KSD 2022

Kaspersky Security Day

# Профессиональные и экспертные сервисы от «Лаборатории Касперского»

Евгений Бударин
Head of Presales

kaspersky 25 лет

# Краткий план презентации

1. MSA
2. Professional services
3. Threat Intelligence
4. MDR
5. Incident Response

# Kaspersky TEAM

# Наш опыт и экспертиза



## GReAT

40+
экспертов

700+
группировок

Отчеты об APT атаках

## Services

120+
инцидентов расследовано

20+
Проектов по анализу защищённости

## TR

40+
экспертов

380 тыс.
новых объектов каждый день

## ICS

20+
экспертов

ICS CERT с 2016

Отчеты об угрозах и уязвимостях

# Kaspersky MSA

# Maintenance Service Agreement

- Приоритетная обработка инцидентов и фиксированный SLA
- Выделенная группа инженеров или персональный менеджер поддержки
- Периодический мониторинг настроек защиты

## Kaspersky MSA | Start

- Время реакции 4 часа
- Выделенная телефонная линия (стандартные рабочие часы)
- 12 премиум инцидентов в год

## Kaspersky MSA | Business

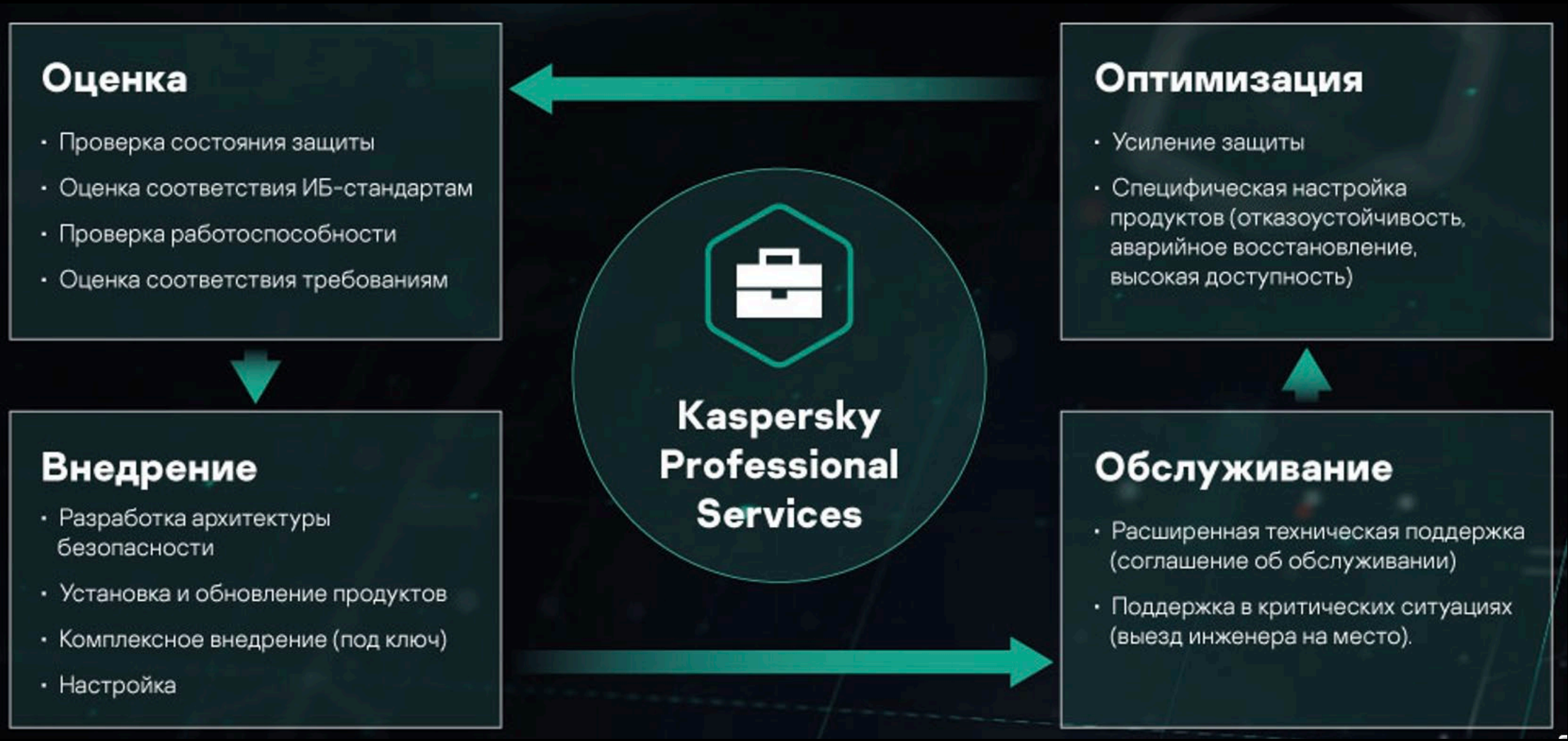
- Время реакции 2 часа
- Доступность 24/7/365
- 36 премиум инцидентов в год

