Стратегия противодействия таргетированным атакам. Опыт «Лаборатории Касперского

Кирилл Керценбаум
Директор по корпоративным решениям
Kaspersky Lab

KASPERSKY lab

Современные целенаправленные атаки

Тенденции и ландшафт угроз

KASPERSKY lab

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

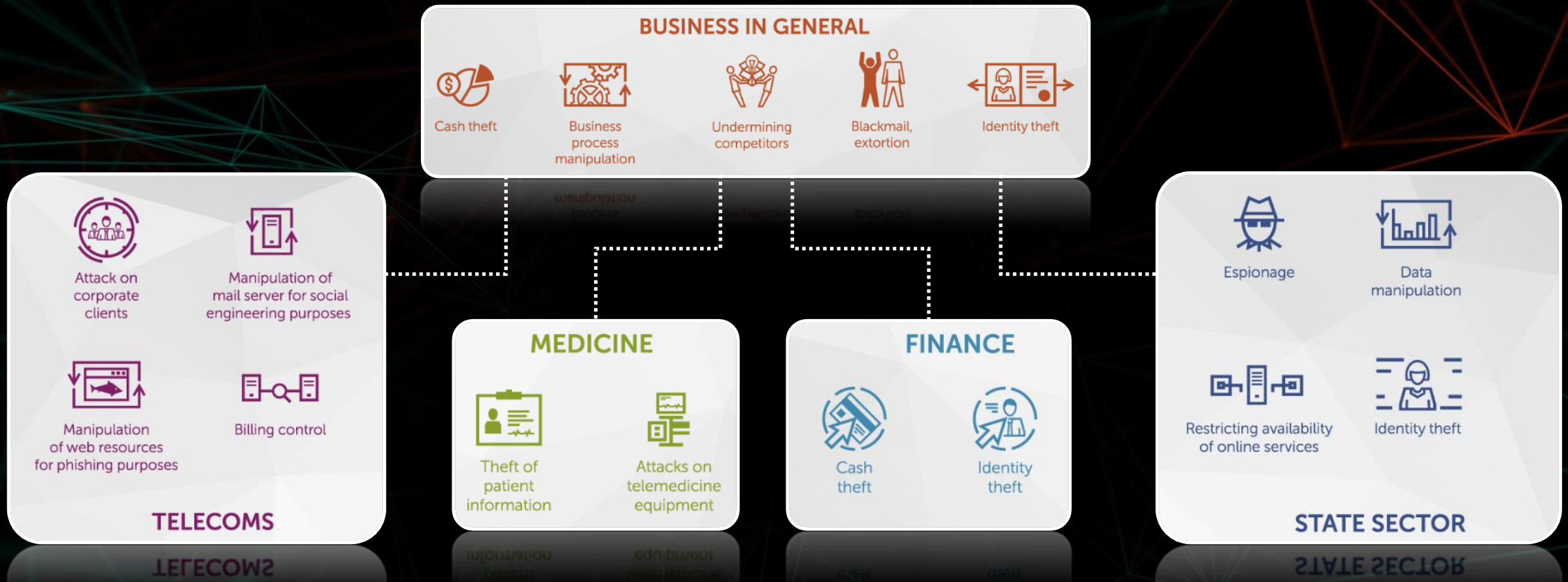
Закрытие уязвимостей
Покупка решений безопасности (DB protection, Endpoint, PIM, SIEM..)
Замена «плохой» системы

