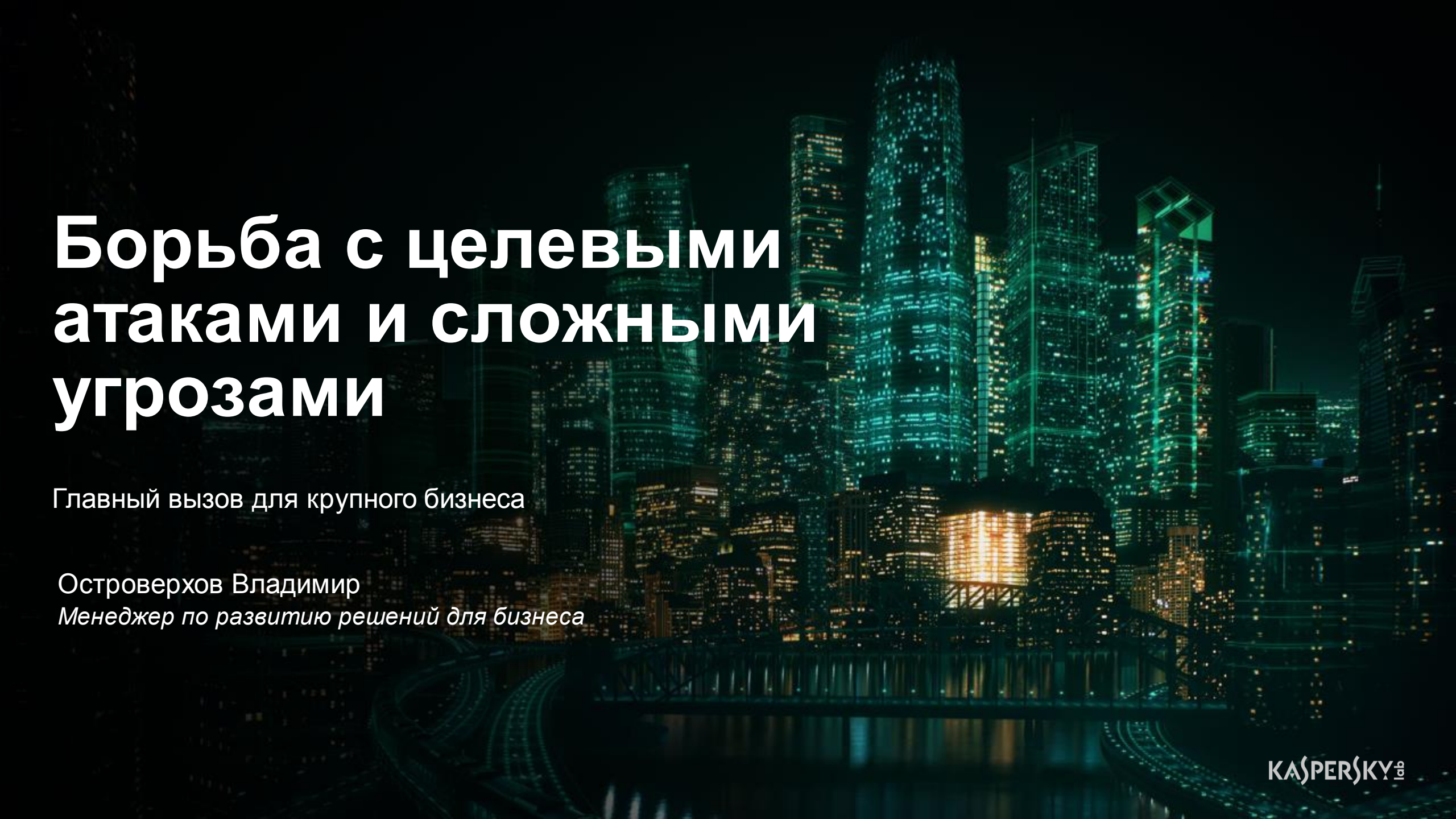


Борьба с целевыми атаками и сложными угрозами

Главный вызов для крупного бизнеса

Островерхов Владимир
Менеджер по развитию решений для бизнеса

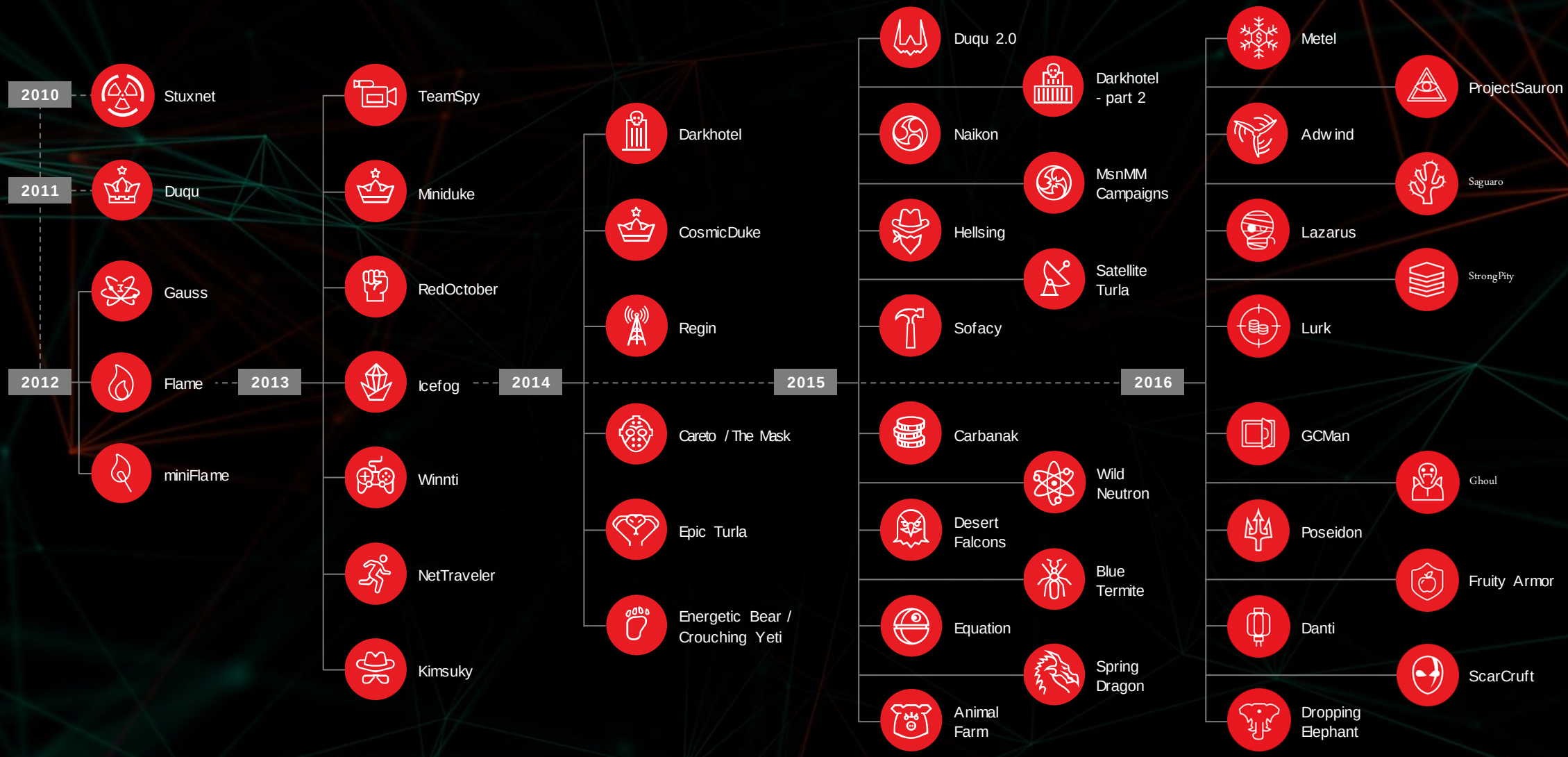
KASPERSKY lab

Современные атаки

Ландшафт угроз для крупного бизнеса

KASPERSKY lab

Главные открытия «Лаборатории Касперского»



90% ущерба от кибератак вызвано целевыми атаками

Прямой ущерб

Реагирование

— IT-консалтинг
— Аудиторы
— PR-активность
— Юристы

+

Упущенная выгода

Сорванные сделки и т. п.

+

Простой

Доходы, упущенные из-за простоя

Связанные с атакой затраты

Системы

— Устранение уязвимостей
— Покупка защитных решений (DB protection, Endpoint, PIM, SIEM)
— Модернизация IT-систем для повышения уровня безопасности

Персонал

— Наем экспертов
— (для обнаружение атак)
— Ужесточение процессов
— (новые роли)

Тренинги

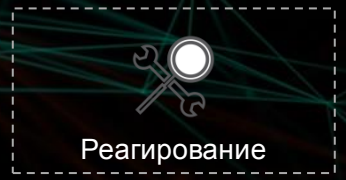
— Повышение осведомленности сотрудников
— Тренинги отдела IT-безопасности

Чтобы предотвратить подобные атаки

KASPERSKY lab

90% ущерба от кибератак вызвано целевыми атаками

Прямой ущерб

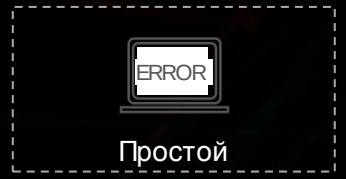


— IT-консалтинг
— Аудиторы
— PR-активность
— Юристы

+

Сорванные сделки и т. п.

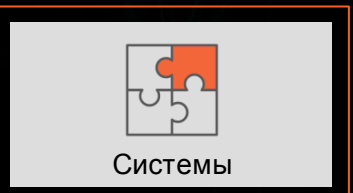
+



Доходы, упущенные из-за простоя

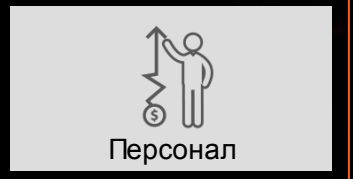
+

Связанные с атакой затраты



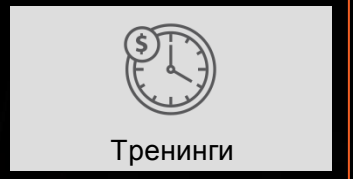
— Устранение уязвимостей
— Покупка защитных решений (DB protection, Endpoint, PIM, SIEM)
— Модернизация IT-систем для повышения уровня безопасности

+



— Наем экспертов
— (для обнаружение атак)
— Ужесточение процессов
— (новые роли)

+



— Повышение осведомленности сотрудников
— Тренинги отдела IT-безопасности

Чтобы предотвратить подобные атаки

KASPERSKY lab

Средний размер ущерба в результате атаки

Средний бизнес

Ущерб в среднем: **$86.5 тыс.**

Крупный бизнес

Ущерб в среднем: **$891 тыс.**

Перераспределение времени IT-специалистов – самый большой источник дополнительных расходов для компаний обоих типов

Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского» и B2B International, 2016

Опрошено: 926 SMB-компаний/590 крупных компаний
Они пострадали от атак как минимум один раз

KASPERSKY lab

Средний размер ущерба в результате атаки

Средний бизнес	Ущерб в среднем: **$86.5 тыс.**
Крупный бизнес	Ущерб в среднем: **$891 тыс.**

Перераспределение времени IT-специалистов – самый большой источник дополнительных расходов для компаний обоих типов

Исследование «Информационная безопасность бизнеса», «Лаборатория Касперского» и B2B International, 2016

Опрошено: 926 SMB-компаний/ 590 крупных компаний
Они пострадали от атак как минимум один раз

KASPERSKY lab

Финансовые затраты на восстановление

200% рост расходов на восстановление в течение первой недели после обнаружения признаков атаки

(благодаря системе детектирования атак)

