



*Как объединить решения
разных производителей в
единую систему реагирования
на инциденты ИБ*

Руслан Барбашин,
Аккаунт менеджер McAfee
ruslans_barbasins@mcafee.com



#ProfitSecurityDay

Эпиграф

Любовь это вам не просто так!
Любовью надо заниматься!

Андрей Кнышев

Содержание:

- **Адаптивная архитектура безопасности (Gartner)**
- **Как интегрировать решения разных производителей**
- **Анонс решений McAfee для ОЦИБ**



Зачем нужна интеграция решений ИБ?

- Автоматизация обмена данными
 - Threat Intelligence (TI)
 - телеметрия
 - ИОС
- Автоматизация изменения политик
- Уменьшение времени обнаружения (MTTD)
- Уменьшение времени реакции и восстановления (MTTR)



!!! Эффективность ИБ !!!





Адаптивная Архитектура Безопасности

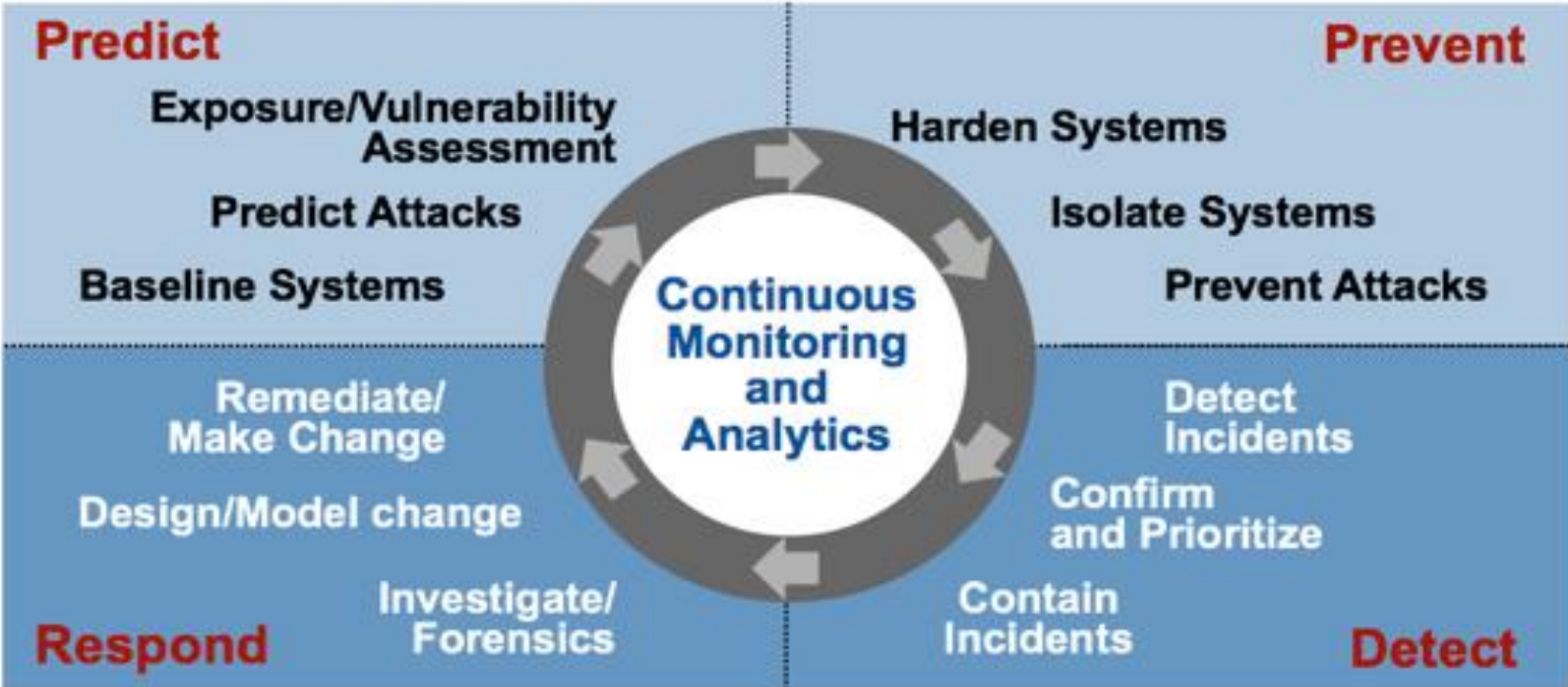
Рекомендации аналитического агентства
Gartner



И много будет странствий и скитаний:
Страна Любви - великая страна!
И с рыцарей своих - для испытаний -
Все строже станет спрашивать она...

Владимир Высоцкий

The Adaptive Security Architecture: Twelve Critical Capabilities of Security



Краткие выводы от Gartner:

- Существующих технологий защиты недостаточно для противостояния современным целенаправленным атакам.
- Большинство организаций до сих пор инвестируют средства только в технологии защиты.
- ***Технологии защиты, предотвращения атак, детектирования и расследования/устранения от различных производителей не интегрированы друг с другом, что приводит к дополнительному хаосу, увеличивает затраты и снижает эффективность ИБ.***
- ИБ не хватает постоянной видимости происходящего для детектирования целенаправленных атак.
- Корпоративные системы находятся под постоянными и не прекращающимися атаками, поэтому понятие «Incident Response» больше не подходит.

Рекомендации от Gartner:

- Поменять понятие «**Incident Response**» на «**Continuous Response**», где предполагается, что системы постоянно скомпрометированы и им необходим непрерывный мониторинг и восстановление.
- Создание **Адаптивной Архитектуры Безопасности** для защиты от целенаправленных атак, используя 12 критических функций от Gartner.
- Направить больше инвестиции на системы обнаружения и быстрого реагирования, и уменьшить на защиту и предотвращение.
- **Отдавать предпочтения производителям, которые предлагают контекстно-ориентированные платформы для сетевой безопасности, безопасности рабочих станций и приложений, а также интегрированный подход к анализу, предотвращению, обнаружению и реагированию на атаки.**
- Развивать **Security Operation Center (SOC)**, который позволяет осуществлять постоянный мониторинг и предотвращение атак.
- Осуществлять полный мониторинг на всех уровнях ИТ: сетевых пакетов, сетевых потоков, активности ОС, контента, поведения пользователей.



А мне приснилось –
Миром правит любовь,

А мне приснилось –
миром правит мечта.

Виктор Цой

Клиент McAfee:

*“Мы можем
обнаружить атаку в
течении 60 секунд,
провести анализ и
ликвидировать атаку в
течении 5 минут”*

<https://www.mcafee.com/enterprise/en-us/assets/case-studies/cs-idc-national-bank.pdf>



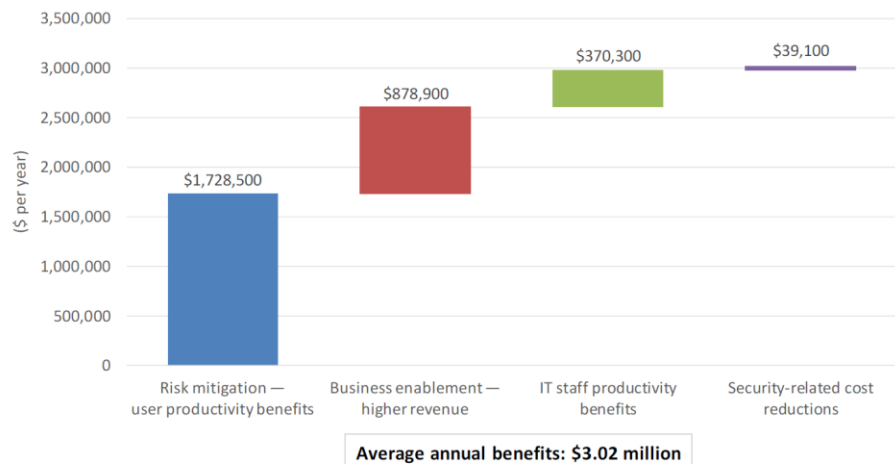
ExpertROI Spotlight Top 100 US FDIC Bank

“Мы можем обнаружить атаку в течении 60 секунд, провести анализ и ликвидировать атаку в течении 5 минут”

Решения: Endpoint, SIEM, TIE, GTI, ATD, DLP

FIGURE 1

Average Annual Benefits



Source: IDC, 2017

Source: <http://idcdocserv.com/US42210917>

- Экономия средств **\$3.02 М** в год
- **ROI 208%** в течении 4 лет
- Период окупаемости **20** месяцев
- На **90%** быстрее расследование инцидентов
- На **77%** меньше инцидентов с причиненным ущербом
- На **98%** меньше времени снижение продуктивности из-за инцидентов ИБ
- **\$5-10 миллионов** дополнительная прибыль
- Мониторинг всех компонентов на **1-2** консолях

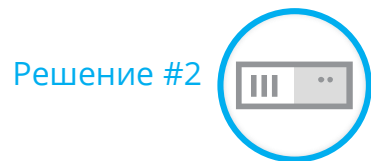
Содержание:

- **Адаптивная архитектура безопасности (Gartner)**
- **Как интегрировать решения разных производителей**
- **Анонс решений McAfee для ОЦИБ**



Межсервисная интеграция до DXL

Для начала интеграция
двух решений



Интеграция решений до DXL

Сначала обмен базовой информацией, *host names*, *credentials*, чтобы решения могли начать обмен данными

Решение #2



Решение #1



Credentials

X Обмен учётными данными

Интеграция решений до DXL

Каждый продукт интегрируется с каждым с использованием специализированного API



Решение #2



Решение #1



Credentials



API



X	Обмен учётными данными
X	Интеграция на уровне API

Интеграция решений до DXL

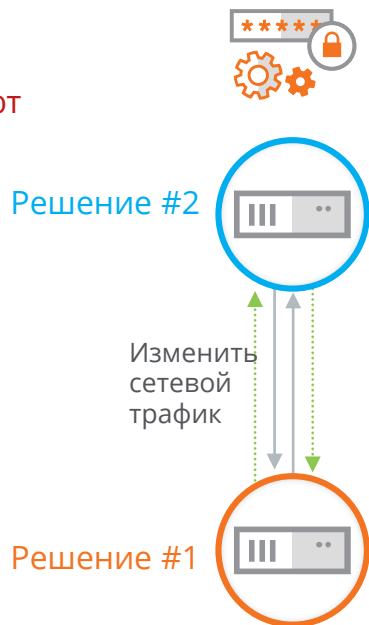
Необходимо
отрегулировать сетевые
политики для
разрешения сетевого
обмена между
решениями (ports,
protocols)



