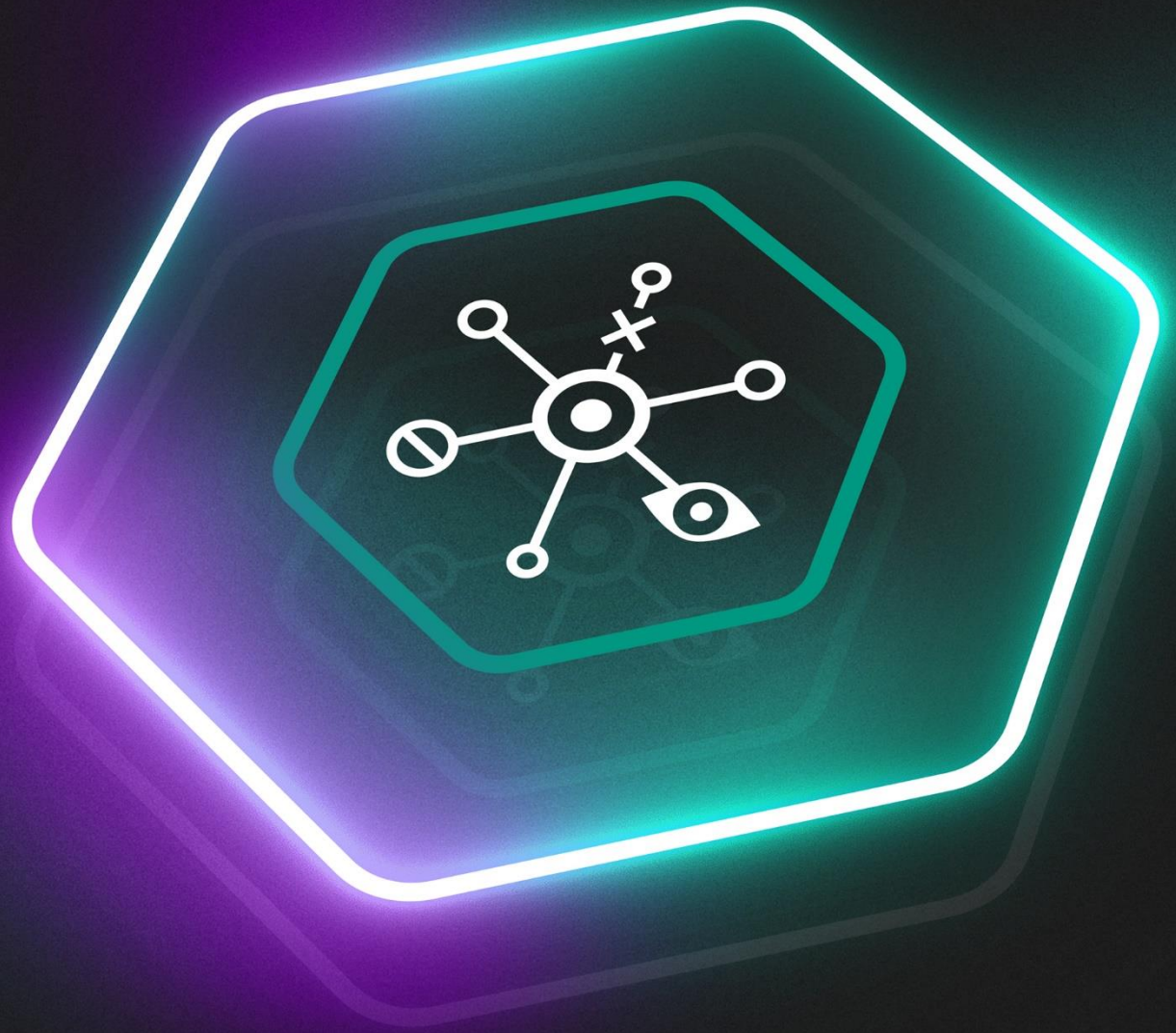
Реальный кейс у партнера (май 2022)



