Подход Лаборатории Касперского к противодействию целевым атакам

Владимир Островерхов
Эксперт поддержки корпоративных продаж направления противодействия целенаправленным атакам «Лаборатории Касперского»

KASPERSKY lab

Взлом государственной важности

- 30 июля 2016 года ФСБ сообщило, что компьютерные сети 20 оборонных предприятий и госорганов подвержены целенаправленным атакам с целью шпионажа
- Вредоносная программа незаметно скачивается и подгружает модули
- Перехватывает и анализирует весь сетевой трафик подверженных атаке рабочих мест
- Скриншоты, доступ к веб-камере и микрофону
- Кей-логгер
- Развитие атаки на смартфоны пользователей
- В ФСБ подтвердили, что программа была модифицирована для каждой жертвы с учетом характеристик ее компьютера
- …

Вся информация из публичных источников СМИ

ЛАНДШАФТ УГРОЗ

Внешние факторы влияющие на корпоративную безопасность

Большинство передовых угроз строятся на базовых техниках и методах социальной инженерии

Существенное снижение затрат и массовый рост предложений (Кибератака-Как-Сервис)

Рост количества атак на поставщиков, 3-их лиц и небольшие компании (SMB)

Внутренние факторы влияющие на корпоративную безопасность

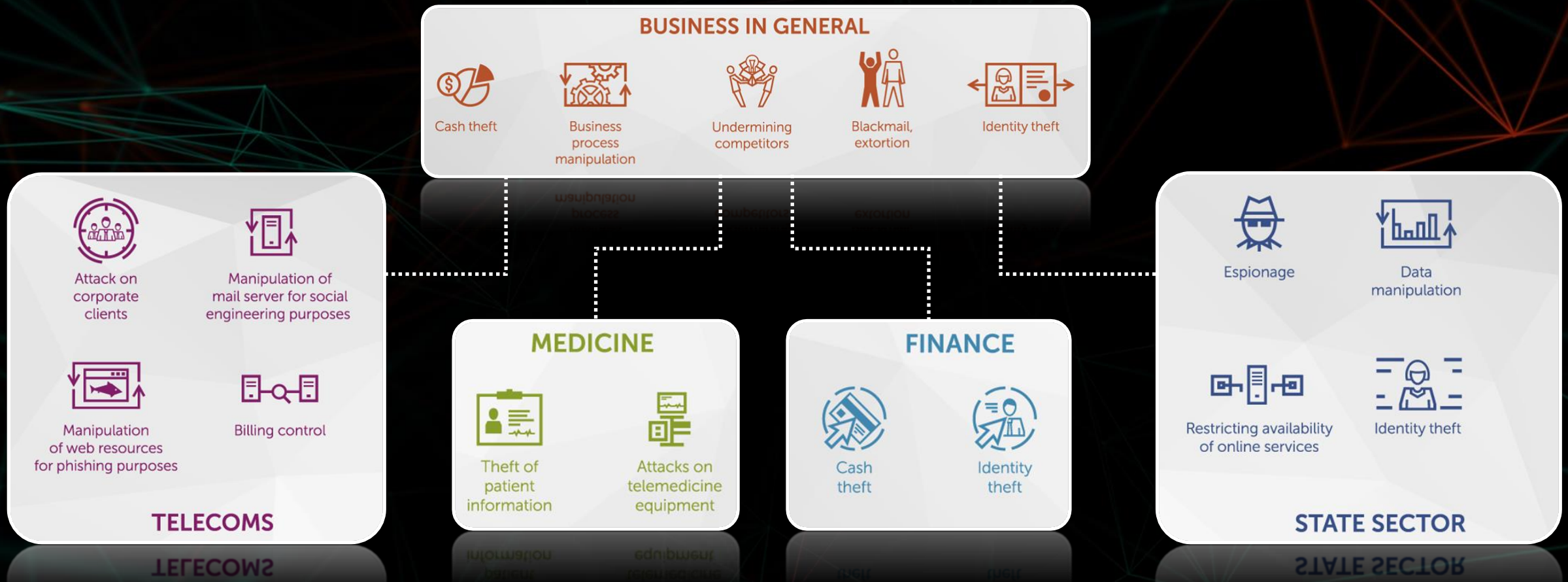
Недостаток оперативной информации в виду динамического усложнения ИТ инфраструктуры

В среднем целевая атака с момента её появления остается необнаруженной более 214 дней

Резкий спад эффективности периметровой защиты

KASPERSKY lab

Иденчиные тактики и методы могут повлечь за собой абсолютно разный результат в зависимости от отрасли



KASPERSKY lab

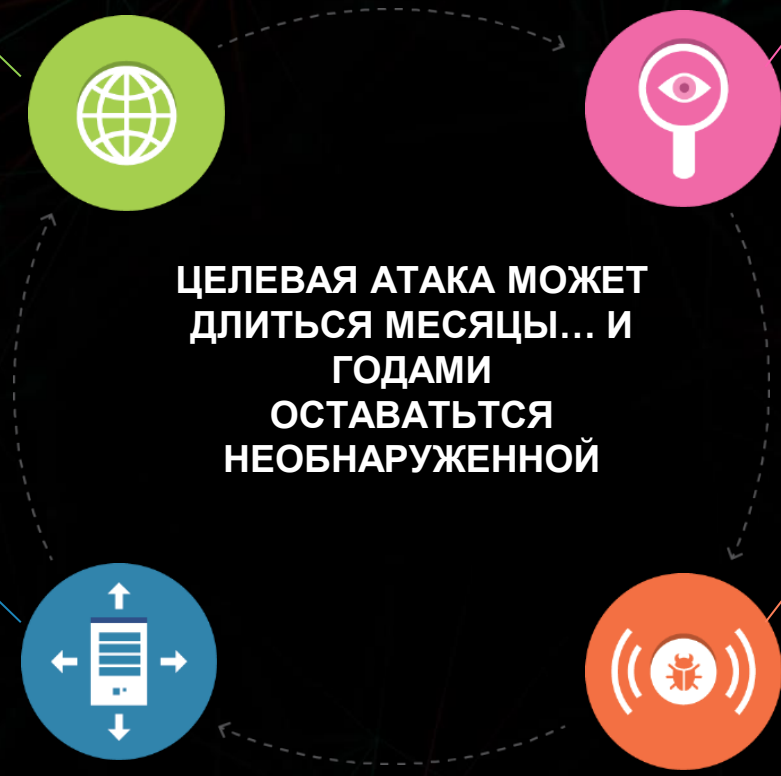
Типовое развитие целенаправленной атаки

НЕГАТИВНОЕ ВОЗДЕЙСТВИЕ

- доступ к информации
- воздействие на бизнес процессы
- сокрытие следов
- тихий уход

ПОДГОТОВКА

- анализ цели
- подготовка стратегии
- создание/покупка тулсета



РАСПРОСТРАНЕНИЕ

- кража идентификационных данных
- повышение привилегий
- налаживание связей
- легитимизация действий
- получение контроля

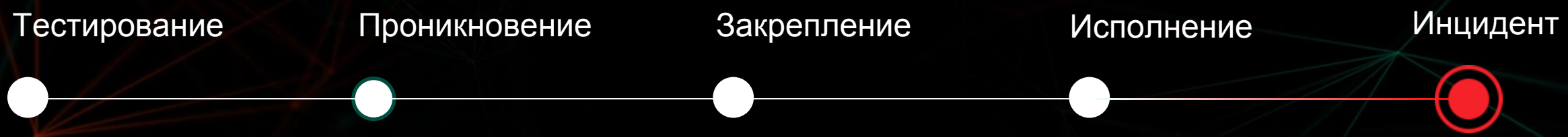
ПРОНИКНОВЕНИЕ

- использование слабых мест
- проникновение внутрь инфраструктуры

KASPERSKY lab

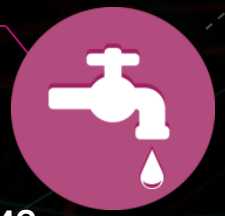
Развитие целенаправленной атаки: Теория и Реальность

В теории… довольно линейное развитие:



Выявление целенаправленных атак традиционными методами

EXFILTRATION ALERTS



- DLP
- поведенческий анализ исходящего трафика
- прокси (MITM)
- NIDS

ABNORMAL ACTIVITIES INCIDENTS

- PIM
- защита баз данных
- контроль доверенной среды

Обнаружение – не только анализ внутренних данных, но и сопоставление с данными внешними.

Threat Intelligence – это краеугольный камень современной ИБ

PREPARATION INDICATORS

- логи межсетевого экрана
- логи web-сервера
- web-firewall

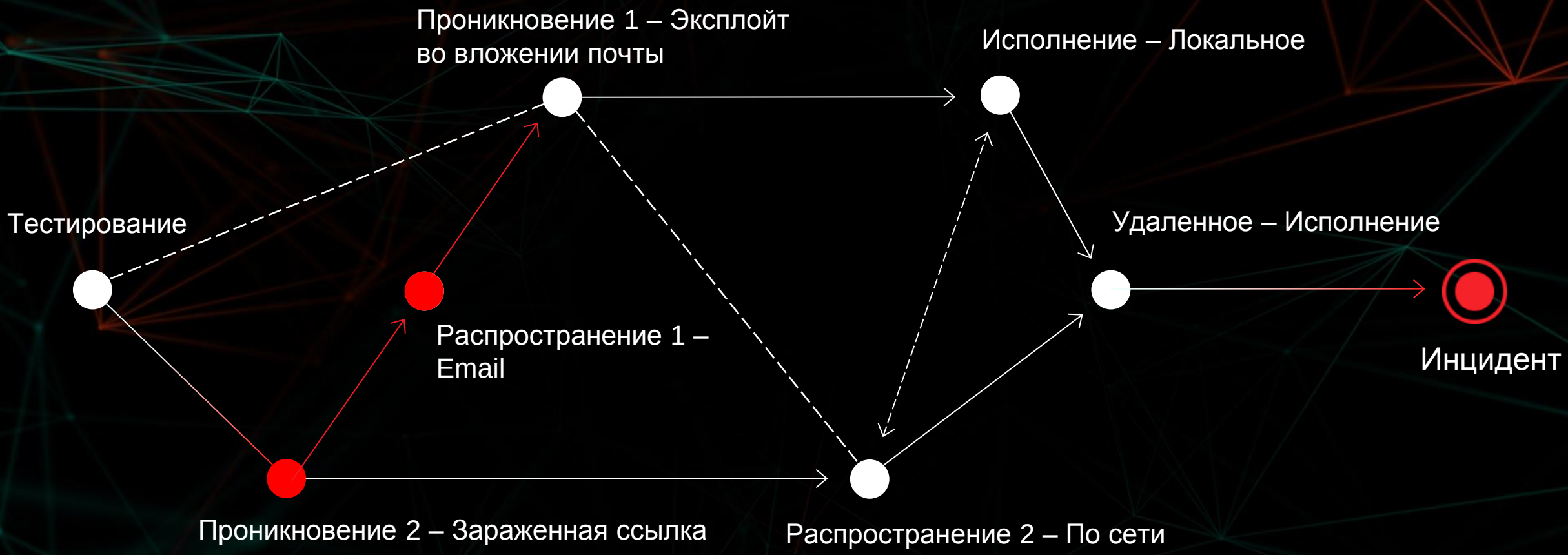
BREACHES EVENTS

- IoC
- mail прокси
- межсетевой экран
- сенсоры трафика
- HIDS, EPP
- логи доступа