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов

Интеграция решений до DXL

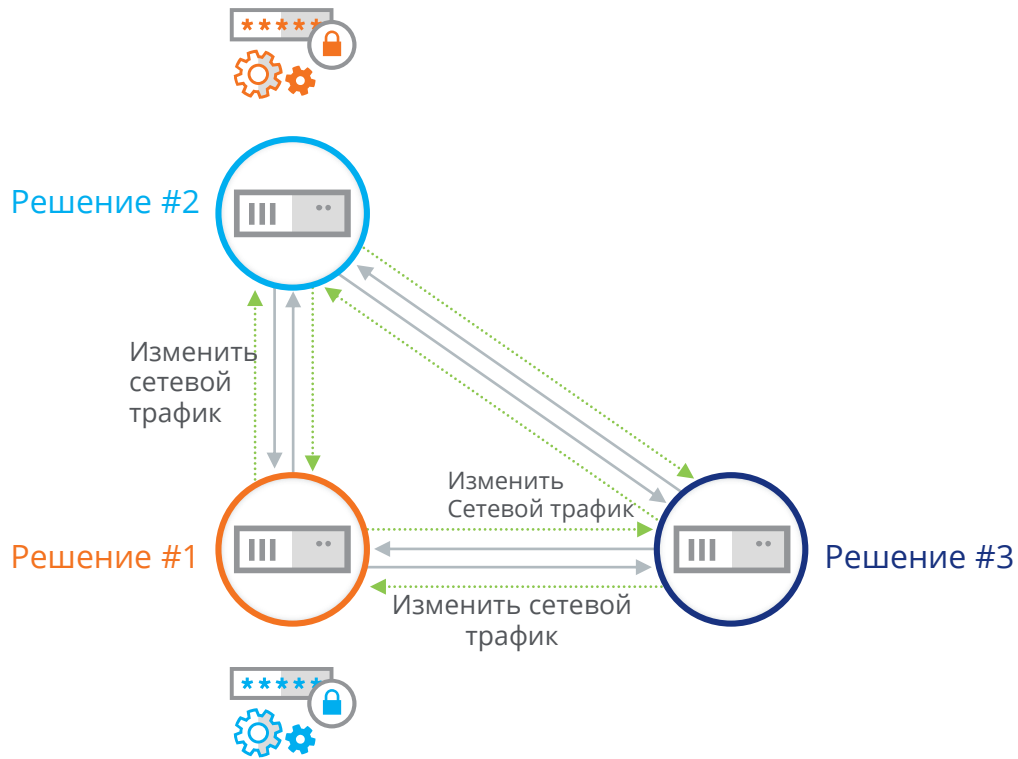
Для получения изменений, решения регулярно опрашивают друг друга



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Интеграция решений до DXL

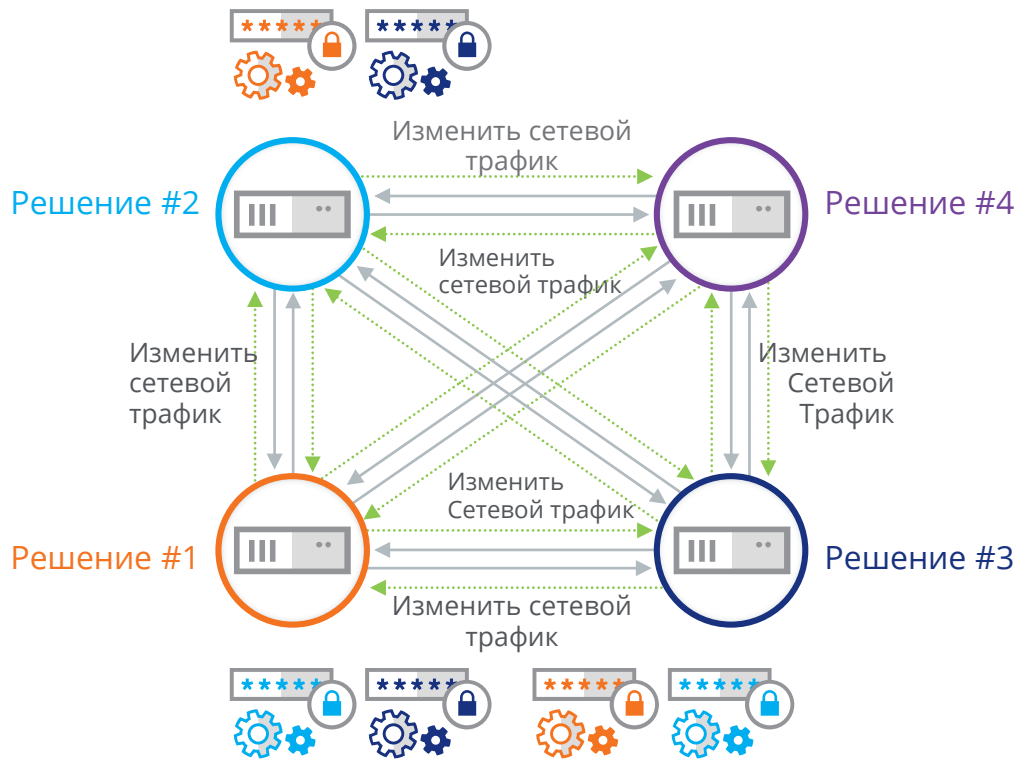
Сложность взаимодействий увеличивается с каждым новым решением



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)

Интеграция решений до DXL

По-моему этим
очень сложно
управлять



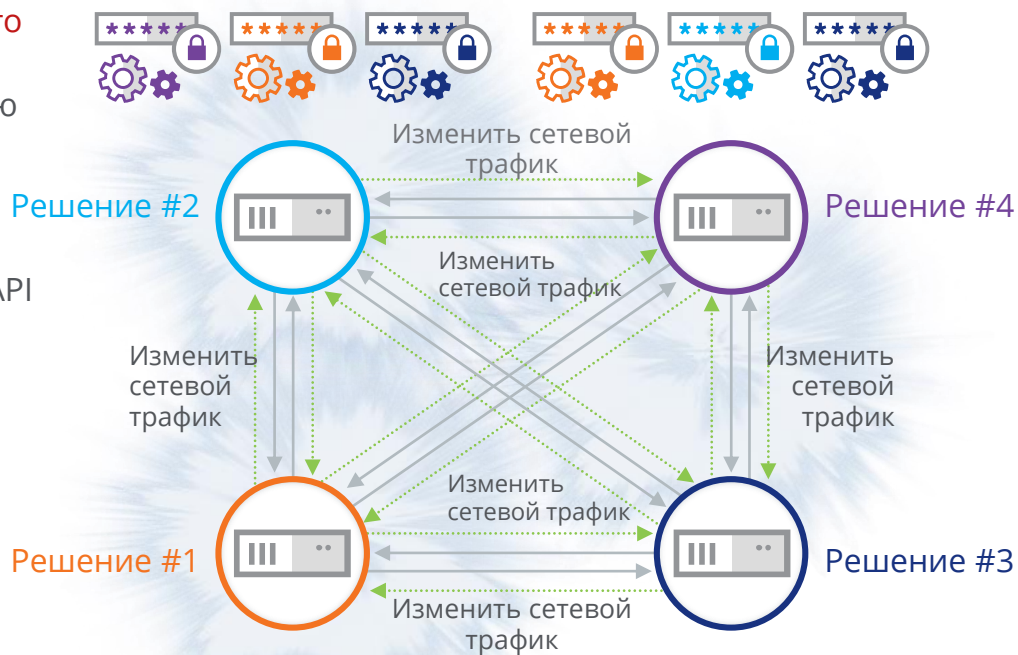
X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)



Интеграция решений до DXL

Затрачено очень много времени и усилий чтобы построить такую сложную систему из нескольких решений.

Когда в одном из продуктов изменится API (что бывает), всё сломалось начинаем сначала!



X	Обмен учётными данными
X	Интеграция на уровне API
X	Регулирование сети для портов и протоколов
X	Опрос изменение (simulate real-time events)





OpenDXL – возможности интеграционной шины

DXL – Data eXchange Layer



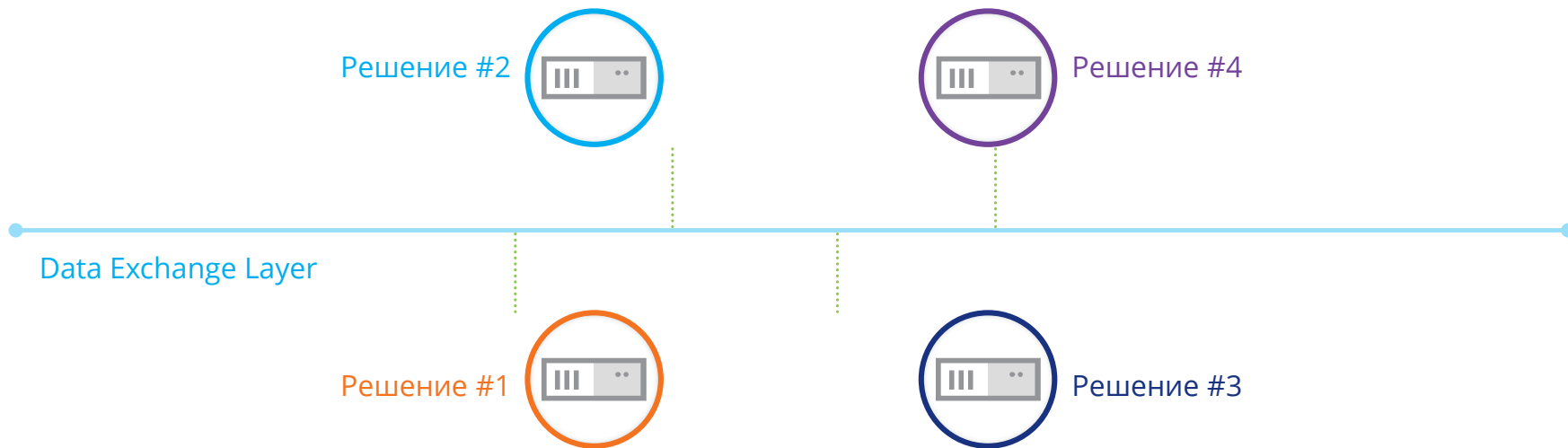
Человек живёт для
того, чтобы
научиться петь от
любви.

Бхакти Вигьяна Госвами

DXL упрощает взаимосвязь

✓ Взаимодействие в рамках единой структуры и протокола

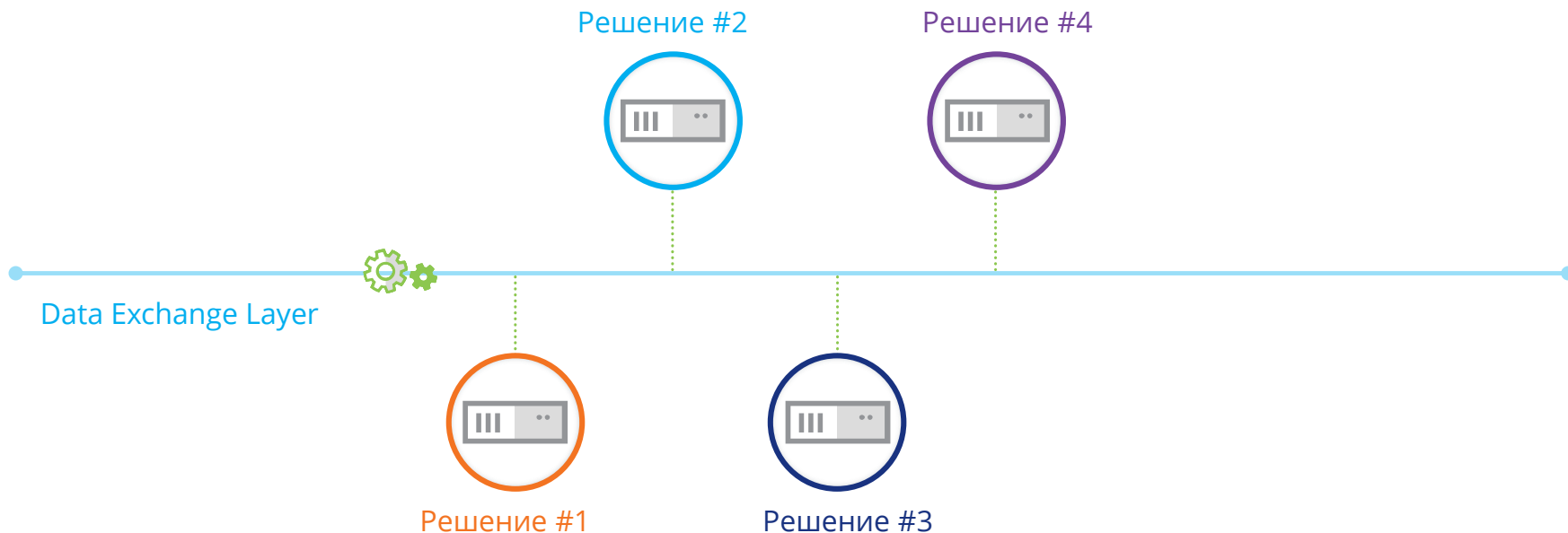
Взаимодействие в рамках единой структуры и протокола