**Стоимость восстановительных работ в зависимости от времени, затраченного на устранение уязвимости*

KASPERSKY lab

Угрозы разных типов и подход к защите от них

1% - целевые, уникальные атаки

9% - сложные атаки

90% - стандартное вредоносное ПО и типовые угрозы

Угрозы разных типов и подход к защите от них

KASPERSKY lab

Актуальные вызовы в области IT-безопасности

Большая часть современных целевых атак используют стандартные для вредоносного ПО методы и социальную инженерию

Обнаружение и реагирование ценнее и выгоднее, чем блокирование и превентивная защита

Реагирование на связанные инциденты дает ложное чувство безопасности

Уменьшение ущерба от целевых атак должно быть комплексным и структурным, а не изолированным

Постоянные отслеживание и сопоставление данных и аналитика угроз – важнейшая часть любого решения нового поколения

Полностью автоматизированная защита часто бессильна перед управляемыми вручную атаками. Важно обеспечить Адаптивную стратегию кибербезопасности

KASPERSKY lab

Актуальные вызовы для крупных компаний

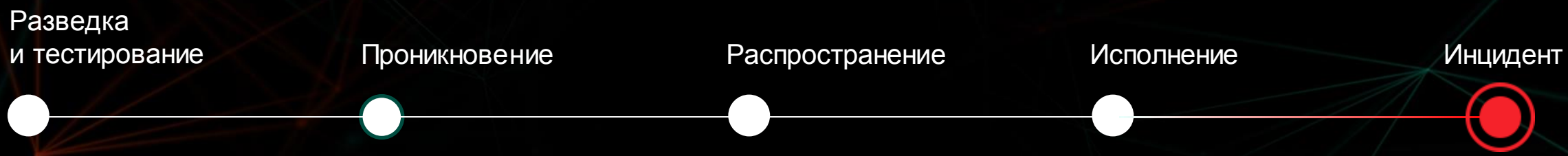
KASPERSKY lab

Цепочка поражения целевой атаки: ожидание vs реальность

В теории… атака развивается прямолинейно:

Цепочка поражения целевой атаки: ожидание vs реальность

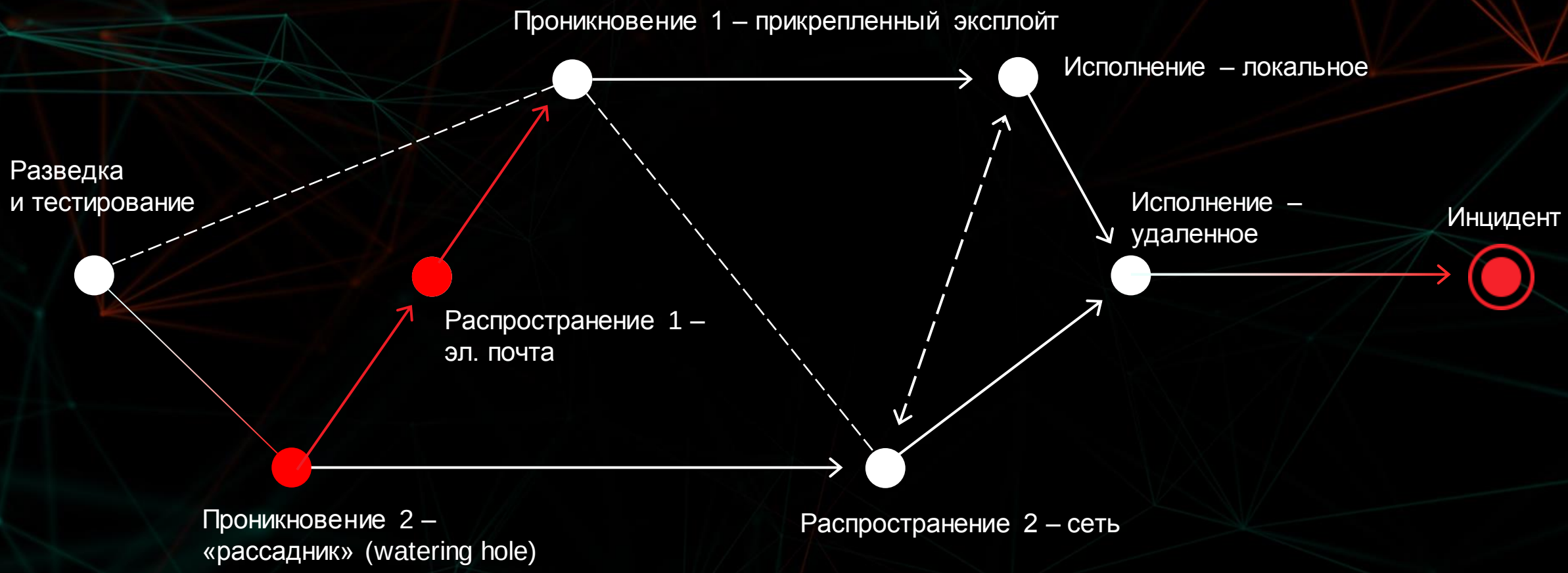
В теории… атака развивается прямолинейно:



KASPERSKY lab

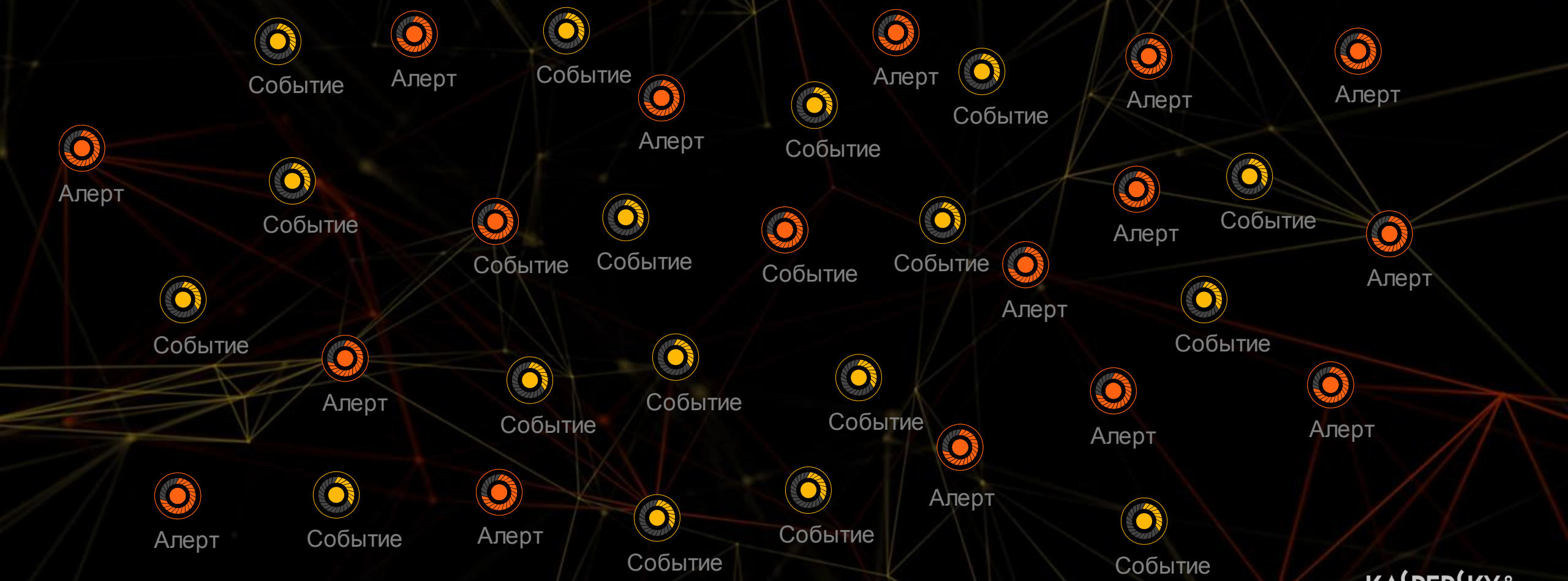
Цепочка поражения целевой атаки: ожидание vs реальность

В действительности атака развивается нелинейно:



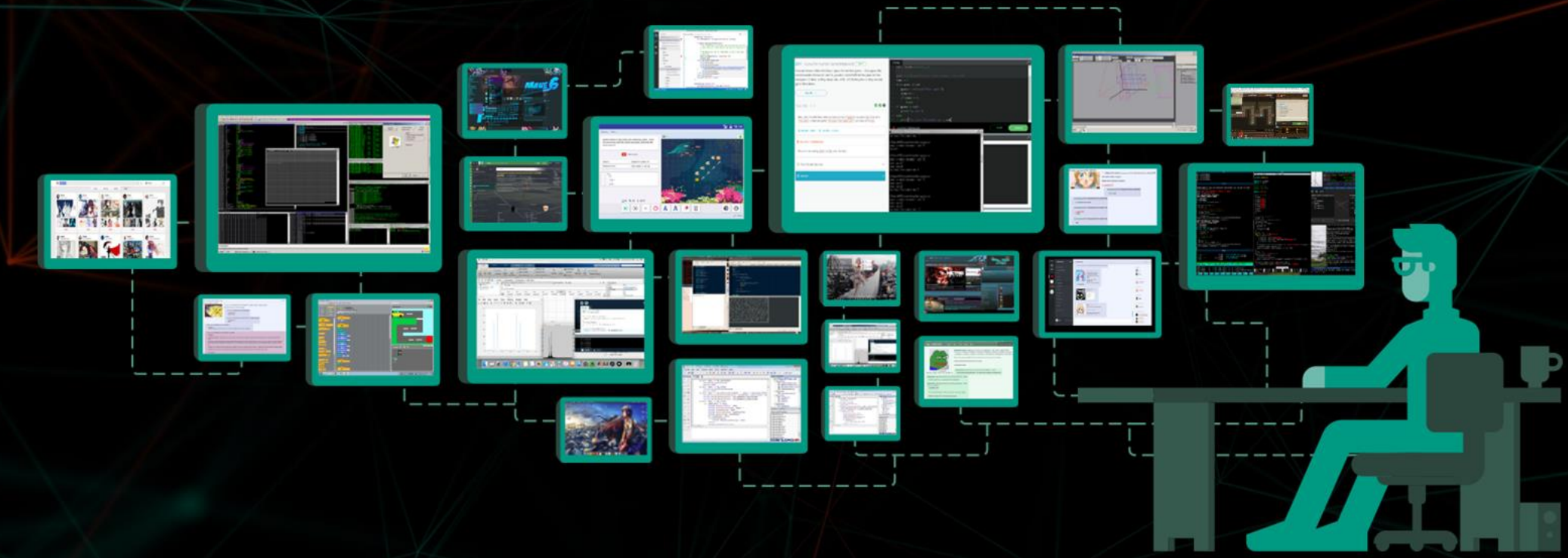
KASPERSKY lab

Разорвать цепочку поражения – путь длиной в тысячу алертов

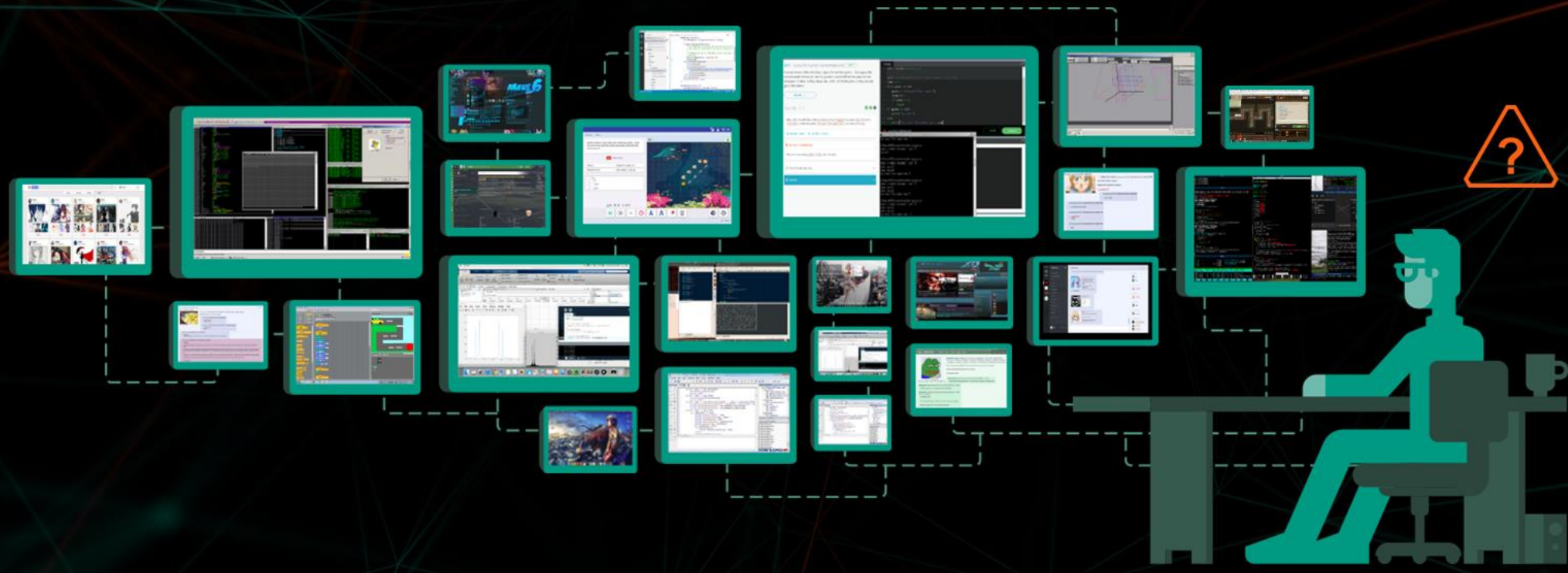


KASPERSKY lab

Также надо сопоставить все точки на этом пути вручную, используя часто несовместимые решения. Это не работает!



KASPERSKY lab



…особенно, когда это лишь один из множества IT-рисков

KASPERSKY lab

Настало время подумать о создании собственного центра обеспечения безопасности (SOC)!

Обнаружение

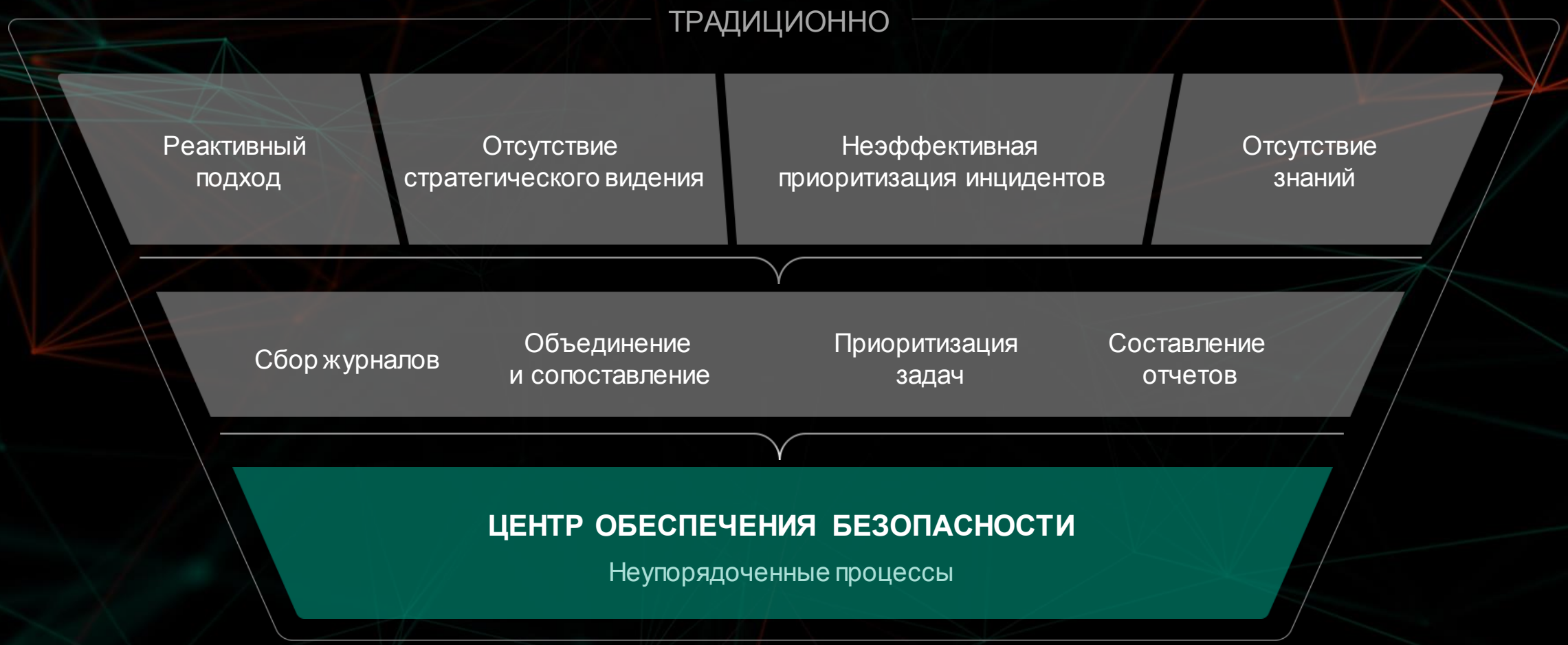
Настало время подумать о создании собственного центра обеспечения безопасности (SOC)!

Обнаружение

Настало время подумать о создании собственного центра обеспечения безопасности (SOC)!

Обнаружение

Однако традиционный подход к созданию SOC требует пересмотра



KASPERSKY lab

Отсутствие возможности реагирования подрывает всю концепцию SOC

Все необходимое для успешного реагирования на атаку

Адаптивная стратегия обеспечения кибербезопасности

KASPERSKY lab

Построение SOC на основе аналитики

Адаптивная стратегия защиты

ПРОГНОЗИРОВАНИЕ

- Анализ потенциальных уязвимостей
- в системе безопасности
- Адаптация мер противодействия
- Предоставление центрам SOC аналитики угроз
- Проактивный поиск угроз

ПРЕДОТВРАЩЕНИЕ

- Снижение риска
- Повышение осведомленности
- Усиление безопасности целевых систем и ресурсов
- Повышение квалификации сотрудников и эффективности защитного решения

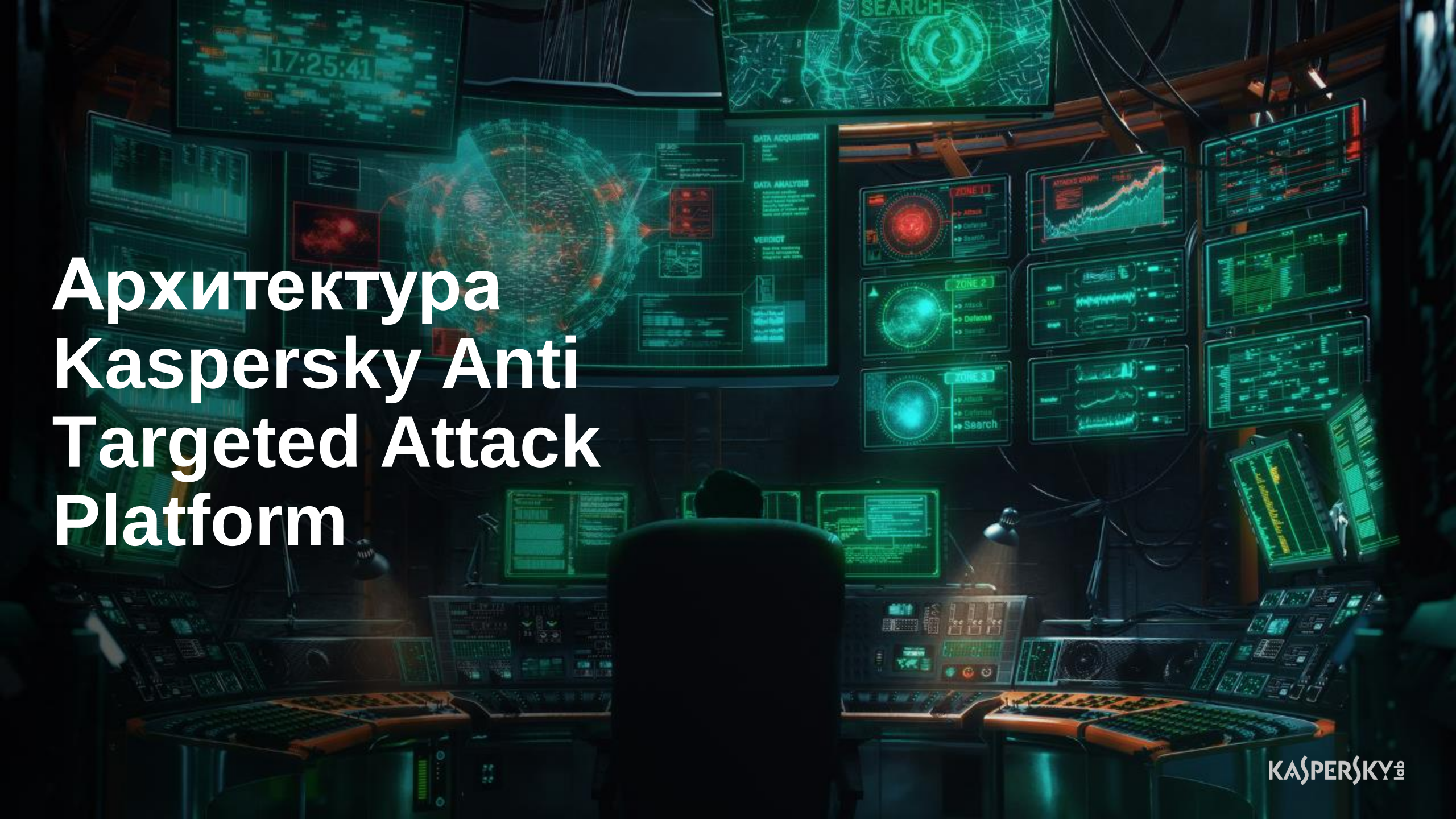
РЕАГИРОВАНИЕ

- Управление инцидентами
- Расследование инцидента
- Нейтрализация с принятием немедленных шагов для минимизации последствий инцидента
- Восстановление

ОБНАРУЖЕНИЕ

- Постоянный мониторинг
- Обнаружение инцидента
- Оценка серьезности инцидента и уровня риска