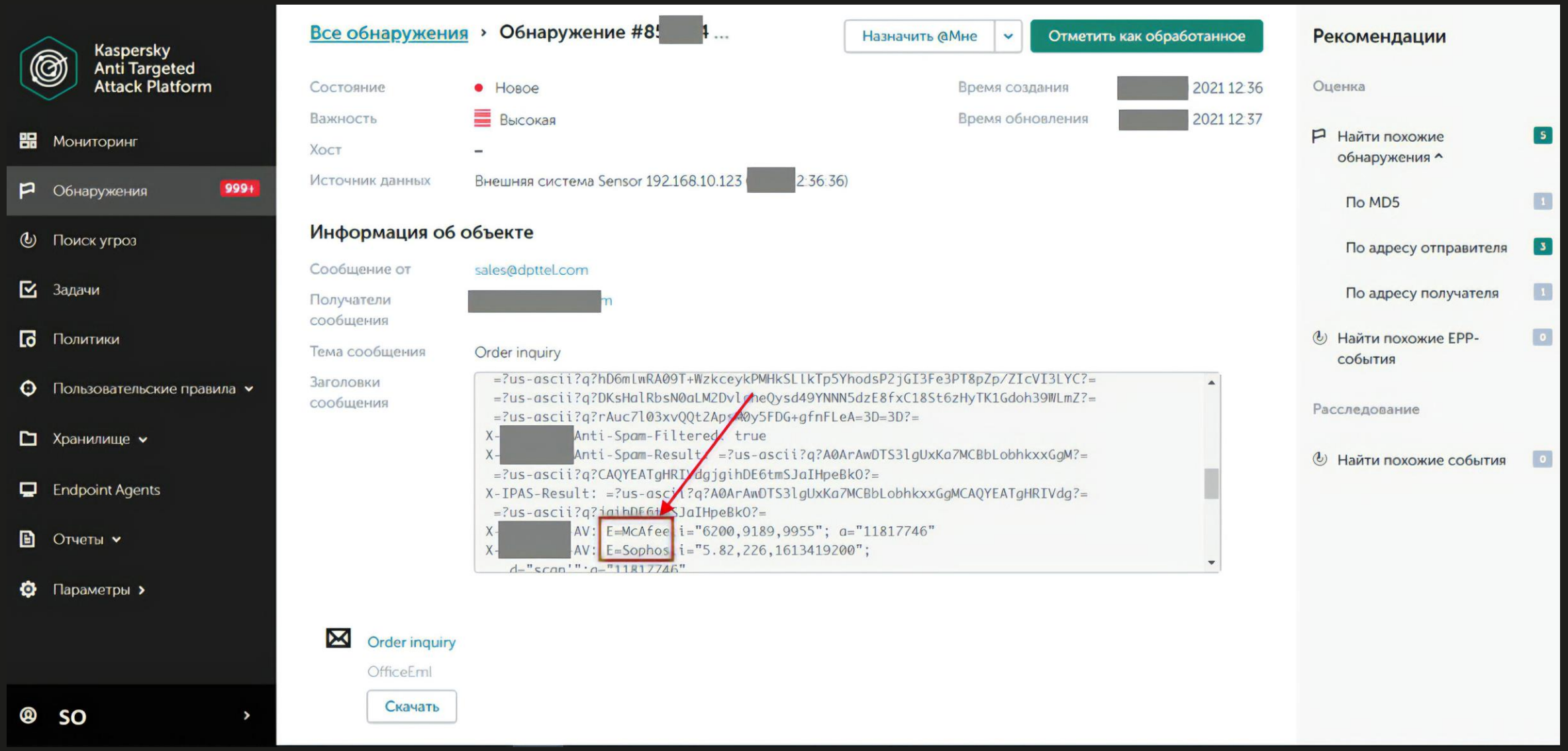
Шпионское ПО на мобильном устройстве (PEGASUS)



