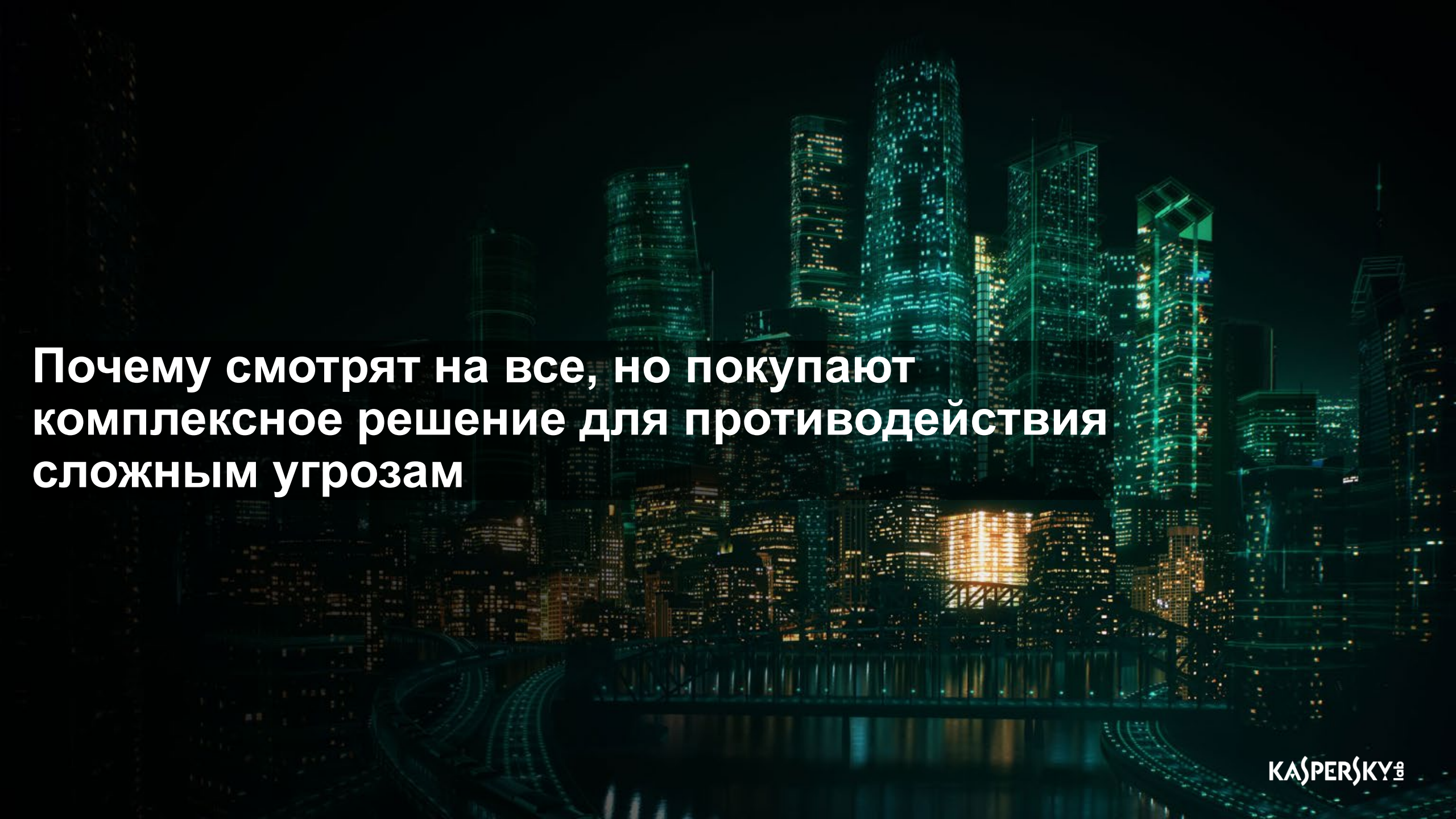
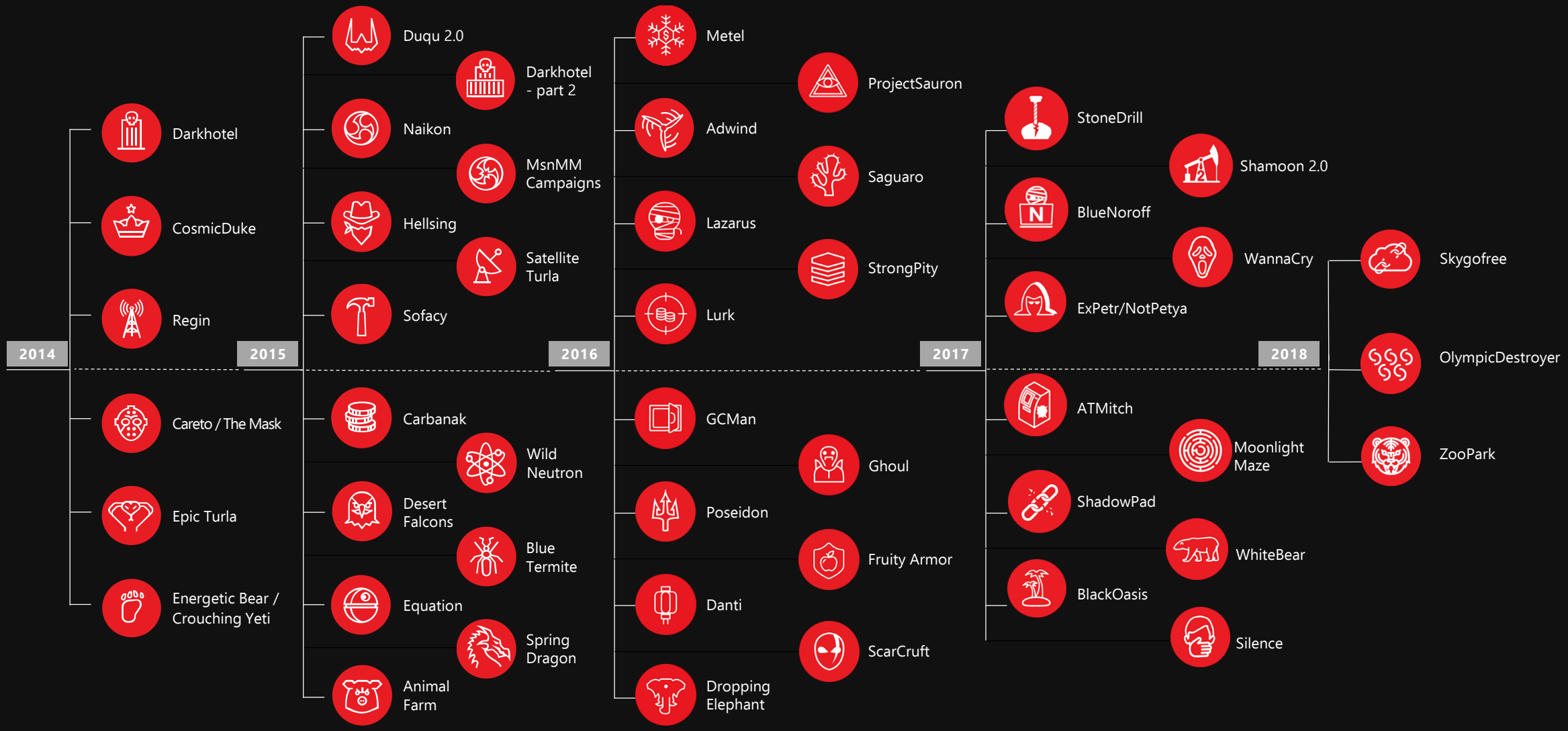