KASPERSKY lab

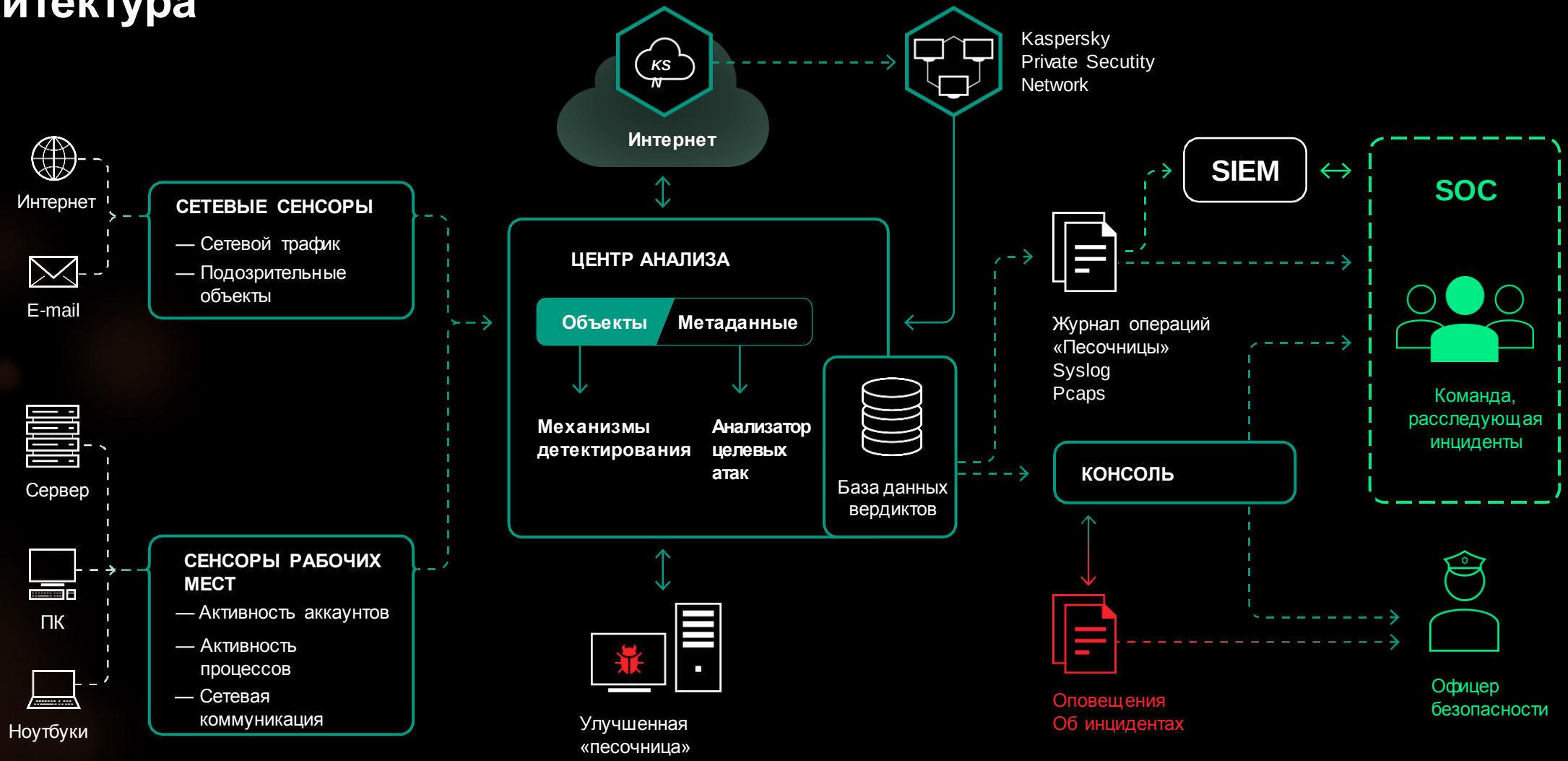


Архитектура Kaspersky Anti Targeted Attack Platform

KASPERSKY lab

Kaspersky Anti Targeted Attack – интегрированная платформа

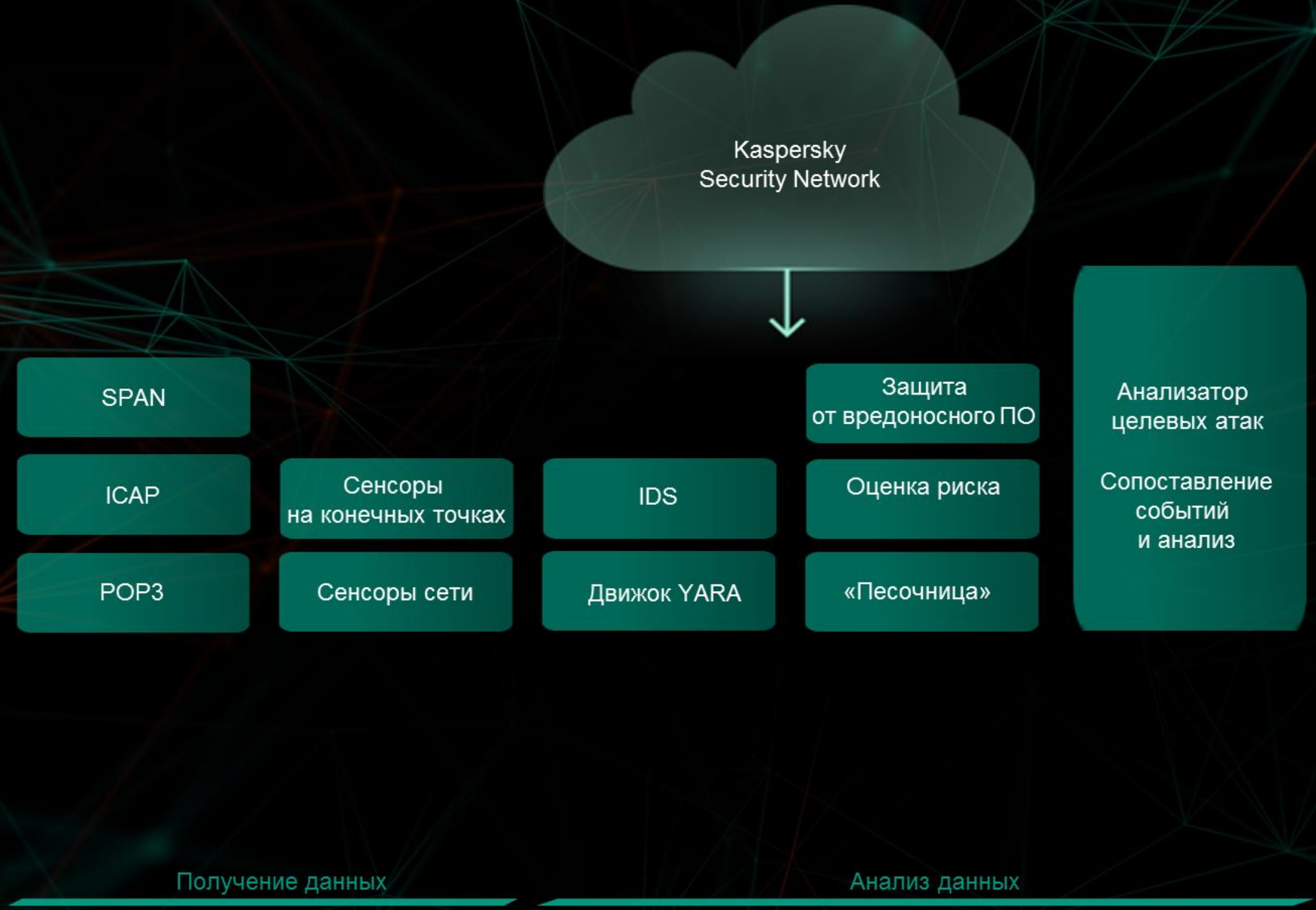
Архитектура

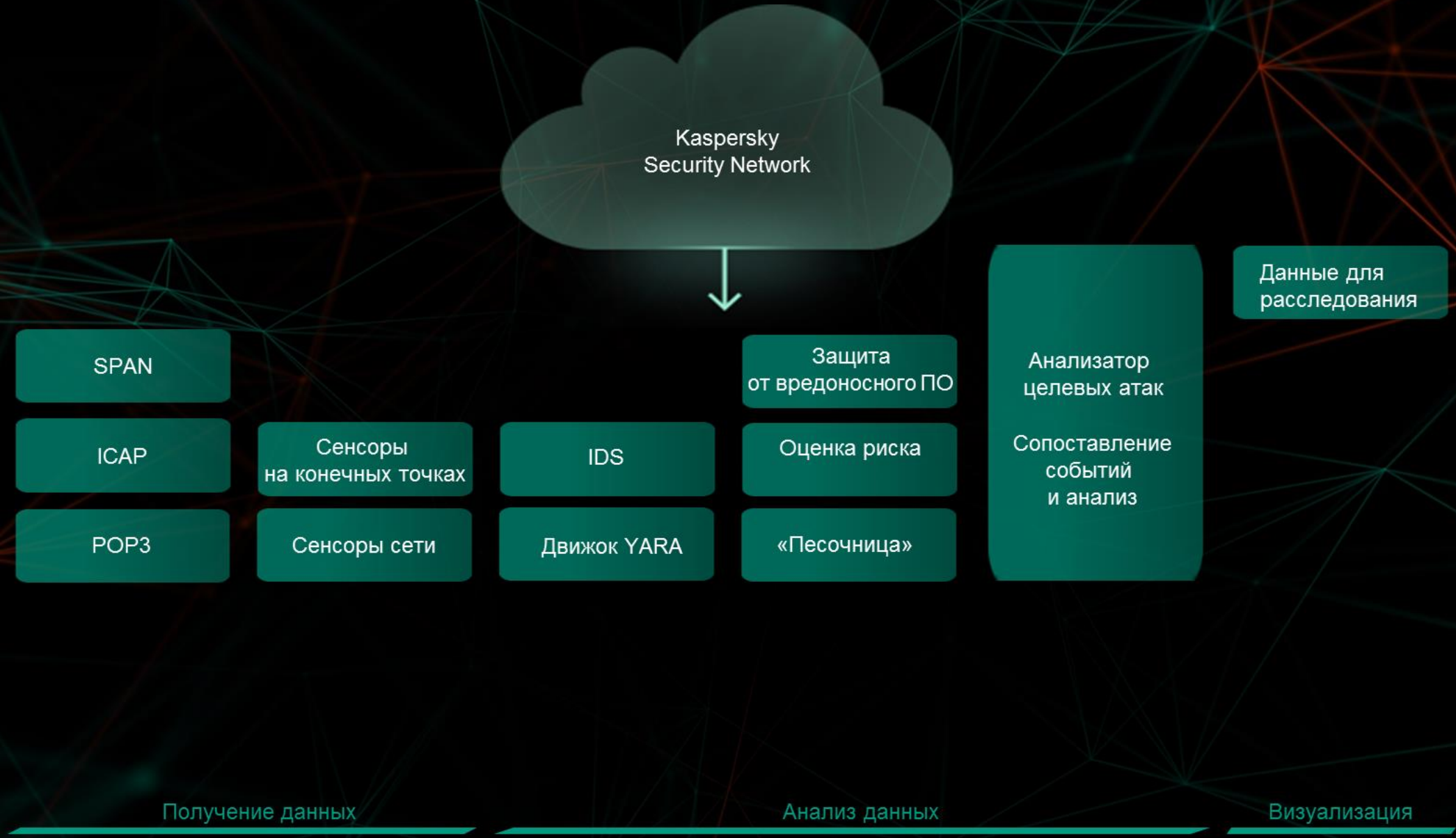


Векторы атаки | Получение данных | Анализ данных | Приоритезация вердиктов | Реагирование