## Kaspersky MSA | Enterprise

- Время реакции 30 минут
- Персональный менеджер поддержки
- Неограниченное количество премиум-инцидентов
- Health check - аудит политик и настроек

# Kaspersky Professional services

# Maintenance Service Agreement



# Kaspersky Threat Intelligence

# Почему Threat Intelligence это важно?

### Приоритизация рисков

Позволяет сосредоточится на критических проблемах

### Принятие решений за счет понимания действий злоумышленников

Повышает эффективность и скорость реагирования на угрозу

### Знание тактик, техник и процедур (TTPs)

Помогает улучшить детектирование угроз

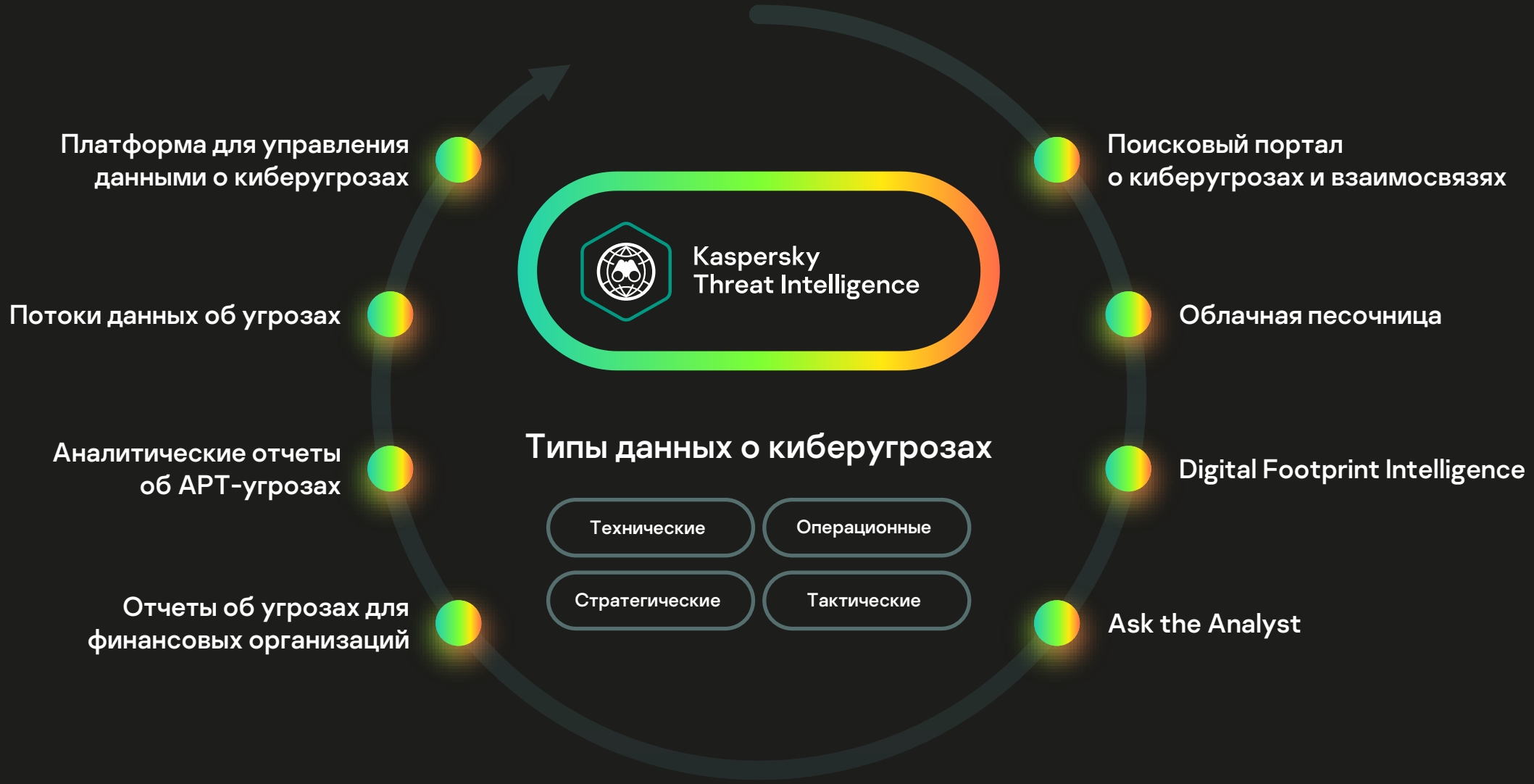
**150+**

Отчетов на различные темы*

* Публикуются командами исследователей

# Портфолио Kaspersky Threat Intelligence





# Digital Footprint Intelligence

# Digital Footprint Intelligence



## Ваши данные

- IP-адреса
- Домены компании
- Emails
- Ключевые слова

Сетевой периметр

Surface, Deep and Dark Web

Kaspersky Knowledge Base

- Отчеты
- Алерты
- 10 takedown-запросов
- Поиск по Dark Web

через источники Kaspersky, Surface и Dark Web

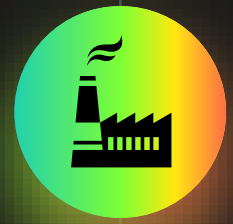