DXL упрощает взаимосвязь

Простой в использовании, **единый для всех компонентов API (DXL API)**

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)

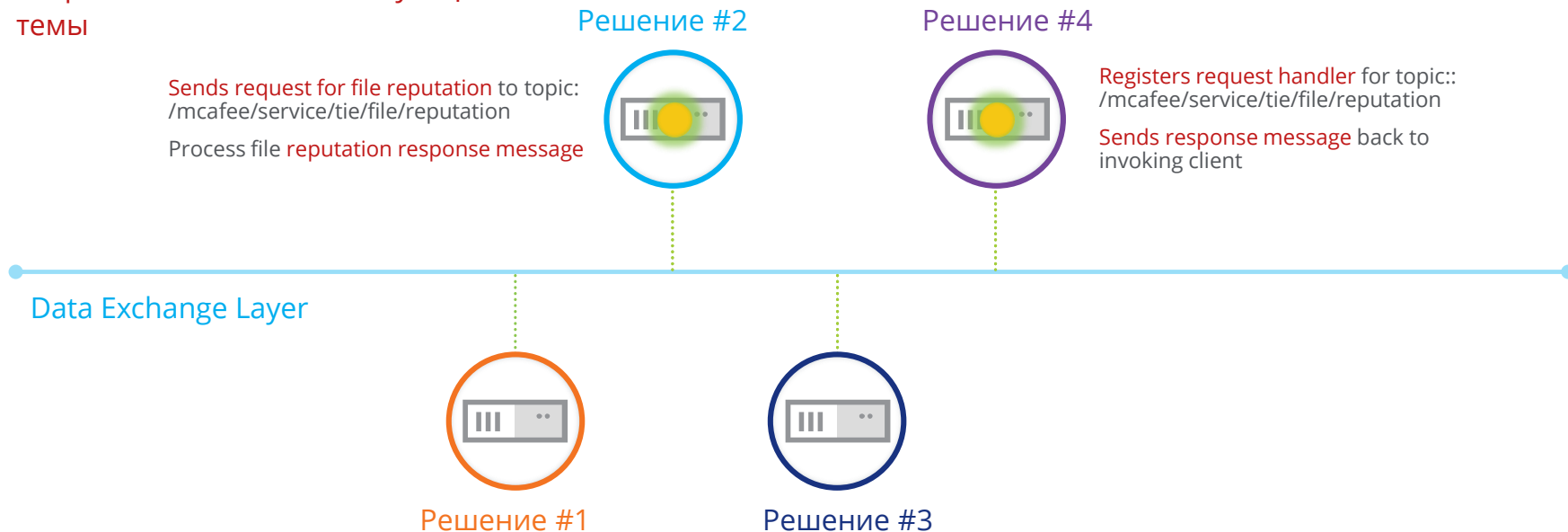


API

DXL упрощает взаимосвязь

Коммуникация построена по принципу multicast, сообщения отправляются в соответствующие темы

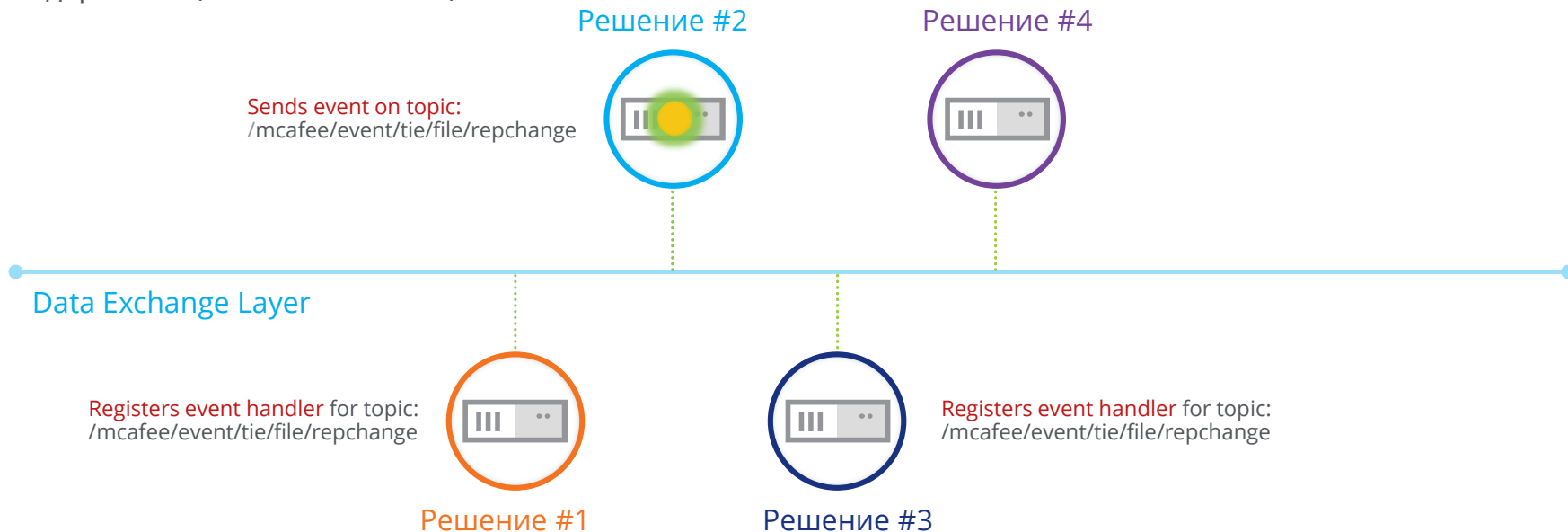
✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации



DXL упрощает взаимосвязь

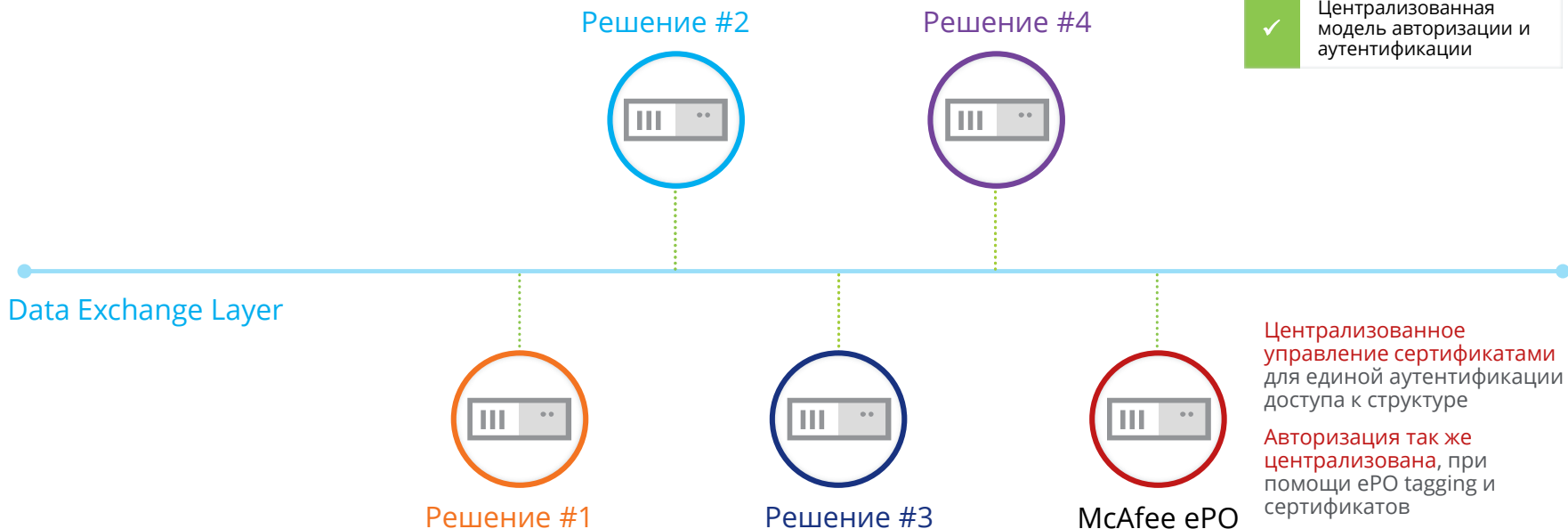
События доставляются ко всем подписчикам темы с минимальными задержками (почти мгновенно)

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)



DXL упрощает взаимосвязь

Централизованная и единая модель аутентификации и авторизации



✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации

DXL упрощает взаимосвязь

Постоянные сетевые соединения (client-to-broker).

Двунаправленная коммуникация.

Отправка события удалённой точке

Решение #2



Решение #4



Data Exchange Layer

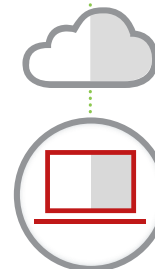
Решение #1



Решение #3



Удалённая точка



Постоянные подключения устанавливаются к структуре со стороны удалённой точки

Постоянные подключения позволяют вести **двунаправленные коммуникации** без осложнений со стороны МСЭ

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации
✓	Постоянные соединения между клиентами и структурой (Firewall friendly)

DXL упрощает взаимосвязь

Несколько режимов связи: Multicast event-based сообщения для всех подписчиков

Решение #2



Решение #4



Data Exchange Layer



Решение #1



Решение #3



✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации
✓	Постоянные соединения между клиентами и структурой (Firewall friendly)
✓	Multicast вещание (event-based)

DXL упрощает взаимосвязь

Multiple Communication modes:

Запрос – Ответ режим общения
«точка-точка» между решениями

Решение #2



Решение #4



Data Exchange Layer



Решение #1



Решение #3

✓	Взаимодействие в рамках единой структуры и протокола
✓	Единый API для всех компонентов (DXL API)
✓	Multicast (topic-based) коммуникации
✓	Почти real-time (без опросная система)
✓	Централизованная модель авторизации и аутентификации
✓	Постоянные соединения между клиентами и структурой (Firewall friendly)
✓	Multicast вещание (event-based)
✓	1-1 связь



Пример использования шины DXL и скриптов openDXL



Помоги, помоги,
я солдат своей
любви..