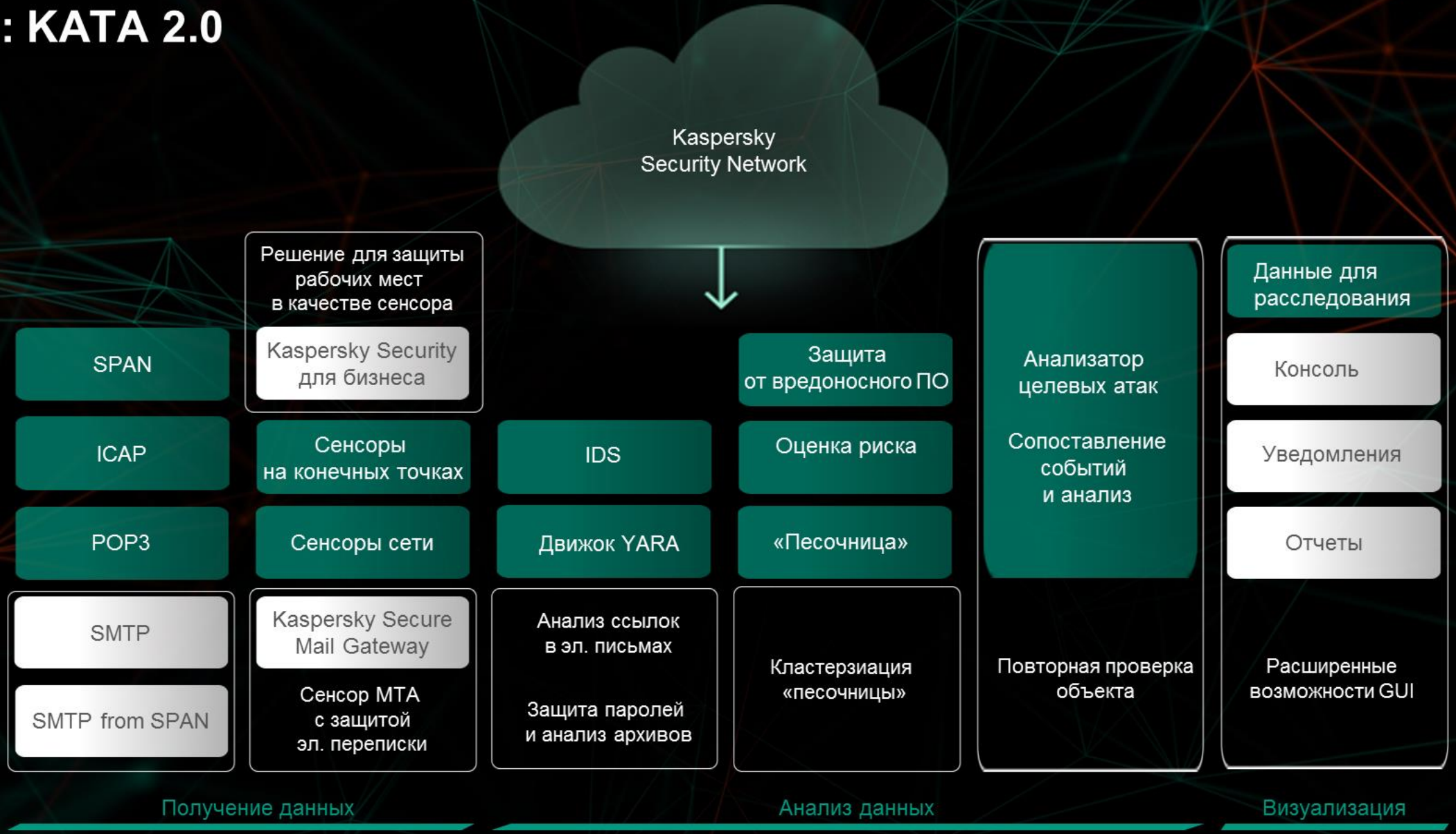
KASPERSKY lab

Получение данных

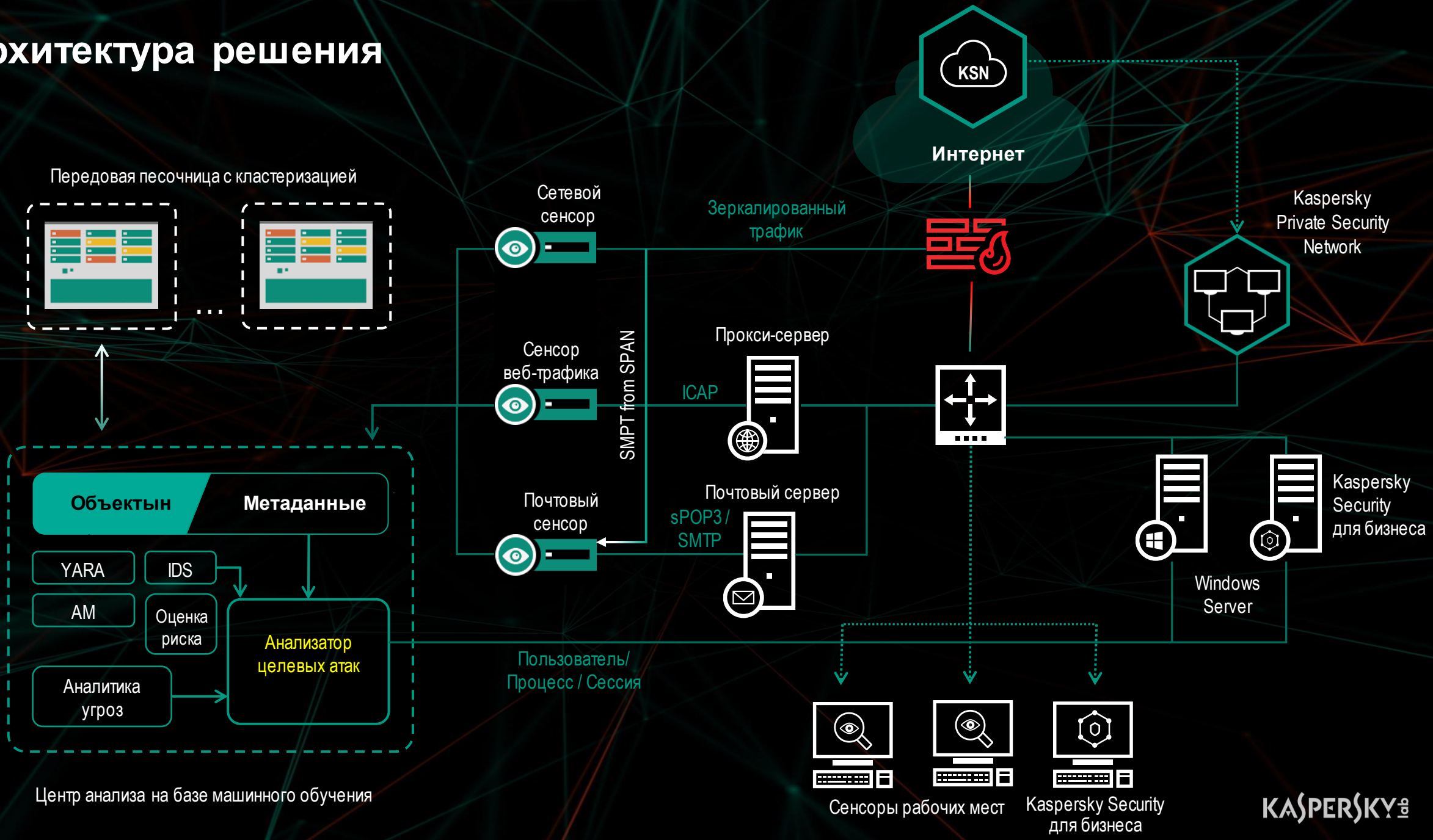

Kaspersky
Security Network
SPAN
ICAP
POP3
Сенсоры
на конечных точках
Сенсоры сети
IDS
Движок YARA
Защита
от вредоносного ПО
Оценка риска
«Песочница»
Анализатор
целевых атак
Сопоставление
событий
и анализ
Получение данных
Анализ данных


Kaspersky
Security Network
SPAN
ICAP
POP3
Сенсоры
на конечных точках
Сенсоры сети
IDS
Движок YARA
Защита
от вредоносного ПО
Оценка риска
«Песочница»
Анализатор
целевых атак
Сопоставление
событий
и анализ
Данные для
расследования
Получение данных
Анализ данных
Визуализация

2017: KATA 2.0

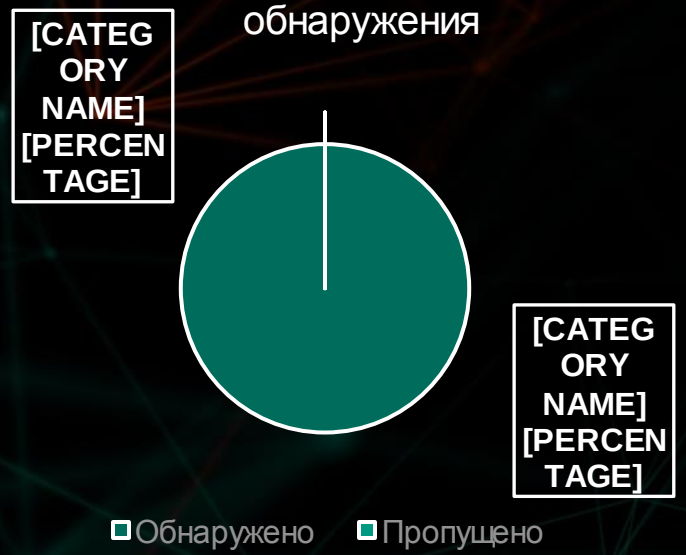

Kaspersky
Security Network
Решение для защиты рабочих мест в качестве сенсора
Kaspersky Security для бизнеса
SPAN
ICAP
POP3
SMTP
SMTP from SPAN
Сенсоры на конечных точках
Сенсоры сети
Kaspersky Secure Mail Gateway
Сенсор MTA с защитой эл. переписки
IDS
Движок YARA
Анализ ссылок в эл. письмах
Защита паролей и анализ архивов
Защита от вредоносного ПО
Оценка риска
«Песочница»
Кластерзиация «песочницы»
Анализатор целевых атак
Сопоставление событий и анализ
Повторная проверка объекта
Данные для расследования
Консоль
Уведомления
Отчеты
Расширенные возможности GUI
Получение данных
Анализ данных
Визуализация

Архитектура решения



Сертификация лабораторией ICSA Labs

KATA: эффективность обнаружения



Тестирование ICSA Labs в апреле-мае 2017 года:

— Тестирование длилось 37 дней

— 1104 теста: 585 атак и 519 проверок на ложные срабатывания

— Упор на новые и малоизвестные угрозы

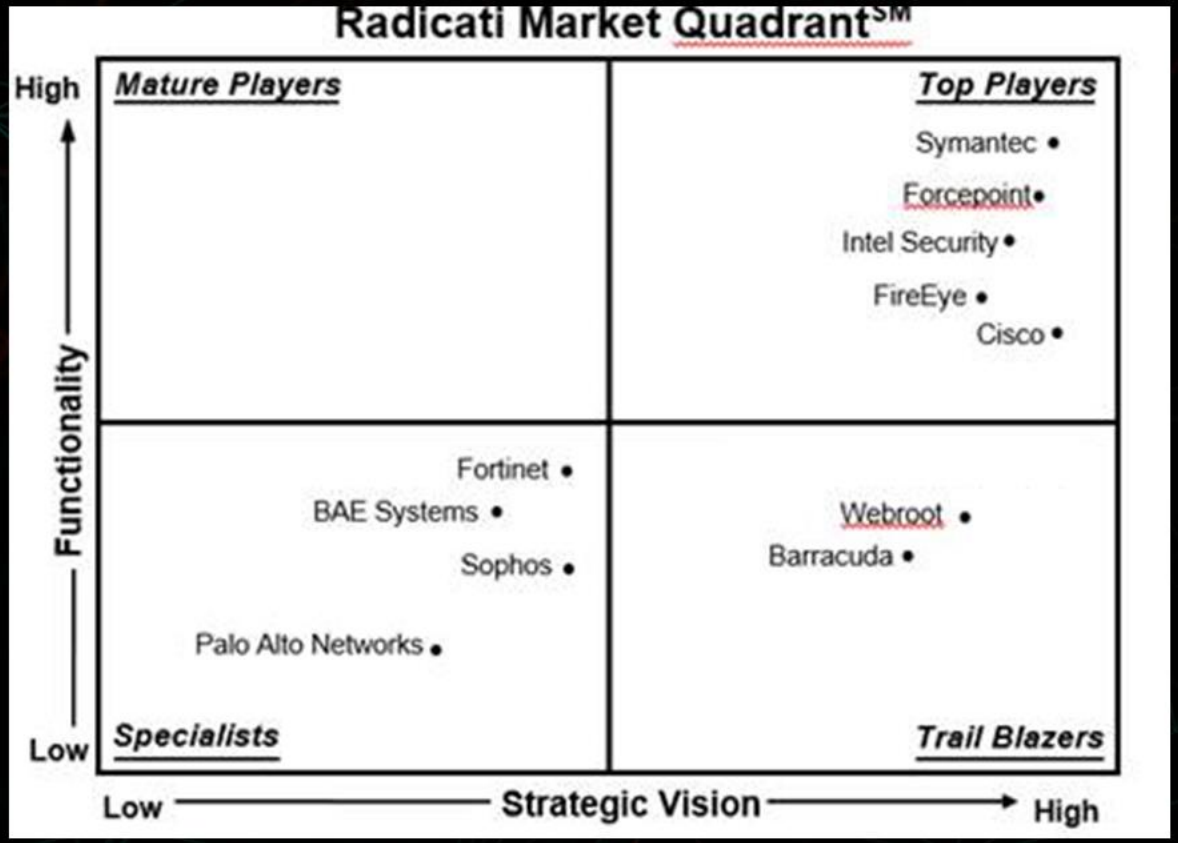
— По итогам тестирования Kaspersky Anti Targeted Attack Platform обнаружило 100% атак и не допустило ни одного ложного срабатывания

— Решение выполнило все условия для получения сертификата ICSA Labs Advanced Threat Defense (ATD)

Сертификация ICSA – это весомое подтверждение того, что компании могут доверить решению защиту своих систем.