KASPERSKY lab

Развитие целенаправленной атаки: Теория и Реальность

В реальности… сложно и нелинейно:



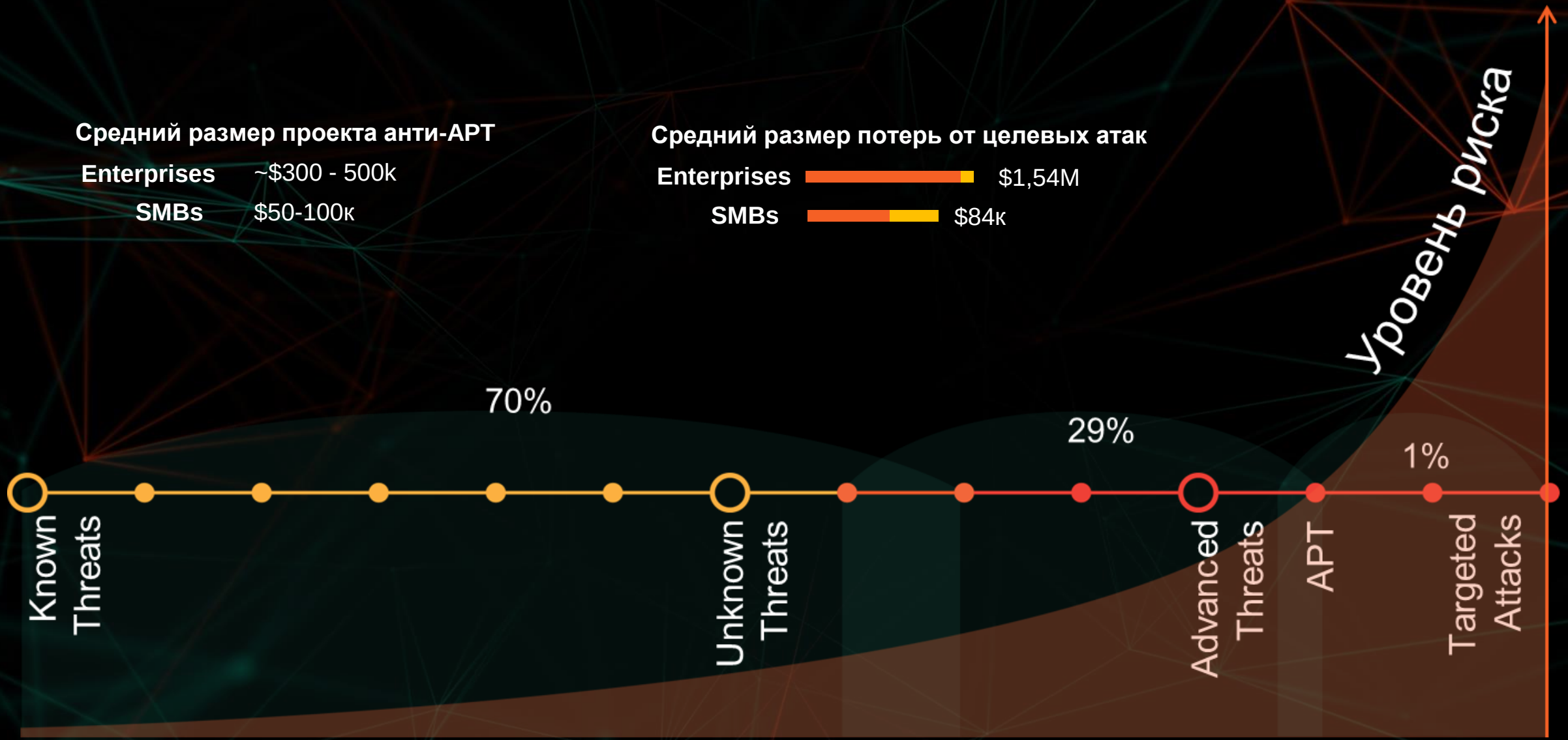
ROI: “1” инцидент может покрыть внедрение анти-APT

Средний размер проекта анти-APT

Enterprises	~$300 - 500k
SMBs	$50-100к

Средний размер потерь от целевых атак

Enterprises	$1,54M
SMBs	$84к



Оценить масштаб угрозы

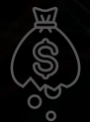
Прямые потери

IT-консалтинг
Аудиторы
PR-активности
Судебные траты

Восстановление

+

Потеря данных, обман и тд.



Возможности

+

Потеря прибыли во время простоя

Простои

Последующие траты

Systems

+

Staffing

+

Training

Чтобы не повторилось вновь

Закрытие уязвимостей
Покупка решений безопасности (DB protection, Endpoint, PIM, SIEM..)
Замена «плохой» системы

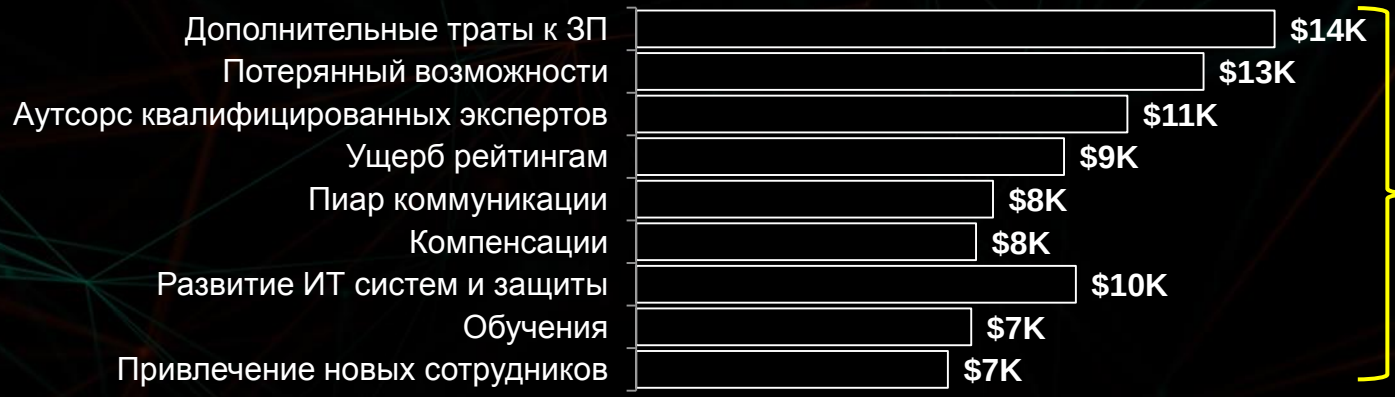
Наём специалистов (ручное обнаружение)
Пересмотр бизнес процессов (новые роли)

Повышение осведомленности сотрудников
Повышение экспертизы службы ИБ

KASPERSKY lab

Статистика потерь за 2016 год от инцидентов ИБ

SMB



Средний ущерб: **$86.5k**

Крупные компании

Средний ущерб: **$891k**

Перераспредленеие трудозатрат ИТ и ИБ служб крупнейшая часть затрат по результату выявленного инцидента

Results from Kaspersky Lab's Corporate IT Security Risks Survey 2016, conducted worldwide by Kaspersky Lab

Base: 926 SMBs/ 590 Enterprises
Suffering At Least One Data Breach

KASPERSKY lab

Выводы при построении передовой корпоративной безопасности

- Большинство «передовых» атак основаны на базовых уязвимостях
- Возможности обнаружить и отреагировать гораздо важнее блокирования и предотвращения
- «Реагирование на скоррелированные инциденты" даёт ложное чувство безопасности
- Защита от передовых угроз должна быть эшелонированно интегрированной, а не «кусочной»
- Мониторинг данных и аналитика должны быть базисом для любого next-gen решения по обеспечению ИБ
- Автоматизация – это «порочный путь» при защите от ручных действий злоумышленников.
  Необходима комплексная стратегия защиты

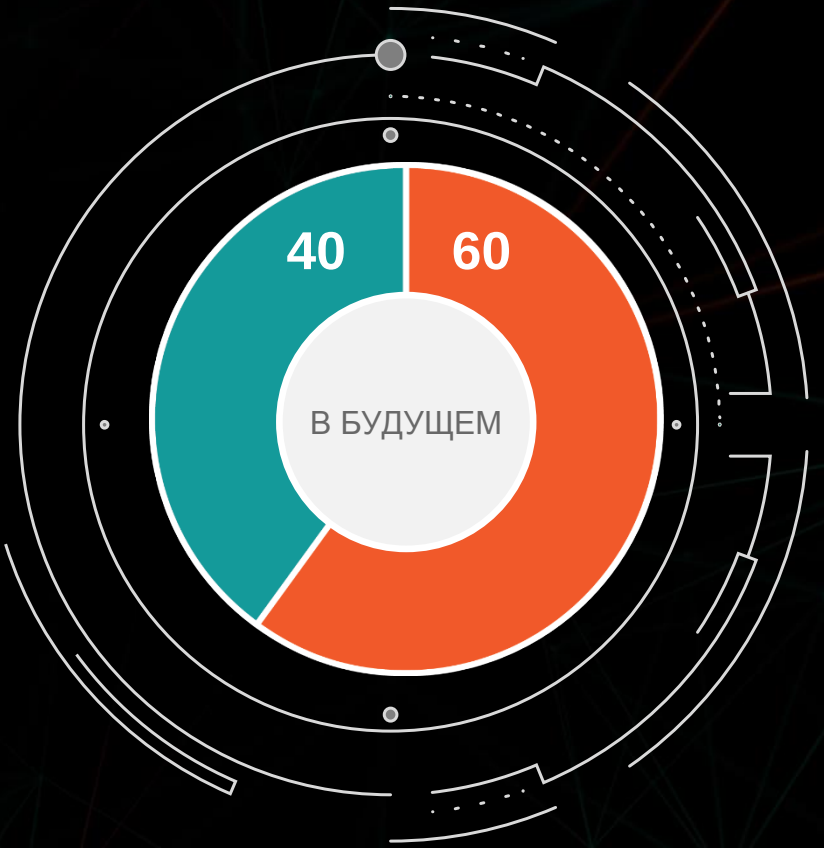
KASPERSKY lab

Эволюция ожиданий бизнеса

Текущий размер инвестиций:
80% на превентивные технологии / 20% на обнаружение, реагирование и прогнозирование
(Крупные компании: 90%/10%)