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

Повышение осведомленности сотрудников
Повышение экспертизы службы ИБ

KASPERSKY lab

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



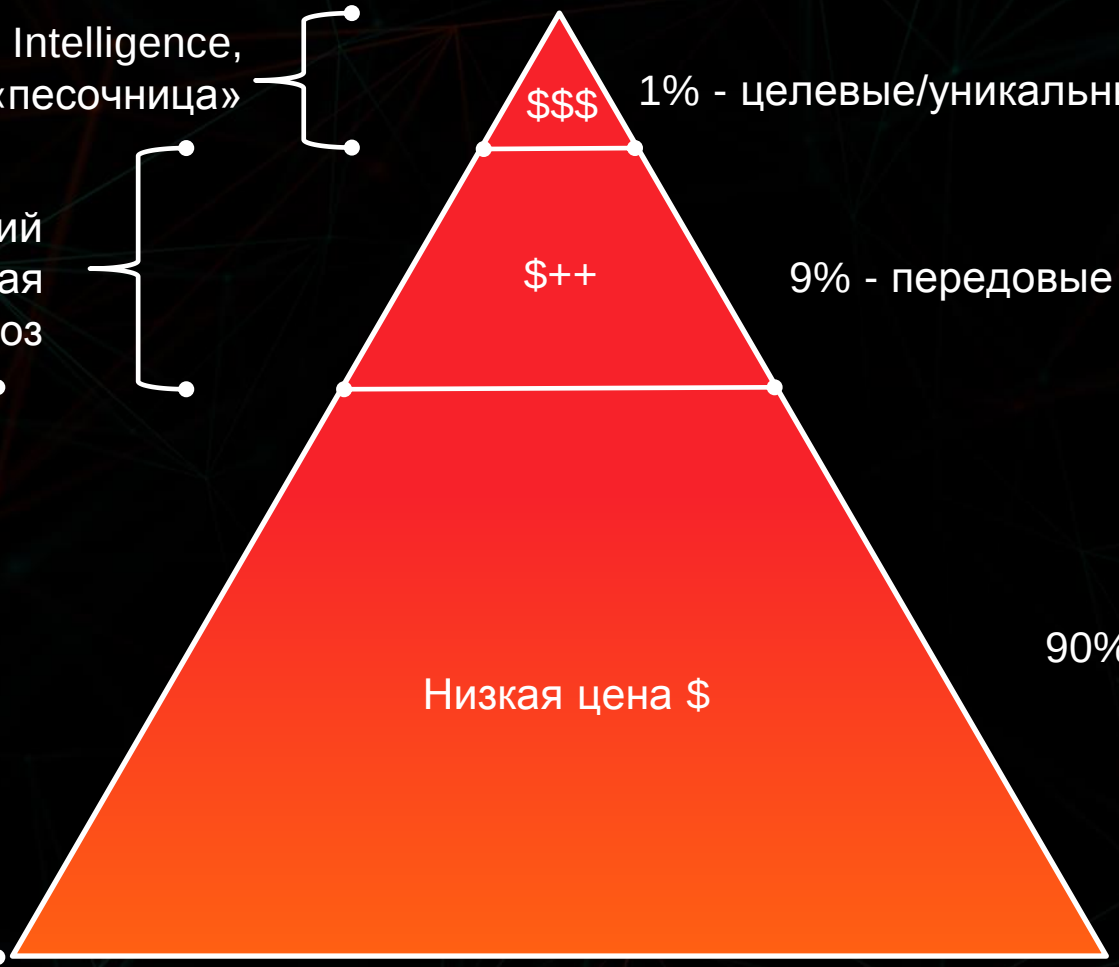
KASPERSKY lab

Таксономия ландшафта угроз и соотвествующих технологий защиты

Машинное обучение, Threat Intelligence, динамический анализ «песочница»

Эвристика и поведенческий анализ, глобальная облачная репутация и статистика угроз

Сигнатуры и правила

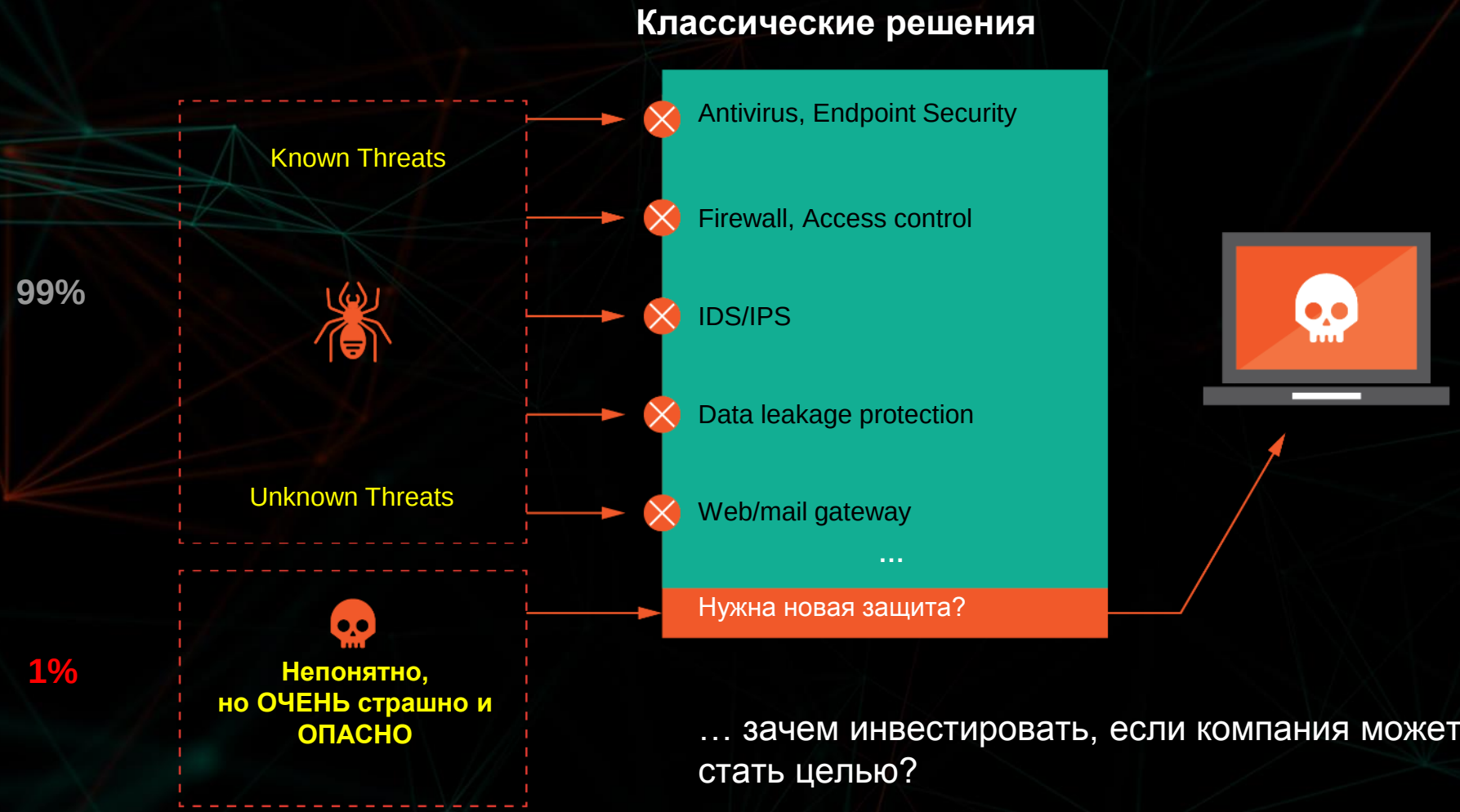


1% - целевые/уникальные

9% - передовые угрозы

90% - распространенные угрозы

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



… зачем инвестировать, если компания может никогда не стать целью?