Radicati group: магический квадрант поставщиков решений для защиты от атак класса APT

«Kaspersky Anti Targeted Attack Platform обнаруживает целевые угрозы на всех этапах проведения атаки: первоначальное заражение, коммуникации с командными центрами, дальнейшее распространение заражения и эксфильтрация данных».

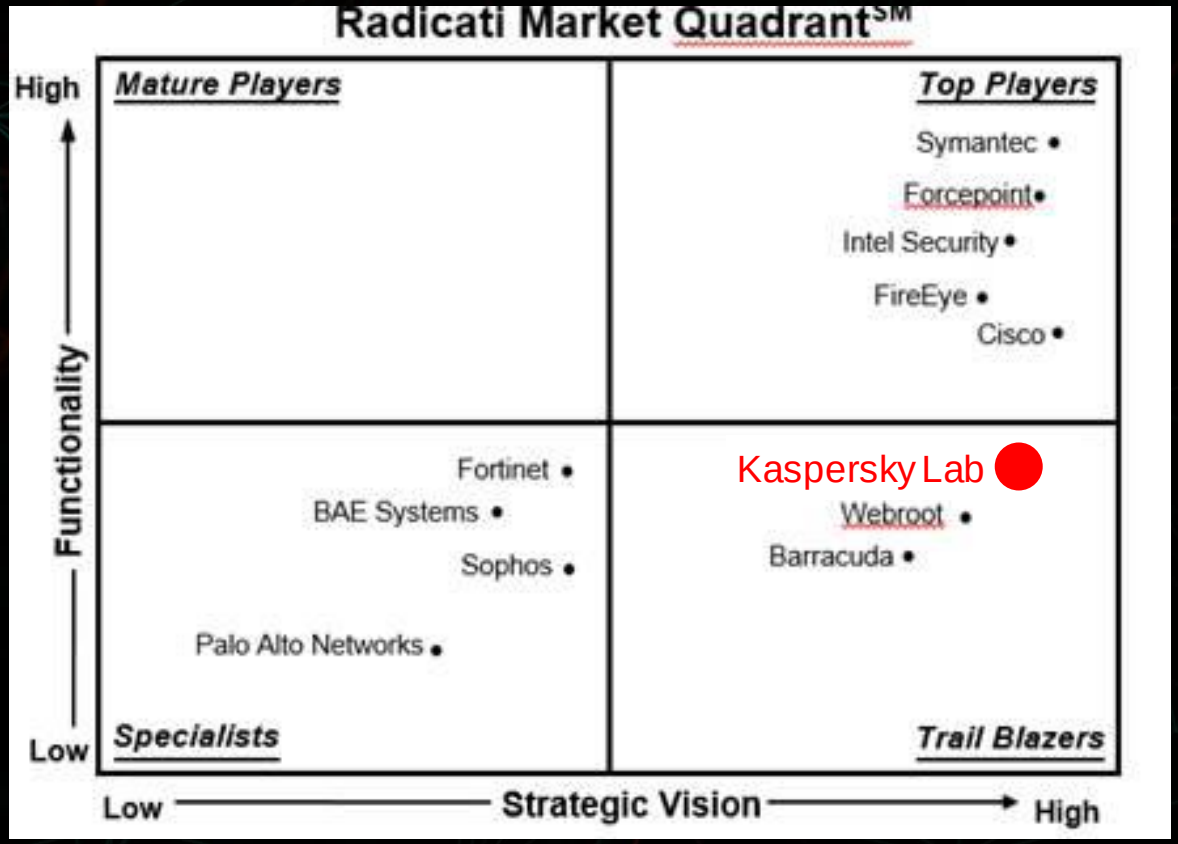


2017

KASPERSKY lab

Radicati group: магический квадрант поставщиков решений для защиты от атак класса APT

«Kaspersky Anti Targeted Attack Platform обнаруживает целевые угрозы на всех этапах проведения атаки: первоначальное заражение, коммуникации с командными центрами, дальнейшее распространение заражения и эксфильтрация данных».



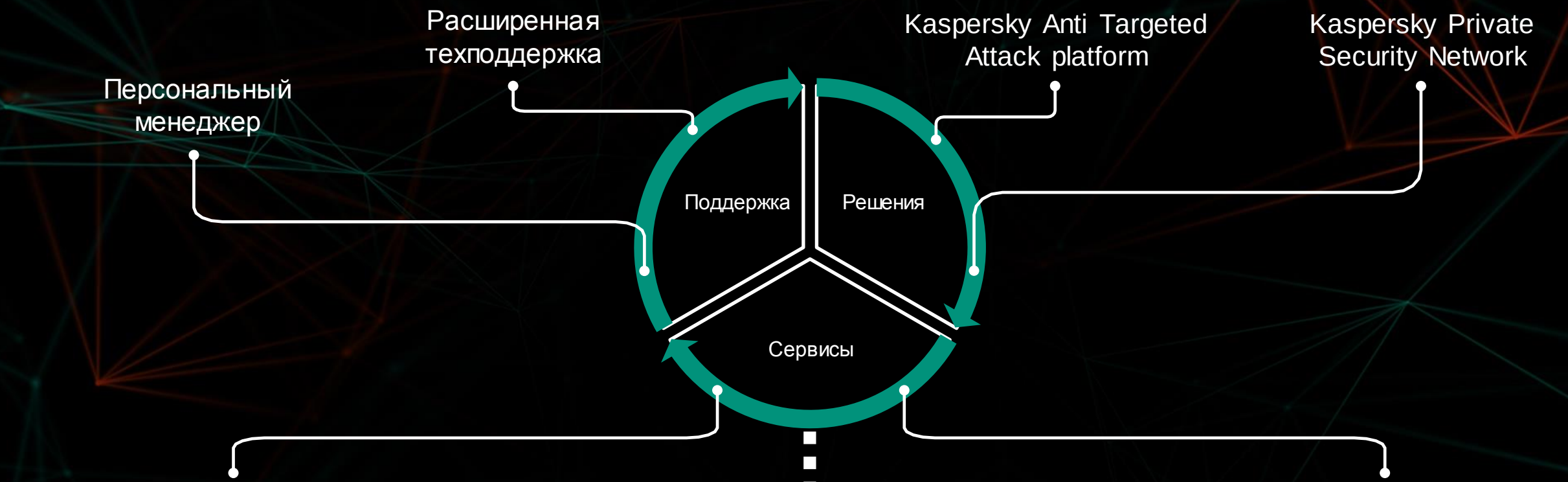
2017

KASPERSKY lab

Комплексная защита от целевых атак

KASPERSKY lab

Комплексная защита от целевых атак

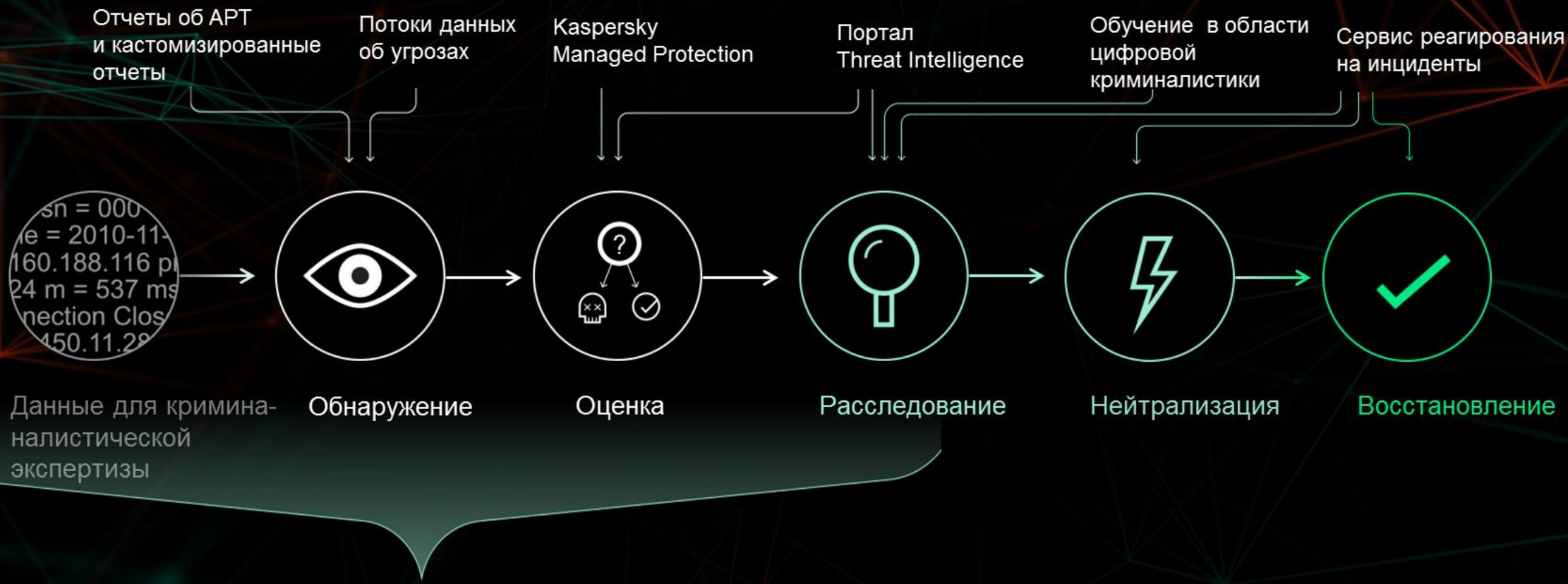


Защита от целевых атак

KASPERSKY lab

От автоматического обнаружения – к реагированию и предотвращению

НА ОСНОВЕ АНАЛИТИКИ



Kaspersky
Anti Targeted Attack

KASPERSKY lab

От автоматического обнаружения – к реагированию и предотвращению

НА ОСНОВЕ АНАЛИТИКИ

Отчеты об APT и кастомизированные отчеты

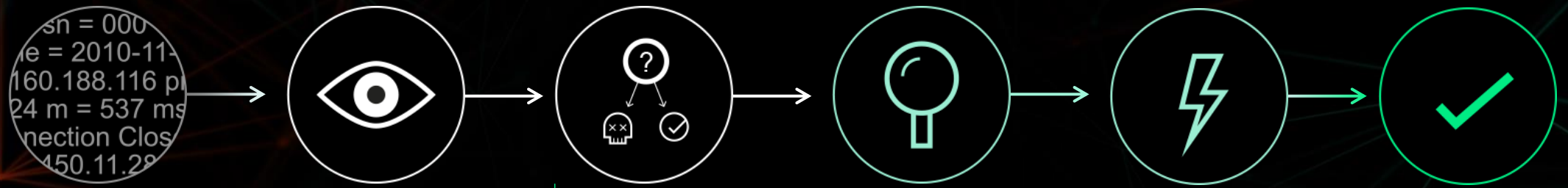
Потоки данных об угрозах

Kaspersky Managed Protection

Портал Threat Intelligence

Обучение в области цифровой криминалистики

Сервис реагирования на инциденты



Данные для криминалистической экспертизы

Обнаружение

Оценка

Расследование

Нейтрализация

Восстановление

ПРИ ПОМОЩИ ТЕХНОЛОГИЙ

Kaspersky Anti Targeted Attack

Обнаружение и реагирование на рабочих станциях и серверах

KASPERSKY lab

Расширьте возможности EDR-решения с помощью технологий обнаружения угроз KATA

KASPERSKY lab

Расширьте возможности EDR-решения с помощью технологий обнаружения угроз KATA

Адаптивная стратегия обеспечения безопасности

KASPERSKY lab

Современный подход к безопасности крупного бизнеса – не только антивирус и защита рабочих мест

KASPERSKY lab

Современный подход к безопасности крупного бизнеса – не только антивирус и защита рабочих мест

Kaspersky Security
для бизнеса
Защита ЦОД
Kaspersky Embedded
Systems Security
…

Потоки данных
Повышение осведомленности
Программы обучения IT-
профессионалов
…

Отчеты об APT-угрозах
Портал Threat Lookup
Targeted Attack
Discovery
…

Kaspersky Anti Targeted Attack
Kaspersky Managed Protection
Сервис реагирования
на инциденты
…

KASPERSKY lab

Борьба со сложными угрозами требует интеграции защитного ПО и сервисов

KASPERSKY lab

Борьба со сложными угрозами требует интеграции защитного ПО и сервисов

Проактивная защита –
Прогнозирование и Предотвращение

Оценка защищенности приложений

Повышение осведомленности

Тренинги для специалистов

Тестирование на проникновение

Портал Kaspersky Threat Intelligence Portal

Кастомизированные отчеты

KES, KSV, KSDC, KESS и т. д.