A'Studio

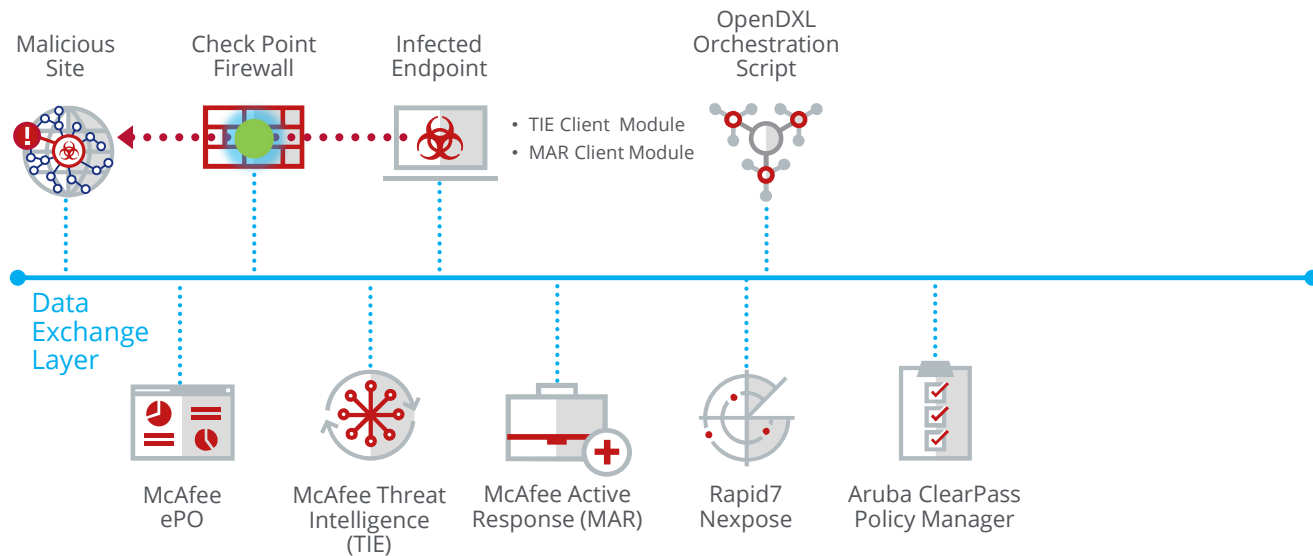
Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

✓ Прослушивание событий от Check Point

Зловред инициирован на инфицированном АРМ, как следствие передача трафика на зловерный сайт

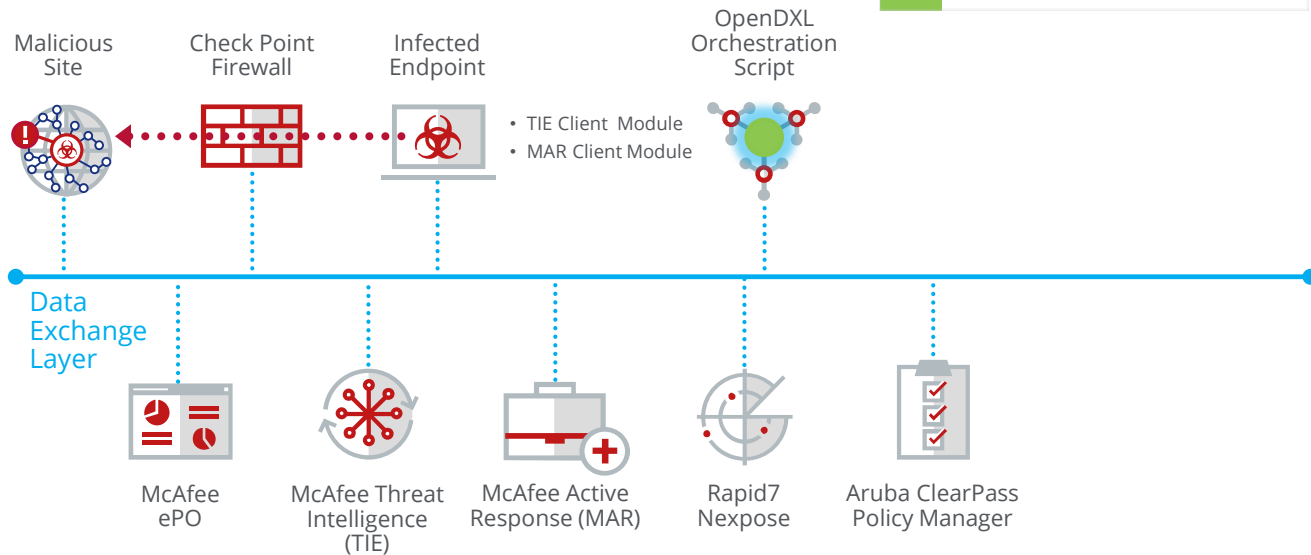
Событие получено OpenDXL хостом



Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрип выполняет запрос через DXL к McAfee Active Response (MAR) для определения систем и процессов (хэш сумм) инициирующих подобные соединения



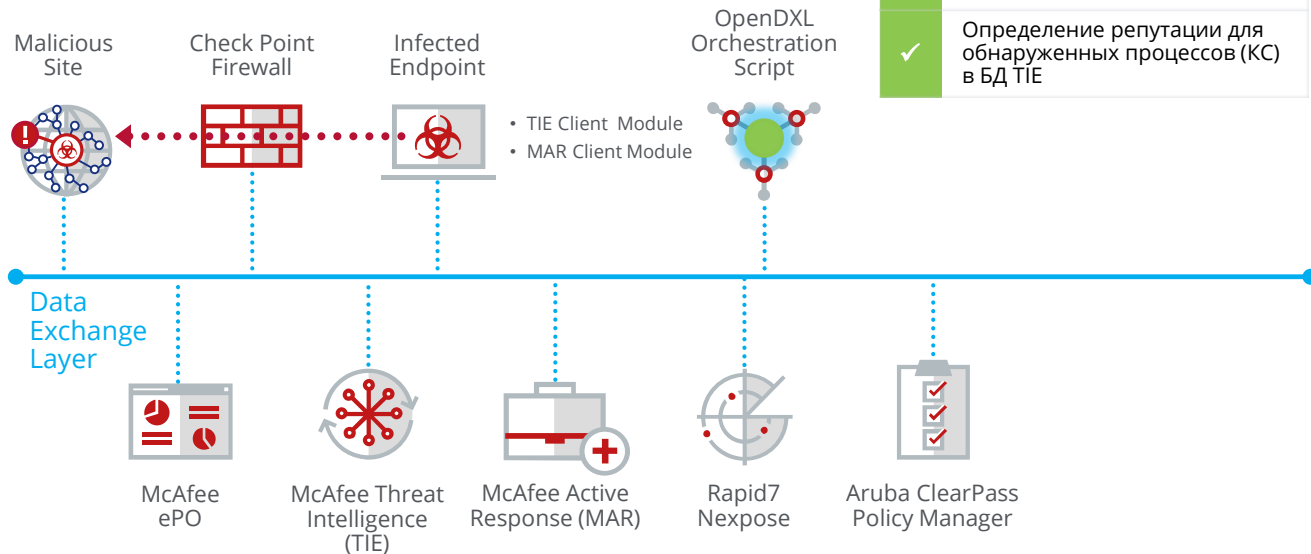
- ✓ Прослушивание событий от Check Point
- ✓ MAR для поиска процессов (по совпадению порта и адреса назначения)

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт определяет репутацию в McAfee Threat Intelligence (TIE) как Known Malicious через DXL

Применённая политика TIE приводит к инициализации процедуры уничтожения вредноноса и изоляции бинарных файлов

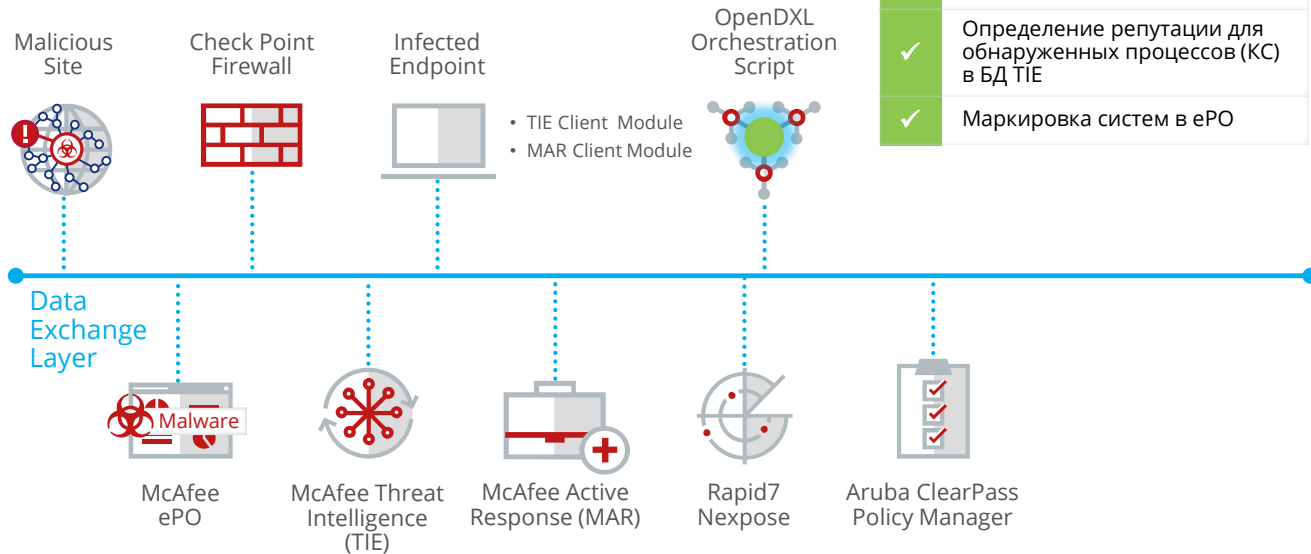


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (КС) в БД TIE

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт маркирует системы содержащие зловред в ePO через DXL

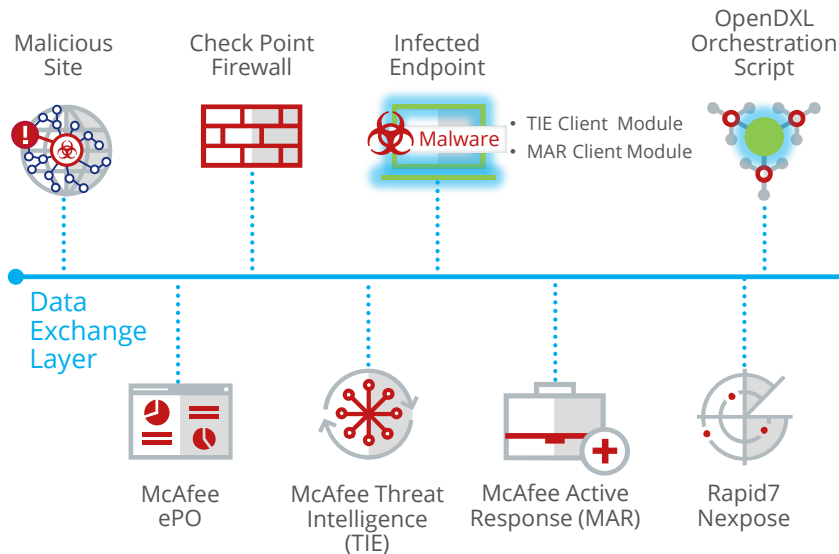


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (KC) в БД TIE
✓	Маркировка систем в ePO

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт отправляет запрос к DXL службе Rapid7 Nexpose для запуска сканирования систем содержащих зловред