KASPERSKY lab

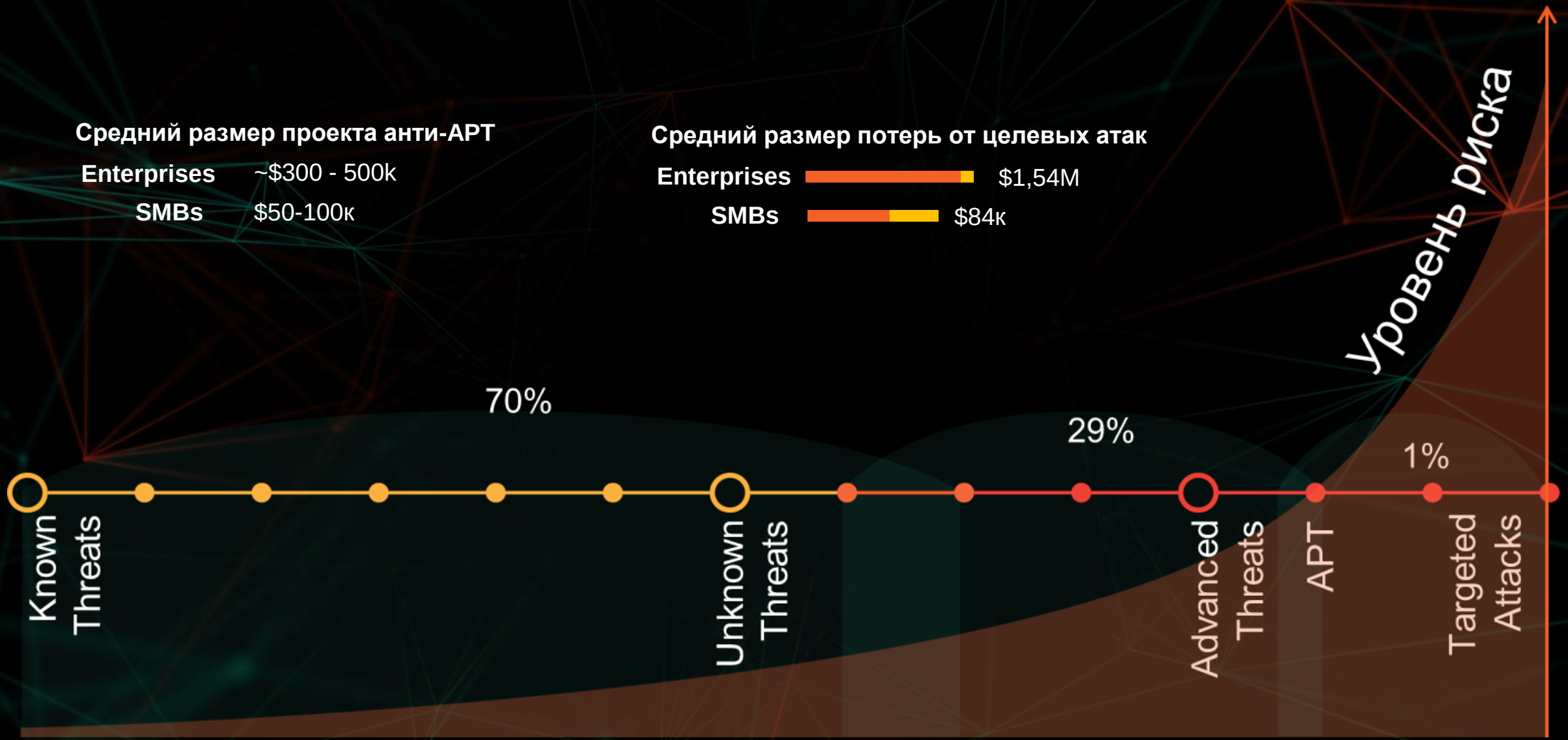
ROI: “1” инцидент может покрыть внедрение анти-APT