Kaspersky Anti Targeted Attack Platform

Защита рабочих мест и реагирование на обнаруженные атаки

Разведка → Доставка → C&C → Установка → Распространение → Активные действия → Скрытие следов

Аналитические отчеты об APT-атаках

Потоки данных об угрозах

Kaspersky Targeted Attack Discovery

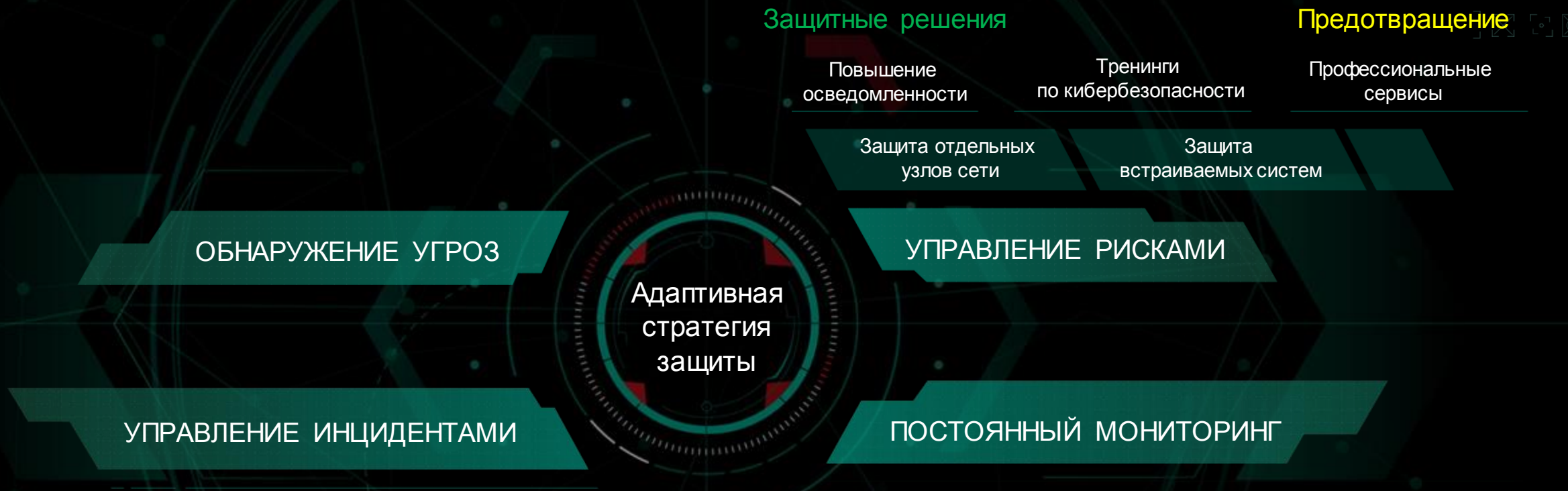
Kaspersky Managed Protection

Реактивная защита –
Обнаружение
и Реагирование

KASPERSKY lab

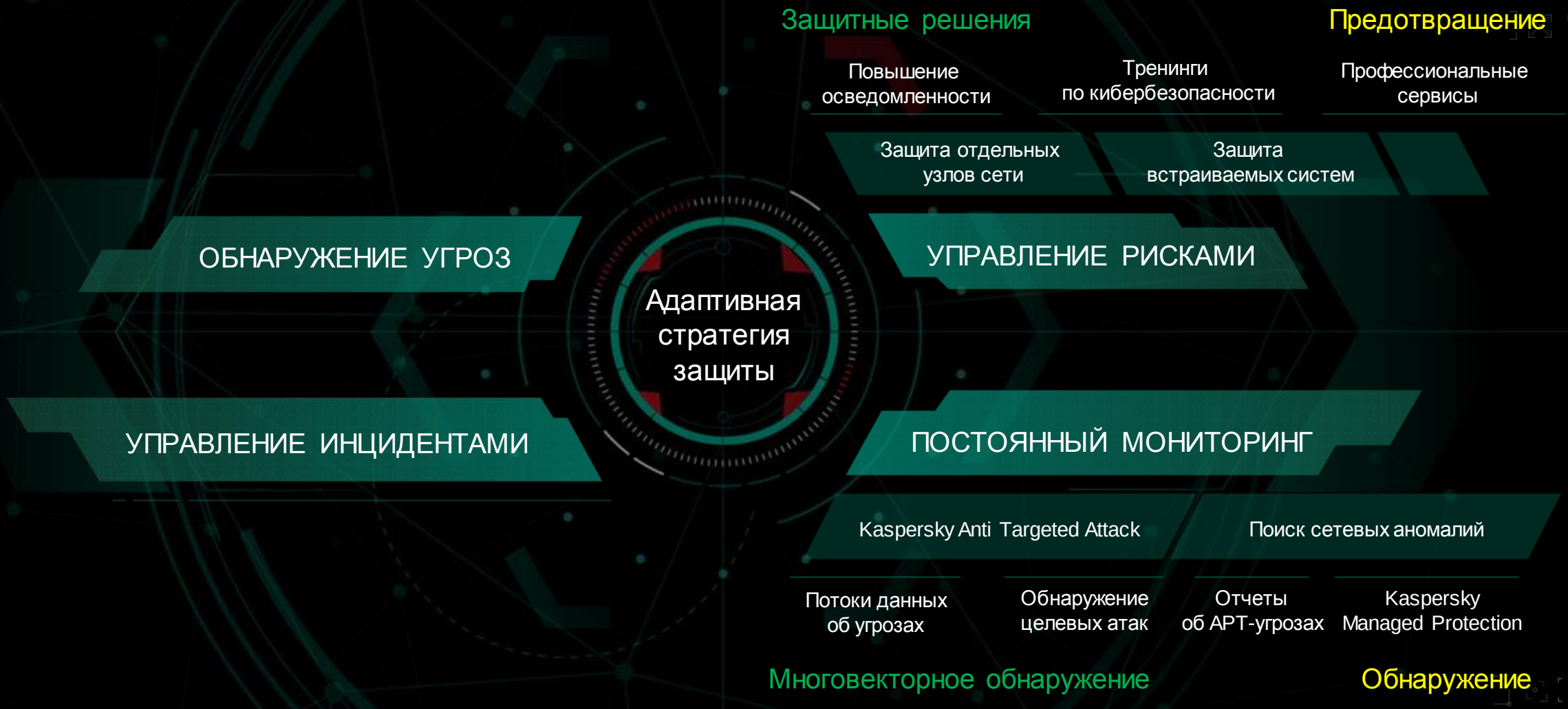
Современная модель обеспечения безопасности расишряет возможности SOC

