Решение для выявления передовых угроз и расследования инцидентов

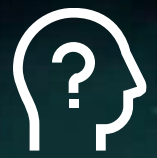
Kaspersky® Endpoint Detection and Response

Александр Тищенко
инженер предпродажной поддержки в ЮФО и СКФО АО “Лаборатория Касперского”

Передовые задачи корпоративной безопасности

Рабочие станции под прицелом

Соответствие регуляторам и внутренним стандартам



Нехватка специалистов

Фокус на ВПО

Ручные/рутинные операции

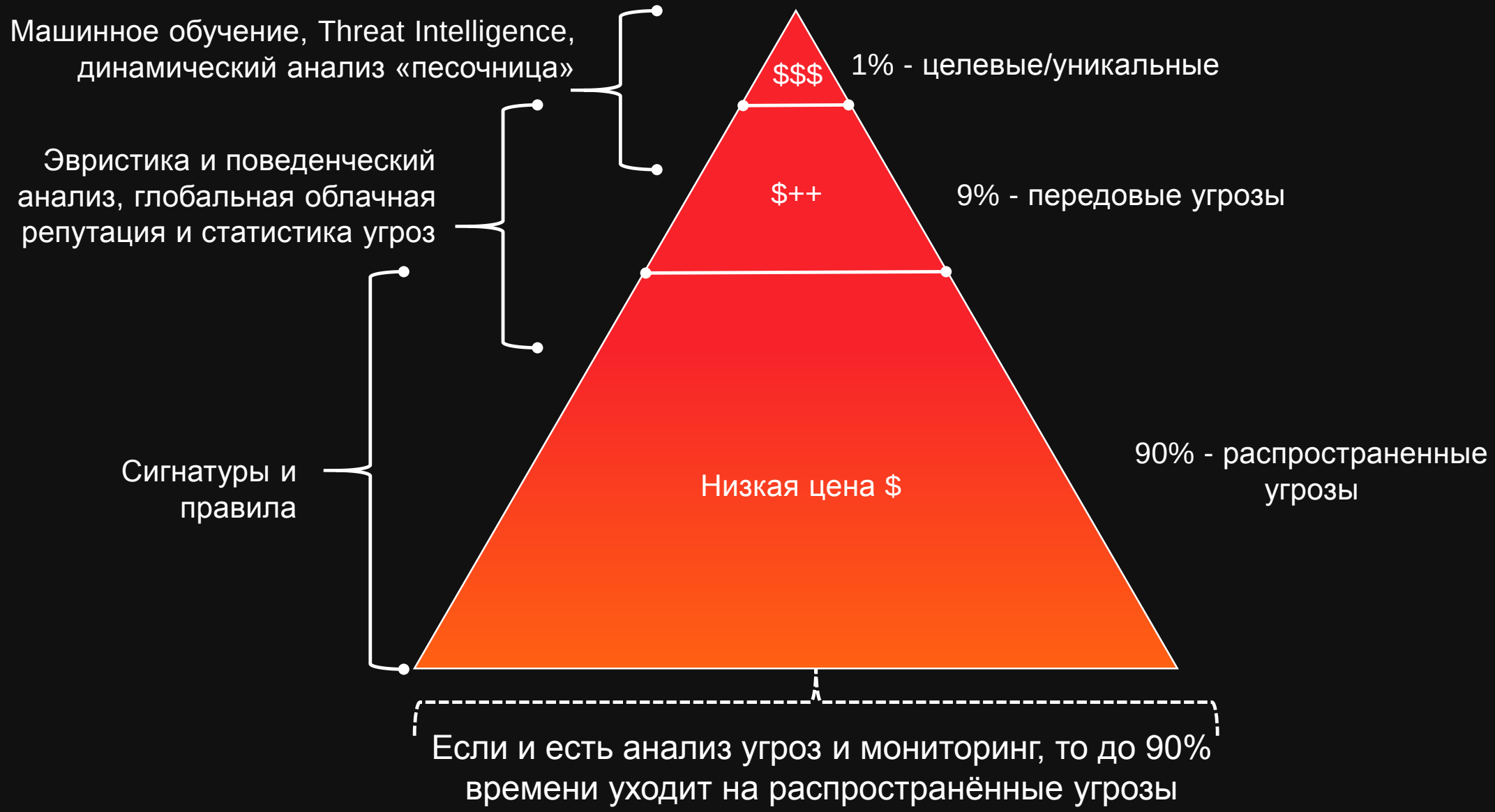
Выбор решений и агента (-ов)

Сложность освоения передовых решений

Разрозненность компонентов

KASPERSKY lab

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



Вопрос оценки масштаба угрозы должен быть поднят ДО инцидента

Прямые потери

IT-консалтинг
Аудиторы
PR-активности
Судебные траты

Восстановление

+

Потеря данных, обман и тд.

Возможности

+

Потеря прибыли во время простоя

Простои

Последующие траты

Системы

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

+

Персонал

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

+

Тренинги

Повышение осведомленности сотрудников
Повышение экспертизы службы ИБ

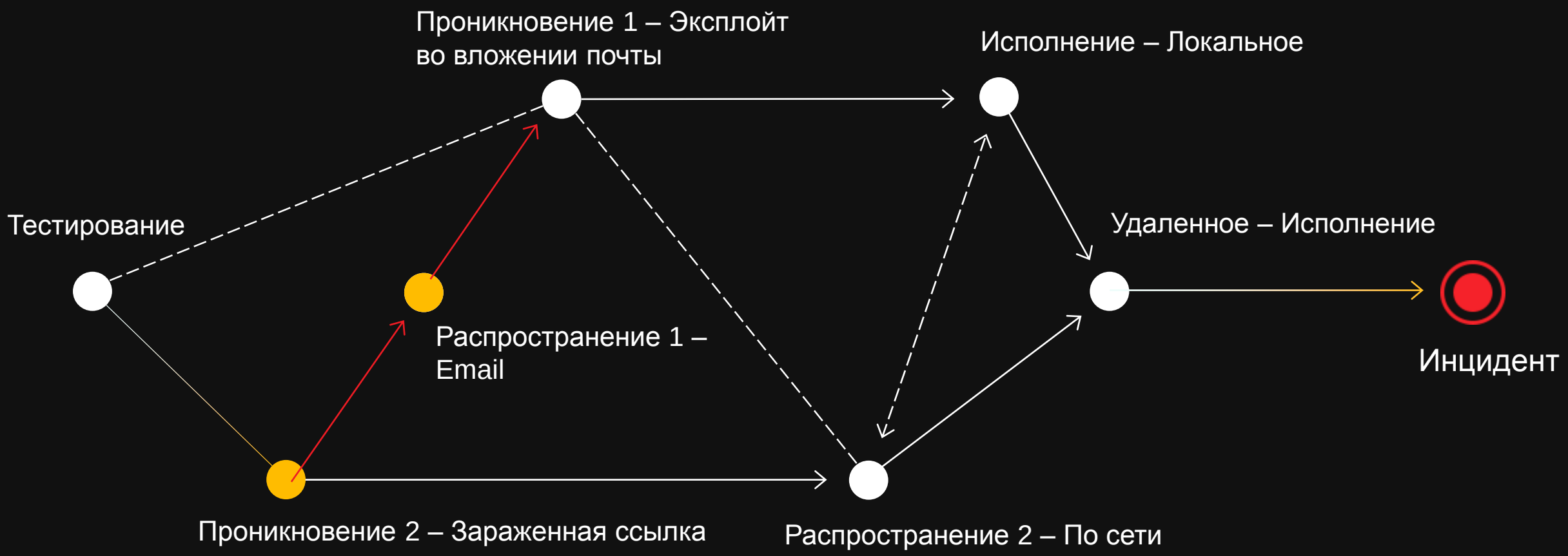
Чтобы не повторилось вновь

ПРОМЕДЛЕНИЕ И НЕХВАТКА РЕАГИРОВАНИЯ ПРИВОДИТ К УВЕЛИЧЕНИЮ ПОТЕРЬ

200% рост затрат на восстановление при промедлении с расследованием и реагированием

**Стоимость восстановления в зависимости от времени необходимого для обнаружения и реагирования*

Вероятное развитие целенаправленной атаки



Сценарии использования на стороне заказчика

В текущей парадигме корпоративной ИБ роль EDR-решения может строится из трёх направлений:

Отдельное EDR решение

KATA

EDR как часть комплексного решения по защите рабочих мест

KEDR KES

EDR как часть решения по защите от передовых угроз

KATA для сетевого анализа

KEDR для расследования и реагирования

АРХИТЕКТУРА РЕШЕНИЯ

ДАННЫЕ

— Сеть
— Веб/Прокси
— Email
— Конечные устройства

АНАЛИЗ

— Механизмы детектирования
— Анализатор целевых атак
— «Песочница»
— Облачные данные *(KSN)*

ВЕРДИКТ

— Консоль
— Syslog
— Журнал операций «Песочницы»
— Pcaps
— Образцы вредоносного ПО

РЕАГИРОВАНИЕ

— Экспертные сервисы «Лаборатории Касперского»

Организация и развитие целостного процесса управления передовыми угрозами корпоративной ИБ

Интеллектуальные экспертные сервисы

Передовые технологии и решения

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response

KASPERSKY lab

Kaspersky EDR в Адаптивной стратегии корпоративной ИБ

ПРОГНОЗИРОВАНИЕ

- Тесты на проникновение
- Оценка защищенности приложений
- Сервис Targeted Attack Discovery
- Kaspersky Threat Intelligence Portal
- Подписка на APT отчеты

ПРЕДОТВРАЩЕНИЕ

- Тренинги по ИБ
- Специализированные решения защиты
  - Защита рабочих мест
  - Защита дата-центров
  - Безопасность встроенных систем
  - …
- Повышение осведомленности
- Индустриальная безопасность

РЕАГИРОВАНИЕ

- Премиальная поддержка – Maintenance Security Agreement
- Сервис реагирования на инциденты
- Цифровая криминалистика
- Анализ ВПО
- Endpoint Detection & **Response**

ОБНАРУЖЕНИЕ

- Кастомизированные отчеты
- Threat data feeds
- Kaspersky Threat Deception
- Kaspersky Managed Protection
- Kaspersky Anti Targeted Attack (KATA)
- Endpoint **Detection** & Response

Kaspersky Endpoint Detection & Response

- **выявление инцидентов ИБ в момент их возникновения на рабочем месте**
  - нарушение политик ИБ и подозрительная/вредоносная активность
  - threat intelligence – выявление известных угроз
  - несанкционированное внесение изменение
  - ретроспективный анализ накопленной информации
  - динамический анализ потенциально опасных объектов с рабочих мест в выделенной «песочнице»

- **локализация инцидента на момент обнаружения**
  - предотвращение распространения угрозы средствами сторонних решений ИБ (например, антивирус/HIPS/DLP/HostFW)
  - карантинизация рабочего места и объектов
  - отключение прав и привилегий скомпрометированных аккаунтов через KES

- **поддержка проведения централизованных расследований инцидентов**
  - централизованный сбор необходимой информации с рабочих мест (дамп памяти, объектов,
  - централизованный «опрос» рабочих мест на предмет IOC или статическим скриптом
  - хранение необходимой информации для ретроспективного анализа

- **предоставление механизмов реагирования на уровне рабочих мест подверженных атаке**
  - откат до прежнего состояния (roll back) и восстановление (repair) посредством KES
  - удаление объектов, записей в реестре и тд.
  - блокирование процессов и несанкционированных активностей

Результат от использования EDR

СНИЖЕНИЕ ОПЕРАЦИОННЫХ ЗАТРАТ

— Автоматизация рутинных операций

— Централизация ключевых этапов реагирования

— Снижение воздействия на бизнес

— Повышение качества работы текущих специалистов

БЫСТРЫЙ РЕЗУЛЬТАТ

— Целостный и унифицированный процесс

— Встроенные автоматические средства

— Оперативное обнаружение угроз

— Соответствие требованиям

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ИБ И ВСЕСТОРОННЕЕ СНИЖЕНИЕ РИСКОВ

— Закрывает имеющиеся пробелы в ИБ

— Развивает традиционные решения передовыми технологиями

— Упрощает понимание угроз и последствий

— Интеграция в процессы ИБ

Предприятия и организации улучшают свою стратегию безопасности, реагируя на современные угрозы. Для киберпреступников конечные узлы по-прежнему остаются главной целью, но современные угрозы невозможно предотвратить традиционными мерами безопасности, что приводит к нарушению критически важных бизнес процессов, снижению эффективности деятельности, репутационным рискам и увеличению эксплуатационных расходов.


Спасибо за внимание!
Вопросы?
KASPERSKY lab
SAVING
THE WORLD
FOR 20 YEARS