Средний размер проекта анти-APT

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

Средний размер потерь от целевых атак

Enterprises	$1,54M
SMBs	$84к



KASPERSKY lab

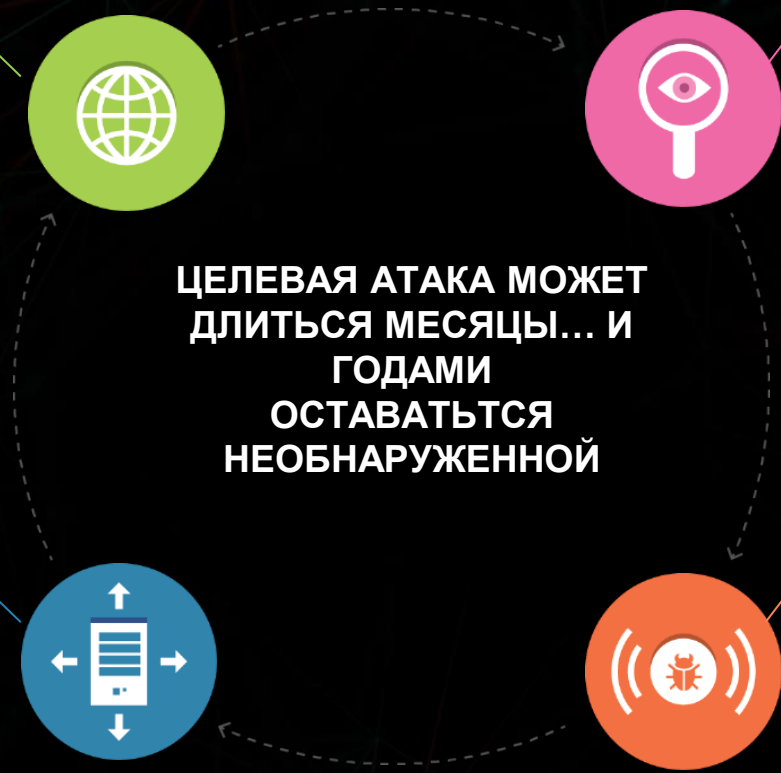
Типовое развитие целенаправленной атаки

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

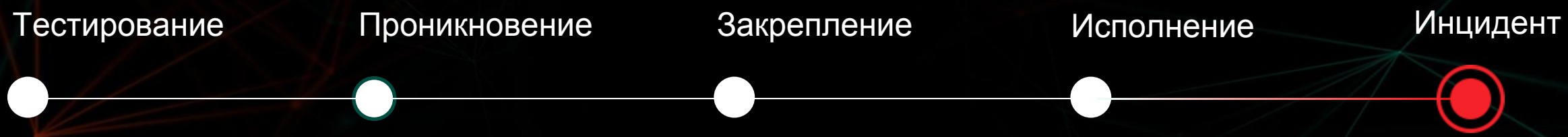
ПРОНИКНОВЕНИЕ

- использование слабых мест
- проникновение внутрь инфраструктуры

KASPERSKY lab

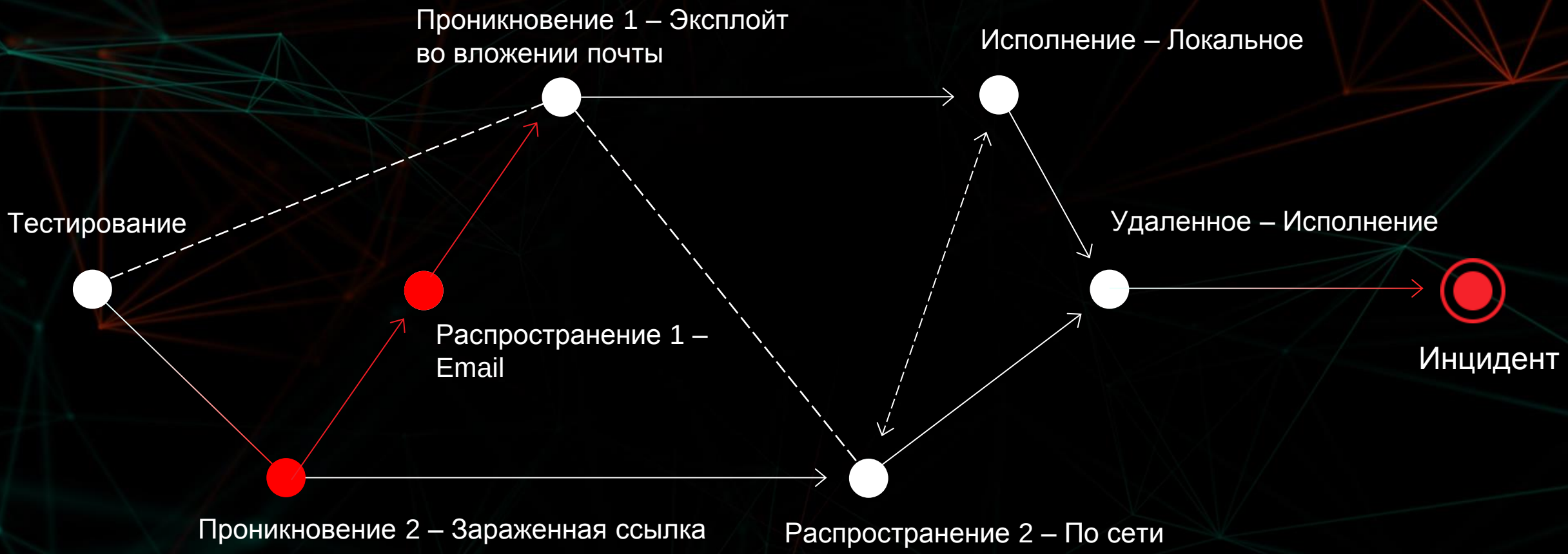
Развитие целенаправленной атаки: Теория и Реальность

В теории… довольно линейное развитие:



Развитие целенаправленной атаки: Теория и Реальность

В реальности… сложно и нелинейно:



Выводы при построении эффективной корпоративной безопасности

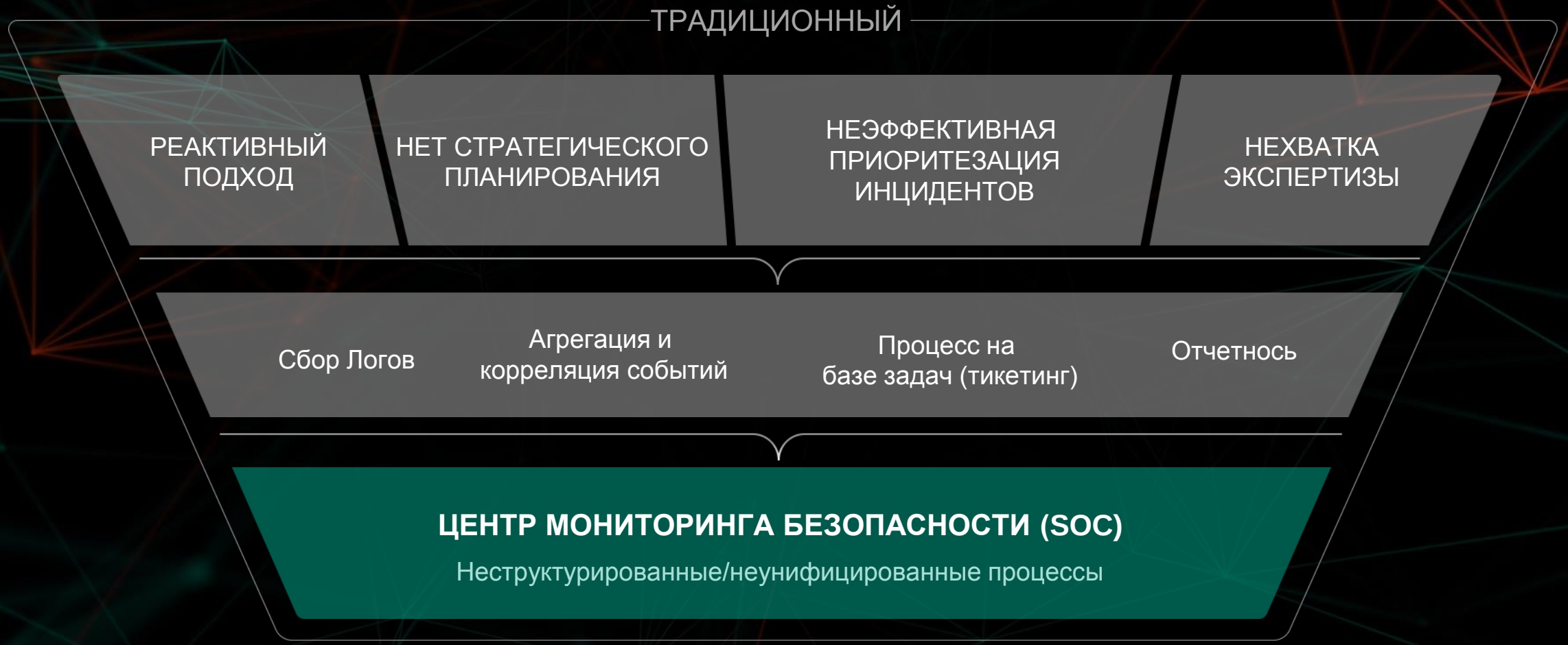
- Большинство «передовых» атак основаны на базовых уязвимостях
- Возможности обнаружить и отреагировать гораздо важнее блокирования и предотвращения
- «Реагирование на скоррелированные инциденты" даёт ложное чувство безопасности
- Защита от передовых угроз должна быть эшелонированно интегрированной, 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

Адаптивная стратегия корпоративной безопасности

Подход «Лаборатории Касперского»

KASPERSKY lab

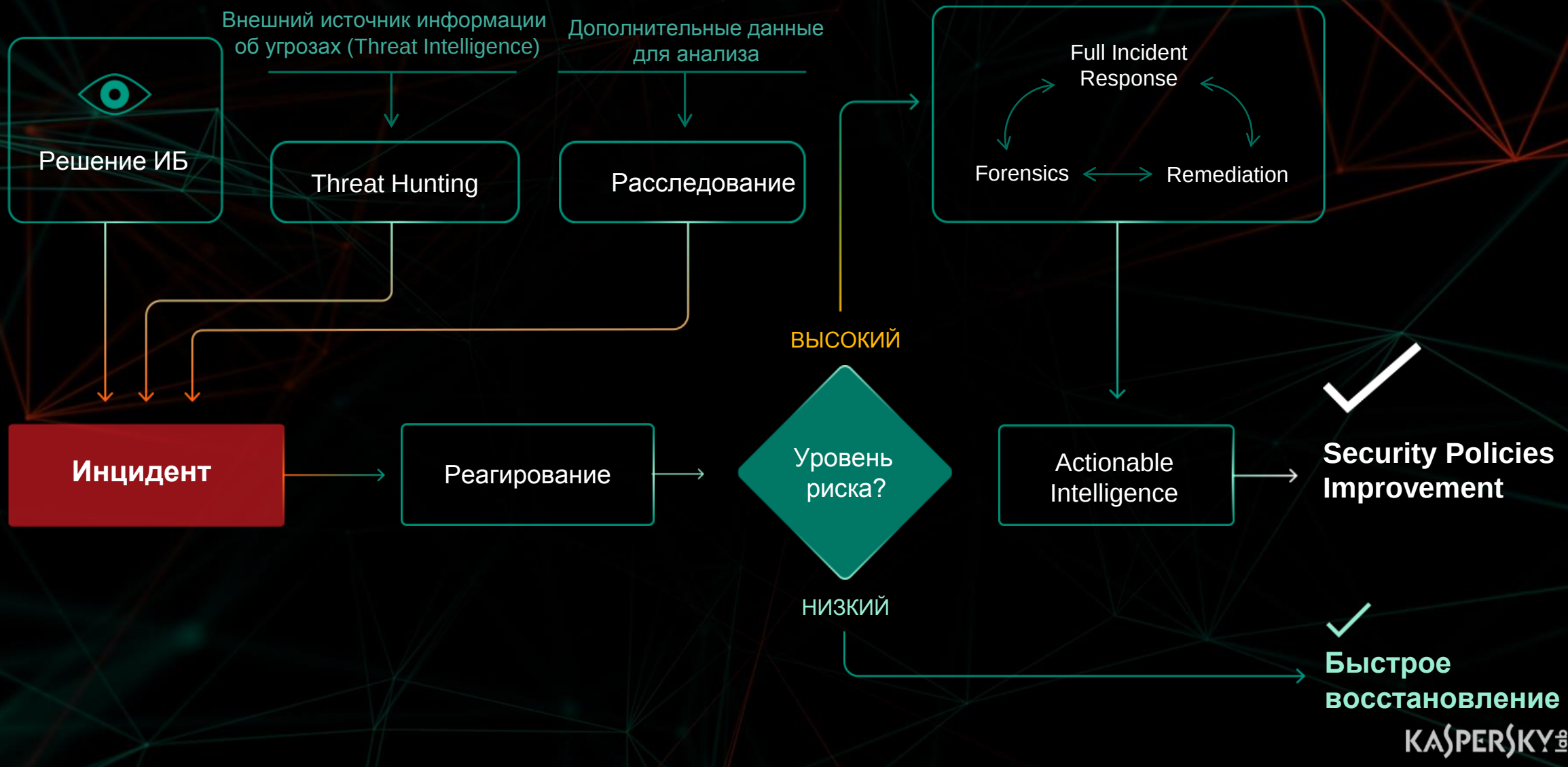
НЕДОСТАТКИ ТРАДИЦИОННОГО ПОДХОДА ДЛЯ ЦЕНТРА МОНИТОРИНГА БЕЗОПАСНОСТИ (SOC)