Планы опрошенных заказчиков
на ближайшие 3 года: 40% / 60%

Основано на опросе, проведенном «Лабораторией Касперского» в ноябре 2015 года среди свыше 6700 компаний по всему миру



KASPERSKY lab

ЗАЩИТА ОТ ЦЕЛЕВЫХ АТАК

Адпативная модель организации ИБ от Gartner

ПРОГНОЗИРОВАНИЕ

- Анализ потенциальных целей злоумышленников
- Управление уязвимостями
- Планирование развития стратегии защиты
- Создание адаптивного SOC

Угрозы

ПРЕДОТВРАЩЕНИЕ

- Снижение рисков проникновения
- Повышение эффективности решений и процессов ИБ
- Повышение осведомленности сотрудников

Атаки

THREAT INTELLIGENCE

РЕАГИРОВАНИЕ

- Оперативное реагирование на инциденты ИБ
- Расследование природы атаки:
  - реконструкция
  - сбор доказательств
  - поиск скомпрометированных активов

Инциденты

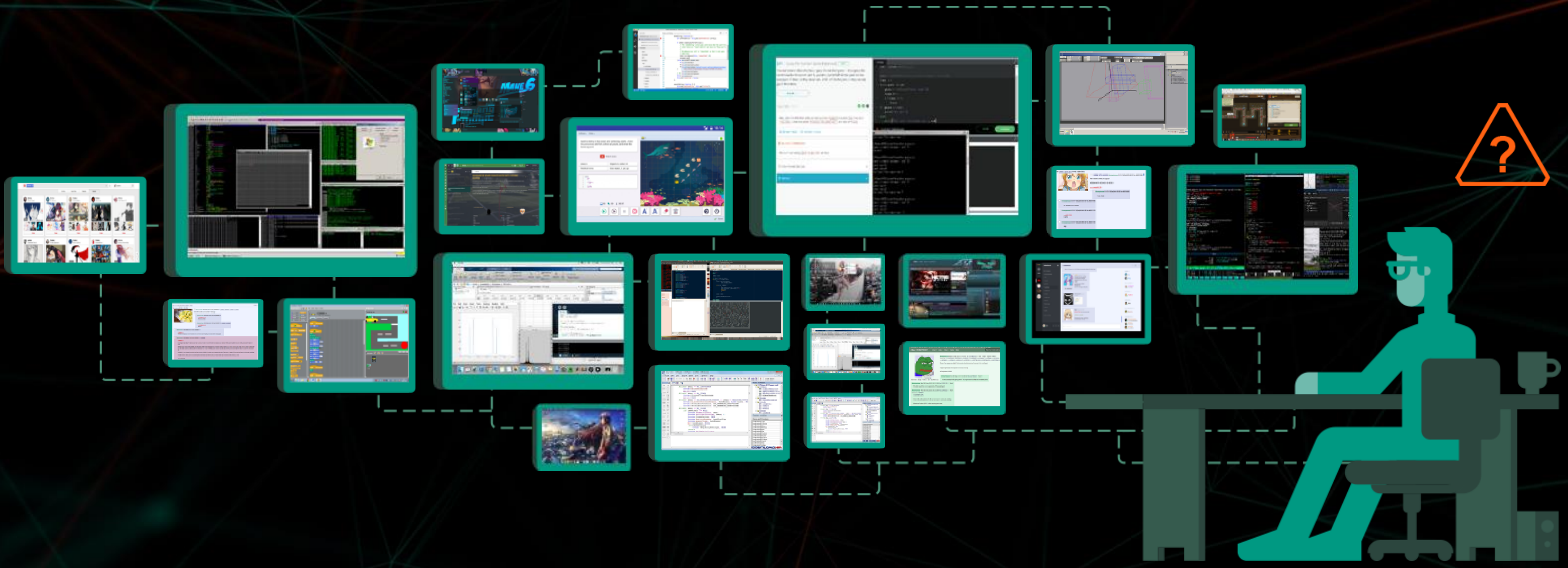
ОБНАРУЖЕНИЕ

- Выявление попыток и фактов существующего проникновения
- Подтверждение и приоритезация событий ИБ

Вторжения

KASPERSKY lab

ЗА[illegible] ЗАГРУЗКИ
С[illegible]НУ… ВРУЧНУЮ НЕ РЕШАЕМА!



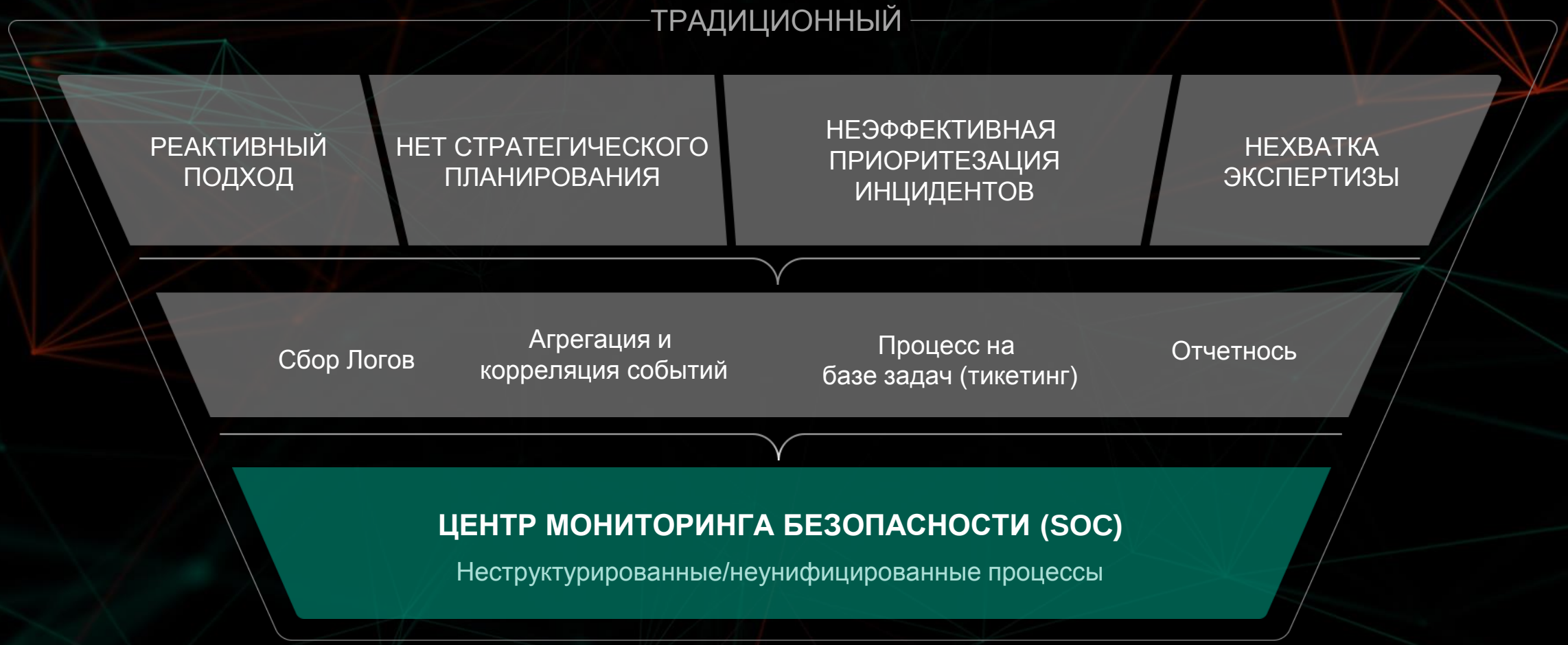
В РЕЗУЛЬТАТЕ ОРГАНИЗАЦИИ ПРИХОДЯТ К ИДЕОЛОГИИ ПОСТРОЕНИЯ ЦЕНТРА МОНИТОРИНГА ИБ (SOC)

ВЫЯВЛЕНИЕ

С ВЫДЕЛЕННОЙ СЛУЖБОЙ МОНИТОРИНГА И АНАЛИЗА

КОРРЕЛЯЦИЯ

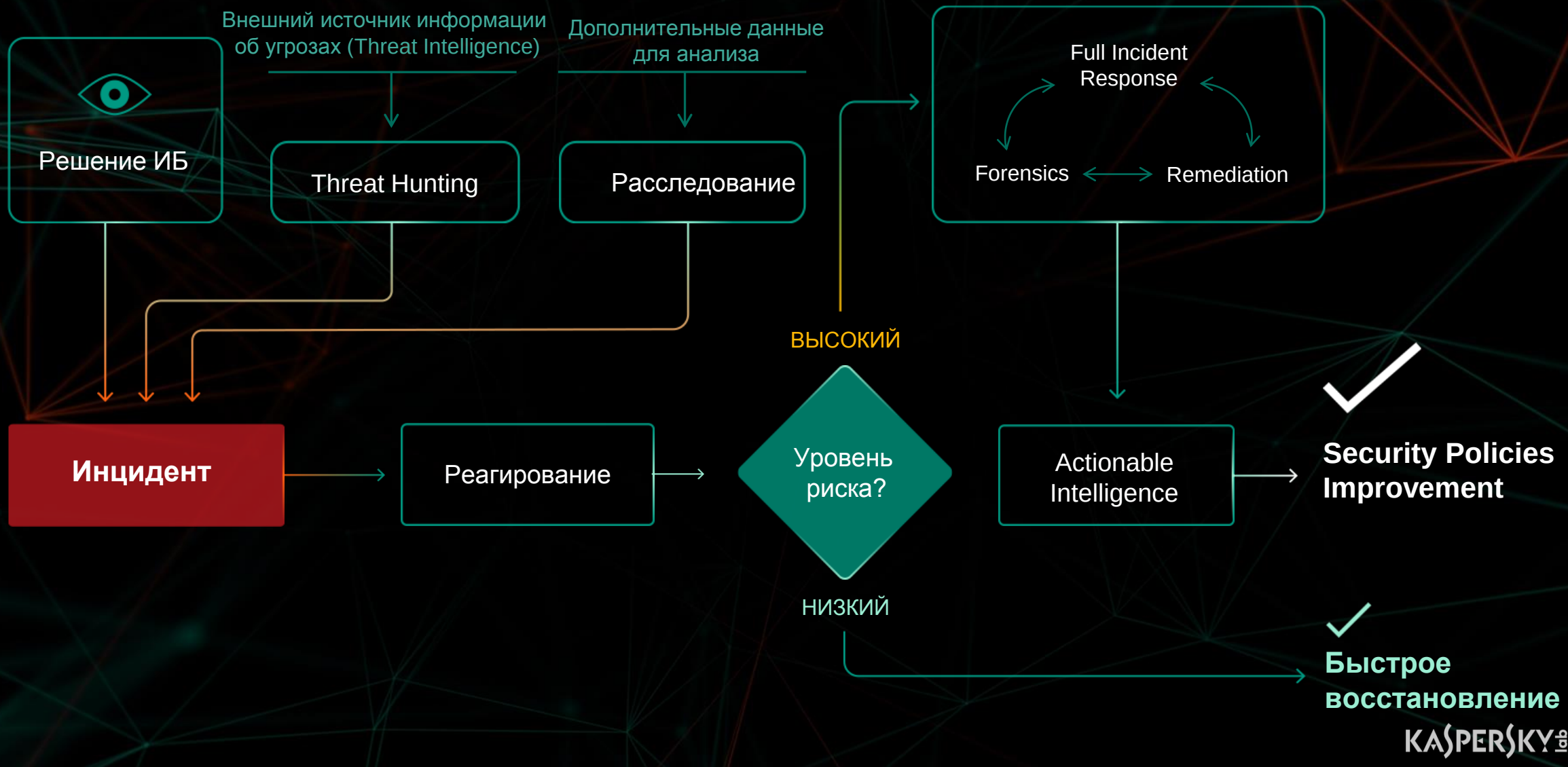
НЕДОСТАТКИ ТРАДИЦИОННОГО ПОДХОДА ДЛЯ ЦЕНТРА МОНИТОРИНГА БЕЗОПАСНОСТИ (SOC)



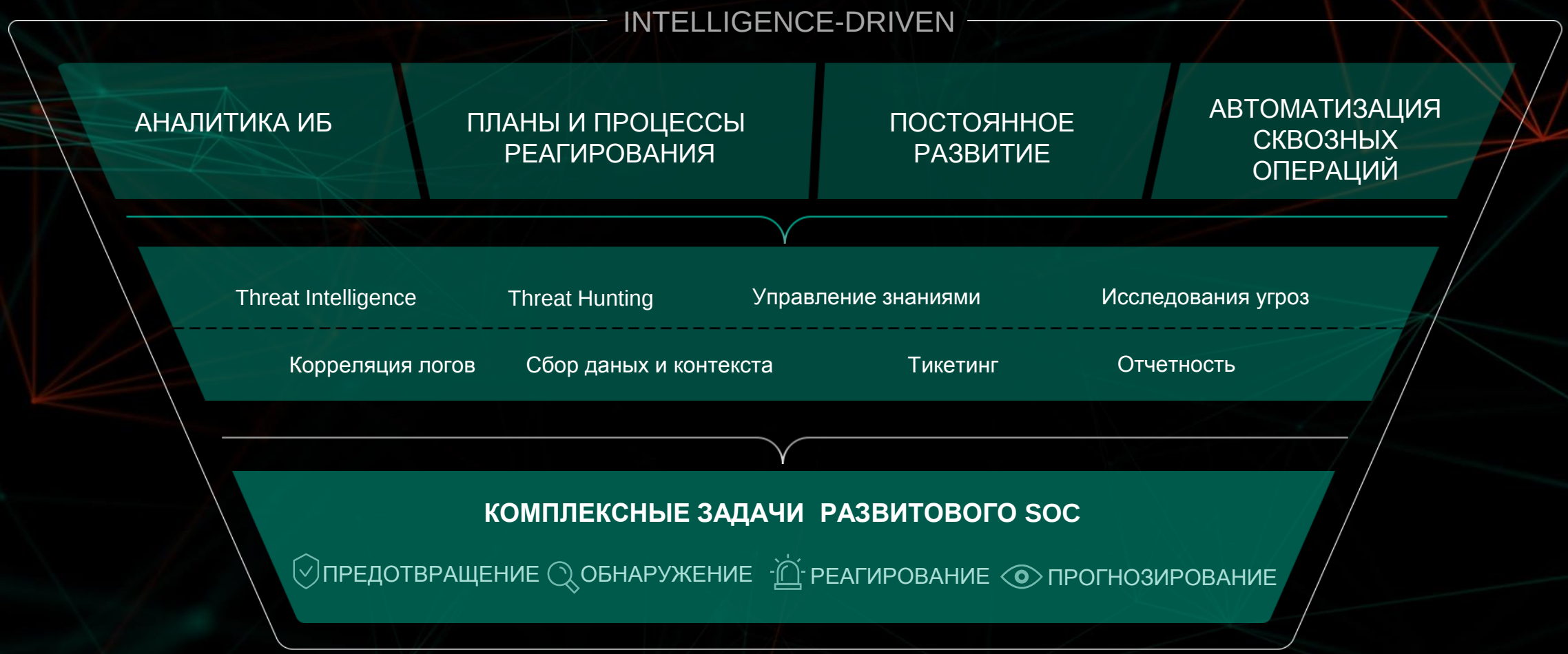
НЕПРОРАБОТАННОСТЬ ПРОЦЕССОВ РЕАГИРОВАНИЯ – НЕДОСТАТОК БОЛЬШИНСТВА ТРАДИЦИННЫХ SOC

РЕАГИРОВАНИЕ

ЗРЕЛЫЙ ПРОЦЕСС РЕАГИРОВАНИЯ НА ОСНОВЕ УПРАВЛЕНИЯ РИСКАМИ И РАССЛЕДОВАНИЯ



Развитый центр мониторинга ИБ должен быть интеллектуальным



Адаптивная стратегия корпоративной безопасности для развития ключевых процессов

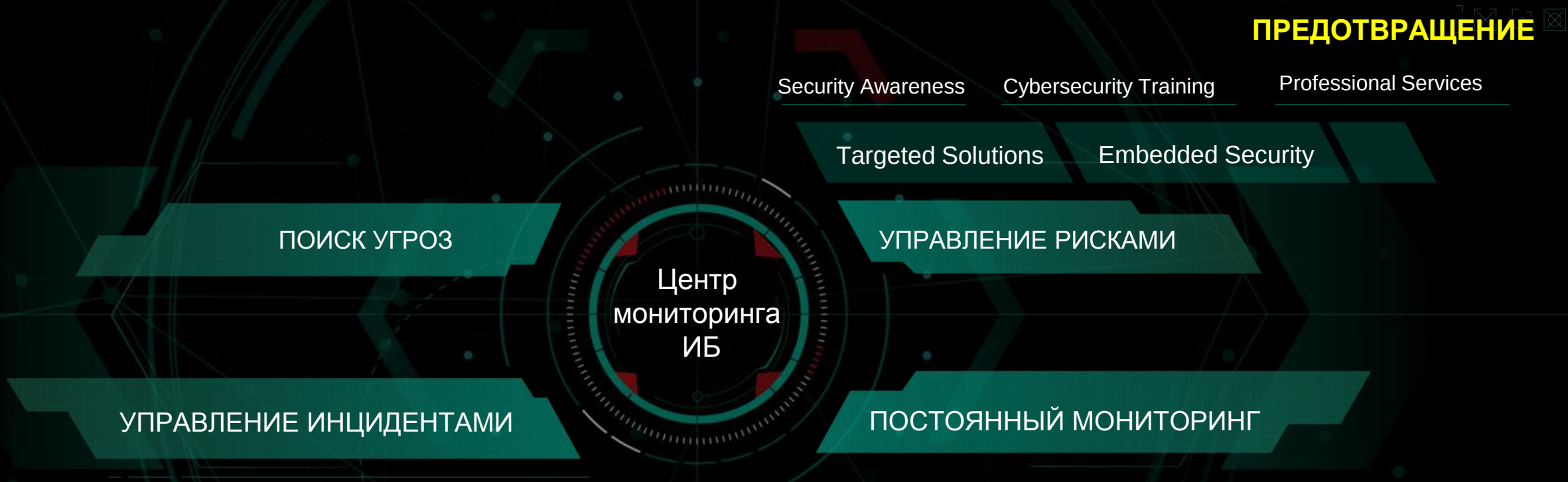
ПРОГНОЗИРОВАНИЕ Глобальная экспертиза

Передовые решения **ПРЕДОТВРАЩЕНИЕ**

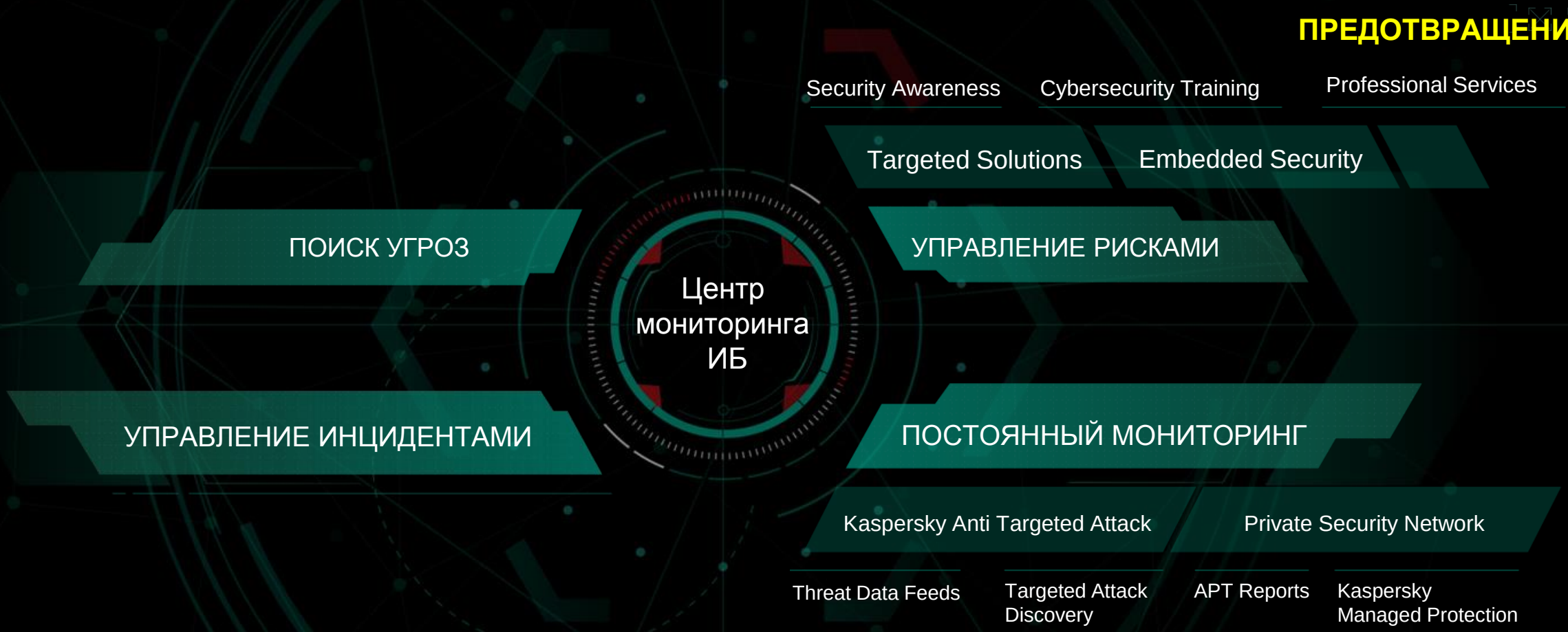
РЕАГИРОВАНИЕ Эффективное реагироание

Многоуровневое обнаружение **ОБНАРУЖЕНИЕ**

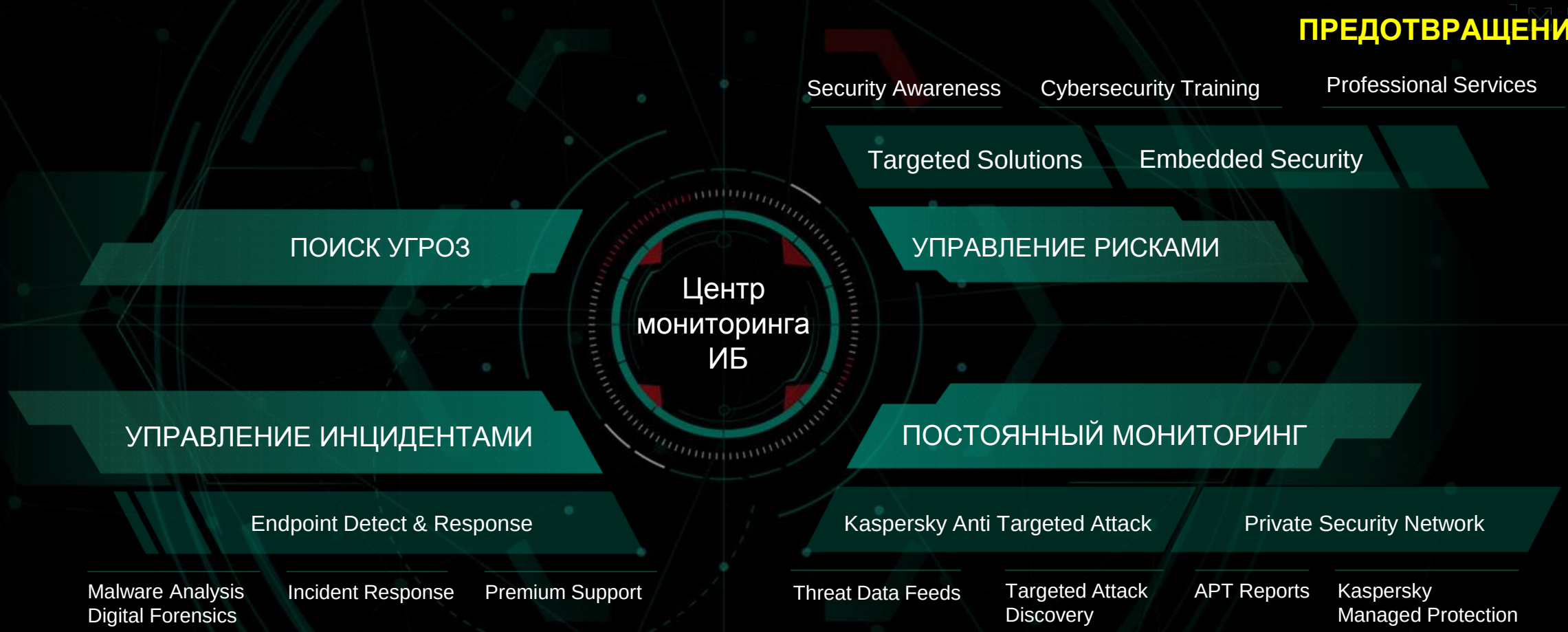
Увеличить стоимость успешного проникновения



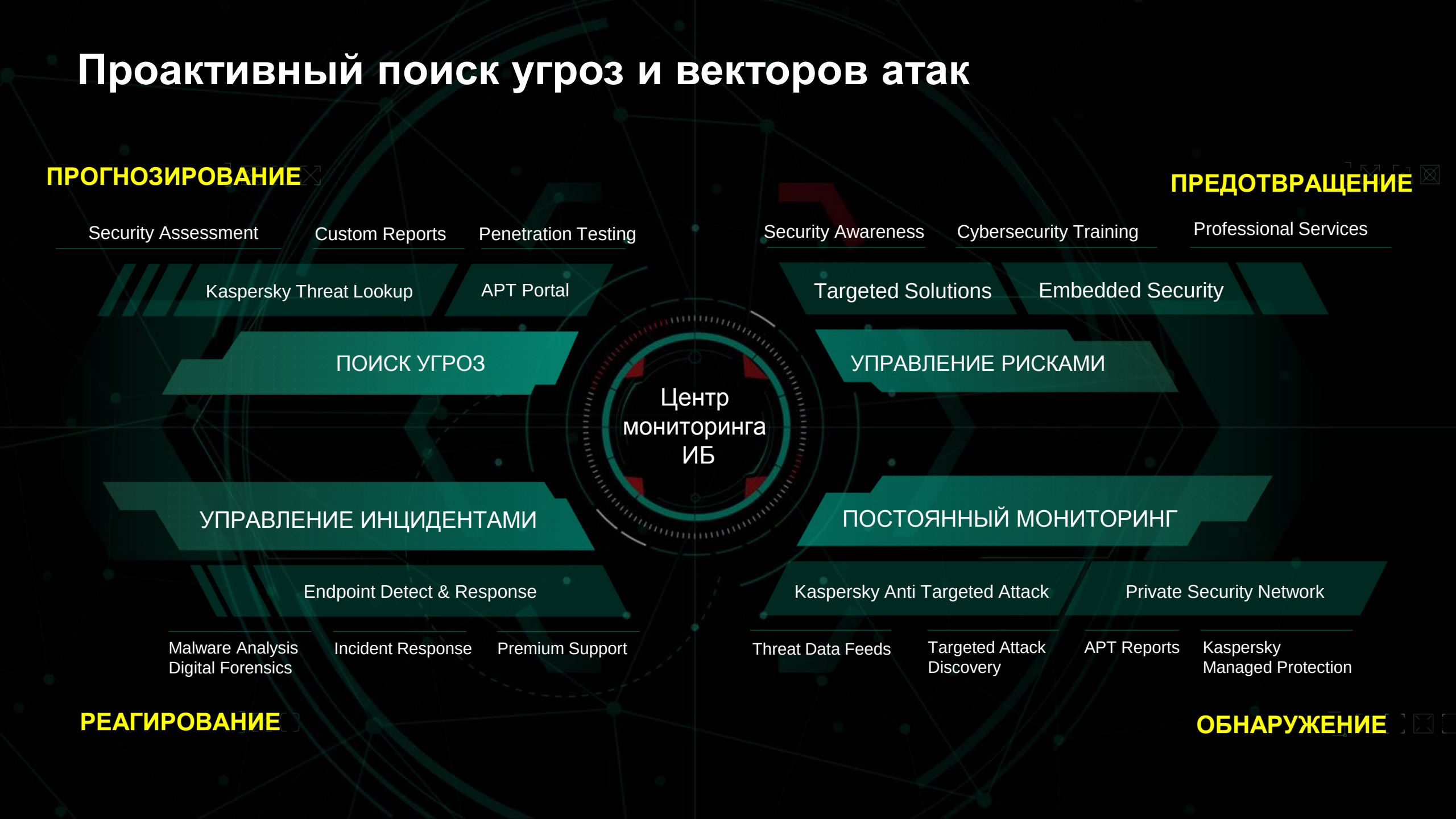
Обнаружить угрозу до того как нанесен ущерб