# Ask the Analyst

# Ask the Analyst

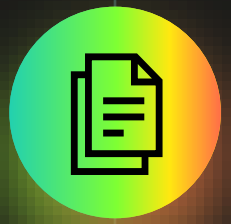


APT
и Crimeware

Анализ
ВПО



ICS-
запросы



Описание индикаторов
или уязвимостей


Darkweb
Intelligence

# Kaspersky MDR

# О разделении задач (a.k.a. «Аутсорсинг»)



## Правильное разделение задач

- Критичность функции
- Степень уникальности
- Соответствие стратегии
- Внутренние компетенции
- Себестоимость
- Возможность создания формальных требований с SLA* и метриками
- Наличие предложения рынке
- Стоимость управления услугой и контроля

## Что надо от поставщика?

- Собственные исследования
- Собственный TI
- Собственный инструментарий
- Клиентская база
- Успех на конкурентных рынках
- Приоритет рынка заказчика
- Продолжительность присутствия на рынке

* SLA – соглашение об уровне сервиса (Service Level Agreement)

# Managed Detection and Response

## Атаки становятся более сложными и эффективными

**~100**

**Инцидентов**

в среднем обнаруживаются в одной компании в год

**27%**

**Организаций**

Становятся жертвами сложных целевых атак

### Рост количества угроз

А также усложнение сценариев атак приводит к тому, что атаки остаются незамеченными

### Нехватка квалифицированных специалистов

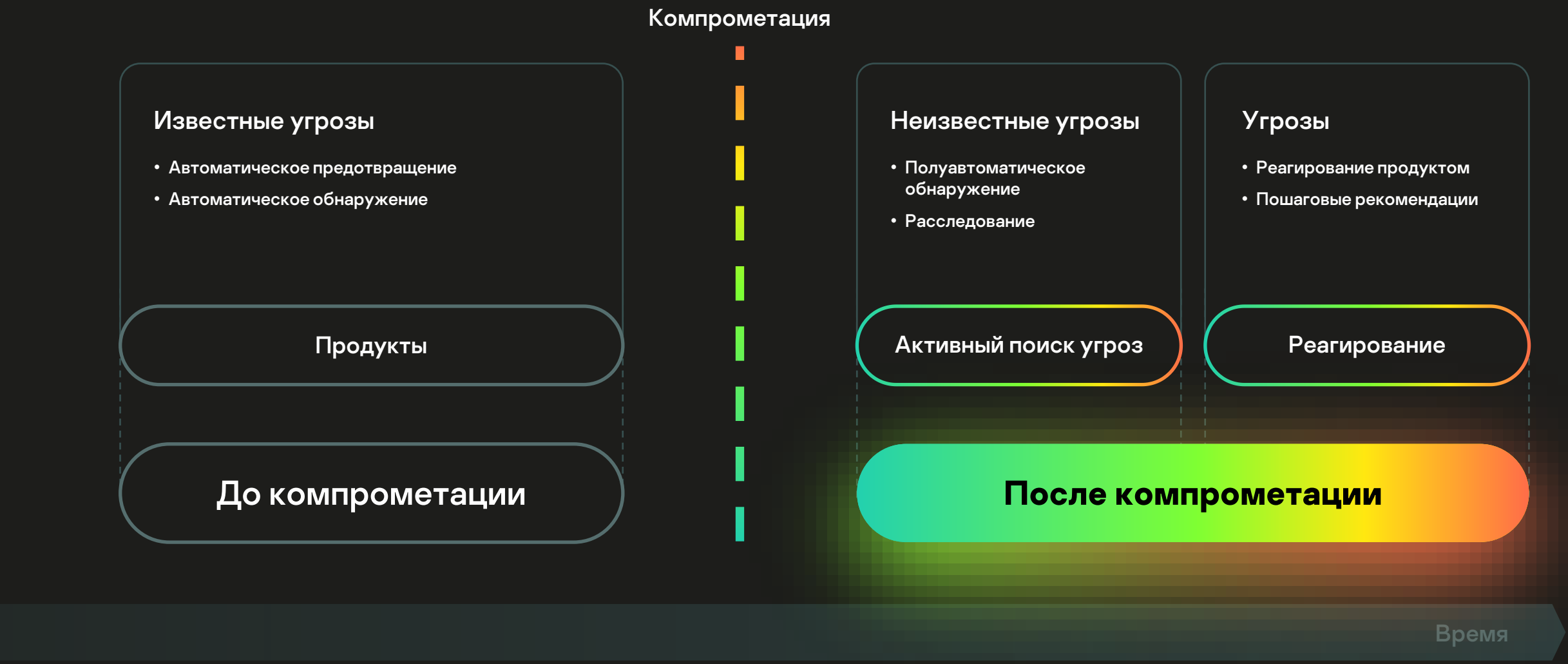
Приводит к неспособности своевременно и качественно обрабатывать события систем безопасности

### Ограничения локального размещения

Преимущества из облака: вычислительные мощности, доступный TI, широта покрытия

# Обзор Kaspersky Managed Detection and Response





# Архитектура инфраструктуры услуги MDR



# Kaspersky Incident Response

# Kaspersky
# Investigation Services

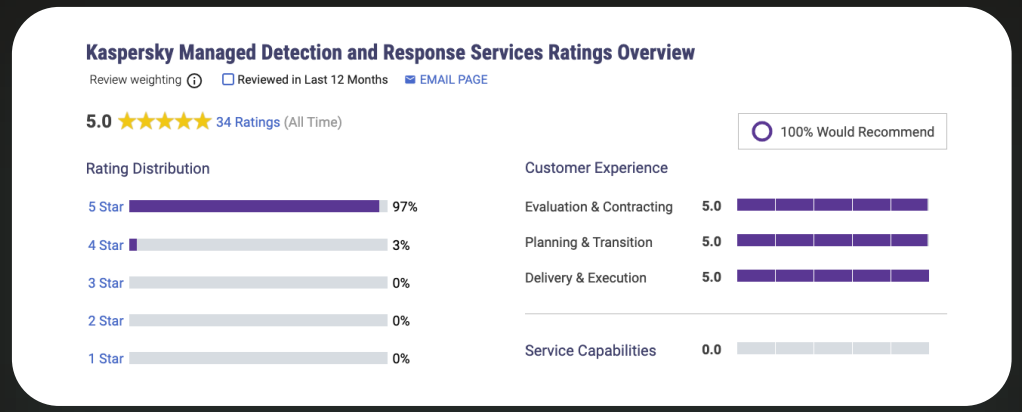
Digital Forensics

Incident Response

Malware Analysis

# Ценность услуг MDR + IR






## Возможность обнаружить современные атаки

Разведданные (TI)

Технологии и контент

Люди и процессы

## Возможность эффективно прореагировать и восстановиться

## Правильное разделение задач – мы конкурируем с лучшими в мире

## Никакой дополнительной инфраструктурной нагрузки

# «Лаборатория Касперского» поможет вам сохранить стабильность бизнеса в новых условиях

## Управляемая защита MDR

Оперативно разворачиваемая управляемая защита
от для тех, кто не располагает временем на осознанный выбор необходимых ИБ решений или как инструмент дополнительного контроля в турбулентное время

**Предложение от «Лаборатории Касперского»**

В течении 3х месяцев для ключевых заказчиков РФ «Лаборатория Касперского» готова оказать бесплатную защиту организации на основе сервиса MDR.

KSD 2022

Kaspersky Security Day

# Спасибо

kaspersky 25 лет