НЕПРОРАБОТАННОСТЬ ПРОЦЕССОВ РЕАГИРОВАНИЯ – НЕДОСТАТОК БОЛЬШИНСТВА ТРАДИЦИННЫХ SOC

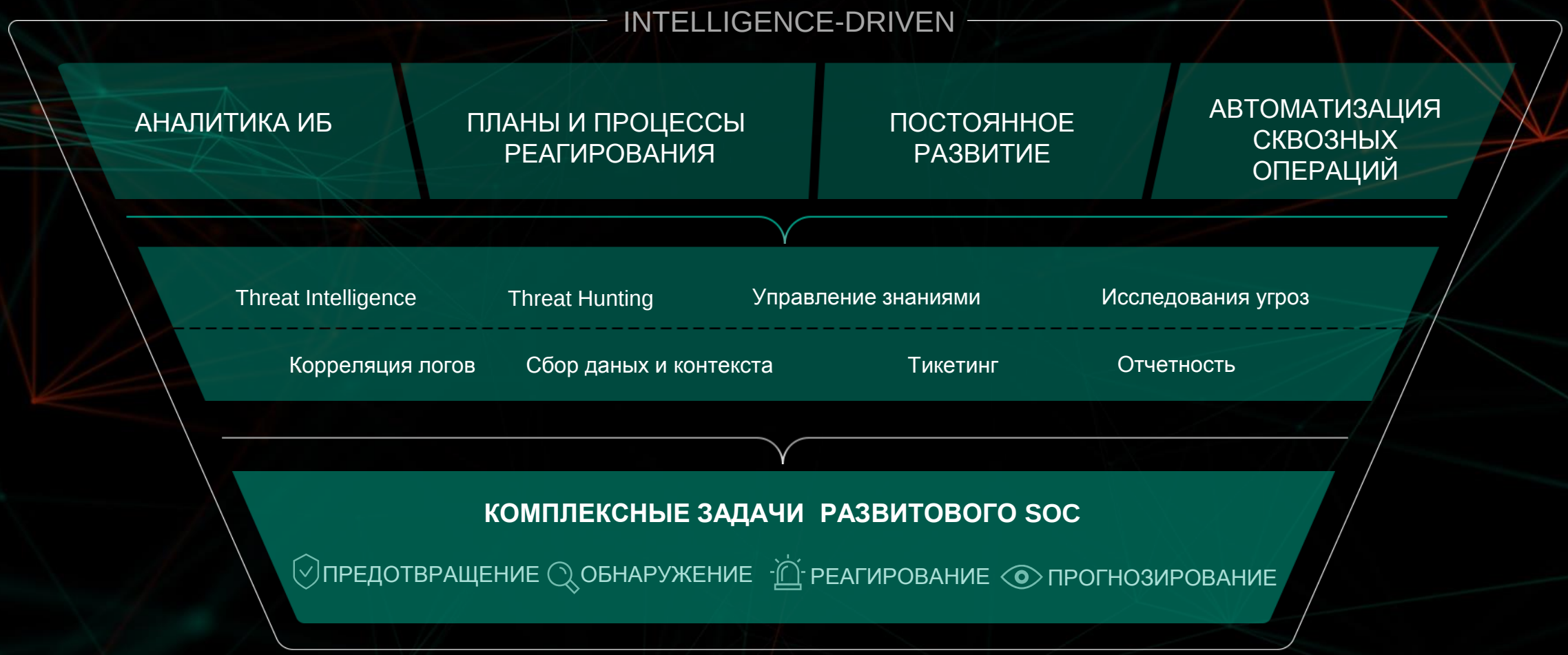
РЕАГИРОВАНИЕ

ЗРЕЛЫЙ ПРОЦЕСС РЕАГИРОВАНИЯ НА ОСНОВЕ УПРАВЛЕНИЯ РИСКАМИ И РАССЛЕДОВАНИЯ



KASPERSKY lab

Развитый центр мониторинга ИБ должен быть интеллектуальным



Адпативная модель организации ИБ

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

Kaspersky Anti Targeted Attack

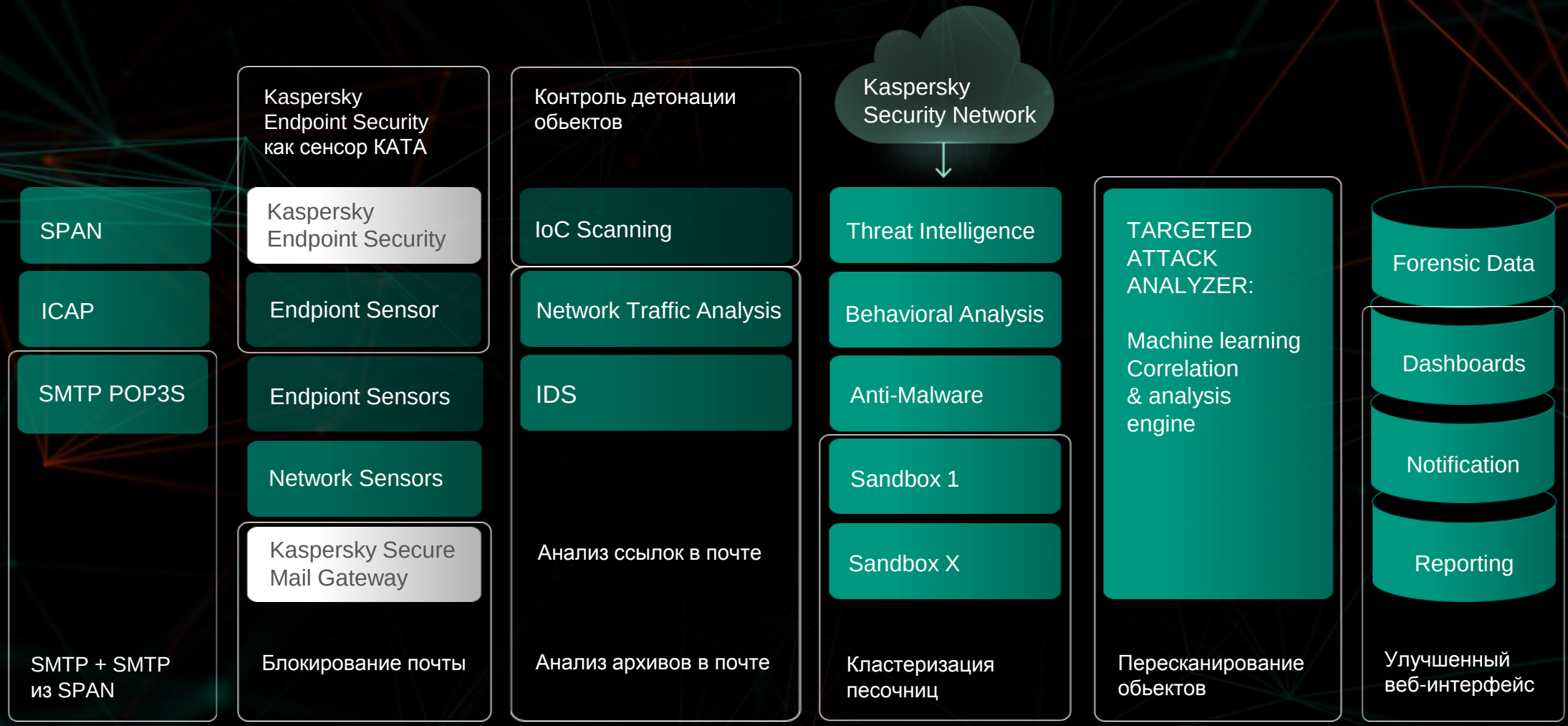
Обзор решения

KASPERSKY lab

Интегрированное решение Kaspersky Anti Targeted Attack

KASPERSKY lab

KASPERSKY ANTI TARGETED ATTACK PLATFORM



Kaspersky Private Security Network – приватная инсталляция базы репутаций и статистики угроз

Соответствие требованиям регуляторов и стандартам ИБ

Kaspersky **Private** Security Network

- Соответствие регуляторам
- Стандарты безопасности
- Бизнес необходимость
- ИТ-требования

Локально размещаемая версия базы KSN

- **Основные преимущества KPSN:**
  - размещение репутационной базы ЛК (полный дамп данных) внутри защищаемой инфраструктуры
  - исключение передачи информации вне контролируемой сети
  - одностороннее получение оперативных обновлений от KSN
  - высокая производительность (сотни тысяч запросов)
  - осведомленность в режиме реального времени

Оценка независимых аналитиков

«Kaspersky's solution did remarkably well during this test cycle - detecting 99.44% of previously unknown threats while having just one false positive»

«The Kaspersky KATA platform detected over 97% of malicious threats that were one hour old or less, and also 98% of threats that were just 2 hours old»

«Kaspersky Labs' KATA demonstrated superb threat detection effectiveness against nearly 550 *new and little-known* threats»

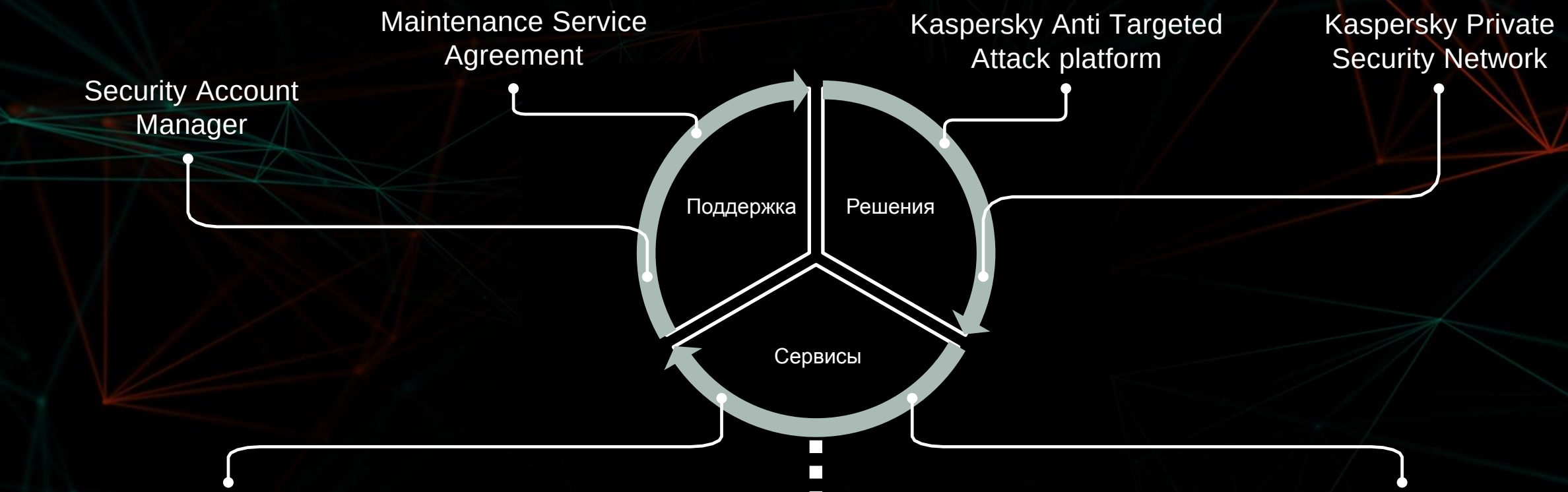
«The Kaspersky's solution provides advanced threat and targeted attack detection across all layers of a targeted attack – initial infection, command and control communications, and lateral movements and data exfiltration»

KASPERSKY lab

Видение ENDPOINT DETECT & RESPOND технологии

KASPERSKY lab

Формирование комплексного анти-APT решения



- Сервис реагирования на инциденты
- Kaspersky Managed Protection

- Тренинги и обучения

TCO

Сопутствующее обучения

Kaspersky Security Training. KATA Administration. 1 day	Консультация по кибербезопасности. Администрирование KATA. 1 день	1-дневная консультация по теме "Внедрение и администрирование KATA": Введение Планирование и развертывание Установка и настройка Оперативный запуск Обработка событий безопасности Позиционирование и конкурентные преимущества (опционально)
Kaspersky Security Training. KATA Security Analyst. 1 day	Консультация по кибербезопасности. Консультация по анализу событий KATA. 1 день	1-дневная консультация по теме "Аналитик безопасности KATA", включающая в себя подробный разбор того как интерпретировать сигналы тревогои, генерируемые системой, какие технологии используются в KATA и как они взаимодействуют, каким образом определяется уровень угрозы/риска. Консультация включает в себя все необходимые знания для управления инцидентами в KATA и дает возможность получить от использования системы максимальный эффект.
Kaspersky Security Training. Incident Response. 5 days	Консультация по кибербезопасности. Расследование инцидентов. 5 дней	5-ти дневная консултьтация по теме "Реагирование на инциденты информационной безопасности": Введение в Реагирование на инциденты Обнаружение и общий анализ Цифровой анализ Разработка правил для обнаружения (YARA, Snort, Bro)

Реагирование на инциденты ИБ

В ходе услуги решаются следующие задачи:

- Выявление скомпрометированных компьютеров и сервисов
- Предотвращение дальнейшего развития атаки и минимизация её последствий
- Сбор данных для дальнейшего анализа включая образы жёстких дисков, лог-файлы, трассировки сетевого трафика, снимки состояния оперативной памяти
- Реконструкция истории инцидента и его логики
- Подготовка плана по восстановлению систем в рабочее состояние

Kaspersky Managed Protection

Сервис предоставляется экспертами центра по мониторингу инцидентов и включает в себя:

- Мониторинг работы установленных продуктов Kaspersky (KES, KATA) с целью выявления активности атакующих за счет проактивного сбора мета-данных сетевой и системной активности.
- Сбор полученной информации с использованием технологий Kaspersky Private Security Network/Kaspersky Security Network
- Анализ полученной информации на предмет наличия следов целевых атак.
- Своевременное информирование клиента о возникшей угрозе

KASPERSKY lab

СПАСИБО!!!

KASPERSKY lab