Построение эффективного процесса реагирования



Проактивный поиск угроз и векторов атак



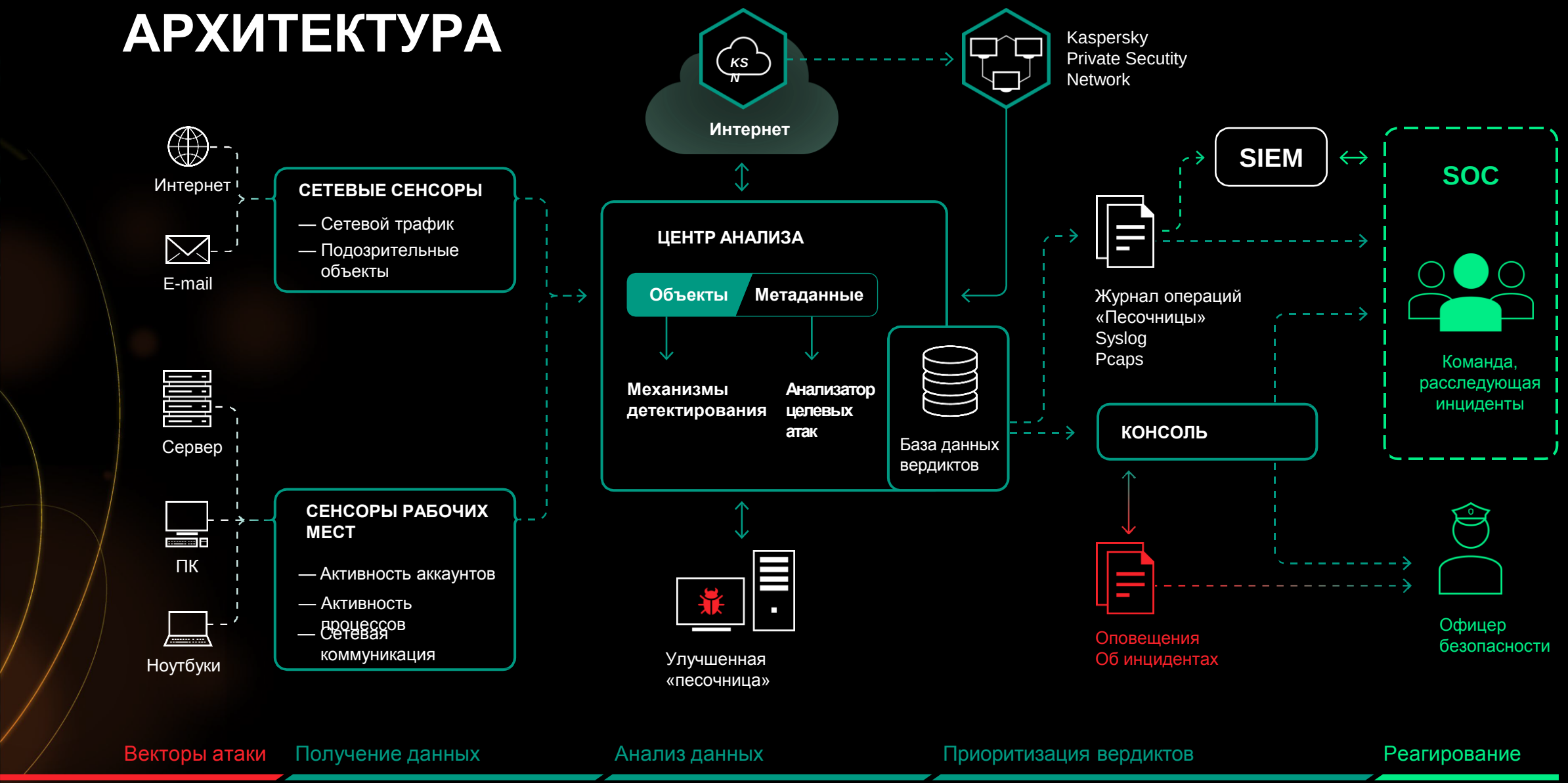
Kaspersky Anti Targeted Attack platform

KASPERSKY lab

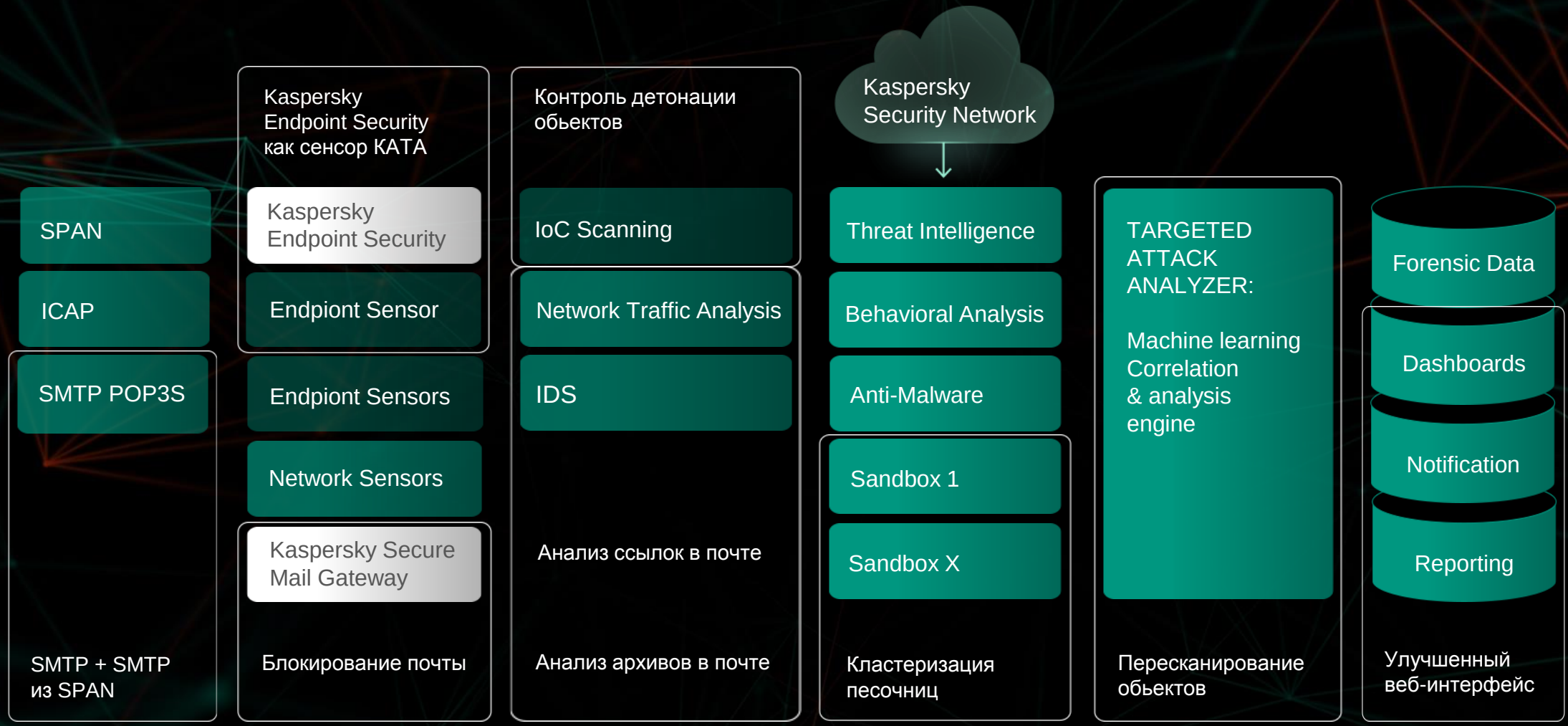
Интегрированное решение Kaspersky Anti Targeted Attack

KASPERSKY lab

АРХИТЕКТУРА



2017: KASPERSKY ANTI TARGETED ATTACK (KATA v.2) PLATFORM



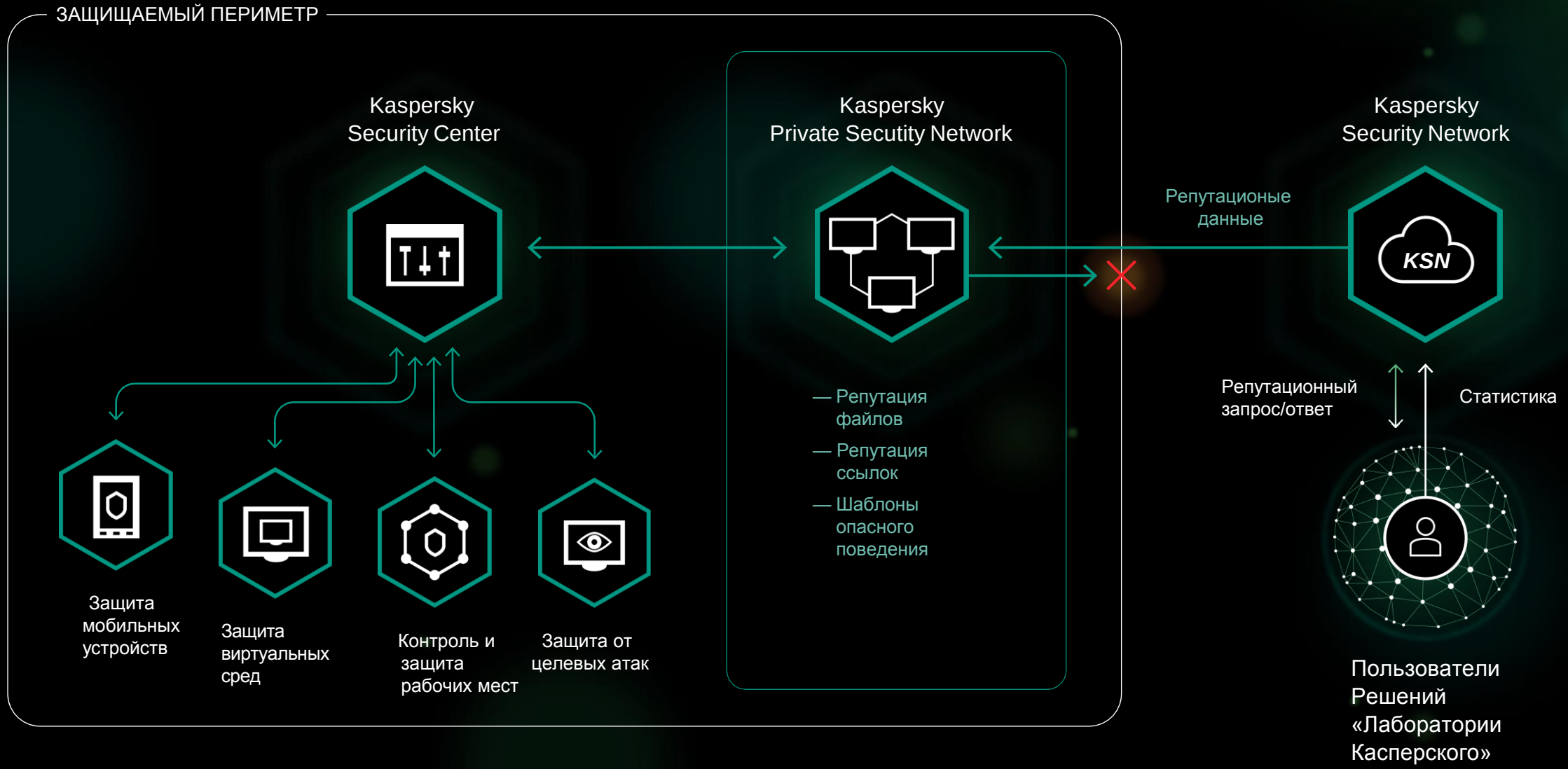
ОБЛАЧНЫЕ ДАННЫЕ ОБ УГРОЗАХ

Информация об угрозах поступает от более 60 млн пользователей

Глобальные данные об угрозах в режиме реального времени

Постоянное использование данных в защитных решениях

KASPERSKY PRIVATE SECURITY NETWORK

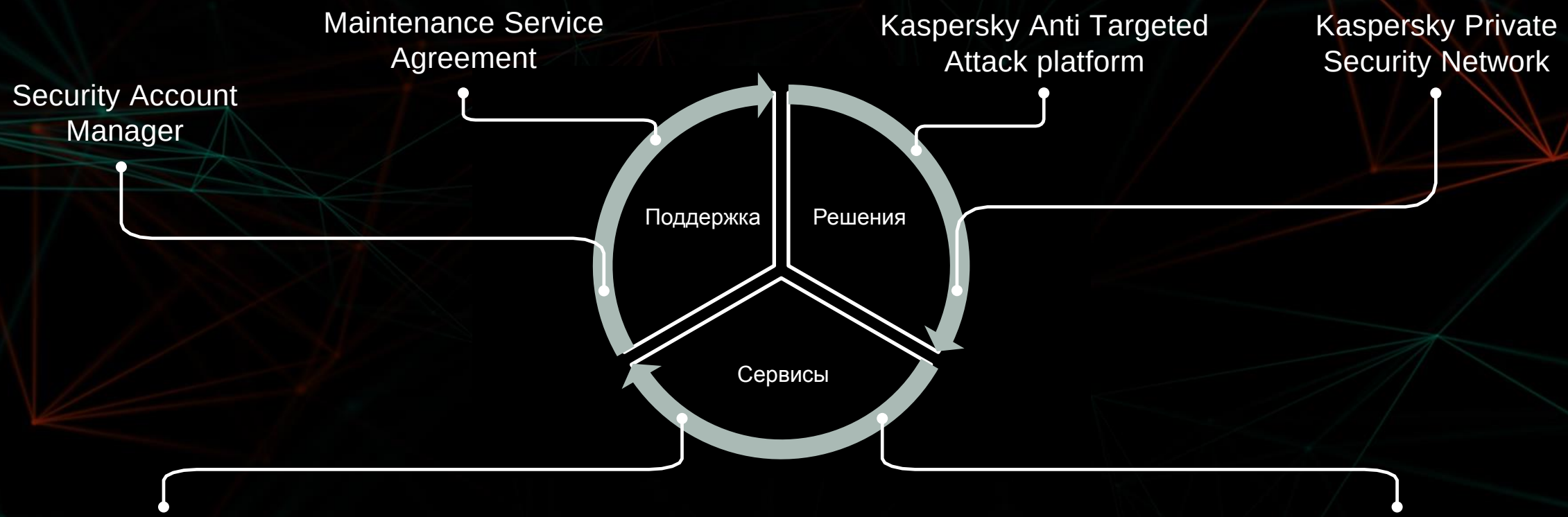


Преимущества решения Kaspersky Anti Targeted Attack

- Гибкость установки и масштабируемость, нет привязки к аппаратному исполнению
- Простота лицензирования
- Сертификация ICSA, последний отчет Radicati Group 2017
- Совместимость с конкурентными и классическими решениями по ИБ
- Многоуровневый анализ целенаправленных атак комплексным взаимодействием разнородных детектирующих механизмов
- Сертификат ФСБ (АВ), наличие в реестре российского ПО
- 2017 – сертификат ФСТЭК (СОВ, анти-APT), сертификат ФСБ (СОВ), СОПКА ready

KASPERSKY lab

Формирование комплексного анти-APT проекта



- Сервис реагирования на инциденты
- Kaspersky Managed Protection

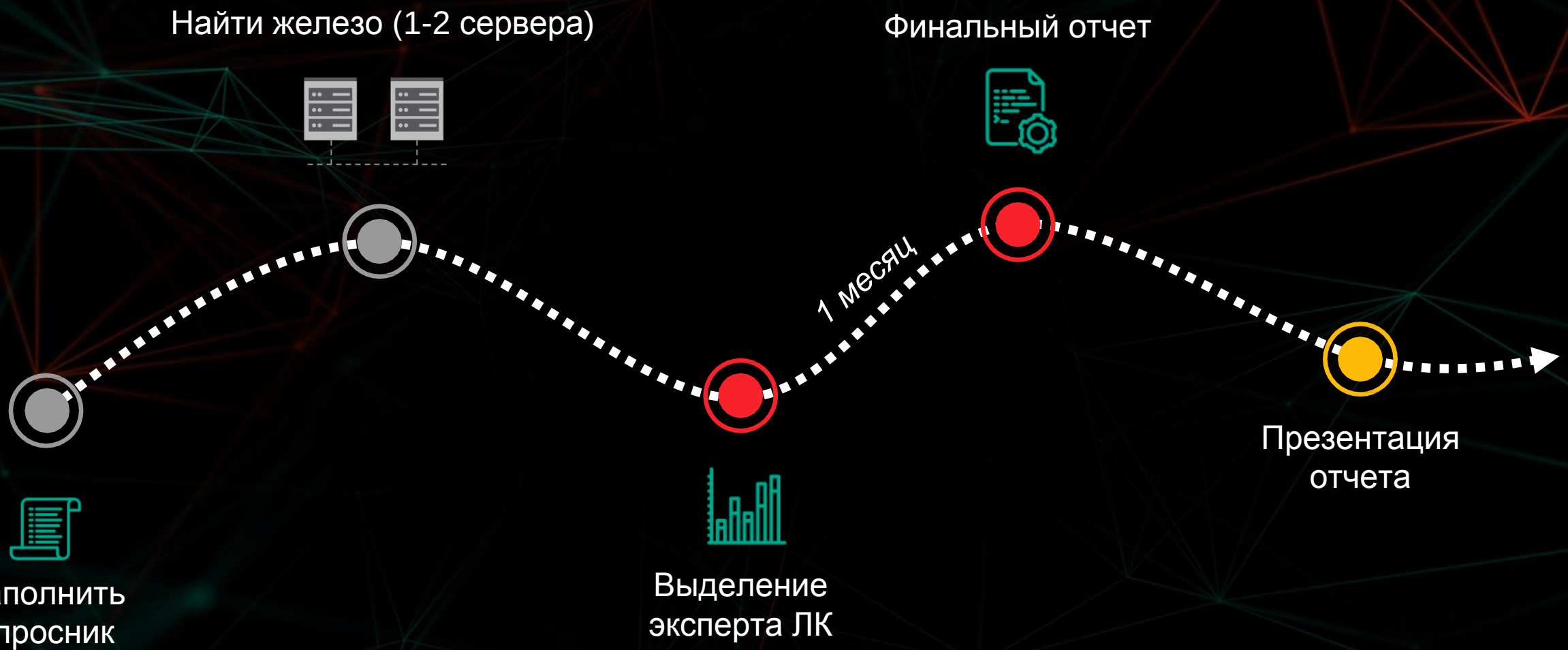
- Тренинги и обучения

Kaspersky Anti Targeted Attack platform

Пилотирование

KASPERSKY lab

Этапы пилотирования



«ЛАБОРАТОРИЯ КАСПЕРСКОГО» НА РЫНКЕ

НАШИ КЛИЕНТЫ

Мы работаем с компаниями из самых разных отраслей. Наши решения и сервисы успешно защищают 270 000 компаний по всему миру.

Общественные организации

Образование

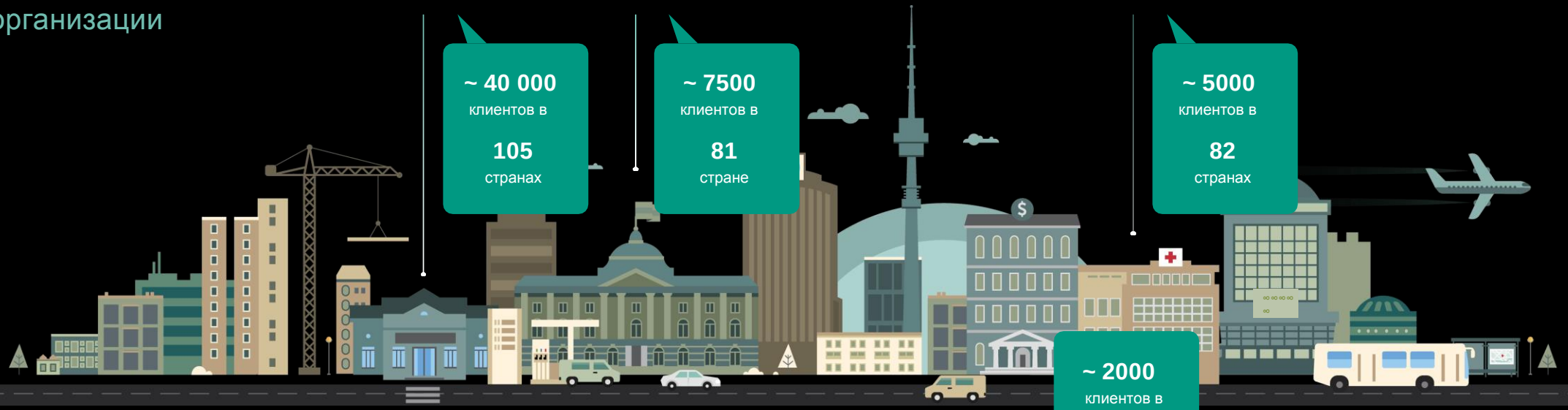
~ 40 000 клиентов в 105 странах

Госучреждения

~ 7500 клиентов в 81 стране

Здравоохранение

~ 5000 клиентов в 82 странах



~ 2000 клиентов в 123 странах

Частные компании

Строительство

Нефть и газ

Медиа

Телеком

Финансы

Технологии

Транспорт

Корпоративные заказчики доверяют «Лаборатории Касперского»

«Во-первых, печально известные Carbanak, GCMAN и другие группировки киберпреступников заставляют всерьез задуматься о комплексной защите от целенаправленных атак, а с помощью KATA мы можем применять еще и превентивные меры.

Во-вторых, решение “Лаборатории Касперского” имеет соответствующий сертификат ФСБ РФ и входит в Реестр отечественного ПО, что было немаловажно для нас. А сервис Kaspersky Managed Protection позволяет нам в особо трудных ситуациях получать поддержку экспертов самого высокого уровня. Так что с учетом всех потенциальных угроз, рисков и затрат решение “Лаборатории Касперского” оказалось лучшим вариантом»,

- Дмитрий Григорович, руководитель по информационной безопасности Управления безопасности и режима

Вся информация из публичных источников СМИ

Корпоративные заказчики доверяют «Лаборатории Касперского»

"Почта России" по результату тендера заключила договор с крупным российским интегратором на сумму **133 млн руб**.

В "Почте России« отметили, важной частью сотрудничества стало взаимодействие по выявлению и устранению последствий компьютерных инцидентов и целевых атак.

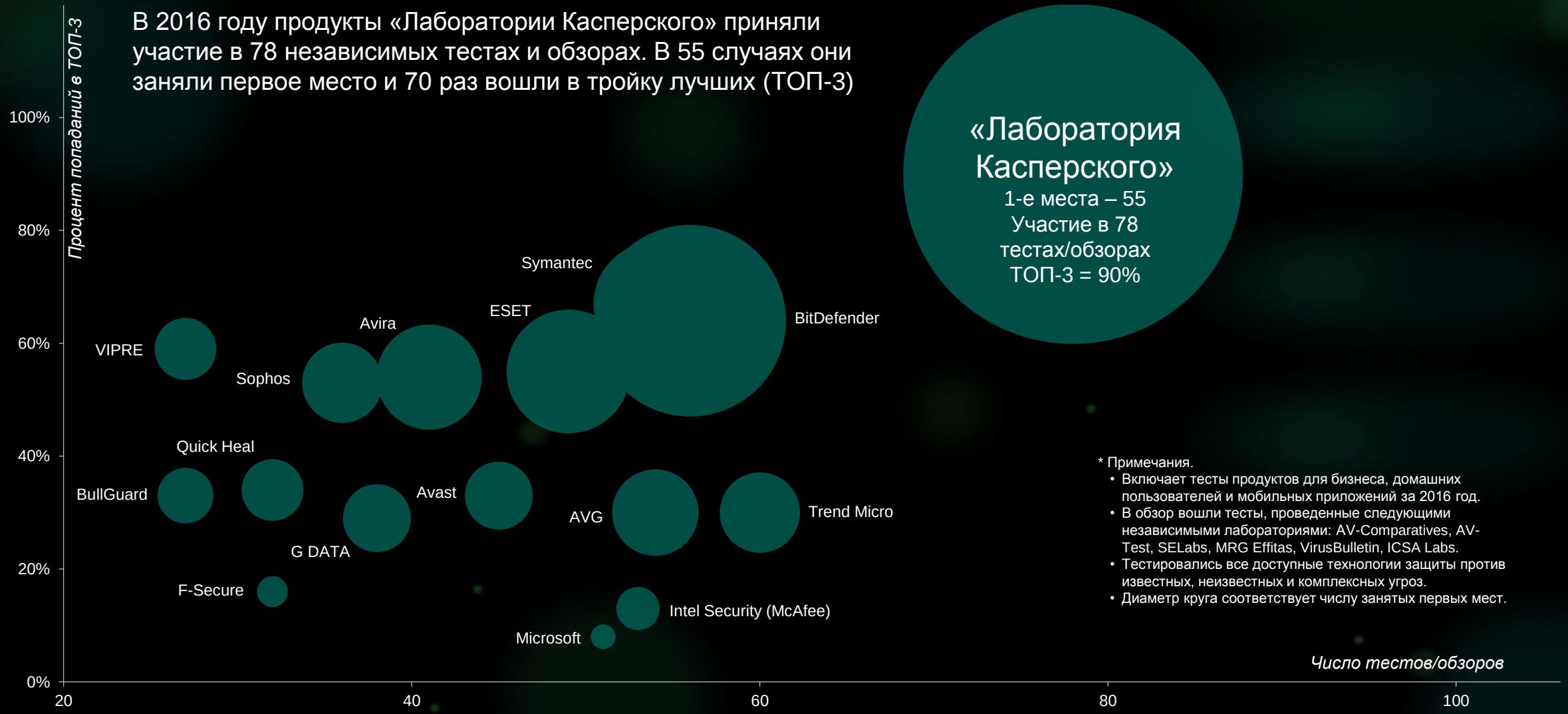
"Для реализации этой задачи были достигнуты договоренности об использовании в будущем экспертных сервисов "Лаборатории Касперского" и специализированной платформы для противодействия сложным и хорошо спланированным кибератакам"

"Принятое решение об использовании комплексной защиты - это логичный шаг в построении по-настоящему всесторонней и продуманной системы противодействия актуальным киберугрозам. Технологии, которые предлагает отечественная "Лаборатория Касперского", не только технически решают наши текущие потребности, но также позволяют получить доступ к обширной базе знаний и экспертному опыту, без которых качественное решение многих задач было бы невозможно",

Вся информация из публичных источников СМИ

МЕЖДУНАРОДНЫЕ НАГРАДЫ И ПРИЗНАНИЕ

В 2016 году продукты «Лаборатории Касперского» приняли участие в 78 независимых тестах и обзорах. В 55 случаях они заняли первое место и 70 раз вошли в тройку лучших (ТОП-3)

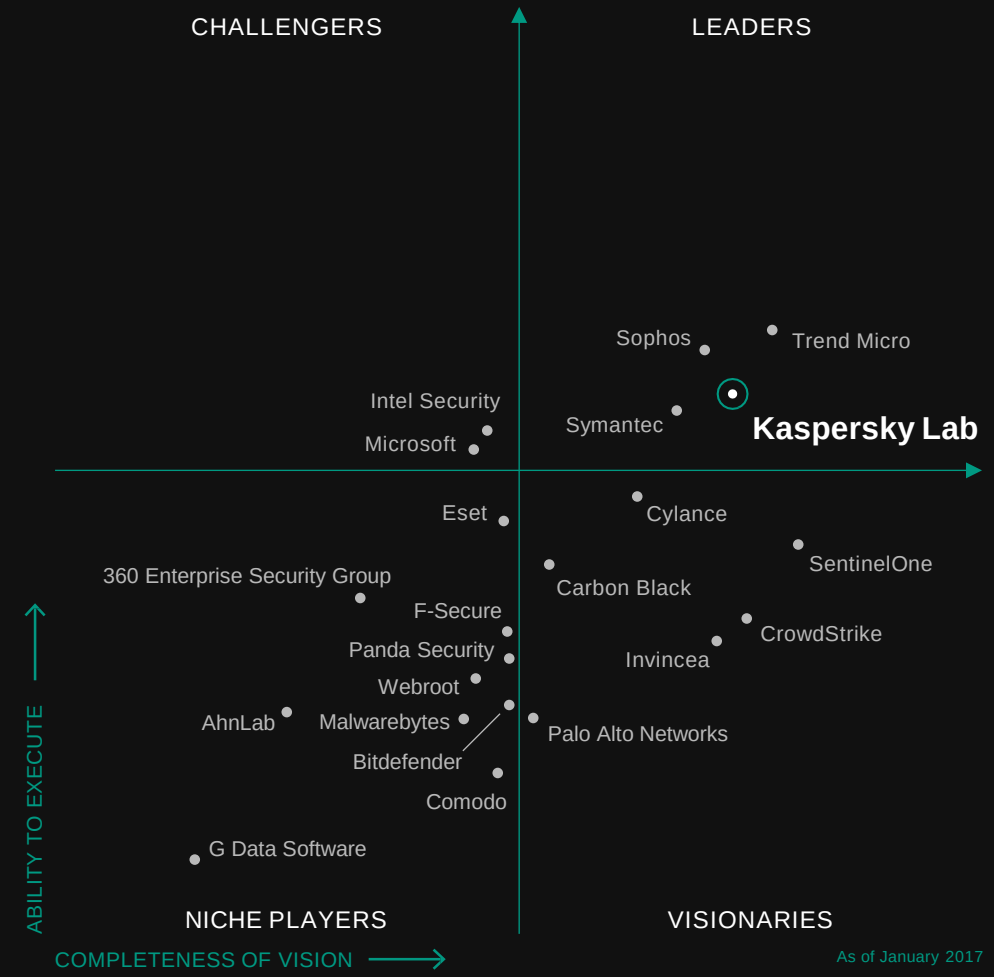


«Лаборатория Касперского»
1-е места – 55
Участие в 78 тестах/обзорах
ТОП-3 = 90%

* Примечания.

- Включает тесты продуктов для бизнеса, домашних пользователей и мобильных приложений за 2016 год.
- В обзор вошли тесты, проведенные следующими независимыми лабораториями: AV-Comparatives, AV-Test, SELabs, MRG Effitas, VirusBulletin, ICSA Labs.
- Тестировались все доступные технологии защиты против известных, неизвестных и комплексных угроз.
- Диаметр круга соответствует числу занятых первых мест.

6 ЛЕТ ПОДРЯД В КАТЕГОРИИ «ЛИДЕРЫ»



Gartner

В 2017 году «Лаборатория Касперского» в шестой раз подряд попала в число «Лидеров» в Магическом квадранте компании Gartner в категории Endpoint Protection Platforms (решения для защиты конечных устройств).

Эксперты высоко оценили деятельность компании по обоим направлениям аттестации: «стратегическое видение» и «эффективность реализации».

Magic Quadrant for Endpoint Protection Platforms, 30 January 2017

ТЕХНОЛОГИЧЕСКИЕ ПАРТНЕРЫ

~ 120 ведущих компаний доверяют нам защиту своих клиентов

— Интеграция технологий
— Собственные марки / Кобрендинг
— Предустановка / Набор продуктов
— Предзагрузка

СПАСИБО!

Контакты ДиалогНаука:
marketing@DialogNauka.ru
8 (495) 980-67-76

KASPERSKY lab