ENDPOINT DETECTION AND RESPONSE (EDR) - ПОЧЕМУ НЕДОСТАТОЧНО СТАНДАРТНОГО АНТИВИРУСА НА КОНЕЧНОЙ ТОЧКЕ?

КРАТКИЙ ОБЗОР РЕШЕНИЙ FIREEYE HX И KASPERSKY EDR

Владимир Соловьев
Ведущий специалист АО «ДиалогНаука»
21 апреля 2020 года

О КОМПАНИИ

- Создана в 1992 году СП «Диалог» и Вычислительным центром РАН
- Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB
- На сегодняшний день «ДиалогНаука» является одной из ведущих российских компаний, специализирующихся в области информационной безопасности

Ключевые клиенты

Введение

- Появление APT-атак
  - ✓ С 2004 года команда реагирования на компьютерные инциденты в Lockheed Martin (LM-CIRT) стала использовать термин APT (Advanced Persistent Threat) в своих исследованиях
  - ✓ Спецслужбы стран и отряды «правительственных хакеров»

Введение

- Появление APT-атак
  - ✓ С 2004 года команда реагирования на компьютерные инциденты в Lockheed Martin (LM-CIRT) стала использовать термин APT (Advanced Persistent Threat) в своих исследованиях
  - ✓ Спецслужбы стран и отряды «правительственных хакеров»
- Признаки APT-атак
  - ✓ Сценарий атаки включает себя несколько этапов
  - ✓ 0day-уязвимости — не обязательный атрибут APT
  - ✓ Рассылка фишинговых писем - часто выделяемый критерий APT
  - ✓ Это долговременная атака (в среднем 150-180 дней)
  - ✓ APT не останавливают отдельные инструменты безопасности (в том числе антивирус…)
  - ✓ Маскировка (общедоступное легитимное ПО, шифрование данных)

Этапы APT-атак

Сбор данных о жертве

- Выявление цели
- Сбор информации
- Разработка стратегии
- Разработка инструментов

Этапы APT-атак

Сбор данных о жертве

- Выявление цели
- Сбор информации
- Разработка стратегии
- Разработка инструментов

Первичное заражение

- Доставка боевой нагрузки
- Эксплуатация уязвимостей в обход СЗИ
- Социальная инженерия
- Инвентаризация сети

Этапы APT-атак

Сбор данных о жертве

- Выявление цели
- Сбор информации
- Разработка стратегии
- Разработка инструментов

Первичное заражение

- Доставка боевой нагрузки
- Эксплуатация уязвимостей в обход СЗИ
- Социальная инженерия
- Инвентаризация сети

Активная фаза/ закрепление

- Распространение в сети
- Поиск ключевой информации
- Повышение привилегий
- Получение удаленного контроля

Этапы APT-атак

Сбор данных о жертве

- Выявление цели
- Сбор информации
- Разработка стратегии
- Разработка инструментов

Первичное заражение

- Доставка боевой нагрузки
- Эксплуатация уязвимостей в обход СЗИ
- Социальная инженерия
- Инвентаризация сети

Активная фаза/ закрепление

- Распространение в сети
- Поиск ключевой информации
- Повышение привилегий
- Получение удаленного контроля

Достижение цели

- Хищение данных
- Изменение данных
- Связь с управляющими серверами
- Сокрытие следов
- Ботнет сеть

APT-группы

-  APT37 (Северная Корея)

Group 123, Group123, Starcruft, Reaper, Reaper Group, Red Eyes, Ricochet Chollima, StarCruft, Operation Daybreak, Operation Erebus, Venus 121

-  APT34 (Иран)
-  APT33 (Иран)

Elfin, MAGNALLIUM, Refined Kitten, HOLMIUM

-  APT32 (Вьетнам)

OceanLotus Group, Ocean Lotus, OceanLotus, Cobalt Kitty, APT-C-00, SeaLotus, Sea Lotus, APT-32, APT 32, Ocean Buffalo, POND LOACH

-  APT19 (Китай)

C0d0so, Sunshop Group

-  APT28 (Россия)

Pawn Storm, PawnStorm, Fancy Bear, Sednit, SNAKEMACKEREL, TsarTeam, Tsar TeamSwallowtail, IRON TWILIGHT, Group 74, SIG40, Grizzly Steppe, TG-4127, Group-4127, STRONTIUM, TAG_0700

Общая статистика по APT-атакам*

- 2017: эпидемии шифровальщиков WannaCry, NotPetya, BadRabbit
- 2018: “side-channel”-атаки и новые уязвимости в микропроцессорах
- 2019: открытые военные операции в киберпространстве, тема кибербезопасности вышла на первый план в политике, а действия киберармий и публичная риторика политических деятелей вокруг кибератак продолжают набирать обороты
  - ✓ **Иран**. Июнь, корпус стражей Исламской революции сбил американский беспилотник. В ответ на это через несколько дней США провели кибератаку на ракетные системы Ирана
  - ✓ **Венесуэла**. Март, в результате саботажа на ГЭС имени Симона Боливара («Гури») в Венесуэле произошло массовое отключение электроэнергии в 22 штатах страны из 23

*Согласно данным отчёта «Hi-Tech Crime Trends 2019/2020» компании Group-IB

Общая статистика по APT-атакам*

- 2017: эпидемии шифровальщиков WannaCry, NotPetya, BadRabbit
- 2018: “side-channel”-атаки и новые уязвимости в микропроцессорах
- 2019: открытые военные операции в киберпространстве, тема кибербезопасности вышла на первый план в политике, а действия киберармий и публичная риторика политических деятелей вокруг кибератак продолжают набирать обороты
  - ✓ **Иран**. 20 июня 2019 корпус стражей Исламской революции сбил американский беспилотник. В ответ на это через несколько дней США провели кибератаку на ракетные системы Ирана
  - ✓ **Венесуэла**. В марте 2019 в результате саботажа на ГЭС имени Симона Боливара («Гури») в Венесуэле произошло массовое отключение электроэнергии в Каракасе и 22 штатах страны из 23

Инциденты за 2019 год в очередной раз подтверждает предположение о том, что критические инфраструктуры многих стран уже скомпрометированы, но атакующие остаются незамеченными до нужного момента

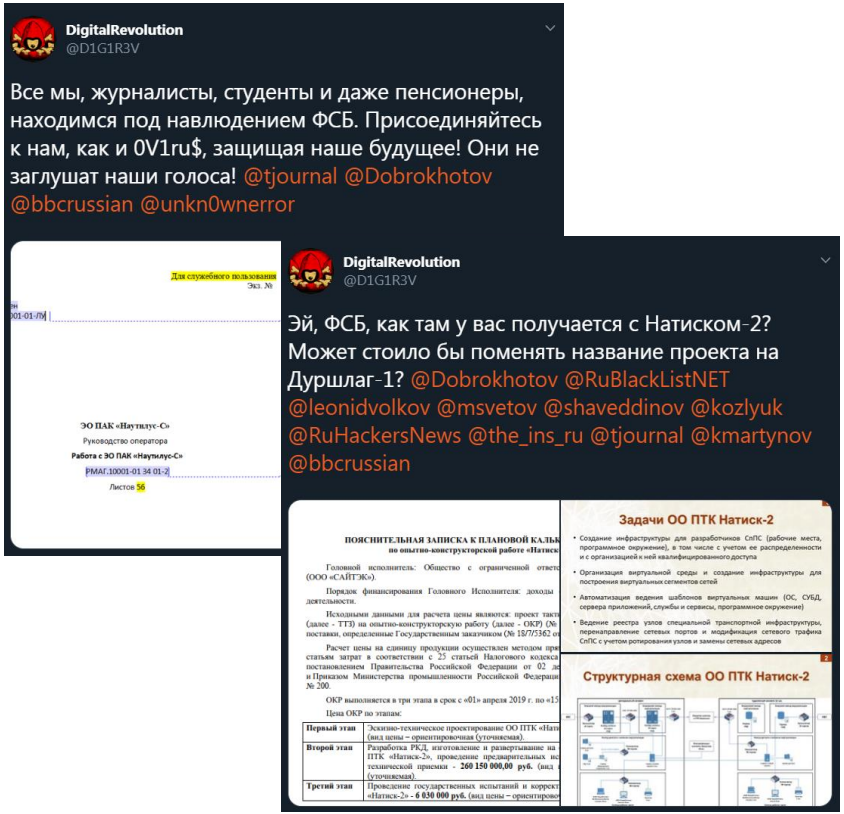
*Согласно данным отчёта «Hi-Tech Crime Trends 2019/2020» компании Group-IB

Ситуация в мире

- Согласно результатам исследования TAdviser и Microsoft, проведенного осенью 2019 года, за год с целенаправленными атаками столкнулись 39% компаний сегмента малого и среднего бизнеса. По данным компании Positive Technologies, более 50% СМБ-компаний присваивают риску APT-атаки высокий уровень опасности
- Наибольший интерес для злоумышленников представляют государственные учреждения, промышленные компании, финансовый сектор и сфера науки и образования

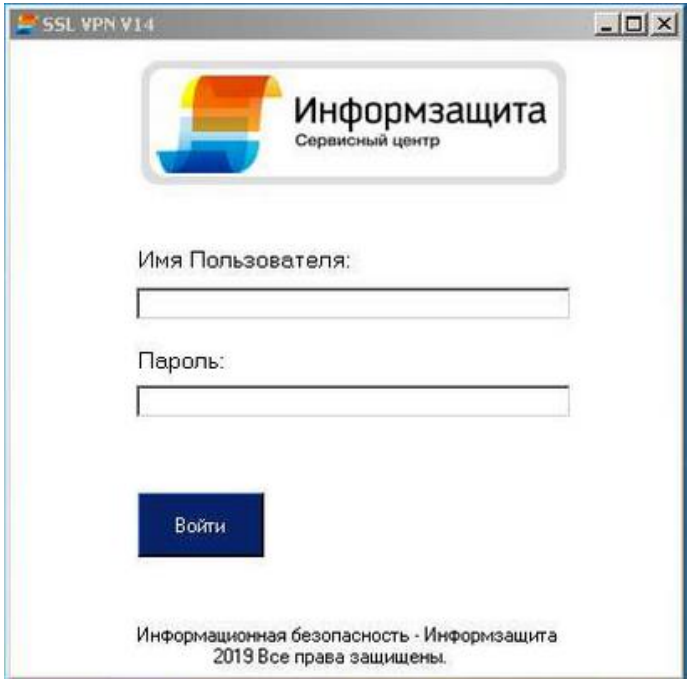
Ситуация в России. Подрядчик ФСБ

- Летом 2019 года ряд изданий сообщили о взломе подрядчика ФСБ — московской компании «Сайтэк». Так, в открытый доступ выложили скриншот интерфейса внутренней сети, а рядом с названиями проектов («Арион», «Реляция», «Гривна» и так далее) стояли имена их кураторов, сотрудников «Сайтэка». Похищенными документами хакеры поделились с журналистами нескольких изданий, и дамп содержал довольно подробное описание проектов «Сайтэка»



Ситуация в России. ПО CloudMid

- В феврале 2019 года на юге России была обнаружена очень специфичная целевая атака. В ней было задействовано ранее неизвестное вредоносное ПО, которое имело на юге России название CloudMid. Эта шпионская программа распространялась по электронной почте, маскируясь под VPN-клиент известного российского поставщика защитных решений, который среди прочего предлагает решения для защиты сети. Сама вредоносная программа достаточно проста и предназначена для кражи документов



Ситуация в России. Банки

Сегмент рынка в России	Кол-во групп	Общее число успешных атак в день	Средняя сумма одного хищения	Средняя сумма хищения в день*	H2 2018- H1 2019 (в RUR)	H2 2018- H1 2019 (в USD)	Рост к прошлому периоду
Хищения у юридических лиц с троянами для ПК	2	0,5	500 000 ₽	250 000 ₽	62 250 000 ₽	$957 692	-89%
Хищения у физических лиц с Android-троянами	5	40	11 000 ₽	440 000 ₽	109 560 000 ₽	$1 685 538	-43%
Целевые атаки на банки	3	—	31 000 000 ₽	—	93 000 000 ₽	$1 430 769	-93%
Фишинг	11	435	800 ₽	348 000 ₽	86 652 000 ₽	$1 333 108	-65%
Обналичивание похищаемых средств	—	—	—	467 100 ₽	158 157 900 ₽	$2 433 198	-85%
Итого	—	—	—	**1 038 000**	**509 619 900 ₽**	**$7 840 306**	**-85%**

- Русскоязычные хакеры перестали атаковать банки в РФ и переключились на зарубежные кредитные организации
- Согласно отчету Group-IB до 93 млн руб, то есть почти в 14 раз сократились потери от целевых атак на банки в России со стороны финансово мотивированных группировок. По сравнению с прошлым периодом, средняя сумма хищения от целевых атак на банки в России упала со 118 до 31 миллиона рублей

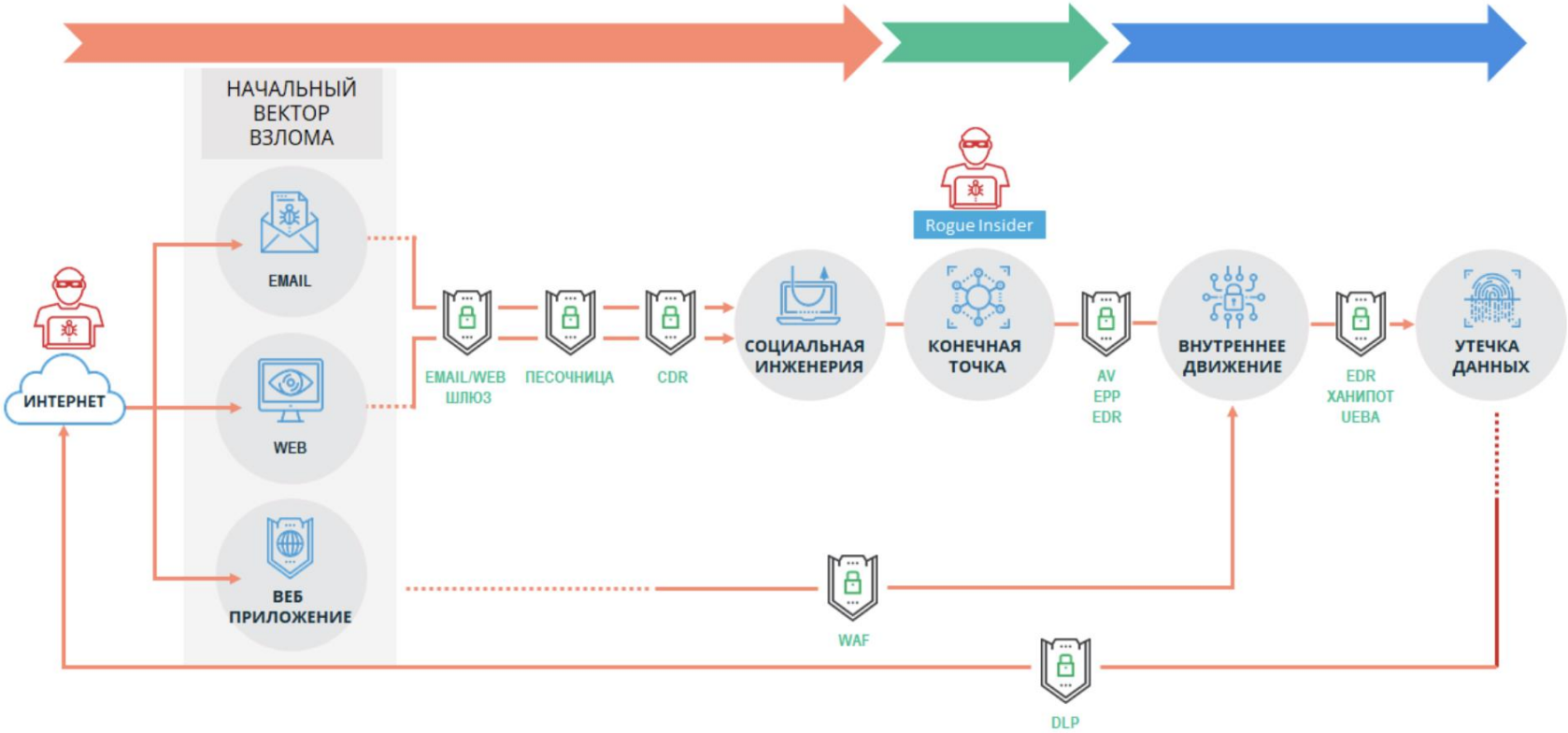
КАК ЖЕ ЗАЩИТИТЬСЯ ОТ APT-АТАК?

И ПОЧЕМУ НЕДОСТАТОЧНО СТАНДАРТНОГО АНТИВИРУСА НА КОНЕЧНОЙ ТОЧКЕ?

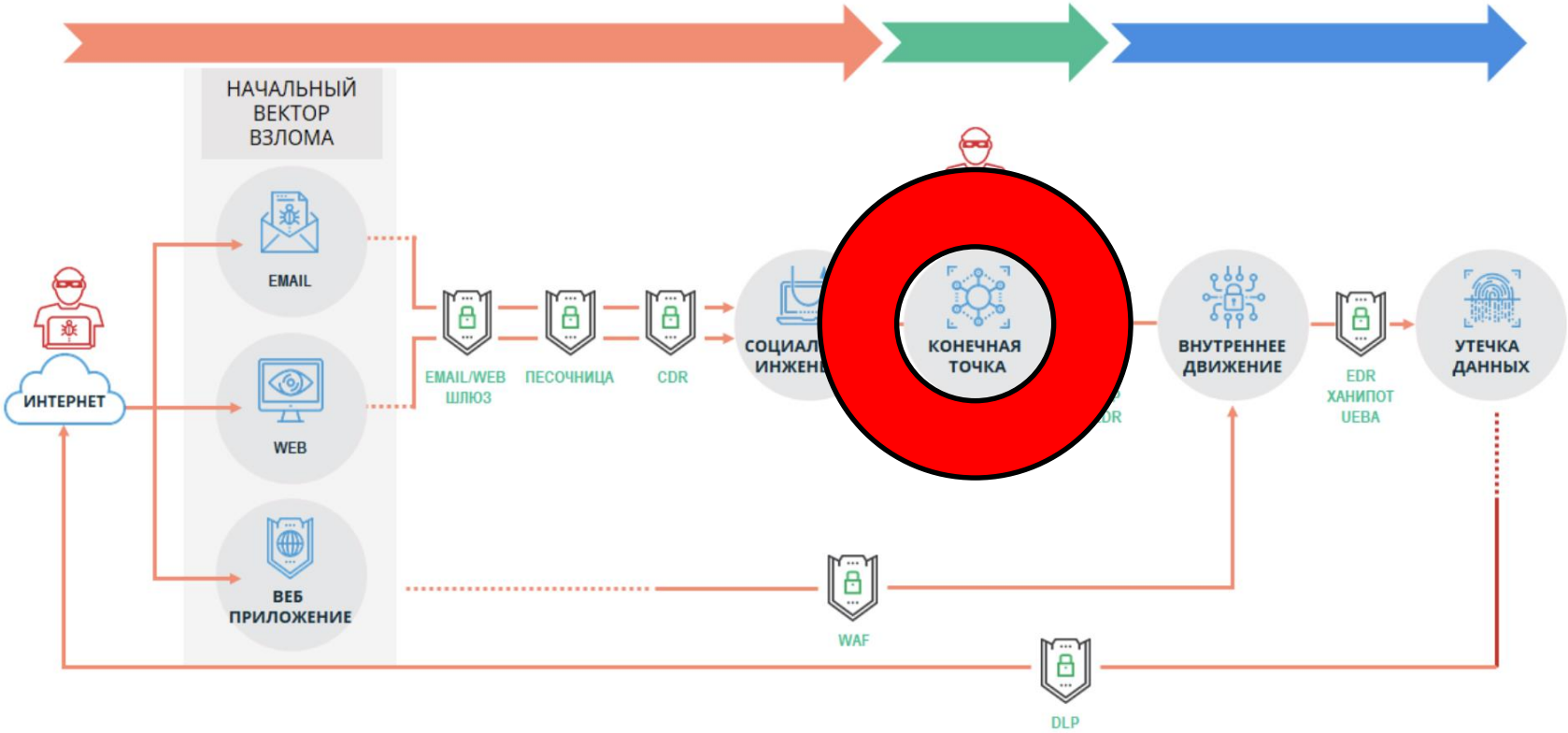
Как же защититься от APT-атак?

- Защита от целевых атак — это комплексная задача, которую нельзя решить используя какой-либо один продукт. Для достижения цели требуется применять весь спектр средств обеспечения информационной безопасности; только в этом случае можно повысить процент успешного обнаружения и нейтрализации атак

Векторы APT-атаки



Векторы APT-атаки



Почему недостаточно стандартного Антивируса на конечной точке?

- Технологии защиты от целенаправленных атак были и раньше, но сейчас они выходят на новый уровень. В первую очередь речь идет о различных инструментах для выявления аномалий – как на конечных точках, так и на уровне сетевой активности. Задачей таких систем является поиск всего необычного, что происходит, а не поиск вредоносного года, что в свою очередь делают стандартные Антивирусы. Это объясняется тем, что во многих случаях атакующие могут вообще не использовать вредоносные программы

Почему недостаточно стандартного Антивируса на конечной точке?

- Технологии защиты от целенаправленных атак были и раньше, но сейчас они выходят на новый уровень. В первую очередь речь идет о различных инструментах для выявления аномалий – как на конечных точках, так и на уровне сетевой активности. Задачей таких систем является поиск всего необычного, что происходит, а не поиск вредоносного года, что в свою очередь делают стандартные Антивирусы. Это объясняется тем, что во многих случаях атакующие могут вообще не использовать вредоносные программы

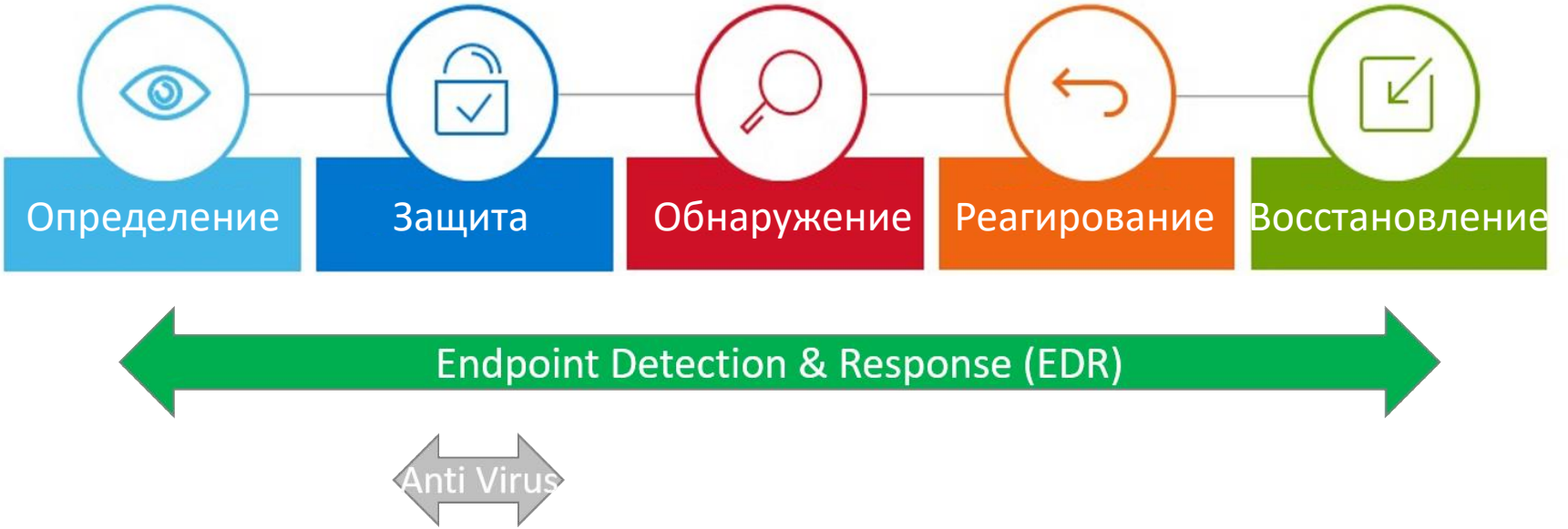
В этом случае могут помочь решения класса EDR (Endpoint Detection and Response - обнаружение атак на конечные точки и оперативное реагирование на них)

EDR - (Endpoint Detection and Response)

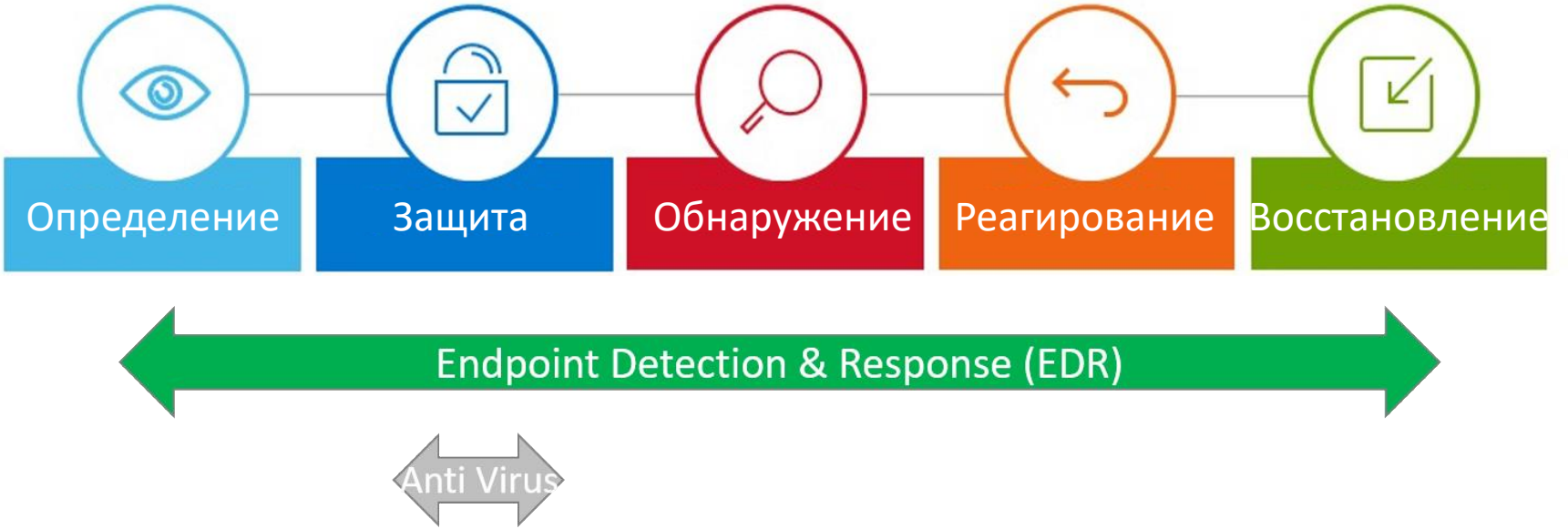
- Решения класса EDR не просто защищают конечную точку от вредоносов, но и моментально обнаруживают новейшие угрозы высокой сложности, а также позволяют оперативно проявлять реакцию на возникшую ситуацию

- Для работы необходима установка Агента на конечной точке

Почему недостаточно стандартного Антивируса на конечной точке?



Почему недостаточно стандартного Антивируса на конечной точке?



Для увеличения эффективности EDR можно использовать, как дополнение к существующему Антивирусу

Разница между EPP (AV) и EDR

EPP (Endpoint Protection Platform)

- Сигнатурный анализ
- Эвристический (статический) анализ
- Межсетевой экран
- Система предотвращения вторжений
- Система контроля подключаемых к конечной станции устройств
- И т.п.

Разница между EPP (AV) и EDR

EPP (Endpoint Protection Platform)

- Сигнатурный анализ
- Эвристический (статический) анализ
- Межсетевой экран
- Система предотвращения вторжений
- Система контроля подключаемых к конечной станции устройств
- И т.д.

EDR (Endpoint Detection and Response)

- Обнаружение аномалий (файловая система, сеть, реестр…)
- Динамический анализ файлов в «Песочнице»
- Система контроля приложений
- Сбор форензики для расследований инцидентов ИБ
- Восстановление данных
- Машинное обучение
- Защита от эксплойтов
- Изоляция конечной точки
- Реагирование на выявленные угрозы
- И т.д.

Основные EDR-решения

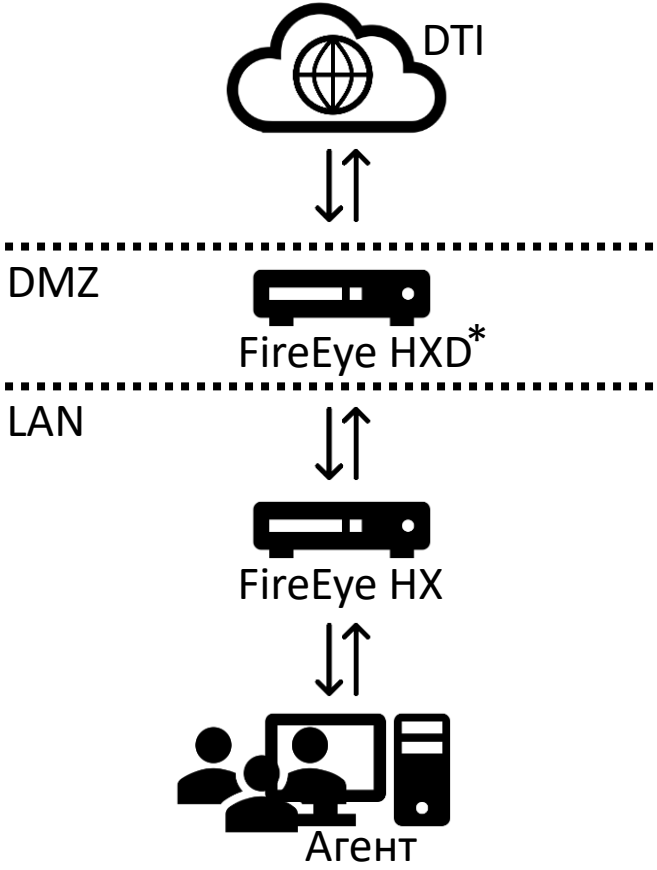
Вендор/решение:

1. FireEye HX
2. Kaspersky EDR
3. Trend Micro Apex One
4. TDS Huntpoint
5. Check Point SandBlast Agent
6. FortiNet FortiClient
7. Symantec EDR
8. Palo Alto Traps
9. Cisco AMP for Endpoints
10. Carbon Black Response
11. CrowdStrike Falcon Insight EDR

*Magic Quadrant for Endpoint Protection Platforms & Endpoint Detection and Response 2019

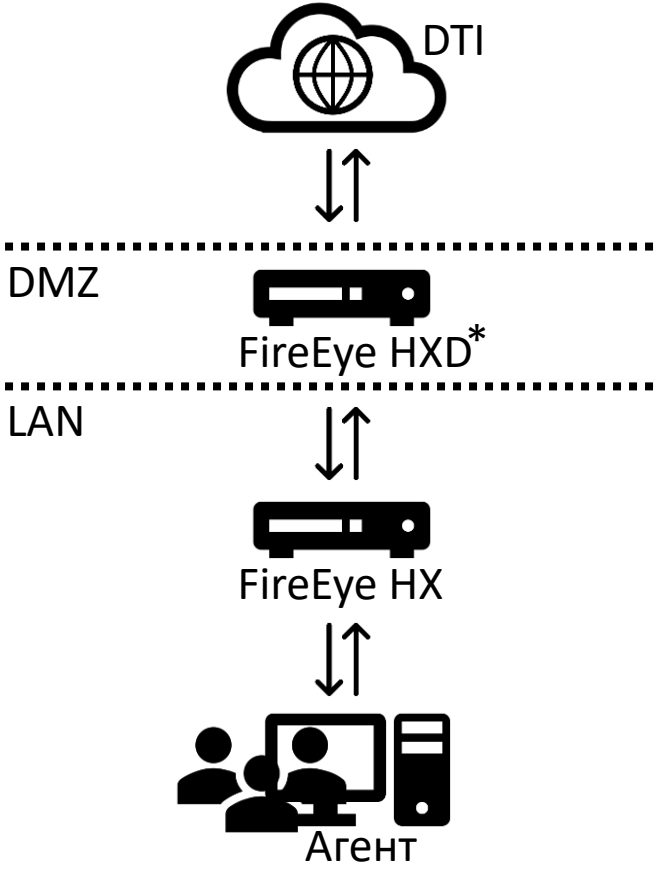
FireEye HX (Endpoint Security)

- Архитектура:
  1. Сервер управления
  2. Агент



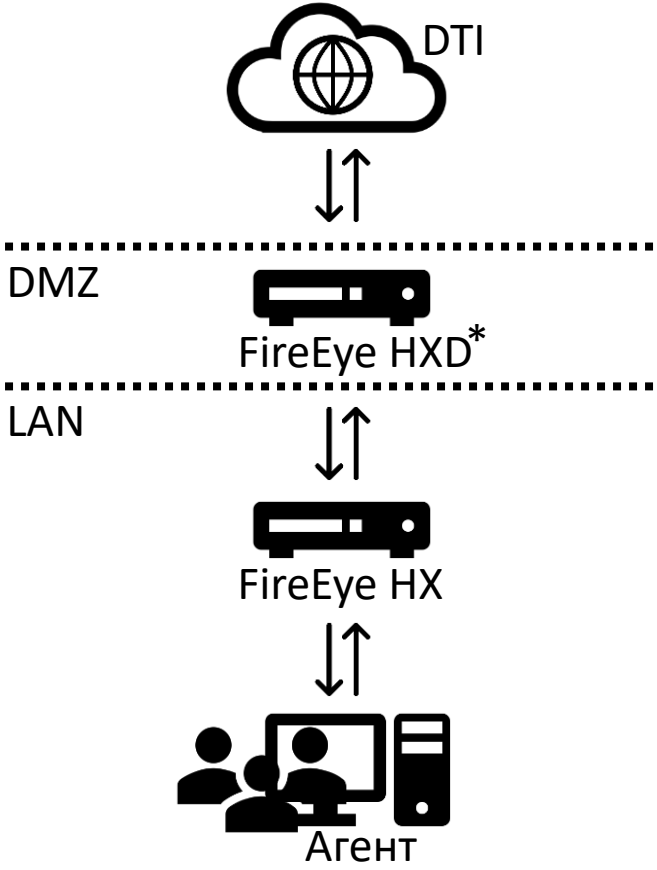
FireEye HX (Endpoint Security)

- Архитектура:
  1. Сервер управления
  2. Агент
- Исполнение:
  1. Hardware appliance
  2. Virtual appliance
  3. Cloud-based appliance



FireEye HX (Endpoint Security)

- Архитектура:
  1. Сервер управления
  2. Агент
- Исполнение:
  1. Hardware appliance
  2. Virtual appliance
  3. Cloud-based appliance
- Лицензирование:
  1. По кол-ву конечных точек (Агентов)
  2. Доп. лицензия для расширенных возможностей



Системные требования для разворачивания Агента

WINDOWS OPERATING SYSTEM VERSIONS	MINIMUM SYSTEM MEMORY (RAM)
Win 7 and Win 7 SP1 (32-bit and 64-bit) Win 8 (32-bit and 64-bit) Win 8.1 (32-bit and 64-bit) Win 10 (32-bit and 64-bit)	1 GB (32-bit), 2 GB (64-bit)
Server 2003 R2 SP2 (32-bit and 64-bit)	512 MB
Server 2008 (32-bit and 64-bit) Server 2008 R2, R2 SP1, R2 SP2 (64-bit) Server 2012 (32-bit and 64-bit) Server 2012 R2 (32-bit and 64-bit) Server 2016 (32-bit and 64-bit)	2 GB

LINUX OPERATING SYSTEM VERSIONS	MINIMUM SYSTEM MEMORY (RAM)
RHEL 6.8+, 7.2+, 8 (64-bit) CentOS 6.9+, 7.2+, 8 (64-bit) SUSE 11.3, 11.4, 12.2, 12.3, 15 Ubuntu 14.04, 16.04, 18.04, 19.04 Amazon Linux AMI 2018.3, AM2 Oracle Linux 6.10, 7.6	2 GB

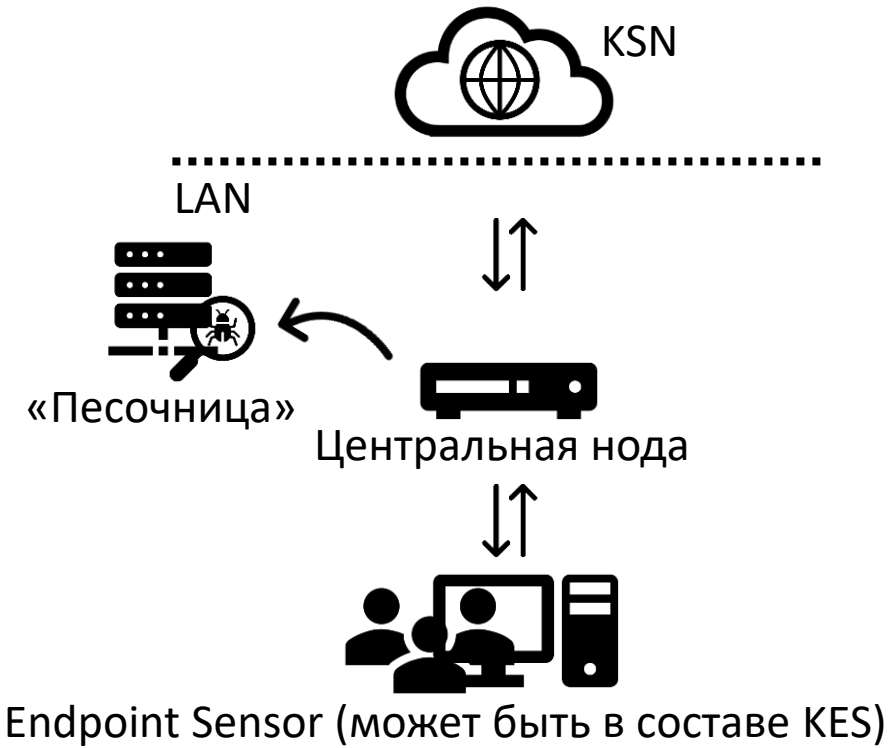
MACOS VERSIONS	MINIMUM SYSTEM MEMORY (RAM)
Mavericks 10.9 (64-bit) Yosemite 10.10 (64-bit) El Capitan 10.11 (64-bit) Sierra 10.12 (64-bit) High Sierra 10.13 (64-bit) Mojave 10.14 (64-bit) Catalina 10.15 (64-bit)	2 GB

Основные возможности и компоненты FireEye HX

- **Malware Scans** – сканирование рабочих станций на наличие ВПО
- **Real-Time Indicator Detection** – механизм поиска ВПО на рабочих станциях с помощью индикаторов компрометации (IoC)
- **Malware Protection** – механизм защиты рабочих станций от вирусов, троянов, червей, кейлогеров, потенциально опасных программ и др. с возможностью помещения файлов в карантин
- **Exploit Guard Protection** – механизм защиты рабочих станций от эксплойтов
- **Enterprise Search** – расширенный и удобный поиск по выявлению угроз на рабочих станциях (Threat Hunting)
- **Data Acquisition** – механизм сбора форензики (дамп диска, оперативной памяти и т.д.)
- **Containment** – механизм изоляции рабочей станции
- **API** – возможность взаимодействия с сервером с помощью REST-запросов (доп. утилита HXTool)
- **Enricher Module** – механизм отправки объектов в выделенную «Песочницу» (FireEye AX)
- **Agent Anywhere™** – механизм связи удаленных Агентов с сервером без использования VPN
- **Интеграция** с другими классами устройств FireEye

kaspersky

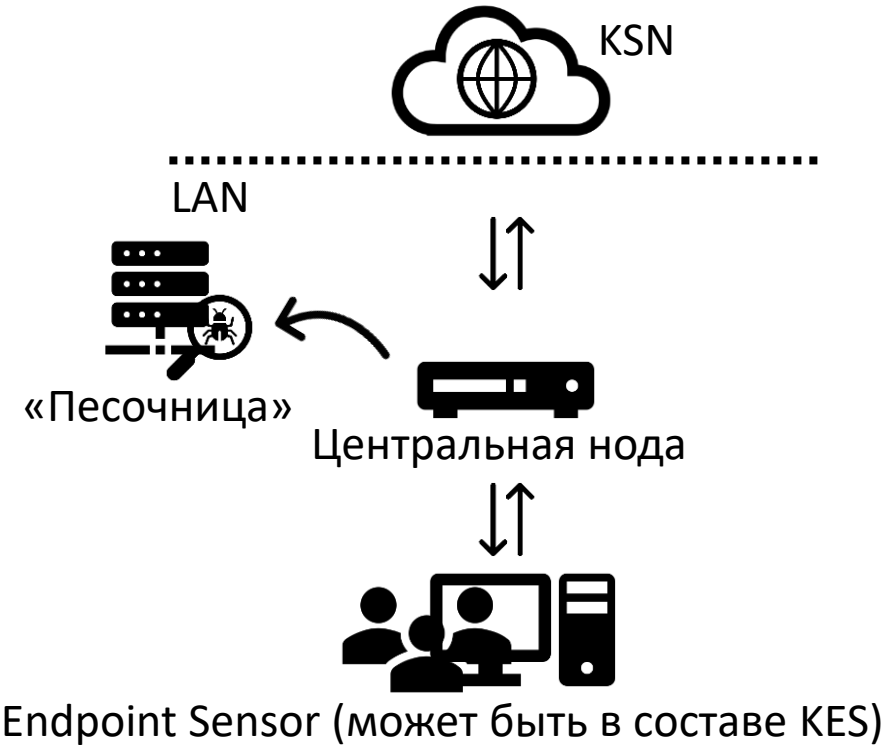
- Архитектура:
  1. Центральная нода (+ Сенсор)
  2. Endpoint Sensor
  3. «Песочница»



Kaspersky EDR (KEDR)

kaspersky

- Архитектура:
  1. Центральная нода (+ Сенсор)
  2. Endpoint Sensor
  3. «Песочница»
- Исполнение:
  1. Программное обеспечение



Kaspersky EDR (KEDR)

kaspersky

- Архитектура:
  1. Центральная нода (+ Сенсор)
  2. Endpoint Sensor
  3. «Песочница»
- Исполнение:
  1. Программное обеспечение
- Лицензирование:
  1. По кол-ву конечных точек (Endpoint Sensors)

Аппаратные требования для разворачивания KEDR

- Конфигурация сервера с компонентом **Central Node** зависит от объема данных, обрабатываемых программой и от пропускной способности канала связи
- Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; 1000 компьютеров с компонентом Endpoint Sensors):
  - ✓ Процессор: 12 ядер (24 потока), 2.7 ГГц
  - ✓ Объем оперативной памяти: 128 ГБ
  - ✓ Дисковая подсистема – два раздела: 2 ТБ свободного пространства для системного раздела и 4 ТБ свободного пространства для хранения данных компонента Targeted Attack Analyzer
  - ✓ Рекомендуется использовать дисковый массив уровня RAID 0, 5, 10 или SSD-диск
  - ✓ Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый

- Конфигурация сервера с компонентом **Sandbox** зависит от объема данных, обрабатываемых программой, от количества одновременно запускаемых виртуальных машин с образами операционных систем, а также от пропускной способности канала связи
- Минимальные аппаратные требования к серверу (пропускная способность канала связи 50 Мбит/сек.; 12 одновременно запускаемых виртуальных машин; 3500 файлов, обрабатываемых за одни сутки):
  - ✓ Процессор Intel с поддержкой VT-x и EPT, 8 ядер, 2.7 ГГц
  - ✓ Процессоры AMD не поддерживаются
  - ✓ Объем оперативной памяти: 32 ГБ
  - ✓ Дисковая подсистема: 300 ГБ свободного пространства
  - ✓ Два сетевых адаптера со скоростью передачи данных по 1 Гбит/сек. каждый

- Рекомендуемая конфигурация **Endpoint Sensor**:
  - ✓ Процессор: 2 ГГц и выше с поддержкой инструкций SSE2
  - ✓ Объем оперативной памяти: 2 ГБ
  - ✓ Дисковая подсистема: 2 ГБ свободного пространства
  - ✓ Один сетевой адаптер со скоростью передачи данных 1 Гбит/с
- Минимальная конфигурация **Endpoint Sensor** :
  - ✓ Процессор Intel® CoreTM i3 Duo 3.10GHz или эквивалентный (с поддержкой SSE2)
  - ✓ Объем оперативной памяти: 40 МБ
  - ✓ Дисковая подсистема: 100 МБ свободного пространства

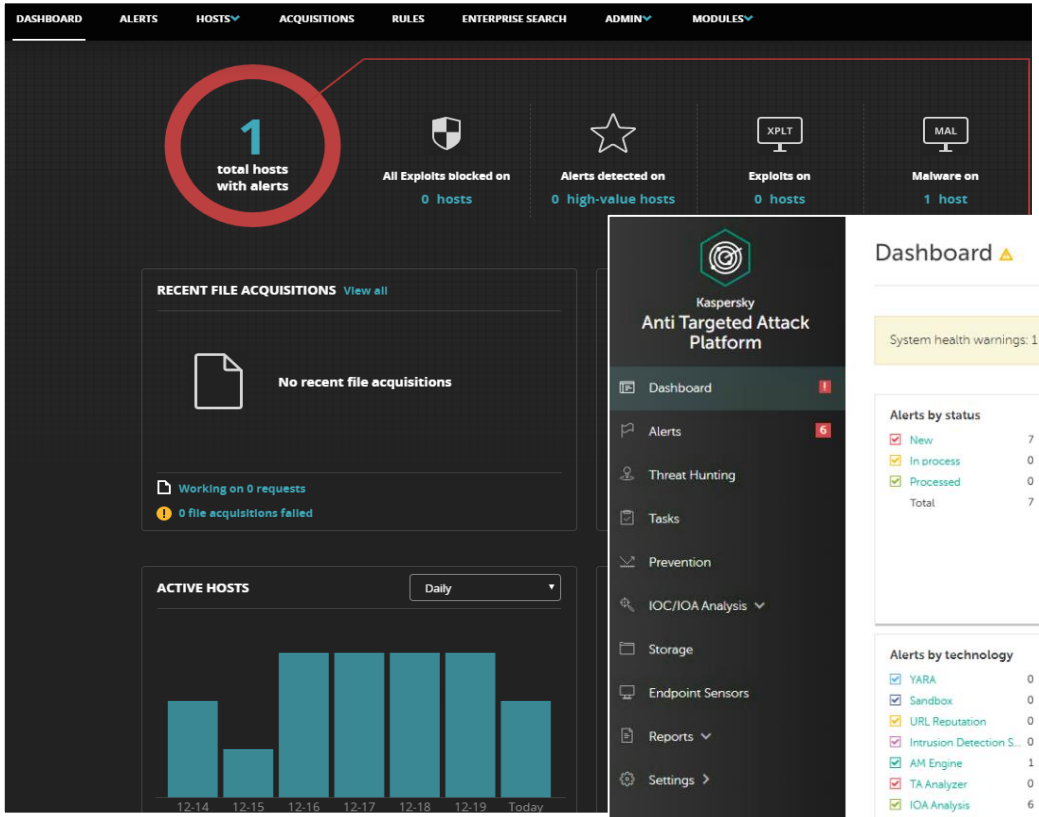
Основные возможности и компоненты KEDR

- При использовании решения Kaspersky EDR компонент Центральная нода, используя компонент Endpoint Sensor, собирает и хранит события операционной системы для последующего автоматического анализа, а также для возможности расследования, с использованием интерактивного интерфейса
- Также Центральная нода предоставляет возможности реагирования (при использовании продукта Kaspersky Endpoint Detection and Response), используя компонент Endpoint Sensor:
  - ✓ Блокировка запуска ПО / скриптов / документов
  - ✓ Завершение процесса
  - ✓ Удаление файла
  - ✓ Получение файла с конечного узла в хранилище на Центральной ноде
  - ✓ Карантин файла / восстановление из карантина
  - ✓ Запуск программы
  - ✓ Выполнение IoC-сканирования на конечных узлах, а также по базе собранных событий
  - ✓ Выполнение сетевой изоляции конечных точек

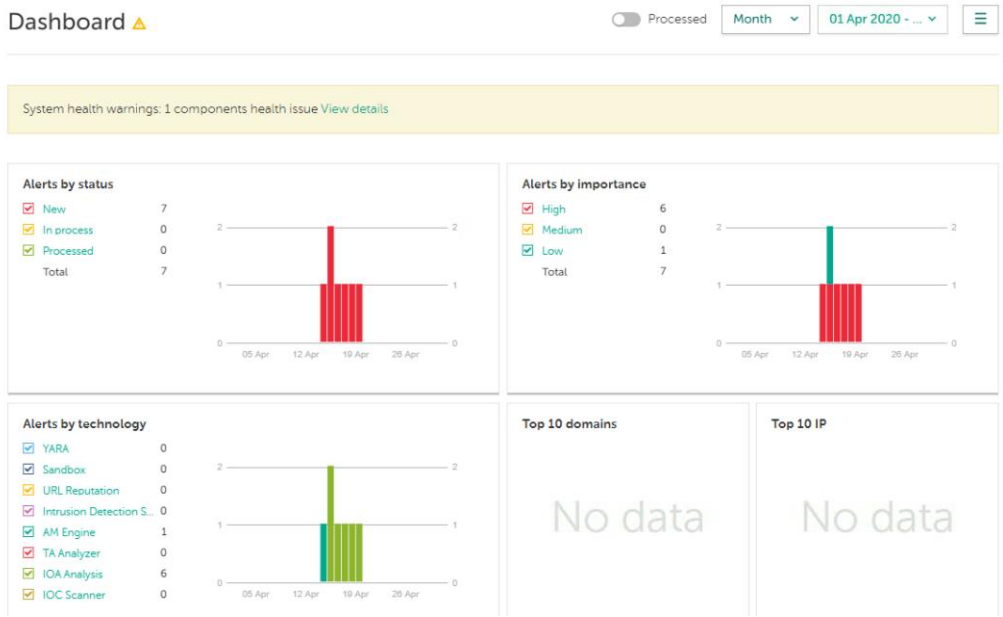
Основные возможности и компоненты KEDR

- **IOC/IOA-анализ** – механизм поиска ВПО на рабочих станциях с помощью индикаторов компрометации (IoC)
- **Threat Hunting** – расширенный и удобный поиск по выявлению угроз на рабочих станциях
- **Antimalware Engine** антивирусный сканер, применяемый в различных решениях Лаборатории Касперского
- **Intrusion Detection System** – модуль обнаружения вторжений, с набором уникальных правил
- **URL Reputation** – репутационный список вредоносных ресурсов
- **Targeted Attack Analyzer** – технология анализа поведения на конечных точках
- **Интеграция** с другими решениями ЛК (KATA, KES)
- **Отправка файлов** в «Песочницу» для динамического анализа

ДЕМО


DASHBOARD
ALERTS
HOSTS
ACQUISITIONS
RULES
ENTERPRISE SEARCH
ADMIN
MODULES
1
total hosts with alerts
All Exploits blocked on
0 hosts
Alerts detected on
0 high-value hosts
Exploits on
0 hosts
Malware on
1 host
RECENT FILE ACQUISITIONS View all
No recent file acquisitions
Working on 0 requests
0 file acquisitions failed
ACTIVE HOSTS
Daily
12-14
12-15
12-16
12-17
12-18
12-19
Today

Kaspersky
Anti Targeted Attack Platform
Dashboard
Alerts
6
Threat Hunting
Tasks
Prevention
IOC/IOA Analysis
Storage
Endpoint Sensors
Reports
Settings


Dashboard
Processed
Month
01 Apr 2020 - ...
System health warnings: 1 components health issue View details
Alerts by status
New 7
In process 0
Processed 0
Total 7
Alerts by importance
High 6
Medium 0
Low 1
Total 7
Alerts by technology
YARA 0
Sandbox 0
URL Reputation 0
Intrusion Detection S... 0
AM Engine 1
TA Analyzer 0
IOA Analysis 6
IOC Scanner 0
Top 10 domains
No data
Top 10 IP
No data

ПО ВСЕМ ВОПРОСАМ ОБРАЩАЙТЕСЬ НА EMAIL

marketing@dialognauka.ru