Укрепление системы безопасности для снижения риска целевых атак

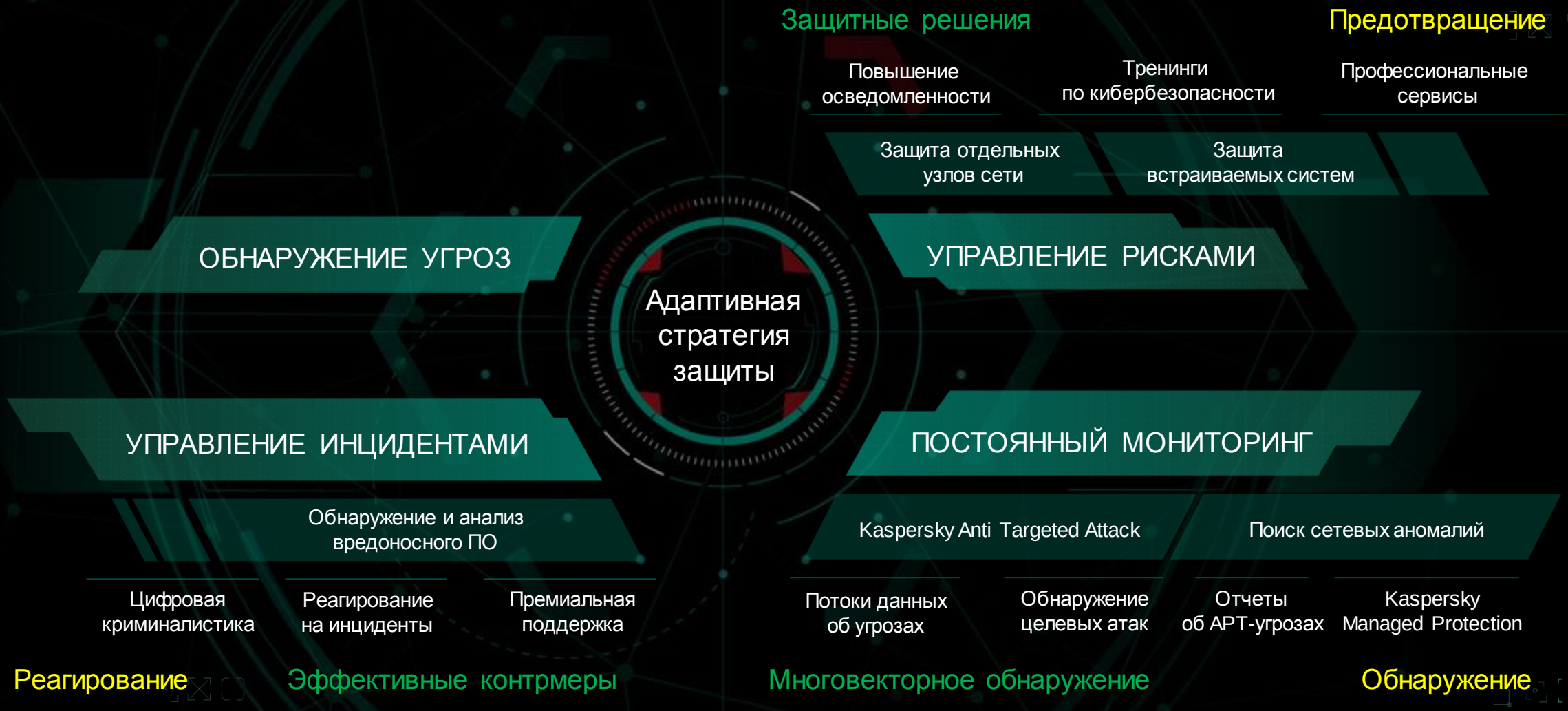


KASPERSKY lab

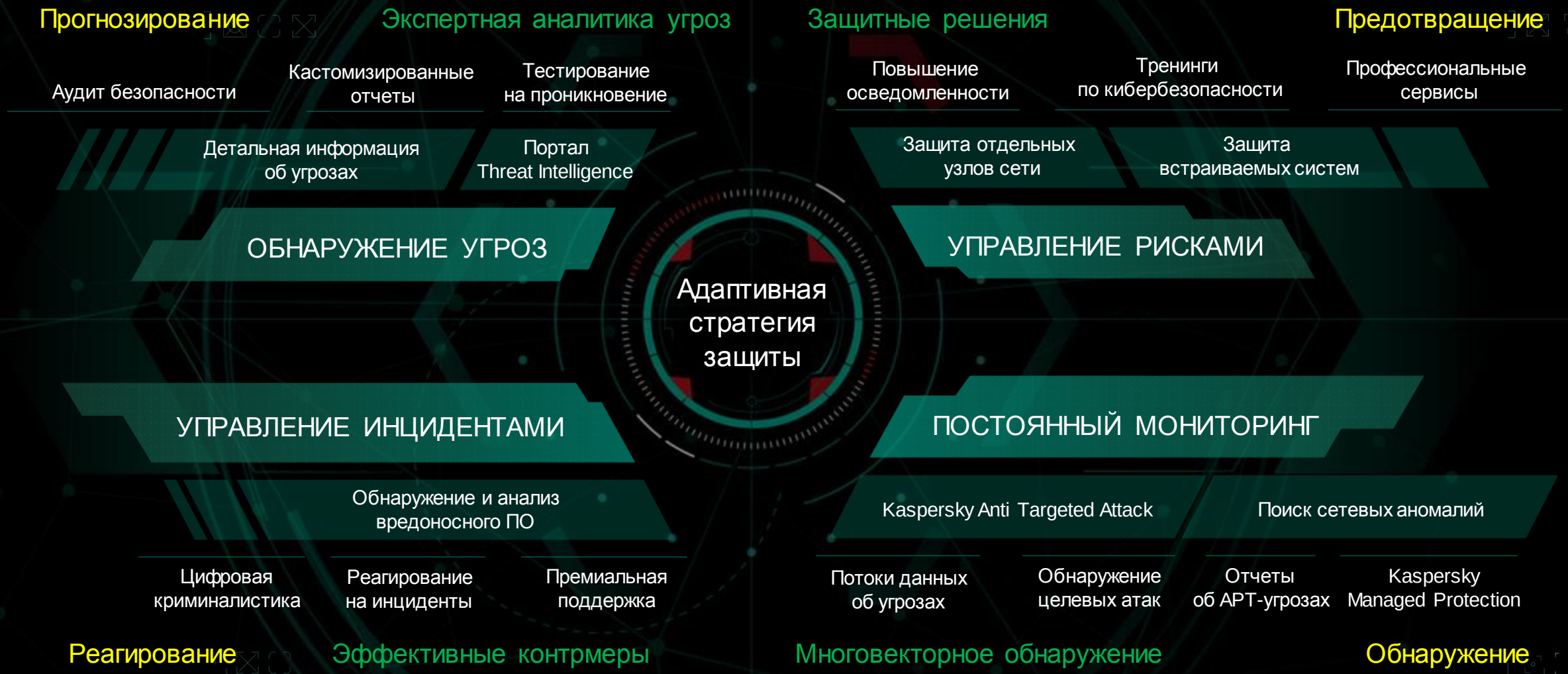
Обнаружение атаки на ранней стадии



Эффективное реагирование на атаку в зависимости от уровня риска



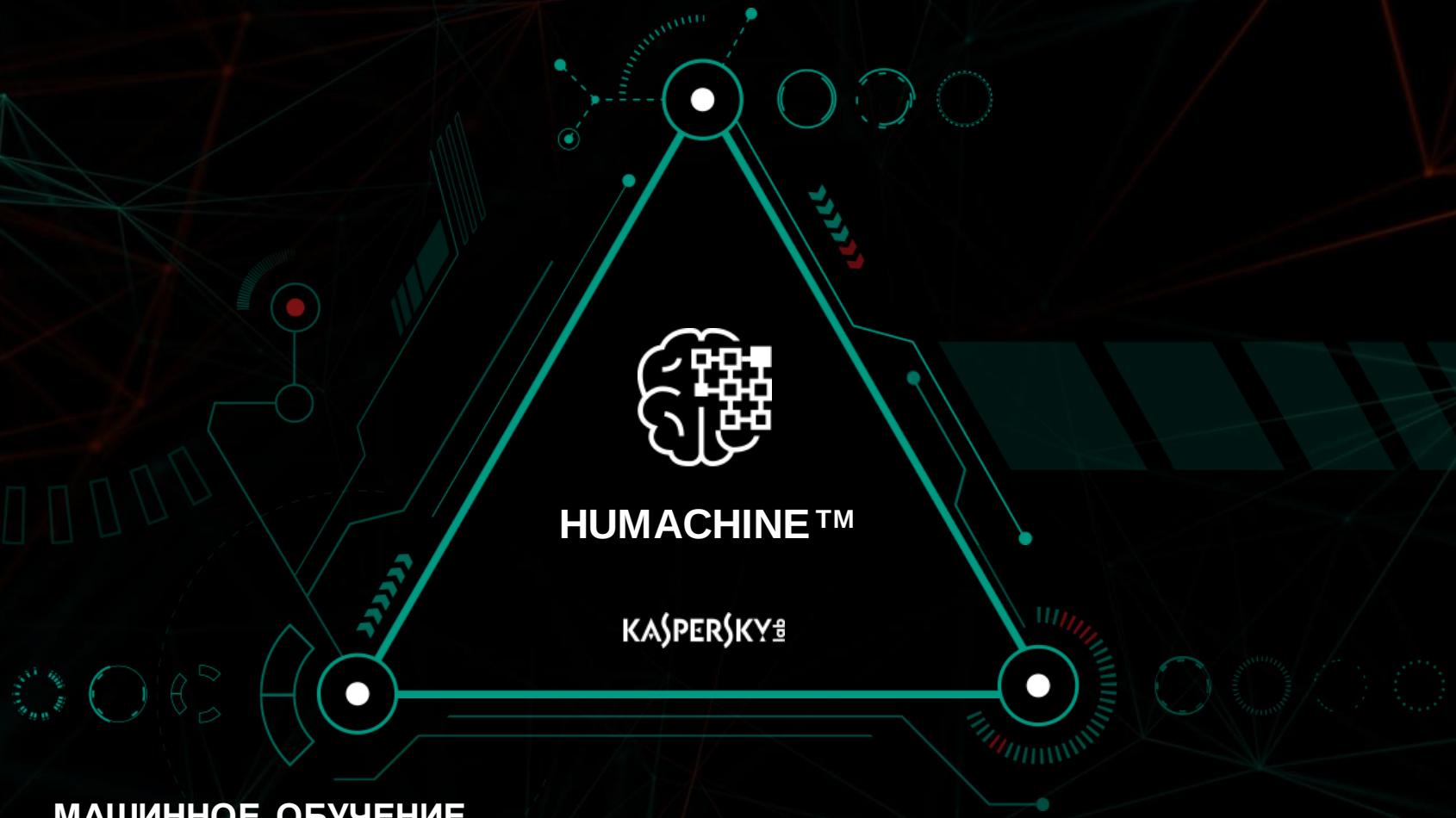
Адаптивная стратегия защиты



KASPERSKY lab

Сочетание аналитики, опыта экспертов и машинногообучения

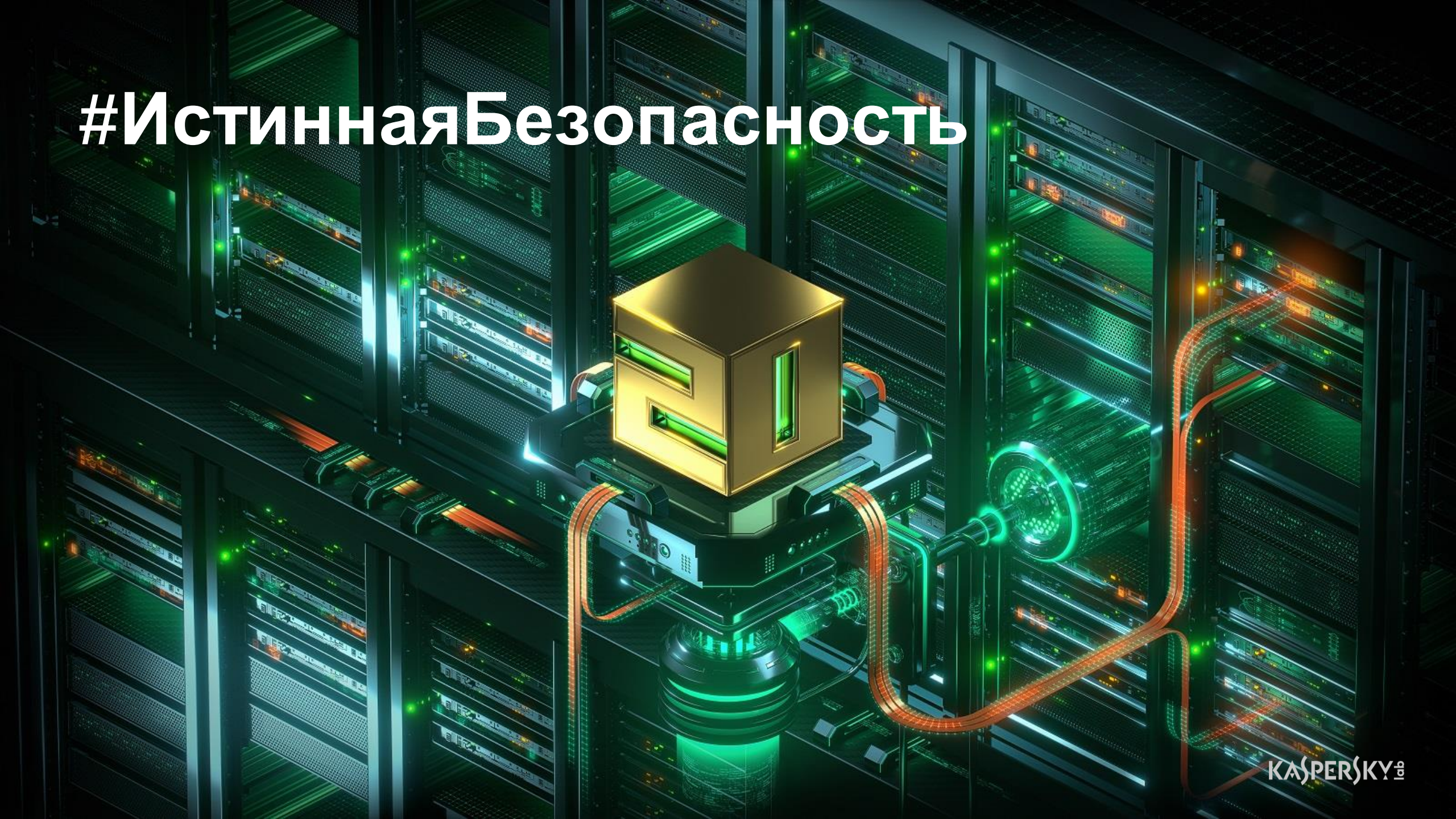
20-ЛЕТНИЙ ОПЫТ ПОИСКА
И АНАЛИЗА УГРОЗ



МАШИННОЕ ОБУЧЕНИЕ

ГЛОБАЛЬНАЯ АНАЛИТИКА УГРОЗ
НА ОСНОВЕ ОБРАБОТКИ
«БОЛЬШИХ ДАННЫХ»

KASPERSKY lab


#ИстиннаяБезопасность
KASPERSKY lab

LET'S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab