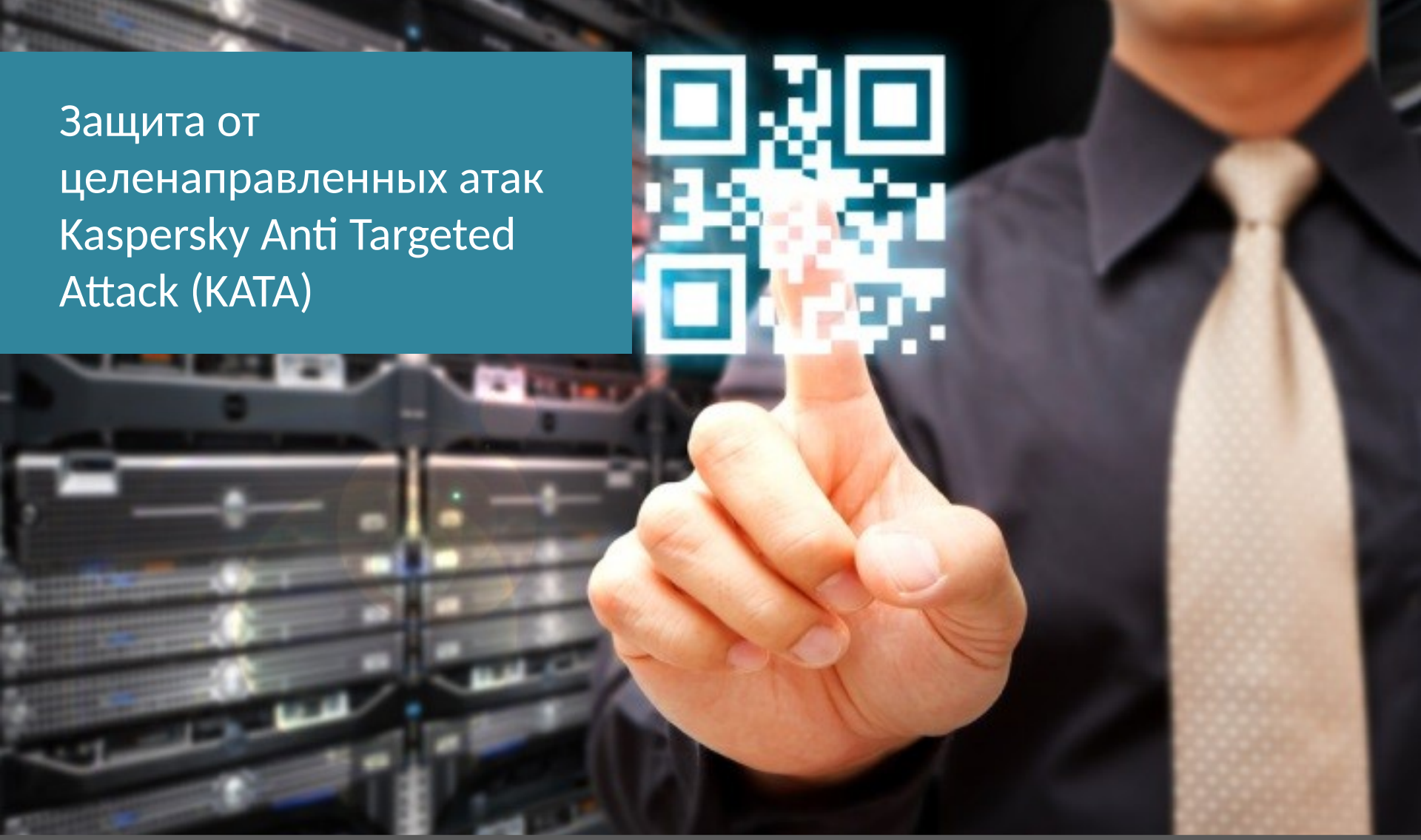
Защита от целенаправленных атак Kaspersky Anti Targeted Attack (KATA)



ПОЛИКОМ ПРО

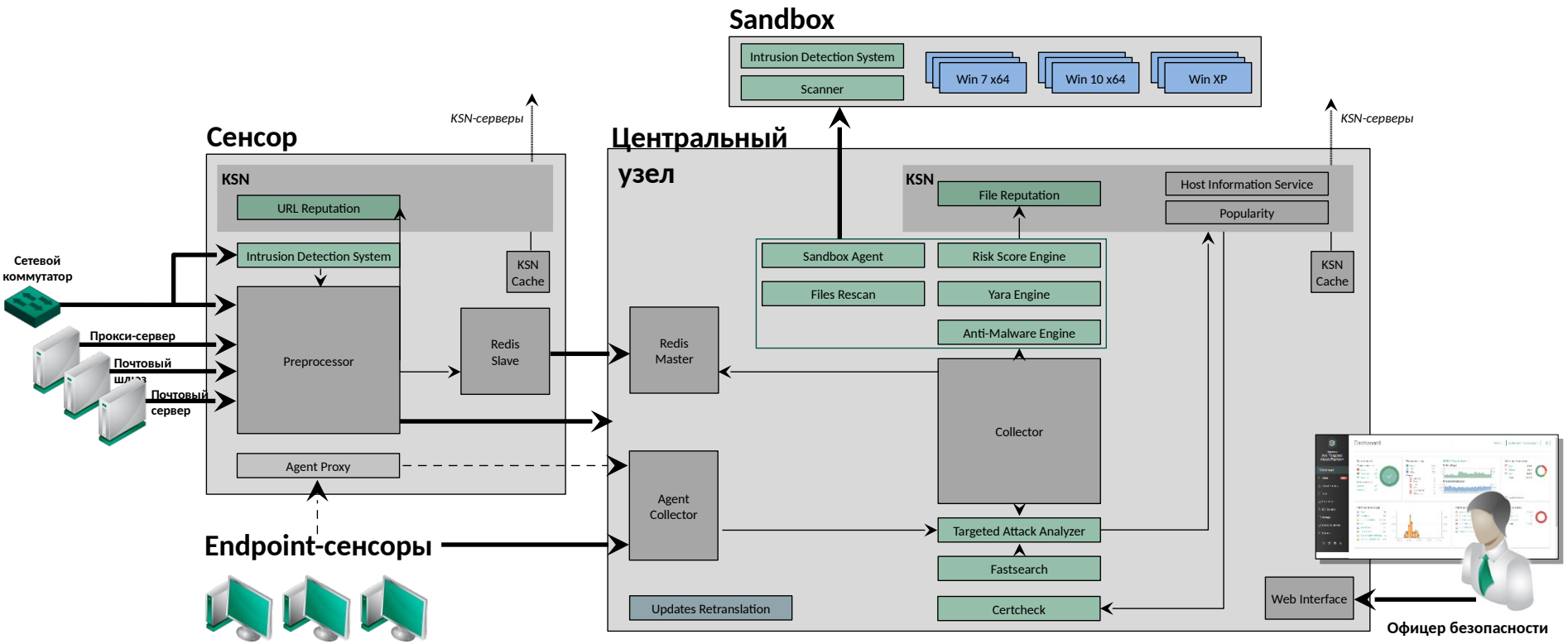
Просто работаем

Ландшафт угроз

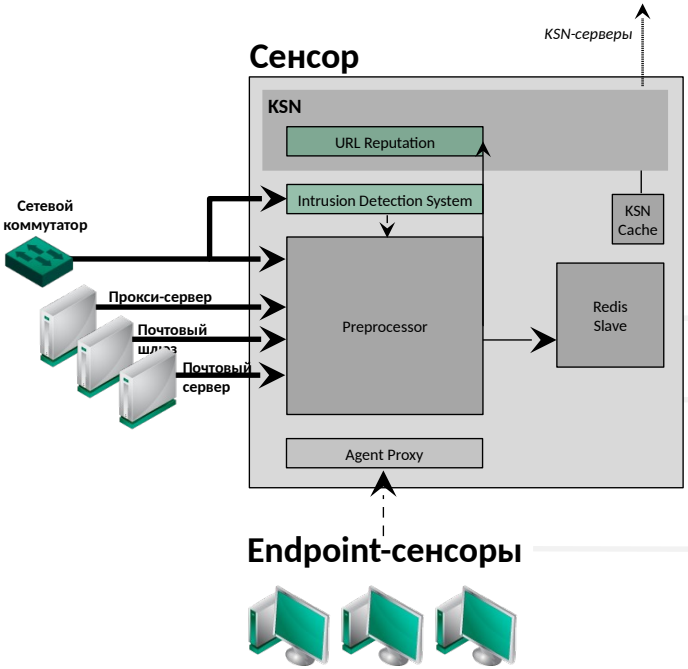
- **Экономический аспект**
  - Почти все происходит в Сети — множество способов монетизировать данные и влиять на реальный мир
  - Эффект масштаба — больше «целей», больше масштаб, меньше стоимость атаки
  - Проникновение и закрепление в компаниях, которые не являются целями, приносит плоды со временем
- **Инфраструктурный аспект:**
  - Глобальная экономика = длинные цепочки поставки
  - Длинные цепочки поставки + атаки через цепочку поставки = кто угодно может оказаться (промежуточной) целью атаки
  - Специализация среди киберпреступников: botnet служба, ransomware как служба, и т.д.
- **Технический аспект**
  - Гонка вооружений в кибер-противостоянии государств — утечка мощных инструментов атаки
  - Использование возможностей не вредоносных программ, часто установленных на компьютерах
  - Социальная инженерия, кража паролей, и т.п.

Ограничения KATA 3.0 / KEDR 1.0	Улучшения в KATA 3.5 / KEDR 1.5
Ограничение в 10,000 Endpoint Sensors на установку	Распределенный режим с несколькими Центральными узлами
5 «стандартных» серверов Sandbox для обработки 4 Гбит/с	3 «стандартных» сервера Sandbox для обработки 4 Гбит/с
Только Windows XP и Windows 7 внутри Sandbox	Windows XP, Windows 7 и Windows 10 внутри Sandbox
Виртуальные машины Sandbox нужно активировать	Виртуальные машины Sandbox уже активированы
Неполный набор инструментов EDR	Новый инструмент EDR: сетевая изоляция
Закрытая экосистема решения	API для получения файлов от сторонних систем
	Прямая загрузка файлов для анализа через веб-консоль
Уязвимость к некоторым методам обхода «песочницы»	Новый режим проверки файлов в песочнице: Quick scan
Endpoint Sensor не пользуется данными KES	Сбор дополнительных данных с KES для анализа и поиска атак
Настройка через текстовый интерфейс	Большинство настроек в Web-интерфейсе
Веб-интерфейс	Больше информации в веб-интерфейсе
Ограничения при проверке архивов с паролем	Настраиваемый список паролей для проверки архивов
Ограниченные инструменты мониторинга	Почтовые уведомления о сбоях в работе компонентов


Этапы реализации целевой атаки
Перед компрометацией
Компрометация
После компрометации
Изучение
Создание
Проникновение
Установка и распространение
Командование и контроль
Осуществление миссии
Исчезновение
Сбор информации о цели в открытых источниках, социальных сетях и другими способами
Подготовка и создание инструментов, необходимых для атаки. Например, эксплойта и трояна для удаленного доступа
Отправка вредоносного пакета будущей жертве по почте или другим способом. Использование социальной инженерии
Эксплуатация уязвимости и установка вредоносного ПО (RAT трояна)
Создание канала для дистанционного управления внутренними активами
Выполнение шагов для достижения целей атаки: кражи данных, саботажа и т.д.
Скрытие своей деятельности

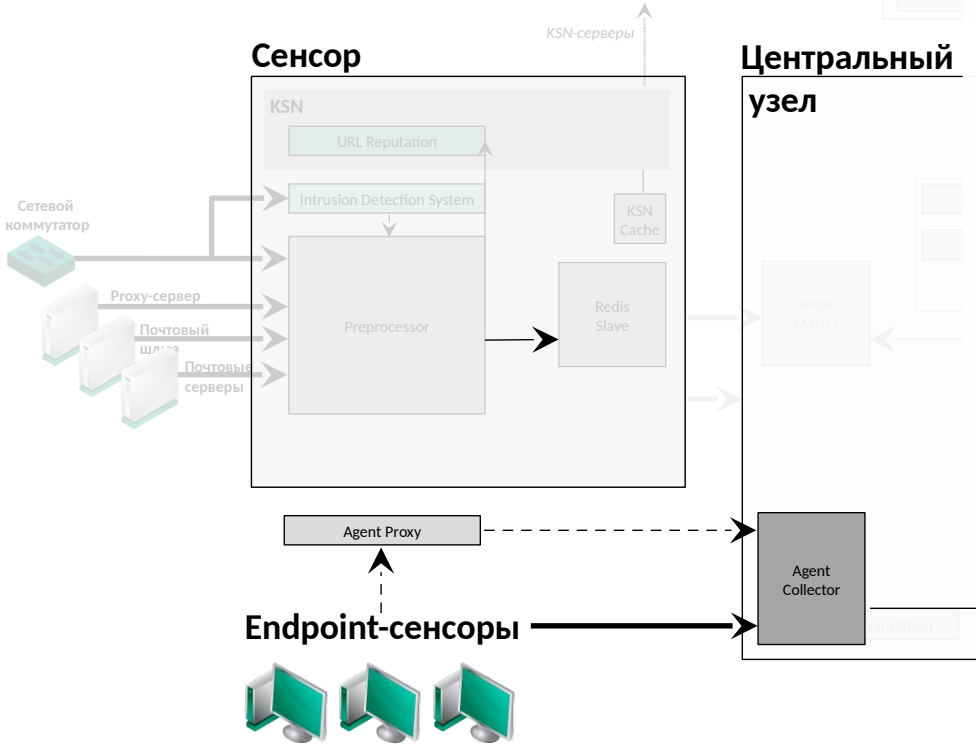

Sandbox
Intrusion Detection System
Scanner
Win 7 x64
Win 10 x64
Win XP
KSN-серверы
Сенсор
KSN
URL Reputation
Intrusion Detection System
KSN Cache
Сетевой коммутатор
Прокси-сервер
Почтовый шлюз
Почтовый сервер
Preprocessor
Redis Slave
Agent Proxy
Endpoint-сенсоры
Центральный узел
KSN
File Reputation
Host Information Service
Popularity
Sandbox Agent
Risk Score Engine
Files Rescan
Yara Engine
Anti-Malware Engine
KSN Cache
Redis Master
Collector
Agent Collector
Targeted Attack Analyzer
Fastsearch
Updates Retranslation
Certcheck
Web Interface
Офицер безопасности

Компоненты KATA | Сенсор



- Получает объекты для проверки от
  - сетевого оборудования
  - прокси-серверов
  - почтовых серверов и почтовых шлюзов
- Проверяет
  - весь трафик модулем обнаружения вторжений
  - URL-адреса технологией URL Reputation
- Извлекает из трафика и передает на Центральный узел
  - файлы
  - характеристики соединений
- Может выполнять роль прокси для Endpoint-сенсоров

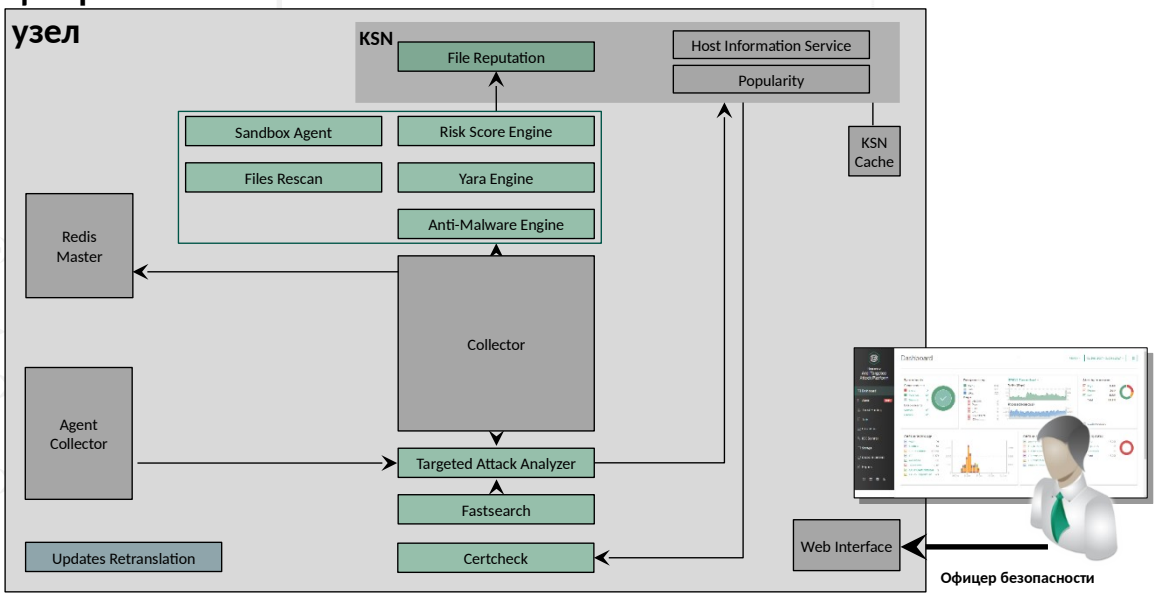
Компоненты KATA/KEDR| Endpoint-сенсор



- Устанавливается на Windows-компьютеры
- Передает на Центральный узле данные об активности
  - Запуск и остановка процессов, загрузка модулей, системные вызовы
  - Создание, изменение и удаление файлов
  - Изменения в реестре
  - Данные об установленных соединениях: откуда, куда, каким процессом
  - События из журнала событий Windows
- Если активированы функции EDR, выполняет задачи
  - Изолирует компьютер в сети (допускаются исключения)
  - Запрещает запускать программы и открывать документы (по MD5/SHA256)
  - Извлекает и посылает на центральный узел файлы для анализа
  - Останавливает процессы и удаляет файлы (по запросу)
  - Запускает файлы и выполняет команды

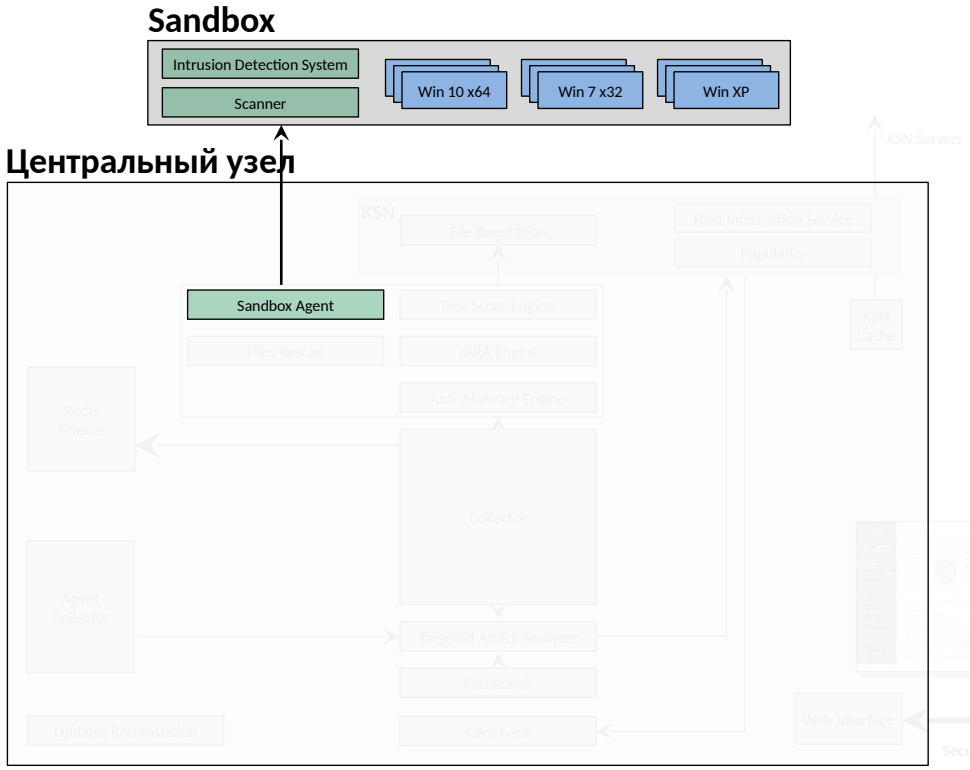
Компоненты KATA | Центральный узел

- Получает объекты и данные от сетевых Сенсоров (или напрямую из трафика)
- Проверяет объекты различными технологиями:
  - антивирусным ядром
  - Yara
  - Risk Score
  - KSN
  - Certcheck
- Передает объекты на Sandbox-сервер и забирает результаты проверки
- Получает данные от Endpoint-сенсоров
- Анализирует данные, выявляет аномалии в сетевой активности и поведении конечных узлов
- Публикует интерфейс для офицеров безопасности
- Поддерживает распределенную установку с несколькими Центральными узлами



Компоненты KATA/KEDR | Sandbox

- Основан на технологиях автоматического анализа файлов, которые совершенствовались в Лаборатории Касперского более 10 лет
- Получает и «активирует» внутри виртуальных машин:
  - Исполняемые файлы и скрипты — запускает
  - Документы Microsoft Office и Adobe — открывает в соответствующих программах
  - URL — открывает в web-браузере
- Анализирует активность внутри виртуальной машины и выносит вердикт
- Всегда является отдельным сервером



Лицензирование KATA

	Стандартная лицензия	Расширенная лицензия	Enterprise-лицензия
Размер компании	До 1,000 сотрудников	До 5,000 сотрудников	До 500,000 сотрудников
Объем трафика	До 100 Мбит/с	До 1 Гбит/с	До 4 Гбит/с
Анализ трафика	Почтовый ИЛИ сетевой	Почтовый И сетевой	Почтовый И сетевой
Количество (сетевых) Сенсоров	1	2	4
Дополнительный Сенсор	Почтовый И сетевой, лицензируются по количеству серверов (Сенсоров)		
Дополнительный Sandbox	Бесплатно		
Дополнительный Центральный узел	Бесплатно для управления Endpoint-сенсорами		

Лицензирование KEDR

	Стандартная лицензия	Расширенная лицензия	KATA EDR agent (дополнение)	KATA Enterprise EDR Agent
Единица лицензирования	По количеству защищенных узлов			
Сервер Sandbox	Не поддерживается	Поддерживается		
Центральный узел	Поставляется бесплатно для управления EDR агентами, возможности Сенсора недоступны		Доступен со всеми функциями по лицензии KATA	
Функциональность KATA	Нет	Нет	Согласно лицензии KATA	Согласно лицензии KATA (полная)

— KEDR продается как отдельное решение или аддон к KATA

— Во всех случаях для управления EDR агентами требуется Центральный узел

Спасибо за внимание!

Квитко Виталий
Инженер сервисной группы
тел: + 7 (812) 325 84 00
e-mail: vkvitko@polikom.ru

ПОЛИКОМ ПРО

Просто работаем.