Почему смотрят на все, но покупают комплексное решение для противодействия сложным угрозам

KASPERSKY lab

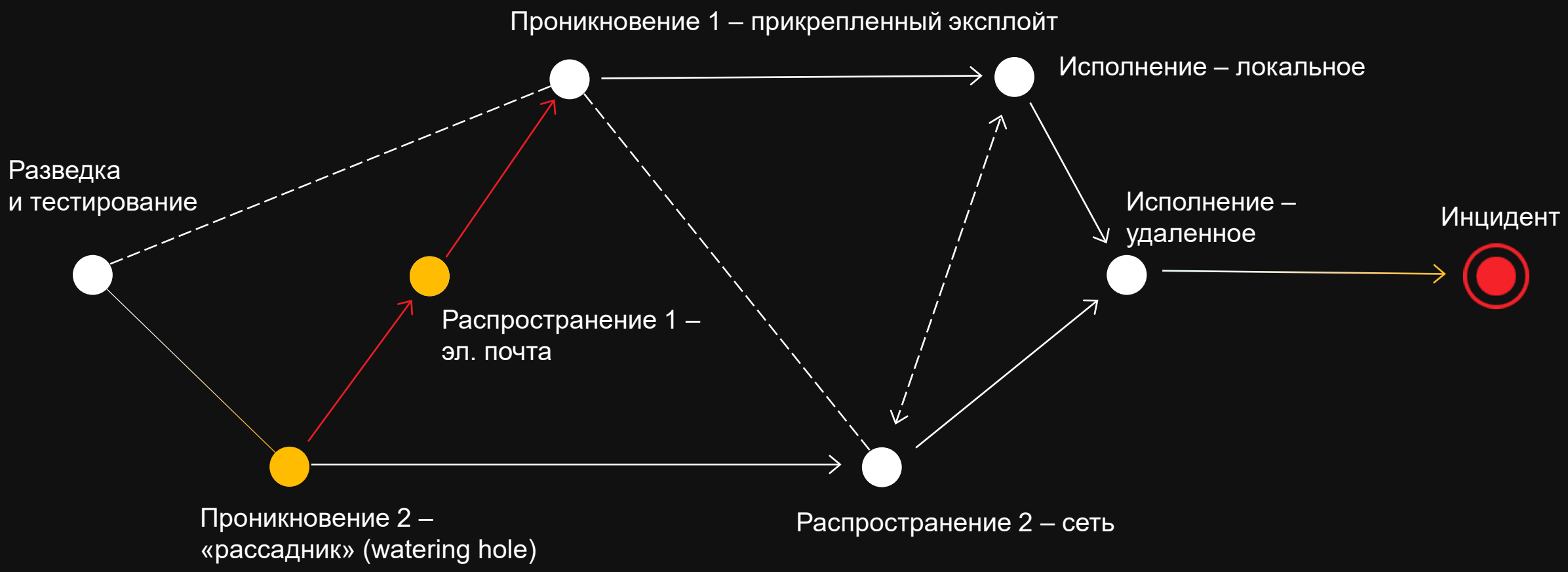
Чем «сложнее» угрозы – тем больше вопросов к «решениям» и списку предлагаемых «инновационных технологий»

Наши исследования



KASPERSKY lab

ПЕРЕДОВЫЕ УГРОЗЫ: СЛОЖНЫЕ И НЕЛИНЕЙНЫЕ

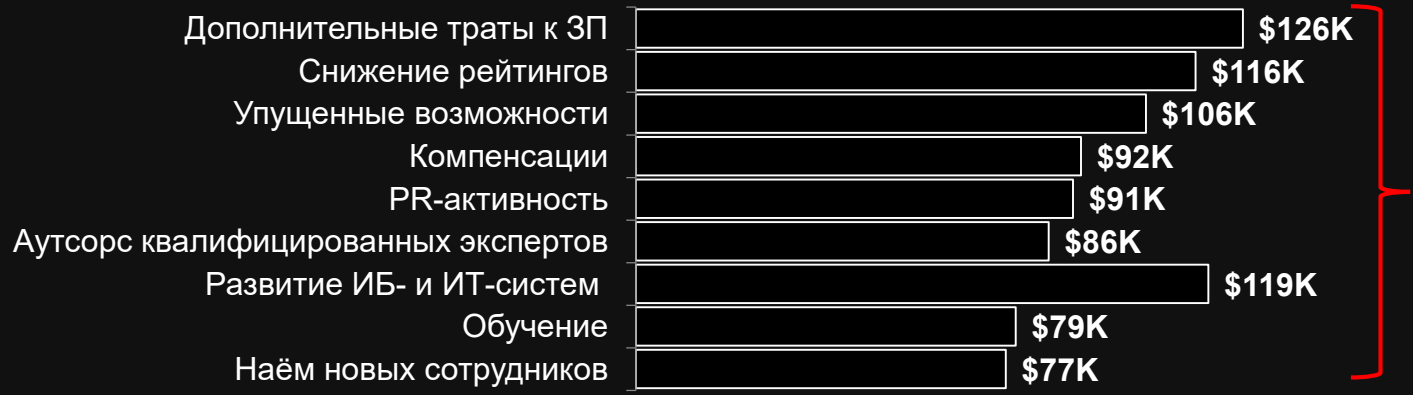


Статистика потерь за 2018 год от одного инцидента ИБ

SMB

Средний ущерб: **$86.5 тыс.**

Крупные компании



Средний ущерб: **$891 тыс.**

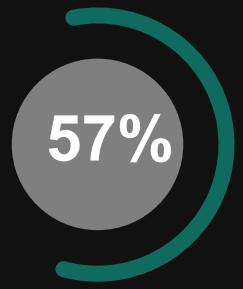
Перераспредленеие трудозатрат ИТ и ИБ служб крупнейшая часть затрат по результату выявленного инцидента

Источник: Исследование рисков информационной безопасности 2018, «Лаборатория Касперского»