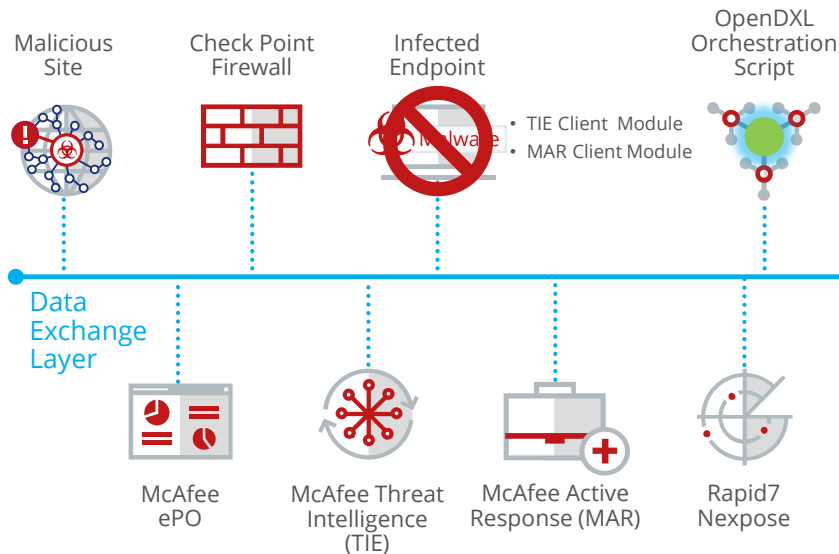


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (КС в БД TIE)
✓	Маркировка систем в ePO
✓	Запуск сканирования систем в Rapid7 Nexpose

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт отправляет запрос к службе DXL Aruba ClearPass для обновления системных атрибутов систем содержащих зловред с целью применения новых политик



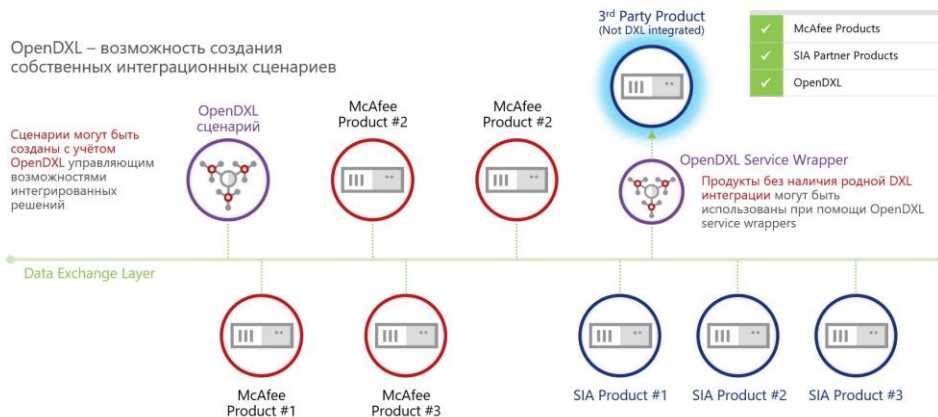
✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (КС) в БД TIE
✓	Маркировка систем в ePO
✓	Запуск сканирования систем в Rapid7 Nexpose
✓	Обновление системных атрибутов в Aruba ClearPass (применение новых политик)

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

OpenDXL Python клиент был
ИСПОЛЬЗОВАН ДЛЯ:

- Скрипт оркестрации запускаемый через зарегистрированный DXL Event listener
- Скрипт оркестрации инициировал следующие службы DXL:
 - McAfee Active Response (MAR)
 - McAfee Threat Intelligence Exchange (TIE)
 - McAfee ePolicy Orchestator (ePO)
 - Rapid7 Nexpose
 - Aruba ClearPass
- DXL service wrapper использовался для вызова Rapid7 Nexpose API
- DXL service wrapper использовался для вызова Aruba ClearPass API



GitHub.com и OpenDXL.com

The screenshot shows the OpenDXL.com homepage. At the top, there is a navigation bar with links for Solutions, Forum, Articles, Learn, and Develop. The main heading is "OpenDXL Solutions". Below this, a text block says "Browse the repository of open source and commercial solutions that have been developed for use with the Data Exchange Layer (DXL) fabric." A prominent "VIEW SOLUTIONS" button is located below the text. The page is divided into two columns: "Solution Releases" and "Forum Discussions".

Solution Releases

- Oct 17th 2019: OpenDXL Java Client (Official) 0.2.4
- Sep 27th 2019: MISP DXL Python Service 0.1.5

Forum Discussions

- Oct 24th 2019: I have some TIE ERROR lines in Orion.log after TIE.set_reputation
- Oct 17th 2019: OpenDXL Java Client (Official)

This site uses cookies. By continuing to browse this site, you are agreeing to our use of cookies.

The screenshot shows the OpenDXL GitHub repository page. The repository name is "OpenDXL" and it is located in Santa Clara, CA. The repository has 40 repositories, 0 packages, 0 people, and 0 projects. The pinned repositories are:

- opendxl-client-python**: OpenDXL Python Client. Python, 89 stars, 32 forks.
- opendxl-client-java**: OpenDXL Java Client. Java, 1 star, 5 forks.
- opendxl-bootstrap-python**: Application which generates the structure and related files necessary for developing a Data Exchange Layer (DXL) integration with Python. Python, 12 stars, 7 forks.
- opendxl-console**: OpenDXL Console is a high-level web-based console for interacting with a DXL fabric. JavaScript, 4 stars, 5 forks.



McAfee Threat Intelligence Exchange (TIE)

Локальное управление репутациями, IOC



McAfee Threat Intelligence Exchange

Systems

TIE Reputations

File Search | Certificate Search | File Overrides | Certificate Overrides

TIE File Reputations : File Search Hide Filter

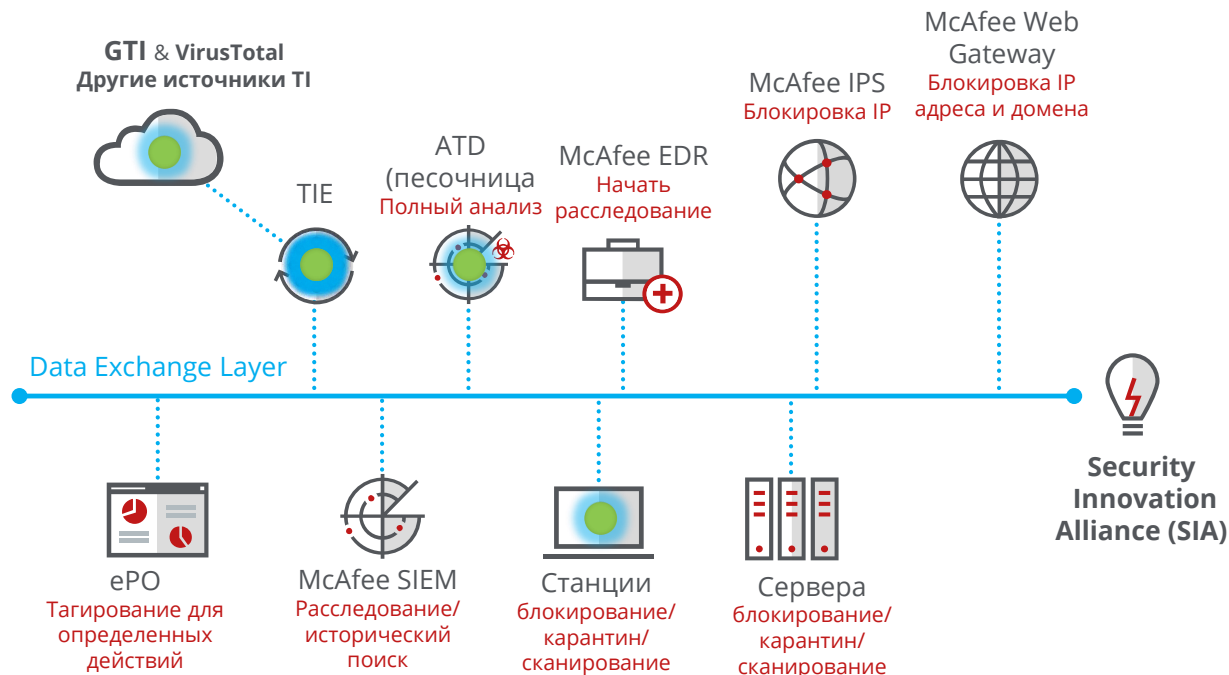
Preset: Last 30 days | Custom: None | Quick find:
Apply Clear
 Show selected rows

	All File Names	Composite Reputation	Enterprise Reputation	Latest Local Reputation	Certificate GTI Reputation	GTI Reputation	ATD Reputation
<input type="checkbox"/>	SDCLT.EXE	● Known Trusted (Latest Local)	Not Available	Known Trusted	Known Trusted	Not Available	Not Available
<input type="checkbox"/>	NLSDATA0009.DLL	● Known Trusted (Latest Local)	Not Available	Known Trusted	Known Trusted	Not Available	Not Available
<input type="checkbox"/>	LIBEGL.DLL	● Most Likely Trusted (Latest Local)	Not Available	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available
<input type="checkbox"/>	LIBGLESV2.DLL	● Most Likely Trusted (Latest Local)	Not Available	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available
<input type="checkbox"/>	CHROME_WATCHER.DLL	● Most Likely Trusted (Latest Local)	Not Available	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available
<input type="checkbox"/>	CHROME.DLL	● Most Likely Trusted (Latest Local)	Not Available	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available
<input type="checkbox"/>	CHROME_ELF.DLL	● Most Likely Trusted (Latest Local)	Not Available	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available
<input type="checkbox"/>	DEMO02.EXE	● Most Likely Malicious (Latest Local)	Not Set	Most Likely Malicious	Not Available	Not Set	Most Likely Malicious
<input type="checkbox"/>	UBPM.DLL	● Known Trusted (Latest Local)	Not Available	Known Trusted	Known Trusted	Not Available	Not Available
<input type="checkbox"/>	WS2_32.DLL	● Known Trusted (Latest Local)	Not Available	Known Trusted	Known Trusted	Not Available	Not Available
<input type="checkbox"/>	CRYPTO.EXE	● Most Likely Malicious (Latest Local)	Not Set	Most Likely Malicious	Not Available	Not Set	Most Likely Malicious
<input type="checkbox"/>	MSPATCHA.DLL	● Known Trusted (Latest Local)	Not Available	Known Trusted	Known Trusted	Not Available	Not Available
<input type="checkbox"/>	ELSCORE.DLL	● Known Trusted (Latest Local)	Not Available	Known Trusted	Known Trusted	Not Available	Not Available

Actions 13 items

McAfee Adaptive Security Architecture

Постоянный обмен репутациями (IOC) по всей экосистеме



JUNIPER
NETWORKS

RAPID7

Check Point
SOFTWARE TECHNOLOGIES LTD.

CISCO

Extreme®
Connect Beyond the Network

Примеры интеграции с openDXL



https://www.cisco.com/c/dam/m/en_us/products/security/technical-alliance-partners/core/assets/pxgrid-mcafee-opendxl-integration-aag.pdf



Адаптивная безопасность для корпораций и государства

Современный подход

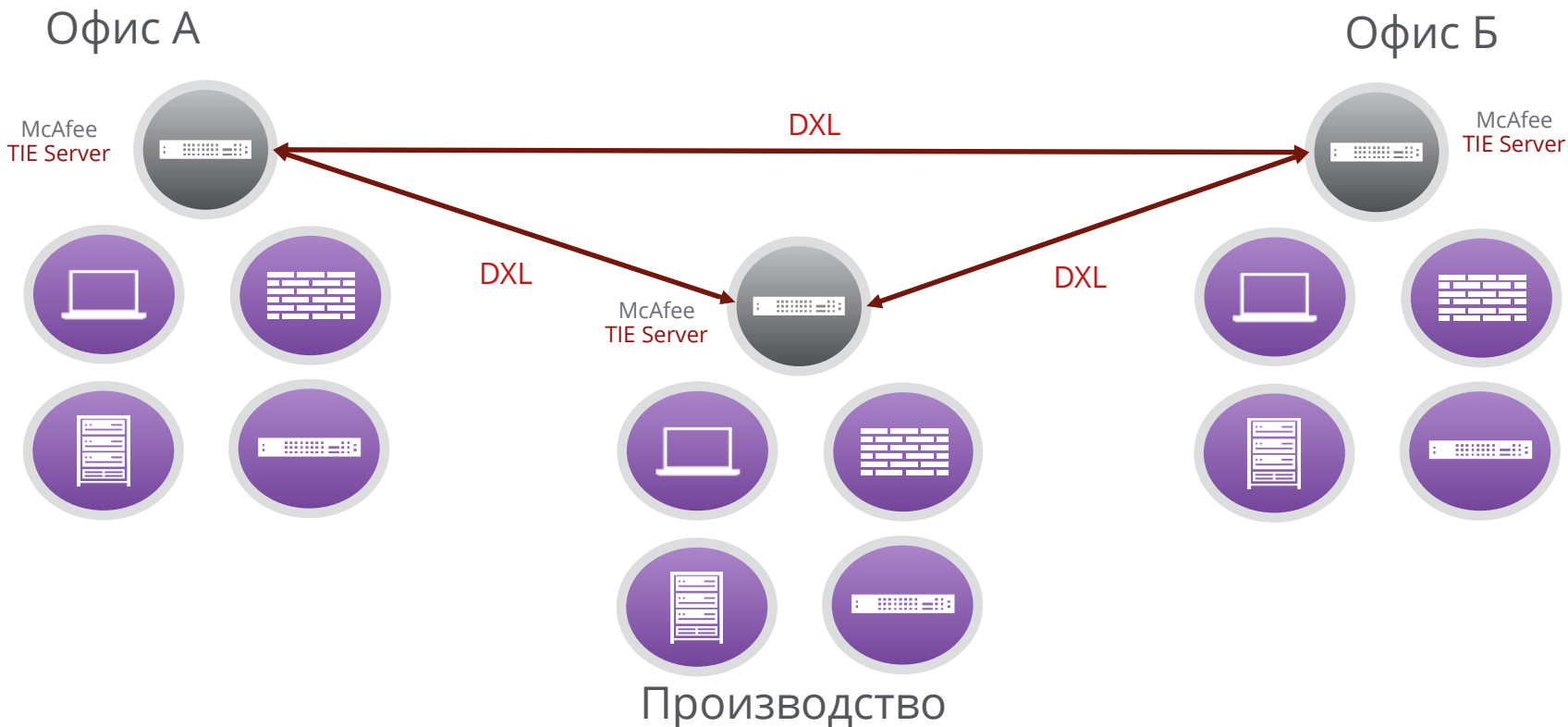


Любить — значит
истину защищать,
Даже восстав против
всей вселенной...

Эдуард Асадов

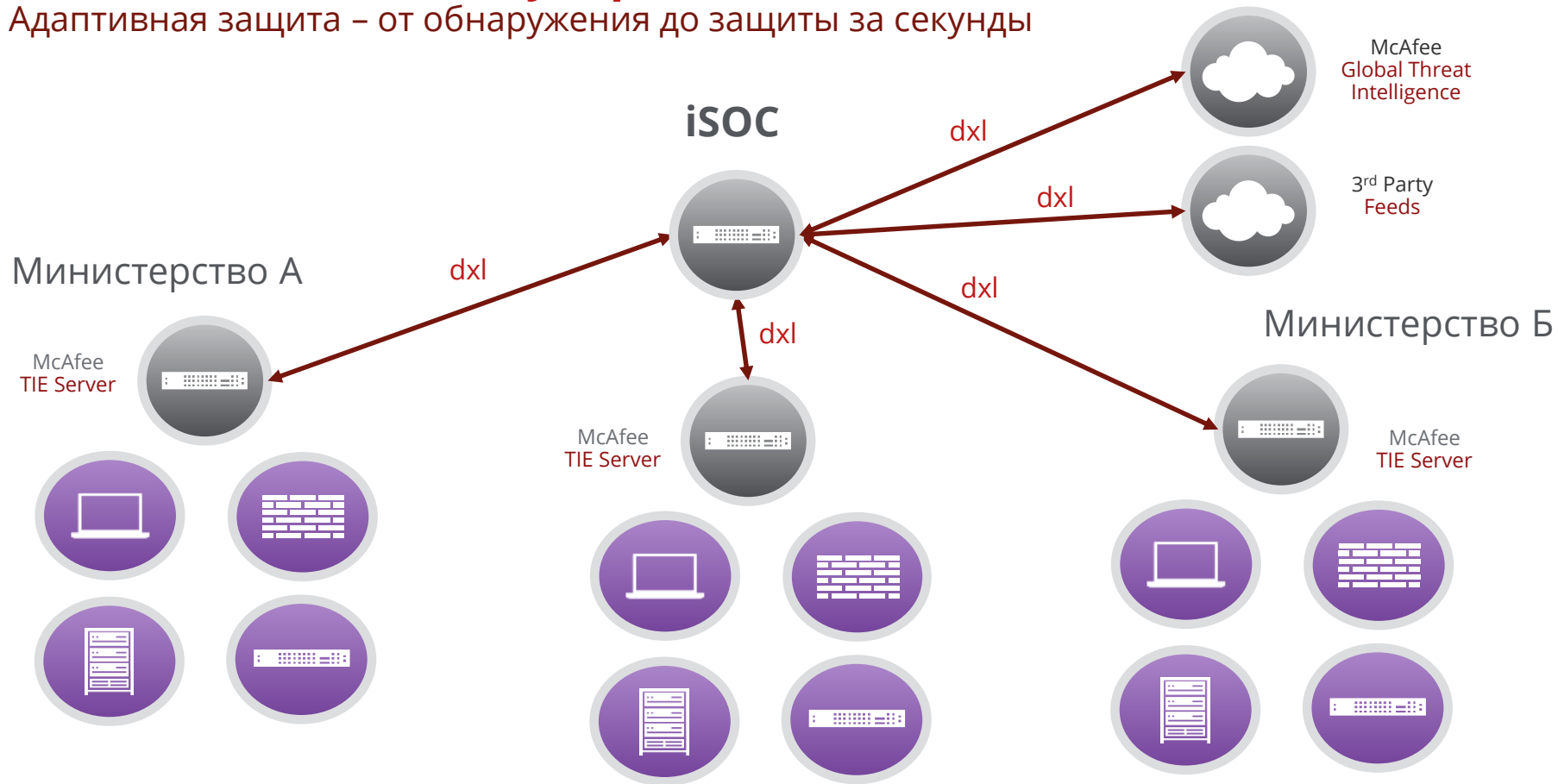
Защита корпорации

Адаптивная защита – от обнаружения до защиты за миллисекунды



Защита для всего государства

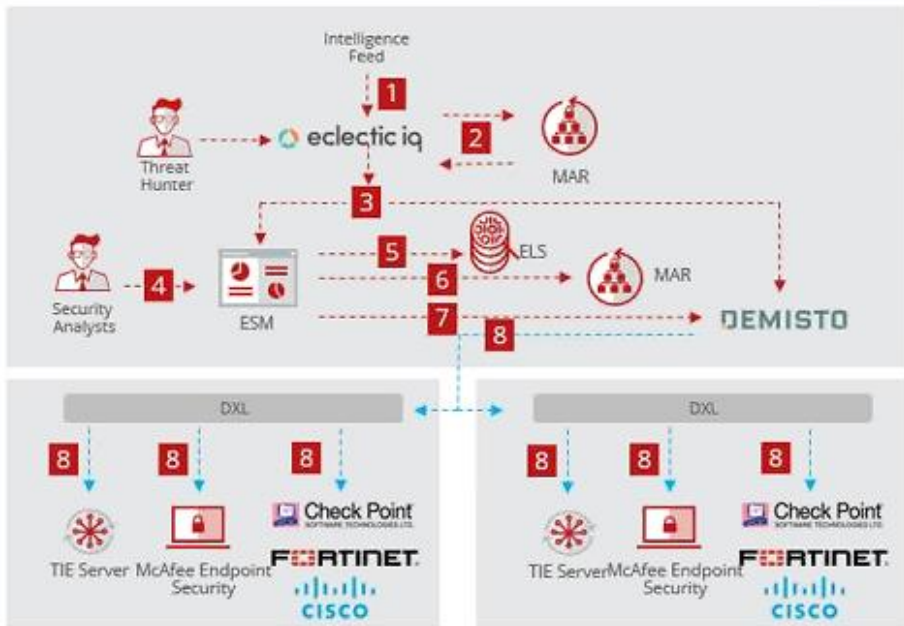
Адаптивная защита – от обнаружения до защиты за секунды



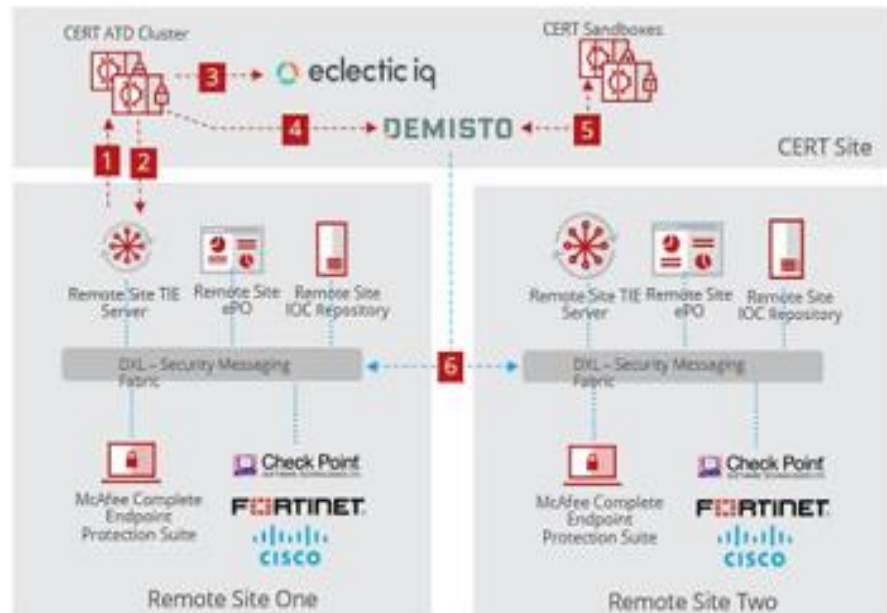
ПРИМЕРЫ АДАПТИВНОЙ АРХИТЕКТУРЫ С DXL

Адаптивная защита – от обнаружения до защиты за секунды

Организация защиты холдинга



Национальный CERT



Содержание:

- **Адаптивная архитектура безопасности (Gartner)**
- **Как интегрировать решения разных производителей**
- **Анонс решений McAfee для ОЦИБ**





McAfee Enterprise Security Manager (ESM)

Высокопроизводительная SIEM платформа
для построения интеллектуального SOC



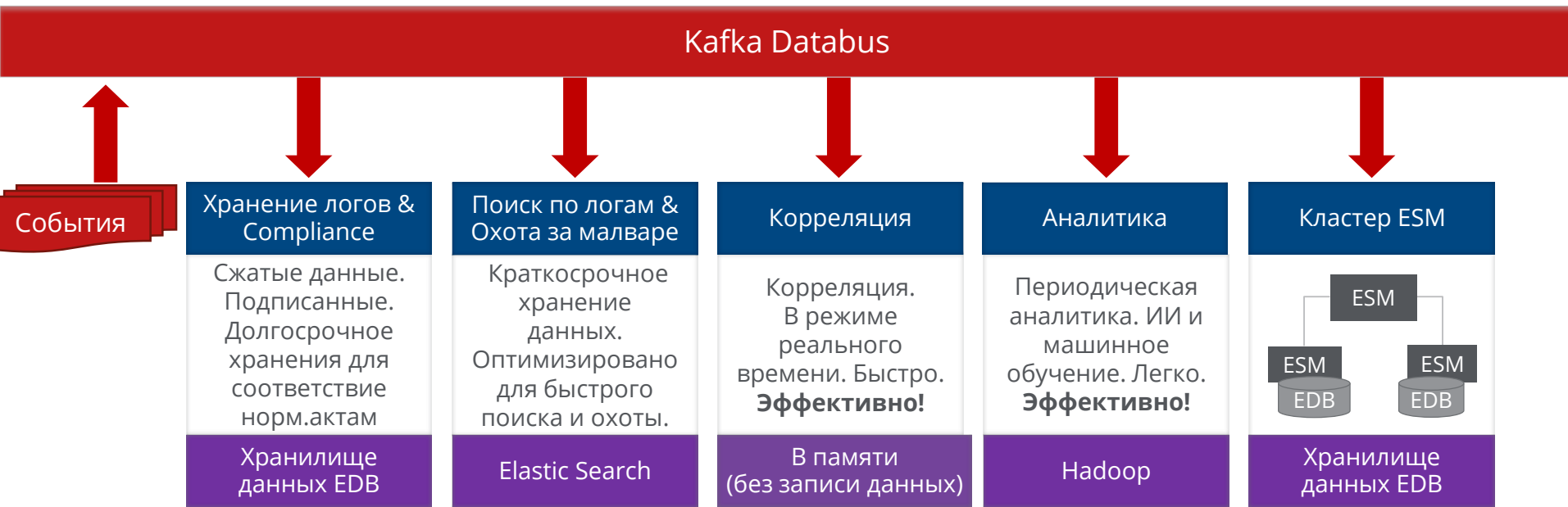
8 лет в квадранте Лидеров Гартнер



- McAfee has implemented a modern SIEM architecture that leverages **big data** technologies, such as **Kafka and Elasticsearch**. The open nature of the data tier allows organizations looking to feed data into or out of ESM to have flexible options.
- User behavior capabilities are available through several options. In addition to basic user monitoring via a content pack for ESM, McAfee offers MBA as a UEBA/analytics offering, plus support for numerous third-party UEBA integrations.
- Application support is strong across databases, ERP solutions, OT and IoT, either leveraging native capabilities or enhanced through the use of its ADM and DAM solutions.
- MI (an add-on subscription product in the Security Operations product portfolio) provides guided incident investigation support for analysts, including context/evidence collection and recommended actions.

McAfee SIEM - Платформа для обработки Big Data -

ESM 11 = Никаких компромиссов. Высокая производительность.
Низкая стоимость владения





MVISION EDR

Мощный инструмент для расследования
инцидентов ИБ



Я искал в этом городе
женщину, ту
единственную, свою...

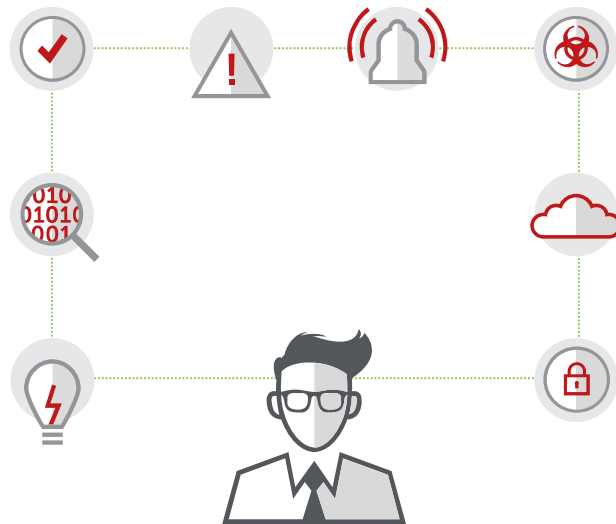
Григорий Лепс

Рабочие станции и сервера генерируют большое количество данных

Сегодня, инструменты EDR требуют **высококвалифицированных аналитиков**

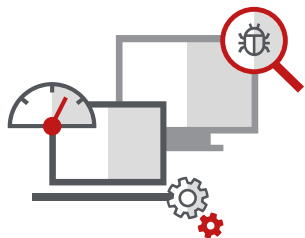
Почему?

- Множество данных - трудно «иголку в стогу сена»
- Множество оповещений и алертов
- Высокая квалификация специалистов – **обычно они в дефиците** – для расследования и интерпретирования алертов



Что такое MVISION EDR?

McAfee Active Response



Мониторинг рабочих станций и серверов, сбор данных

Детектирование подозрительного поведения

Быстрый поиск

Быстрый ответ



Улучшения



Простая облачная архитектура

Расширенный сбор данных и их обновление

MITRE ATT&CK™ методология расследования



McAfee Investigator



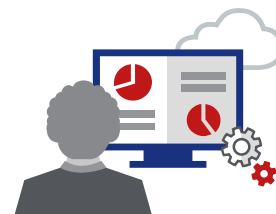
Динамический гид по расследованиям

Автоматизированный анализ

Сбор данных по всей организации

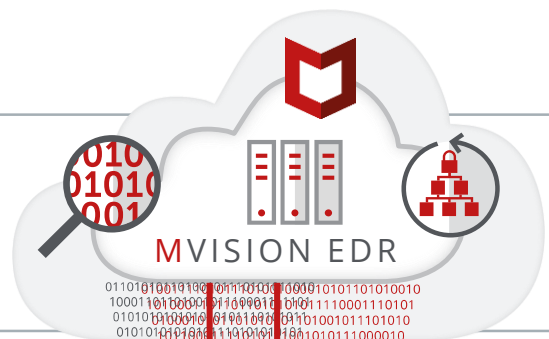


MVISION EDR



Мощное средство для детектирования, расследований и ответной реакции – в простом виде

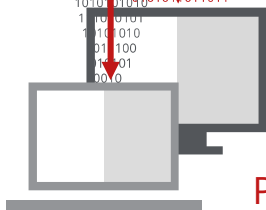
Обнаружение и устранение угроз – быстрее и проще



- Поведенческий анализ
- Файловые и безфайловые атаки
- Работает с любыми вендорами
- Быстрое внедрение новых аналитических алгоритмов

Постоянный мониторинг

Реакция

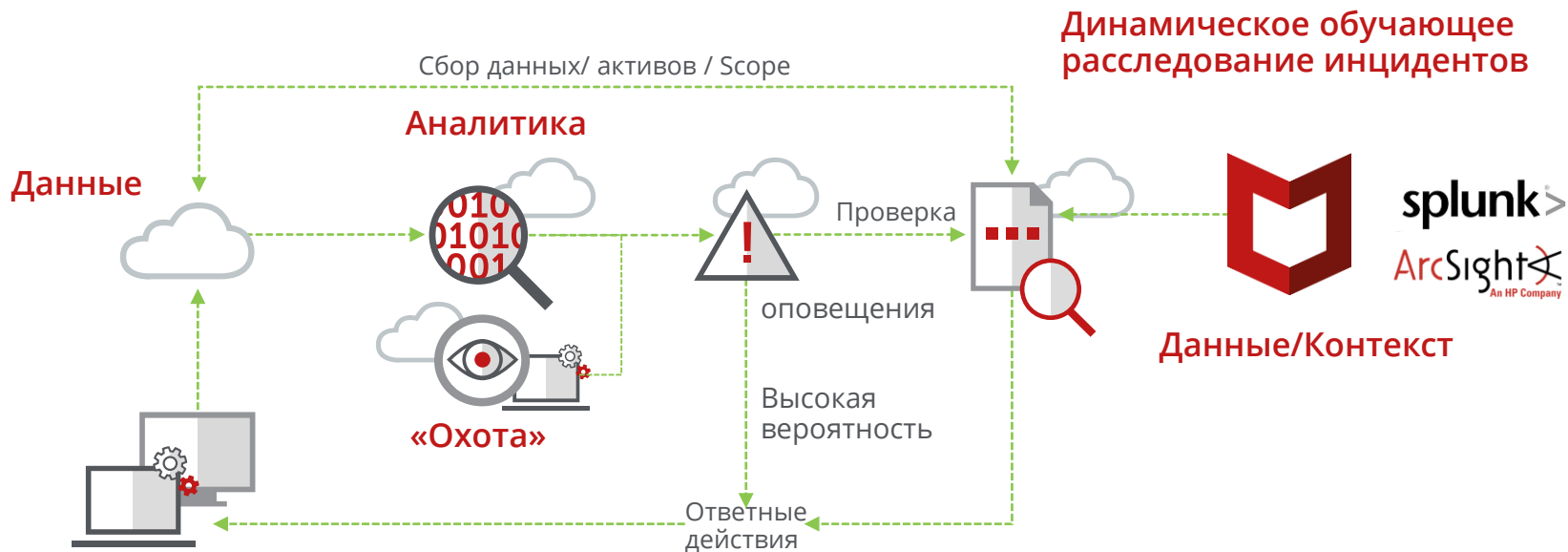


Рабочие станции и сервера

- **Детектирование основанное на стандарте MITRE ATT&CK™**
- Скоростной и постоянный процесс позволяющий определять фазу атаки, связанные с атакой риски и приоритет противодействий
- **Расстановка приоритетов оповещений** позволяет аналитикам понять степень риска и опасности
- **Визуализация данных позволяет** аналитикам быстро понять почему система выделила данное событие. Дальнейшее действие : игнорировать, ответное действие, *расследование.*

Новый подход McAfee к задачам EDR

Скоростное разрешение с высокой долей вероятности



Панель расследования MVISION EDR

McAfee Investigator

Investigation Workspace

10 Key Findings

Out of 1,413 Artifacts Discovered

Search

Current Investigation

HHGTTG42 joshua.newman

Incident declared

Unspecified

Last updated: 18 May 09:40 pm Show more

Investigation Guides

Show

- Does VT/GTI flag it as known with malicious reputation?
Malicious IP address(es) reputation report(s) from netstat entries
Malicious IP address(es) reputation report(s) from DNS lookups
Malicious FQDN(s) reputation report(s) from DNS lookups
- Does the endpoint contain processes running from suspicious directories?
Process(es) running from suspicious directories
- Does the endpoint contain running processes uncommon for the company?
2 uncommon process(es)
- Is there evidence of hacking or admin tools used on the device?
Admin or hacking tool(s) running on device
- Does the endpoint contain evidence of malware persistence?
File(s) referenced in auto-start entries with suspicious indicators
Process(es) loading uncommon files
- Is the process opening the socket expected to do so?
Socket(s) being opened by process(es)

Панель расследования MVISION EDR

The screenshot displays the McAfee Investigator interface. At the top left, the McAfee logo and the word "Investigator" are visible. The main workspace is titled "Investigation Workspace" and shows "10 Key Findings" and "Out of 1,413 Artifacts Discovered". A search bar and a "Current Investigation" dropdown are also present.