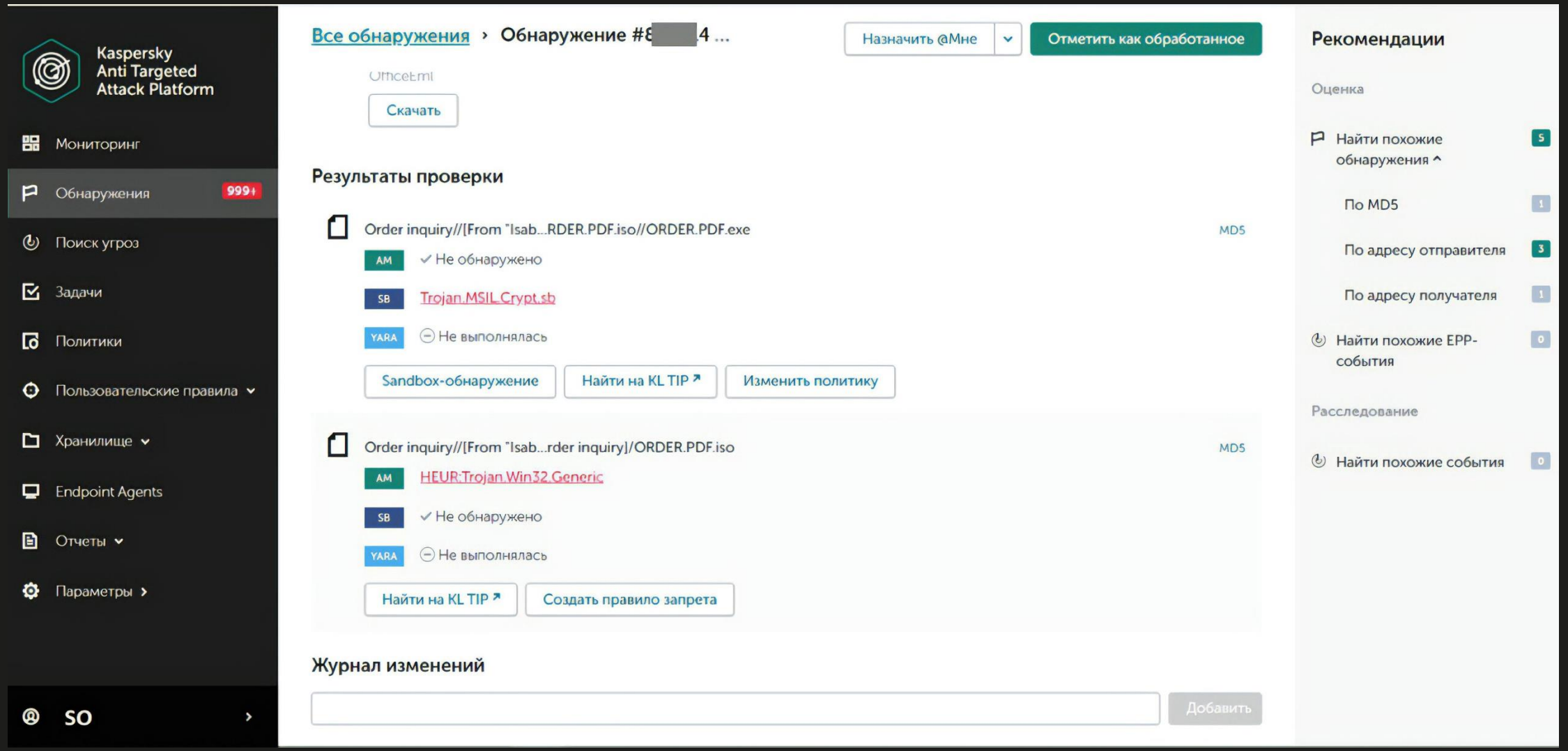
Реальный кейс у клиента (2021)



Письмо, которое прошло несколько проверок …



Содержит потенциальный шифровальщик



Плейбуки CERT Societe Generale

https://github.com/certsocietegenerale/IRM/tree/main/RU

Руководство по IR от Kaspersky

https://box.kaspersky.com/f/26b68439676f4739baa6/

Спасибо