Опрошено: 926 SMBs/ 590 Enterprises
Пострадали минимум от одной утечки данных

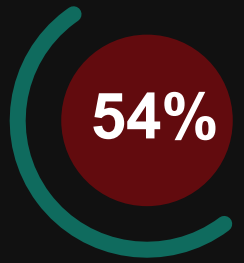
KASPERSKY lab

Современные вызовы



Сложность и комплексность IT инфраструктуры

Увеличение количества и сложности угроз



Соответствие требованиям регуляторов

Задачи современных организаций

Обезопасить бизнес от сложных угроз

- обеспечить непрерывность функционирования бизнес-процессов
- исключить утечку данных
- сохранить репутацию и стабильное развитие бизнеса

Следовать требованиям регуляторов

- выстроить процесс расследования и реагирования на сложные инциденты
- своевременно предоставлять в нужном объеме информацию о найденных компьютерных инцидентах

- ✓ без привлечения дополнительных ресурсов
- ✓ при снижении общих трудозатрат ИТ и ИБ департаментов

Источник: Kaspersky Lab 2018 The Chief Information Security Officer Survey

Пошаговое построение комплексной защиты

Kaspersky Threat Management and Defense

Традиционная защита
Превентивные технологии

Передовые технологии

Проактивный поиск угроз
Threat Intelligence

Ландшафт массовых угроз

Сложные угрозы

Специально подготовленные атаки

Первый шаг

Блокировка максимального числа угроз

Автоматическая блокировка угроз

Второй шаг

Максимальная автоматизация на этапе обнаружения и реагирования на сложные угрозы, которые были пропущены превентивными технологиями

Автоматическое обнаружение, корреляция и реагирование

Третий шаг

Готовность к атакам уровня APT: Высокий уровень экспертизы, ручной поиск угроз, продвинутый пользователь знаний TI

Наши предложения – 1 шаг

Превентивные технологии

Первый шаг

Блокировка максимального числа угроз

- Почта → **Kaspersky Secure Mail Gateway**
- Веб → **Kaspersky Security for Web Gateway***
- Конечные точки → **Kaspersky Endpoint Security**
- Облака → **Kaspersky Hybrid Cloud Security**

- Отсеивание в автоматическом режиме большого количества мелких нерелевантных сложным атакам инцидентов
- Повышение эффективности выявления угроз уровня APT
- Обогащение передовых технологий по обнаружению контекстной информацией для эффективного расследования
- Обратная передача вердиктов от систем обнаружения для автоматического блокирования
- Фундаментальный шаг на пути построения комплексной стратегии защиты от сложных угроз

*В ближайшем roadmap

Наши предложения – 2 шаг

Передовые технологии

Второй шаг

Максимальная автоматизация на этапе обнаружения и реагирования на сложные угрозы, которые были пропущены периметровой защитой

Сеть

Kaspersky Anti Targeted Attack

Конечные точки

Kaspersky Endpoint Detection and Response

- Увеличение кол-ва качественно обработанных инцидентов
- Сокращение трудозатрат
- Соответствие требованиям

- Автоматическое обнаружение сложносоставных угроз
- Централизованное хранение данных и вердиктов для возможности ретроспективного анализа и оперативного предоставления детальной информации о произошедших инцидентах
- Встроенная корреляция событий и формирование макроинцидента для ускорения процесса расследования
- Централизованная постановка задач по реагированию из единой консоли на всех этапах расследования инцидента

KASPERSKY lab

Наши предложения – 3 шаг

Третий шаг

Готовность к атакам уровня APT: Высокий уровень экспертизы, ручной поиск угроз, продвинутый пользователь знаний TI

Проактивный ручной поиск угроз

Повышение эффективности SOC

Повышение уровня внутренней экспертизы

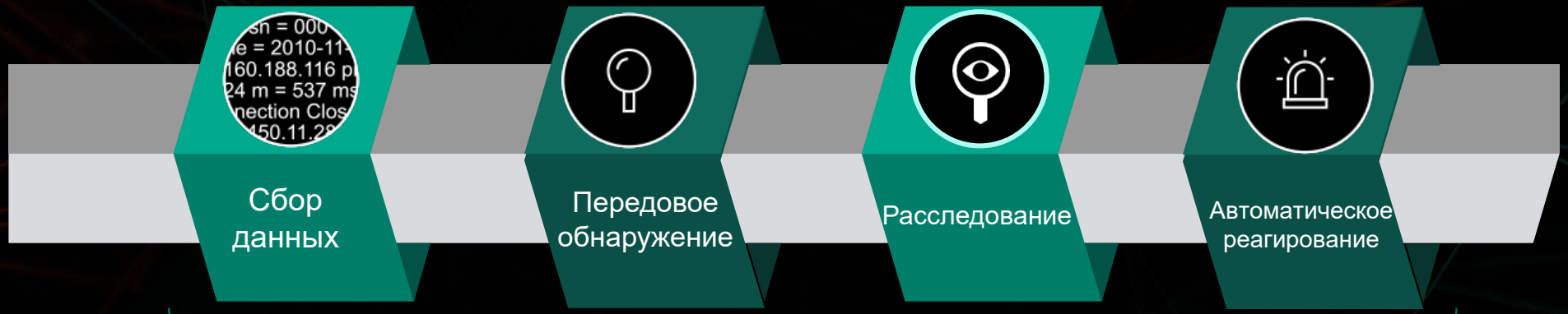
Предоставление экспертных сервисов

- Сведение к нулю вероятности разрушительных последствий от сложных инцидентов
- Ускорение процесса обнаружения сложных угроз на ранних стадиях и увеличения кол-ва качественно обработанных инцидентов
- Формирование полной законченной картины в вопросе комплексной стратегии защиты от сложных угроз
- Соответствие требованиям законодательства а отношении защиты КИИ
- Стабильность бизнеса

KATA/KEDR

Сетевой уровень

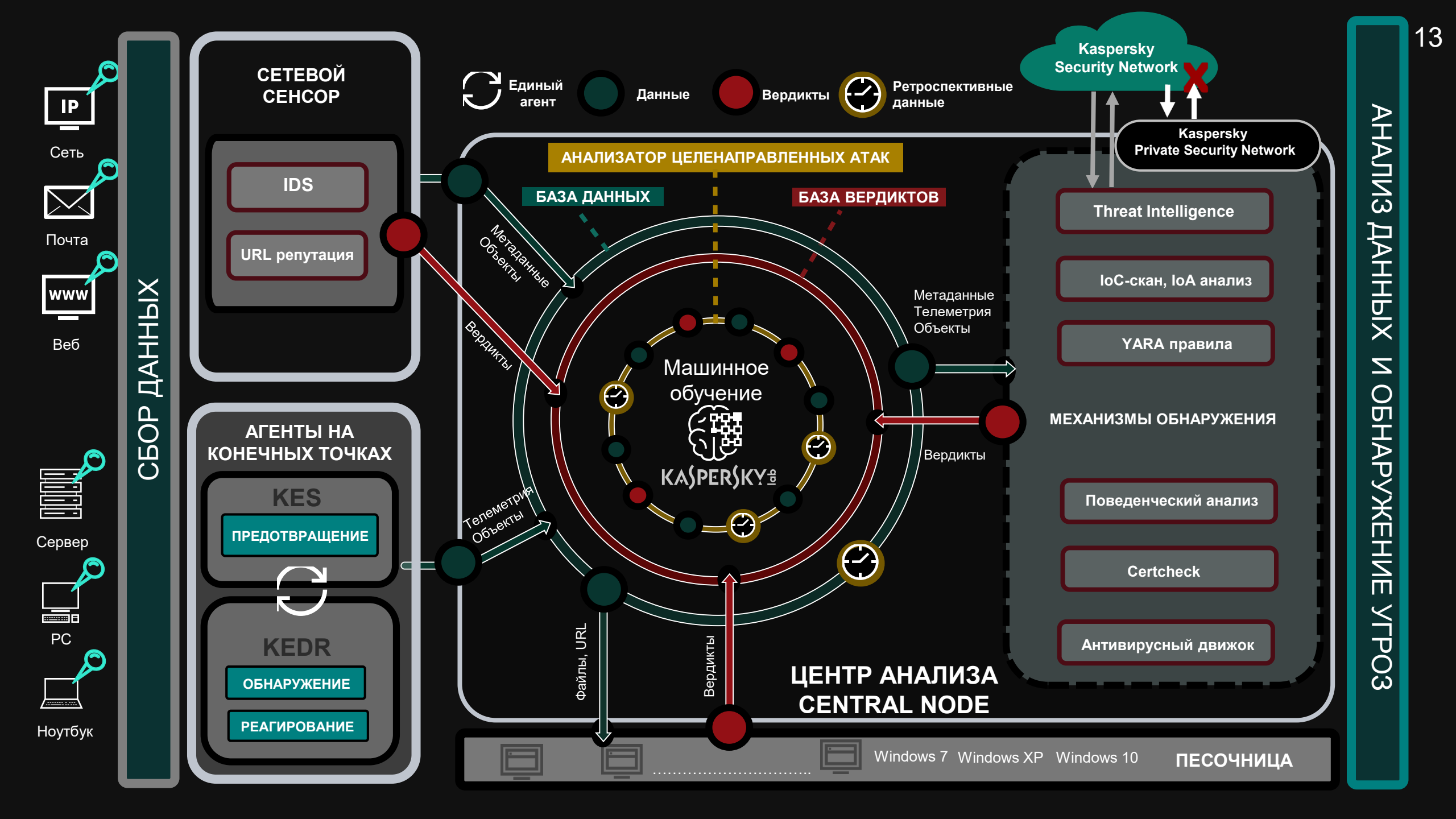
Kaspersky
Anti Targeted Attack platform



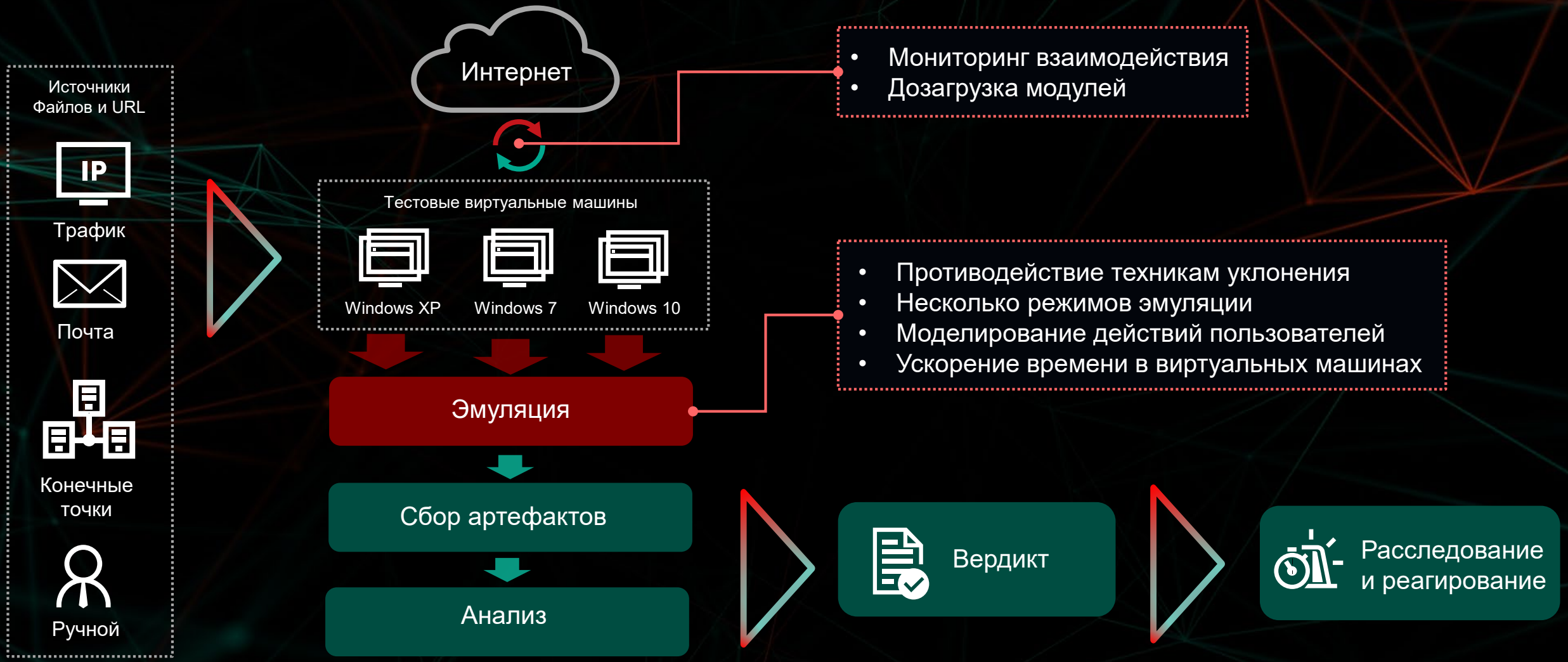
Уровень рабочих мест

Kaspersky
Endpoint Detection and Response

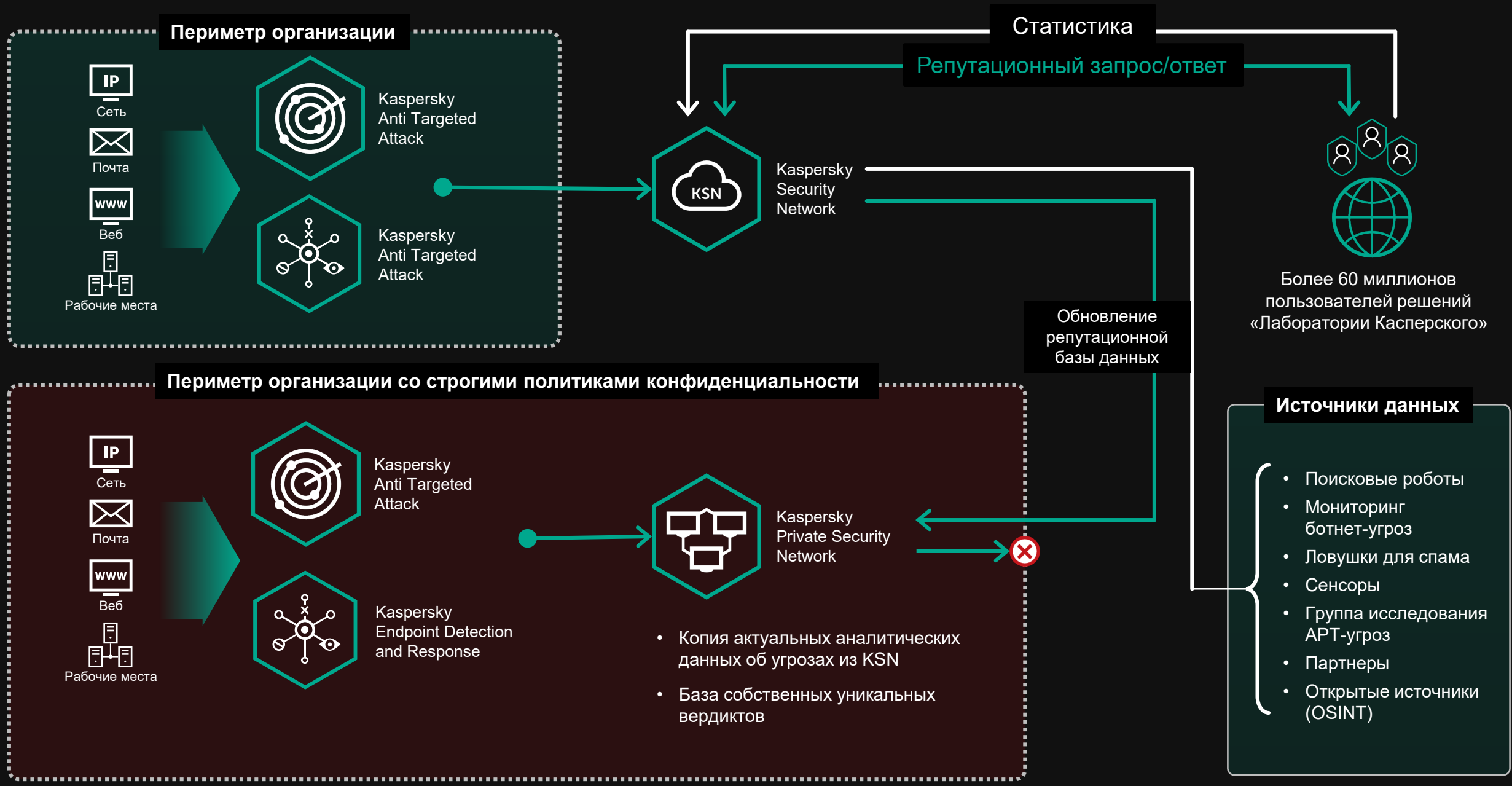
KASPERSKY lab


СБОР ДАННЫХ
IP
Сеть
Почта
WWW
Веб
Сервер
PC
Ноутбук
СЕТЕВОЙ СЕНСОР
IDS
URL репутация
АГЕНТЫ НА КОНЕЧНЫХ ТОЧКАХ
KES
ПРЕДОТВРАЩЕНИЕ
KEDR
ОБНАРУЖЕНИЕ
РЕАГИРОВАНИЕ
Единый агент
Данные
Вердикты
Ретроспективные данные
Kaspersky Security Network
Kaspersky Private Security Network
АНАЛИЗАТОР ЦЕЛЕНАПРАВЛЕННЫХ АТАК
БАЗА ДАННЫХ
БАЗА ВЕРДИКТОВ
Машинное обучение
KASPERSKY lab
Метаданные
Объекты
Вердикты
Телеметрия
Объекты
Файлы, URL
Вердикты
Метаданные
Телеметрия
Объекты
Вердикты
Threat Intelligence
IoC-скан, IoA анализ
YARA правила
МЕХАНИЗМЫ ОБНАРУЖЕНИЯ
Поведенческий анализ
Certcheck
Антивирусный движок
ЦЕНТР АНАЛИЗА
CENTRAL NODE
Windows 7
Windows XP
Windows 10
ПЕСОЧНИЦА
АНАЛИЗ ДАННЫХ И ОБНАРУЖЕНИЕ УГРОЗ

Передовая песочница



Глобальная облачная/локальная репутационная база KSN/KPSN



Основные преимущества KATA/KEDR

Один программный продукт с единой веб консолью

Автоматизация рутинных операций и наглядное представление

Быстрый поиск IoC, сопоставление с IoA и доступ в TI

Централизованный процесс реагирования

Снижение рисков ИБ

Соответствие требованиям

Взаимодействие с превентивными технологиями и обогащение SIEM/SOC

Автоматический сбор и централизованное хранение данных

Самостоятельный проактивный поиск угроз

Оптимизация затрат/сокращение трудозатрат на процесс обработки сложных инцидентов

KASPERSKY lab

Максимальная автоматизации и удобство эксплуатации

Увеличение общего числа качественно обработанных инцидентов

за счет

Повышение уровня вовлеченности существующих специалистов ИБ

ПРОБЛЕМА: Недостаточная автоматизация, загрузка квалифицированных кадров рутинными операциями

- ✓ Максимальной автоматизации операций, связанных с процессами обнаружения, расследования и реагирования на инциденты
- ✓ Поддержки встроенной автоматической корреляции разрозненных событий
- ✓ Предоставления ИБ специалисту единого удобного инструмента с интуитивно понятным интерфейсом для действий по расследованию и реагированию
- ✓ Отображения полной картины инцидента в виде дерева событий для оперативного принятия мер
- ✓ Детальной оценки киберугроз за счет формирования максимально полного представления обо всех этапах спланированной злоумышленниками атаки

KASPERSKY lab

Автоматический сбор и централизованное хранение данных

Автоматический сбор, запись и хранение телеметрии/ вердиктов позволяет:

- получать доступ к ретроспективным данным, необходимых при расследованиях в случаях недоступности скомпрометированных рабочих станций или при шифровании данных злоумышленниками.

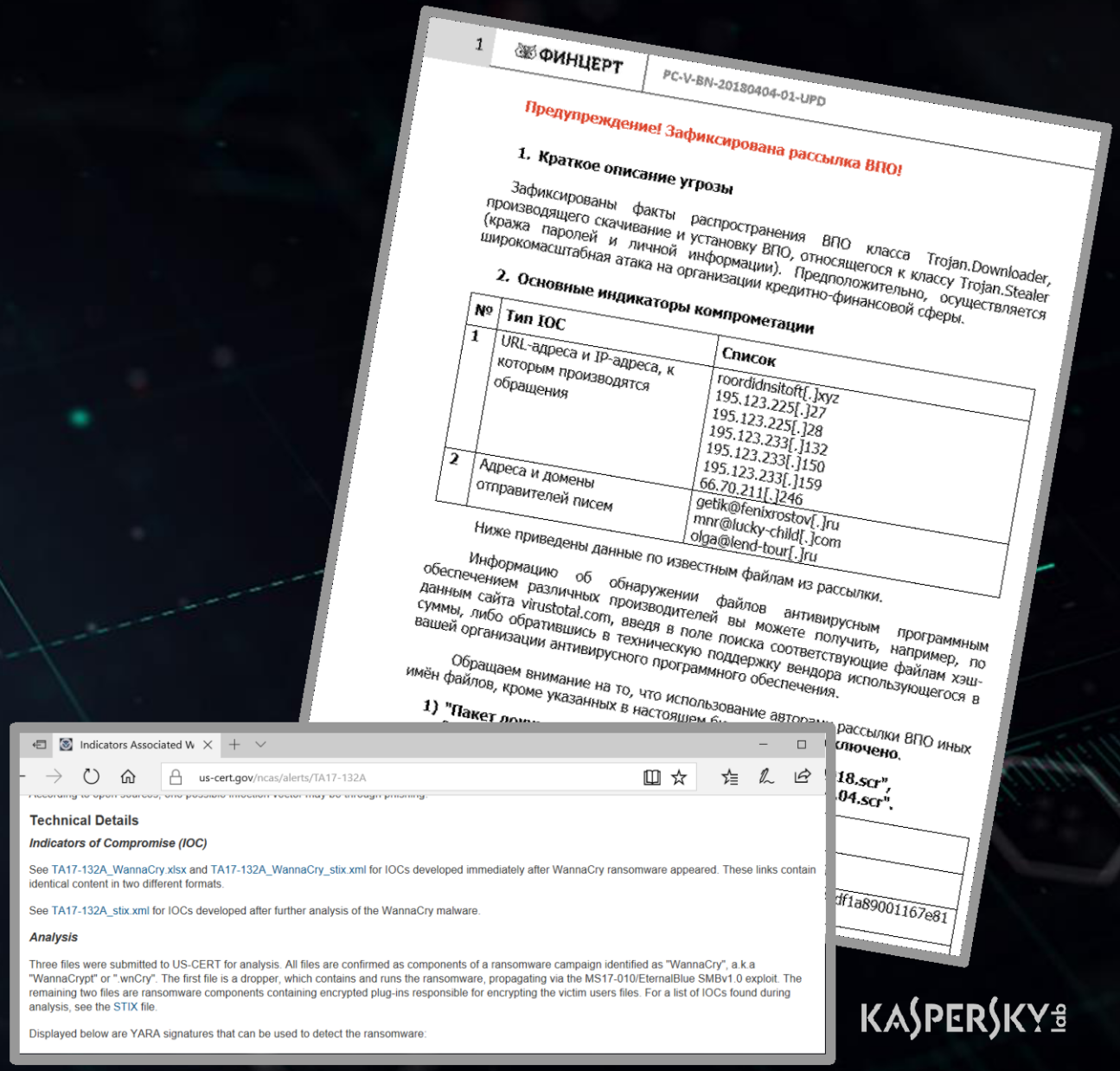
- своевременно предоставлять информацию об обнаруженных угрозах службе реагирования и регулирующим органам, в соответствии с требованиями российского законодательства по обеспечению безопасности КИИ

ПРОБЛЕМА: Отсутствие возможности у организаций получить доступ к данным для проведения расследования

Быстрый поиск индикаторов компрометации (IoC)

- Централизованная загрузка IoC от ФинЦЕРТ / иных источников данных об угрозах
- Следование предоставляемым рекомендациям
- Поддержка автоматических сценариев IoC-проверки для упрощения работы специалистов службы ИБ по выявлению IoC на инфраструктуре
- Сканирование инфраструктуры рабочих мест в режиме реального времени или по расписанию
- Пересканирование базы ретроспективных данных

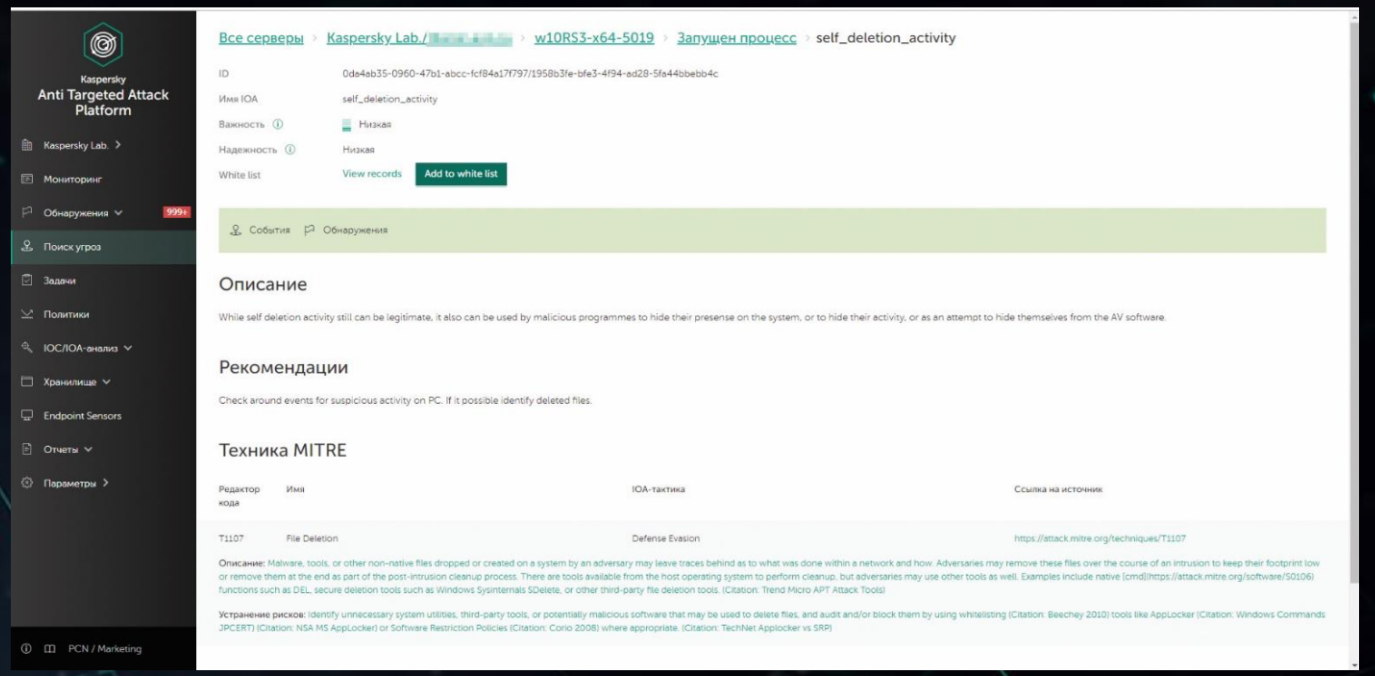
ПРОБЛЕМА: Ручная проверка сети на наличие индикаторов, игнорирование рекомендаций/ предупреждений



KASPERSKY lab

Анализ индикаторов атак и соответствие MITRE ATT&CK

- Классификация событий и их автоматический анализ на предмет соответствия уникальным индикаторам атак (IoA) Лаборатории Касперского
- Сопоставление событий с глобальной базой знаний MITRE ATT&CK
- Возможность создания собственной базы IoA. Формирование сценариев обнаружения с учетом специфики защищаемой инфраструктуры
- Обогащение подозрительных событий понятным описанием, трактовкой, примерами и рекомендациями по противодействию

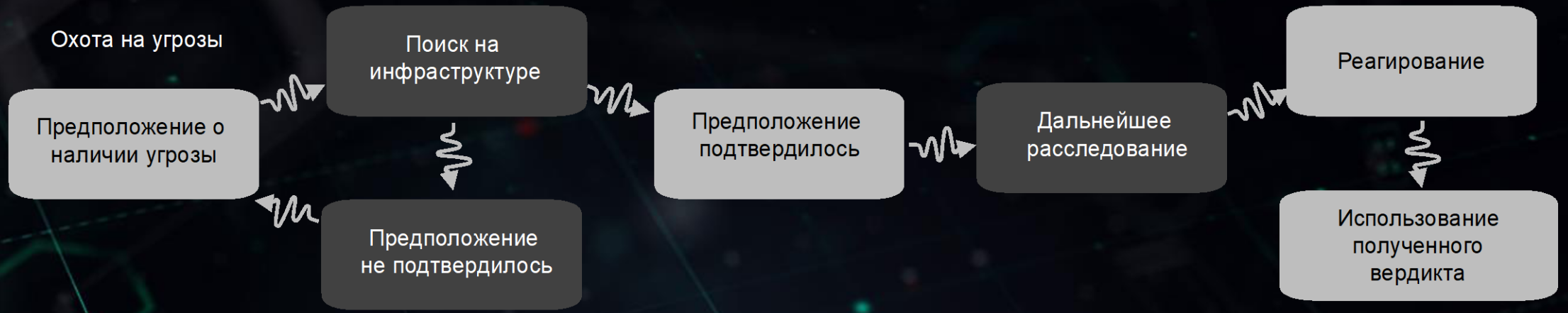


- ✓ Повышение эффективности и скорости расследования инцидентов
- ✓ Принятие оперативных мер по реагированию на инциденты

ПРОБЛЕМА: Недостаток контекстной информации для расследования

KASPERSKY lab

Проактивый поиск угроз (Threat Hunting)



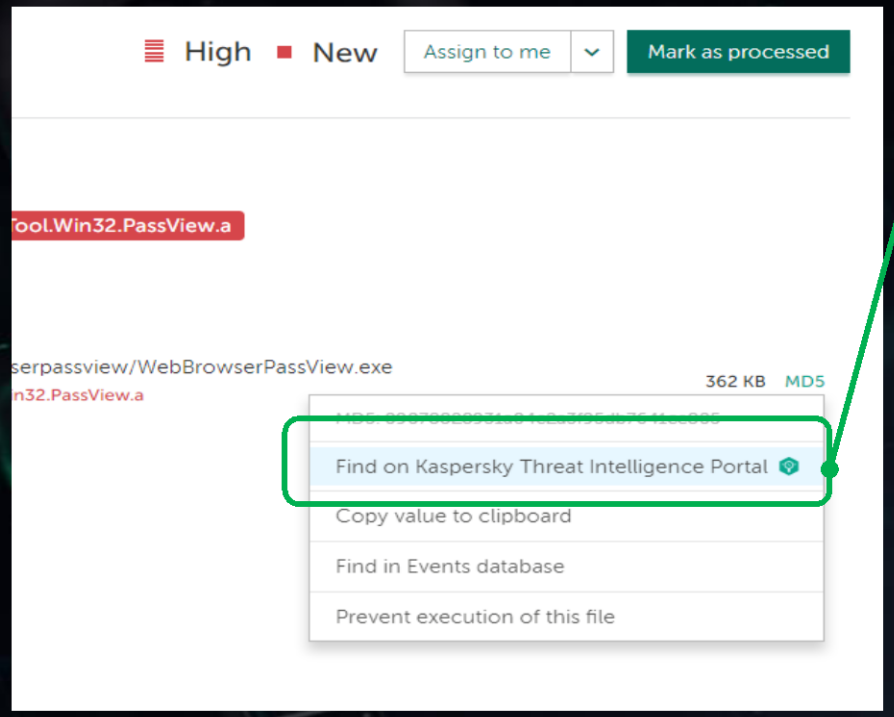
Инструмент для самостоятельного проактивного поиска угроз (Threat Hunting) позволяет:

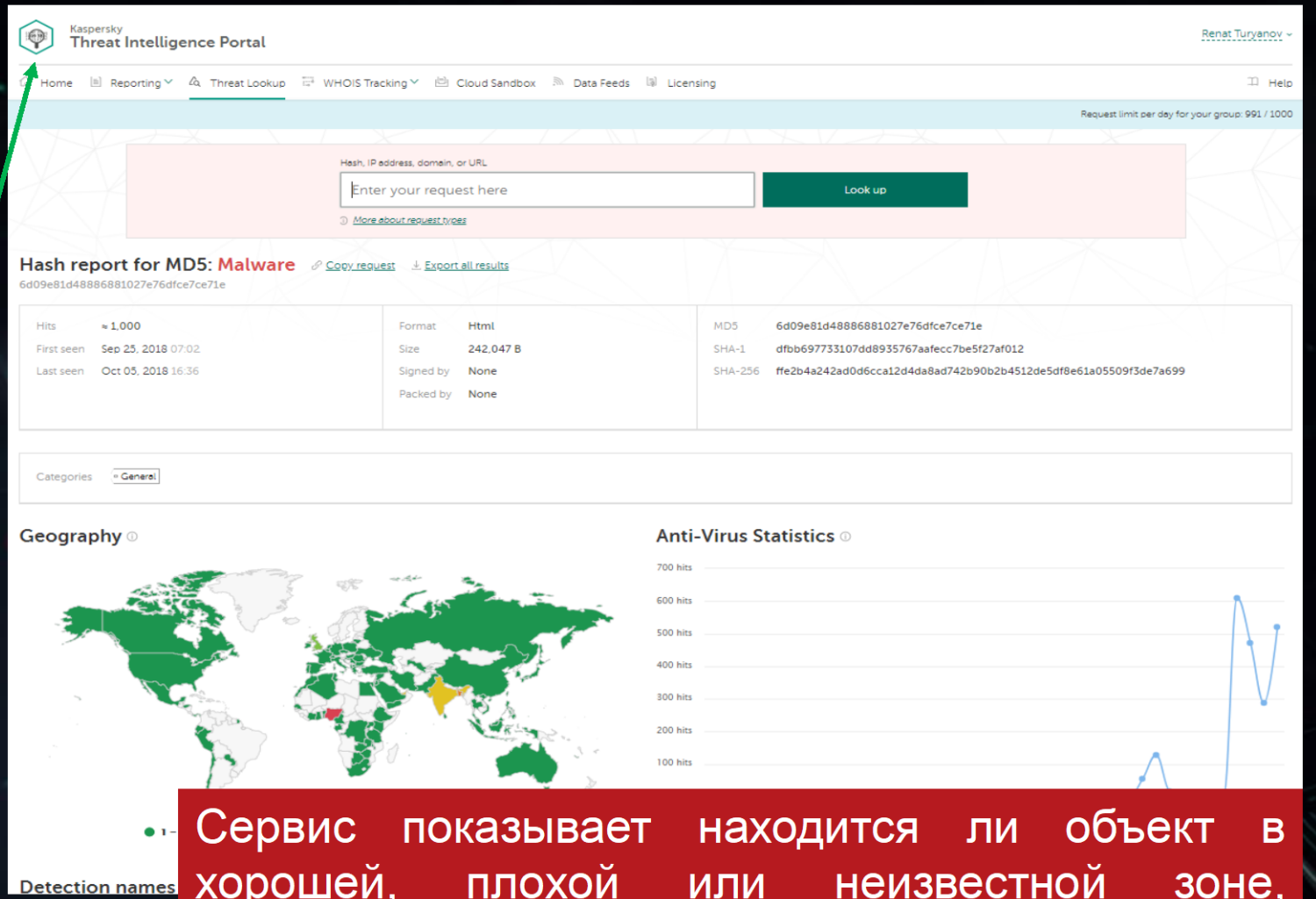
- Составление сложных запросов на поиск нетипичного поведения, подозрительных активностей или иных признаков вредоносных действий
- Учет в поиске особенностей и специфики защищаемой инфраструктуры
- Повышение вероятности раннего обнаружения действий киберпреступников

Процесс поиска новых угроз, не обнаруженных различной автоматической предотвращающей (EPP) и детектирующей логикой (EDR)

ПРОБЛЕМА: Не все угрозы можно автоматически заблокировать/обнаружить

Усиление процесса расследования





- Лицензии KATA / KEDR включают 1000 запросов в год к TI порталу
- Доступ к порталу осуществляется непосредственно через веб-интерфейс KATA / KEDR.

Сервис показывает находится ли объект в хорошей, плохой или неизвестной зоне, обеспечивая богатый набор контекстных данных, чтобы ответить на вопросы: кто, что, где, когда, которые помогут вам принимать своевременные решения и действия

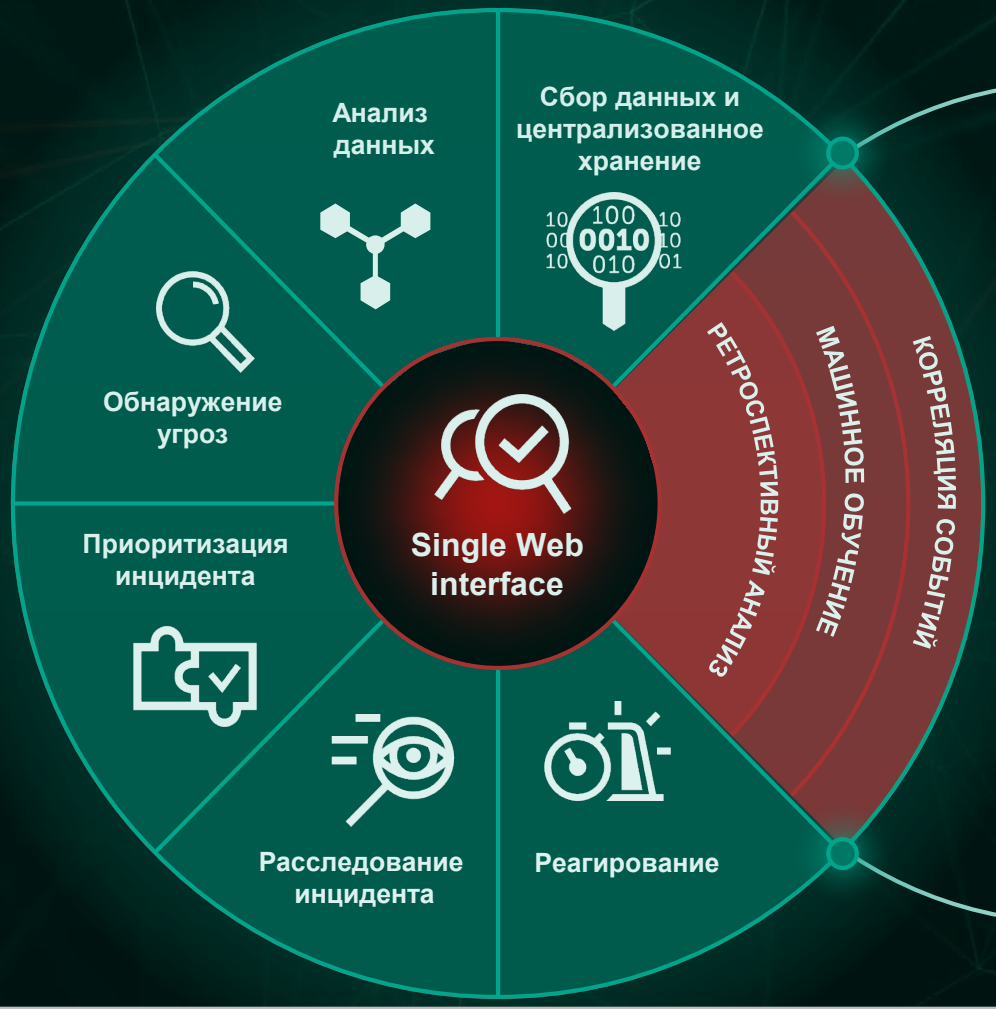
Kaspersky Threat Management and Defense

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response

Kaspersky Cybersecurity Services

Единый инструмент автоматизации для анализа данных сети и конечных точек и реагирования на инциденты



- IoC-поиск
- IoA-анализ
- YARA правила
- Анализ Android файлов
- Репутационная база угроз
- Антивирусный движок
- Поведенческий анализ
- Проверка сертификатов
- URL репутация
- IDS
- Песочница

Экспертные сервисы

- Доступ в портал Threat Intelligence
- Тренинги по безопасности
- Поиск угроз Threat Hunting
- Реагирование на инциденты

KASPERSKY lab