On the left side, there is a sidebar with "Investigation Guides" and "Analyst guide". The "Analyst guide" section is expanded, showing a "Malware alert triage" with several questions and answers. The questions include:

- There is a security threat, we can confirm malicious activity.
- Does the endpoint contain evidence of suspicious outbound network connections?
- Did the endpoint connect to IPs or domains with malicious reputation?
- Does VT/GTI flag it as known with malicious reputation?
- Does the endpoint contain evidence of malicious files activation?
- Does the endpoint contain processes running from suspicious directories?
- Does the endpoint contain running processes uncommon for the company?

The main area of the interface shows a complex network diagram of processes and artifacts. A central node is highlighted with a blue gear icon, and a "Process Details" panel is open on the right side. The panel shows the following information:

- name:** `alfoxbqlq.exe`
- processId:** 6700
- commandLine:** `"C:\Users\joshua.newman\AppData\Local\Temp\pArad6DA78.tmp\alfoxbqlq.exe"`
- publisher:**
- description:**
- product:**
- version:**
- fileVersion:**
- createTime:**
- rawData:**

Below the process details, there are sections for "Suspicious Indicator", "Prevalence", and "Evidence Notes".

Change the Game with MVISION EDR

Быстрое обнаружение и реакция

- Обнаружение в «облаке»
- ATT&CK™ стандарт для отчетности
- Помощь в расследовании под руководством искусственного интеллекта

Сделать больше с существующим и кадрами

- Динамические расследования под руководством системы

Скоросная Ответная реакция

- Обезвреживание в один клик
- Интеграция в экосистему



McAfee Advance Threat Defense

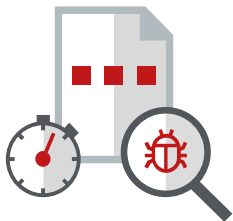
Обнаружение сложных
целенаправленных атак



McAfee Advanced Threat Defense Advanced Analysis

Песочница + Глубокий анализ вредоносных программ

Стандартные средства



Использование **сигнатур, репутаций, эмуляций**— для быстрого выявления известных атак и вредоносных файлов.

Анализ большего числа файлов.

Быстрые результаты



Динамический анализ



Запуск файла в “защищенной” и контролируемой среде.

Наблюдение за исполнением программы файла и поиск вредоносного **поведения**.



Статический Анализ кода (Искусственный интеллект)



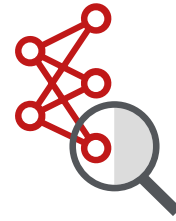
Убрать «шелуху» и **найти** выполняемый код.

Анализ **ВСЕХ** атрибутов и инструкций для выявления действий вредоносного кода.

Нахождение к какому **семейству вредоносного кода** относиться файл



Нейронные сети (Машинное обучение)



Обнаружение шаблонов кода скрытых угроз.

Анализ **типичного поведения** вредоносных программ.

Детализированные отчеты и выдача их в стандартизированном виде

Threat Analysis Report

McAfee Threat Analysis Report		
File Name	PROTOTYPE.exe	Threat Level ● 5 - Very High
Malware Name	Malware Dynamic	Engine ● Sandbox
File Submitted	2017-11-06 11:06:23	Processing Time 17 seconds
File Size	45,056 bytes	Sandbox Replication 9 seconds
Show More	Hash Values	File Details Environment
MDS Hash Identifier	E2CFE1C9703352C42763B48489FC356	
SHA-1 Hash Identifier	FD384A9CF228F4C371E938C469A3A39D64B7	
SHA-256 Hash Identifier	258E20D6193BC55856A23A82D9F664911AD51D5824BAE95EBCFD6E573D6975	
	Hide hash values	
File Type	PE32 executable (console) Intel x86	
Digital Signature Verified	Unsigned	
Customer	Not Available	
Description	Not Available	
Product Name	Not Available	
Version Info	Not Available	
File version	Not Available	
Strong Name	Not Available	
Original Name	Not Available	
Internal Name	Not Available	
Copyright	Not Available	
Comments	Not Available	
	Hide file details	
Microsoft Windows XP Professional Service Pack 3 (build 3000, version 5.1.2600)		
Internet Explorer version: 6.0.2900.5512		
Microsoft Office version: 2003		

Assembly Code, Graph Analysis, and Indicators of Compromise

```

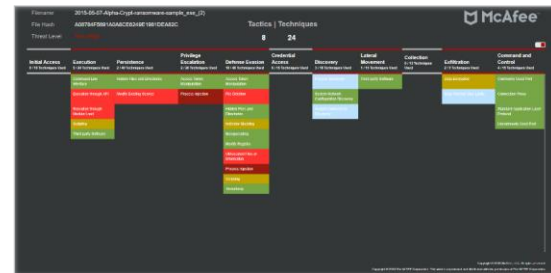
0x69 100401002 3224      mov     esi, esi
0x70 100401003 397424 00    cmp     dword ptr esi:[esp+0], esi
0x71          push    esi
0x72 100401008 74 07        je     short 00401011
0x73 100401006 6B 10w04000  push    dword ptr esi:[esp+10]
0x74 100401005 EB 05        jmp     00401016
0x75          ----->
0x76 100401011 6B 10w04000  push    dword ptr esi:[esp+10], esi
0x77          ----->
0x78 100401016 6B 10w04000  push    dword ptr esi:[esp+10]
0x79 100401018 FF15 10814000  call   dword ptr ds:[408110]
0x80          //call MOVCRP: fopen
0x81 100401021 80F8      mov     esi, eax
0x82 100401023 59        pop     ecx
0x83 100401024 3B56      cmp     edi, esi
0x84 100401026 59        pop     ecx
0x85 100401027 75 04        jnz     short 0040102d
0x86 100401028 3300      xor     eax, eax
0x87 100401026 EB 34        jmp     004010E1
0x88          ----->
0x89 10040102d 397424 10    cmp     dword ptr esi:[esp+10], esi
0x90 100401031 57        push    edi
0x91 100401032 6B 01      push    byte ptr esi:[esp+8]
0x92 100401034 6B 00w030000  push    byte ptr esi:[esp+8]
0x93 100401039 FF7424 18    call   dword ptr esi:[esp+18]
0x94 100401036 74 08      je     short 00401047
0x95 100401038 FF15 1A814000  call   dword ptr ds:[408110]
0x96          ----->
0x97 100401010  [Dropped Malware File]
0x98 100401010  [Dropped Malware File]
0x99 100401010  [Dropped Malware File]
0x01          ----->
    
```

"Dropped Malware Files": [

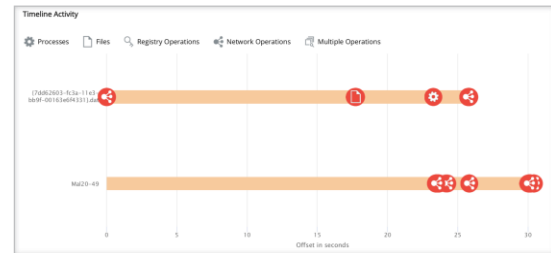
```

{
  "Name": "@WanaDecryptor.exe",
  "factor": "100.00"
}
    
```

MITRE ATT&CK™ mapping

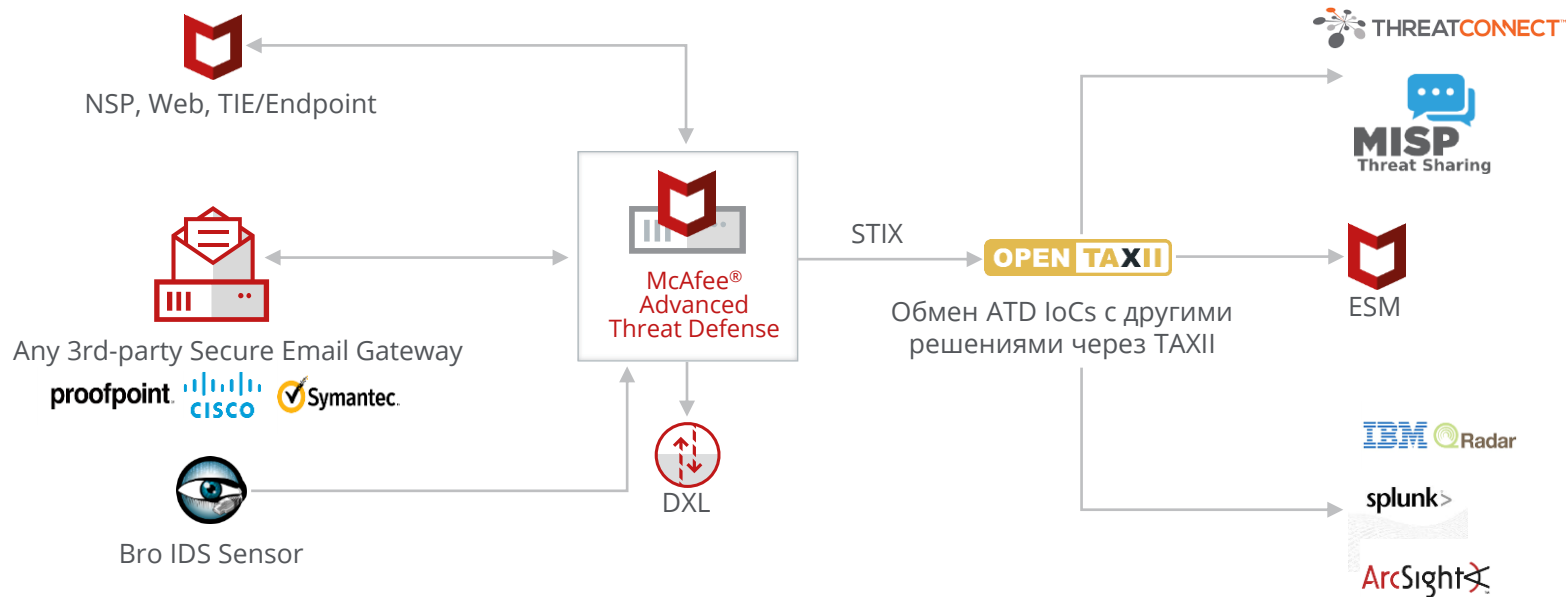


Threat Timeline



Открытая платформа, интеграция с другими решениями ИБ

Автоматизация действий по защите и детектированию и интеграция через открытую платформу



All you need is
All you need is
All you need is
LOVE is all you need!



John Lennon



Бренд McAfee

Мы верим в то, что ни один человек, продукт или организация не может защитить цифровой мир в одиночку.

Поэтому мы переделали McAfee беря во внимание совместную работу: Люди работают вместе. Решения работают вместе. Организации работают вместе.

Наша цель – вдохновить на совместную работу наших клиентов, партнеров, и даже конкурентов – сделав этот мир более защищенным.

McAfee. Together is power.
Вместе - сила.

McAfee. The device-to-cloud cybersecurity company.





Мы работаем для Вашего успеха и всегда готовы помочь и предоставить консультации по вопросам информационной безопасности! Будем рады Вашим запросам!

Наши контакты:

Руслан Барбашин, McAfee
Территориальный менеджер
+7 727 350 5498
Ruslans_Barbasins@mcafee.com

Присоединяйтесь в соц.сетях:
www.facebook.com/ruslans.barbasins
www.linkedin.com/in/ruslansbarbasins/

Кирилл Креккер, Монт
McAfee Product Manager

Mobile: +7(702) 216-05-90;
Office: +7(727) 355-60-05, int. 161
kkrekker@mont.com



McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC.