McAfee
Together is power.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КАК создать интеграционную платформу и не сойти с ума?

Антон Тихонов, компания Монт

CYBERscape v2.5

Network & Infrastructure Security

Advanced Threat Protection

NAC

SDN

DDoS Protection

DNS Security

Network Firewall

Deception

ICS + OT

Network Analysis

Web Security

Endpoint Security

Endpoint Prevention

Detection & Response

Application Security

WAF & Application Security

Application Security Testing

MSSP

Traditional MSSP

Advanced MSS & MDR

Encryption

Mobile Security

Risk & Compliance

Risk Assessment & Visibility

Security Ratings

Pen Testing & Breach Simulation

GRC

Security Awareness & Training

IoT

IoT Devices

Automotive

Connected Home

Messaging Security

Identity & Access Management

Authentication

IDaaS

Privileged Management

Identity Governance

Consumer Identity

Security Consulting

Blockchain

Fraud & Transaction Security

Cloud Security

Container

Infrastructure

CASB

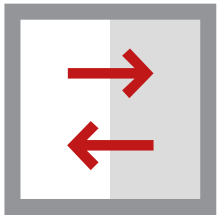
Security Analytics

Что делать?

Куда бежать?

- Много технологий, много производителей, низкая связность, сложность оперативного реагирования
- Сложные при внедрении и поддержании интеграции вида точка-точка
- Возможность интеграции решения полностью зависит от желания и способности третьей стороны
- Традиционные модели обмена данными (запрос-ответ, публикации по планировщику) увеличивают инерционность системы
- Приложения не могут получить доступ к требуемой информации для максимально быстрого и эффективного реагирования.

DXL...

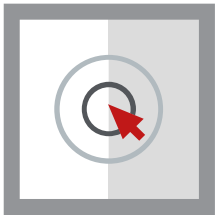


Открытый

DXL полнодуплексная коммуникационная платформа объединяющая решения ИБ в единую экосистему.

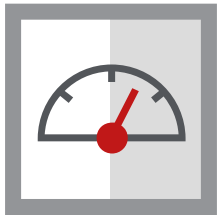
Абстрактный

DXL стандартизованный коммуникационный уровень абстракции для любых приложений вне зависимости от их собственной



Простой

DXL предельно упрощает интеграционные сценарии, являясь при этом открытой платформой для включения новых приложений.



Быстрый

Благодаря высокой производительности, гибкости и масштабируемости укрепляется основа для обнаружения и реагирования на инциденты ИБ.

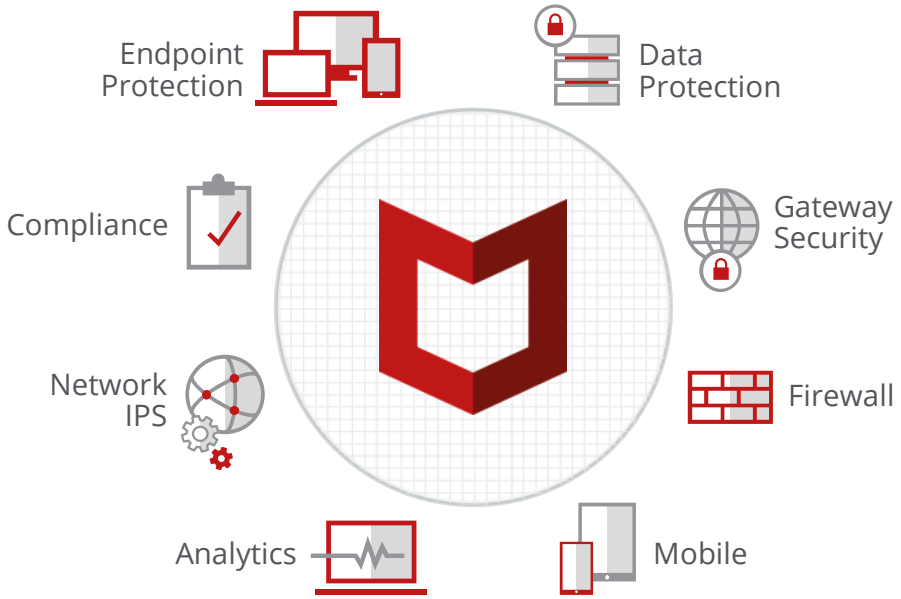
Security Information Application Framework

Эволюция DXL: McAfee

Решения McAfee

Первоначально DXL использовался исключительно для решений McAfee (“Security Connected”).

- McAfee Endpoint Security (ENS)
- McAfee ePolicy Orchestrator (ePO)
- McAfee Threat Intelligence Exchange (TIE)
- McAfee Active Response (MAR)
- McAfee Enterprise Security Manager (ESM)
- McAfee Advanced Threat Defense (ATD)
- McAfee Web Gateway (MWG)
- McAfee Application Control (MAC)
- McAfee Network Security Platform (NSP)
- McAfee SiteAdvisor (SAE)
- McAfee Data Loss Prevention (DLP)
- Intel Internet of Things (IoT)



Эволюция DXL: SIA Partners

SIA Partners

Connected Today

Advanced Cyber Security
aruba a Hewlett Packard Enterprise company POC
Avecto
BIGFIX An IBM Company
BeyondTrust VISIBILITY. KNOWLEDGE. ACTION.
boldonjames A ClearIQ Company
Check Point SOFTWARE TECHNOLOGIES LTD.
CICADA Security Technology
cisco
DFLABS CYBER INCIDENTS UNDER CONTROL
DIGITAL DEFENSE INCORPORATED
Extreme Connect Beyond the Network
FORCEPOINT
GURUCUL
HUAWEI
IBM Security
Infoblox CONTROL YOUR NETWORK
intel
INTERSET
Lumeta
MINERVA
MobileIron
Phantom
proofpoint
RAPID7
sas
SWIMLANE
tenable network security
THREATQ
TYCHON
TITUS
TRAPX SECURITY

In Testing or Development Today

ANOMALI
Attivo NETWORKS
ayehu
AUTONOMIC SOFTWARE
DEMISTO
ForeScout
NIKSUN
paloalto NETWORKS
servicenow
SIEMPLIFY
SYNCURITY
THREATCONNECT

In Design

BUFFERZONE
cloudera
CYBERARK
CYPHORT
eclectic iq
FORTINET
JUNIPER NETWORKS
Indegy Industrial Cyber Security
SECURONIX
THALES
twosix LABS
vmware airwatch

Current as of September 18, 2018

Примеры возможностей интеграции DXL

SIA Partners

Check Point SOFTWARE TECHNOLOGIES LTD.	▪ **SandBlast** integration with DXL, TIE and ePO ▪ Publishing Topics: File Reputation, IOC, Threat Event Data, Mobile ▪ Subscribing Topics: IOC, File Reputation Updates
cisco	▪ **pxGrid/Cisco ISE integration with DXL and ePO** ▪ Publishing Topics: New Asset Discovery Information, Policy Change, Events ▪ Subscribing Topics: Threat Event, ePO queries
RAPID7	▪ **Nexpose** integration with DXL, TIE and ePO ▪ Publishing Topics: IOC, Vulnerability, New Asset Discovery Information ▪ Subscribing Topics: IOC, File Reputation, Threat Event, Vulnerabilities
TRAPX SECURITY	▪ **Deception Grid** integration with DXL, TIE and ePO ▪ Publishing Topics: File Reputation, IOC, Threat Event Data ▪ Subscribing Topics: IOC, File Reputation, Threat Event

Эволюция DXL: DXL SDK

Пользовательский SDK и открытый клиент на Python позволяет интегрировать собственные решения

Customer SDK

Прослушивание сообщений	▪ Доступные темы: IOC, File Reputation, New Asset Discovery, Threat Event, Vulnerabilities…
Публикация сообщений	▪ Собственные темы: Trigger events, threat events, orchestration workflows/scripts, user information….
Новые службы	▪ Wrap existing APIs for in-house developed, IT, and competitor apps and expose them to DXL, leverage consistent authentication ▪ Entirely new native services (BYO TIE!)
Оркестирование приложениями	▪ Sequence single, multiple, or simultaneous actions based on events (scans, remediation, data collection) ▪ Integrate with in-house developed, IT, and competitor apps

Развитие DXL

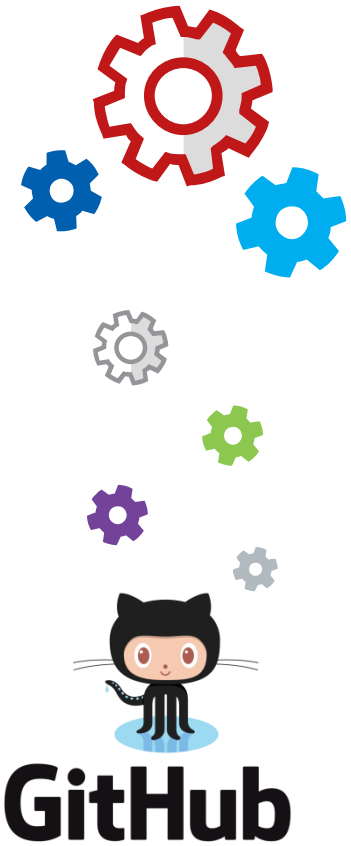
OpenDXL

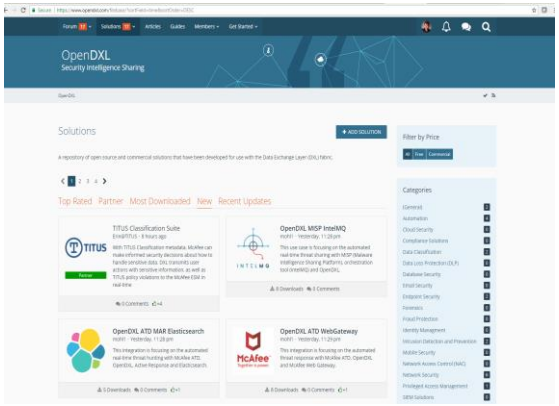
Эволюция DXL: OpenDXL

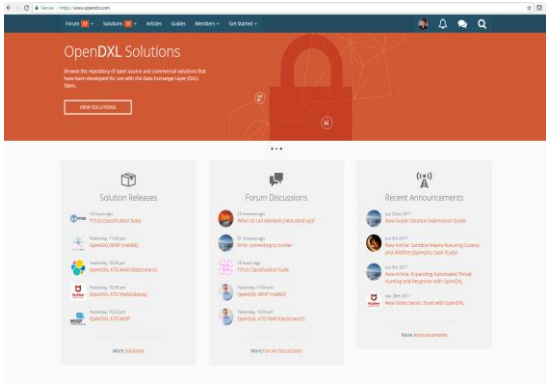
OpenDXL.com и GitHub

OpenDXL это возможность создать свои собственные DXL интеграции

- Скрипты оркестрации
  - Реагирование на события DXL: устранение, расследования, расширенное сканирование и и т.п.
- Новые службы DXL
  - Service Wrappers: подключите к DXL те решения которые to этого сами не умеют с использованием API
  - Создавайте новое
- Публикуйте новые события DXL
  - Создайте новые события для новых реакций и цепочек событий







DXL – Пример использования

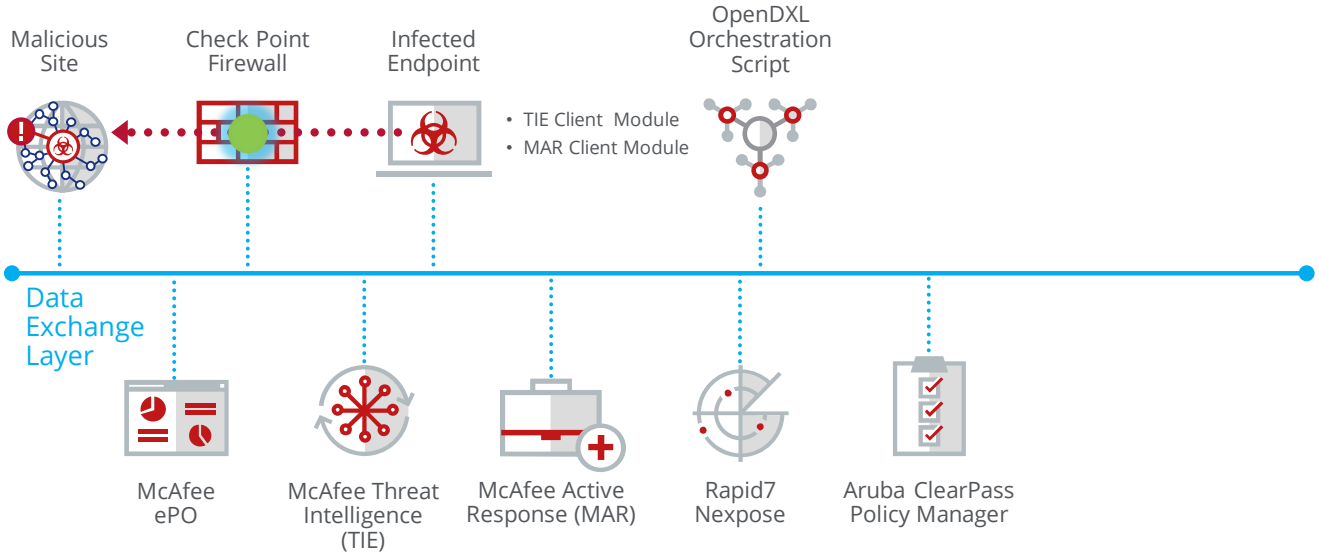
Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

✓ Прослушивание событий от Check Point

Зловред инициирован на инфицированном APM скак следствие передача трафика на зловредный сайт

Событие получено OpenDXL хостом

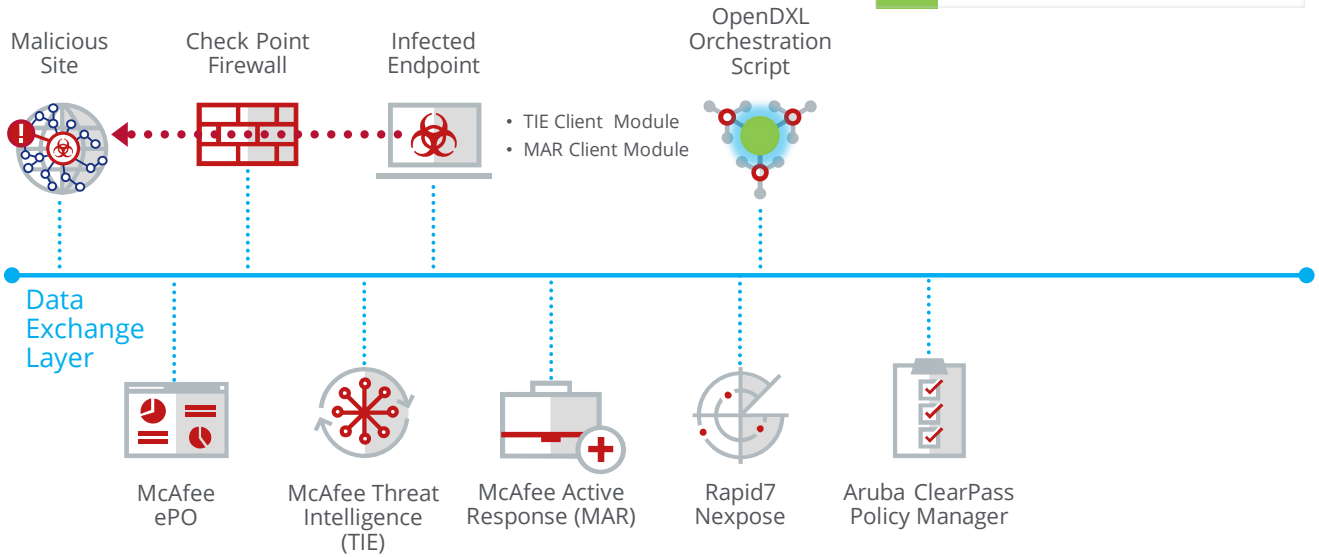


Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

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

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

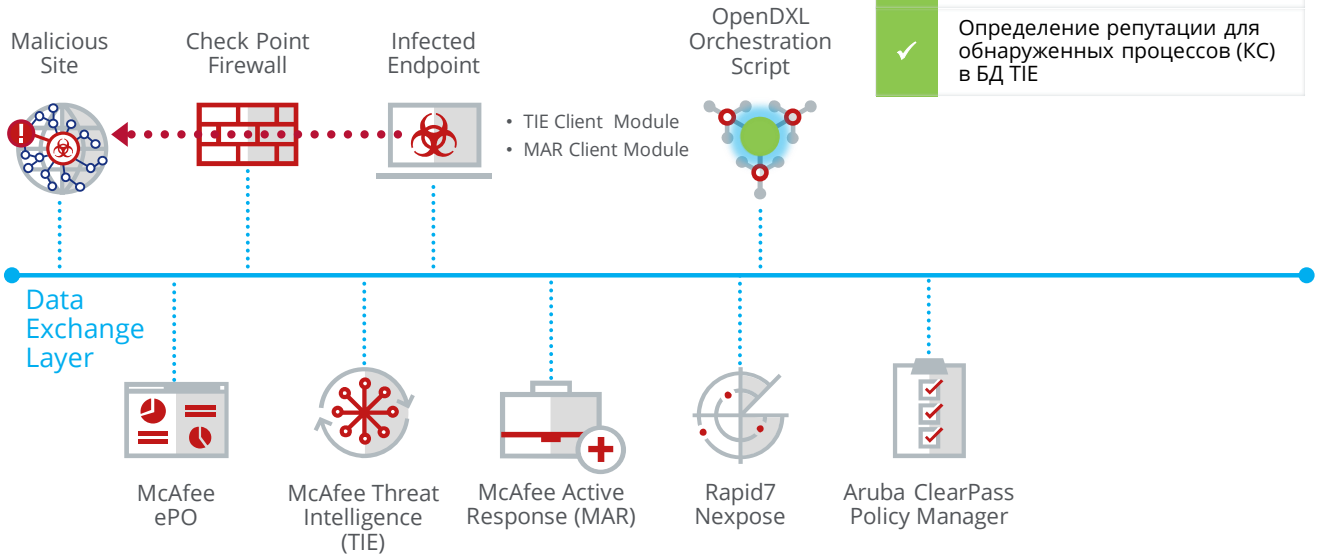


Пример – OpenDXL сценарий

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 вредоноса и изоляции бинарных файлов

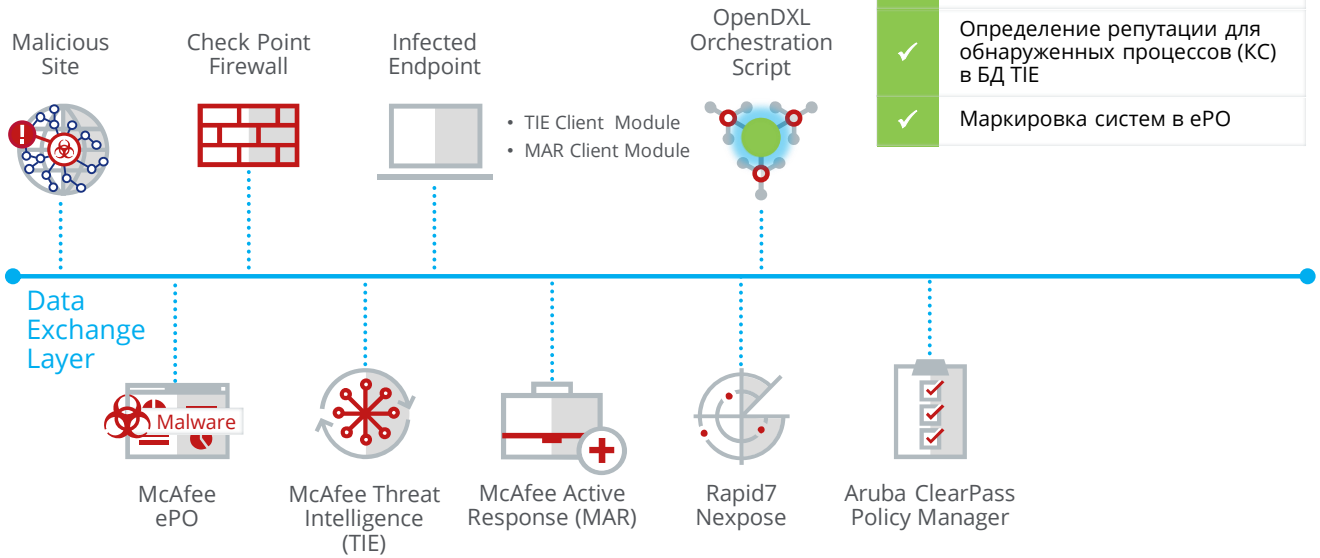


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (КС) в БД TIE

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

Скрипт маркирует системы содержащие зловред в ePO через DXL

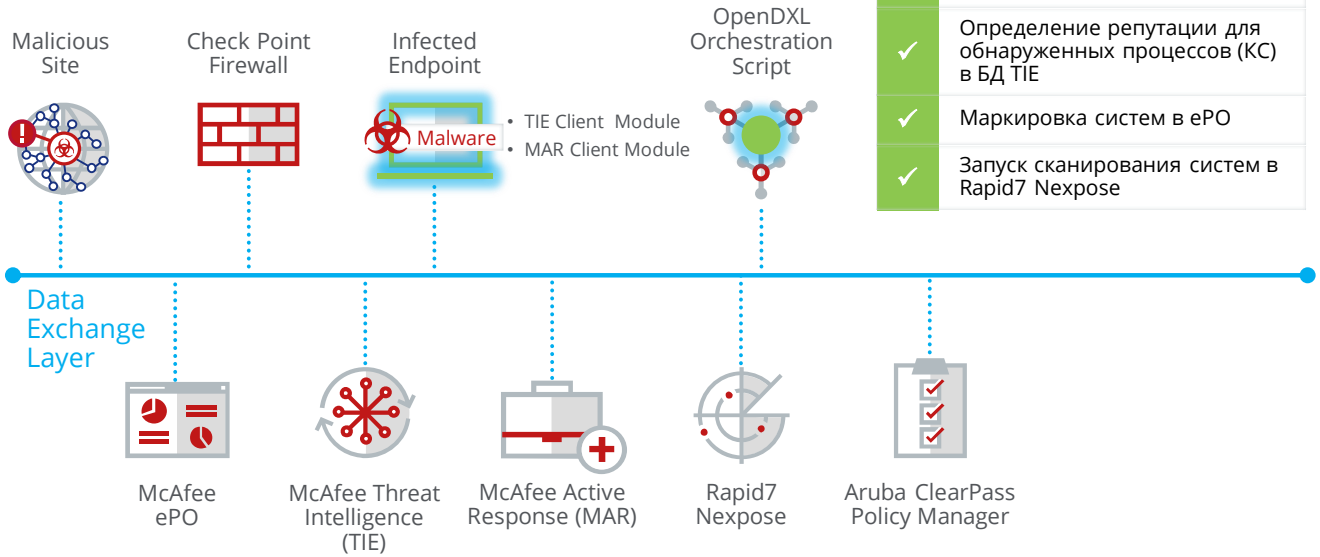


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (KC) в БД TIE
✓	Маркировка систем в ePO

Пример – OpenDXL сценарий

Какие возможности даёт OpenDXL?

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

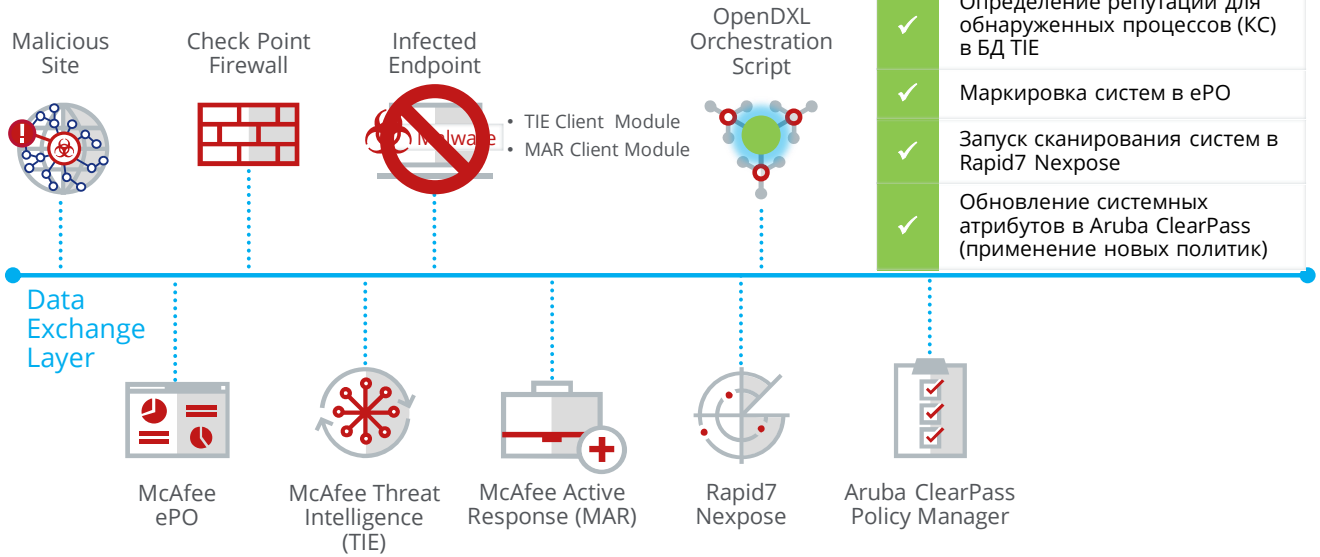


✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (KC) в БД TIE
✓	Маркировка систем в ePO
✓	Запуск сканирования систем в Rapid7 Nexpose

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



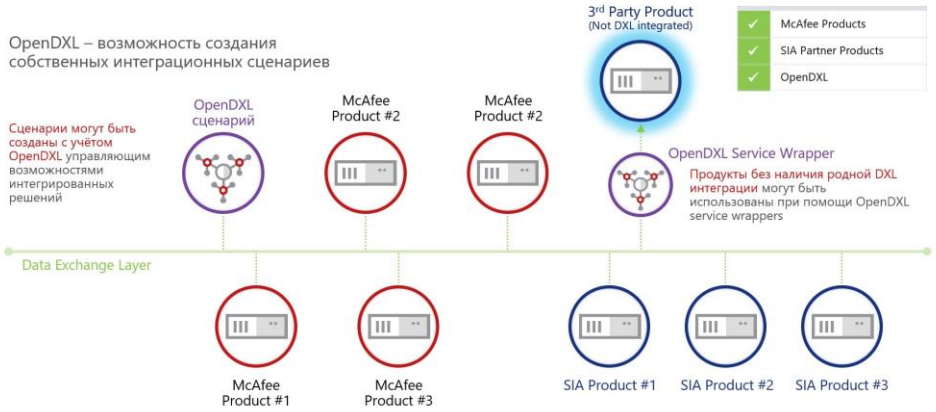
✓	Прослушивание событий от Check Point
✓	MAR для поиска процессов (по совпадению порта и адреса назначения)
✓	Определение репутации для обнаруженных процессов (КС) в БД TIE
✓	Маркировка систем в ePO
✓	Запуск сканирования систем в Rapid7 Nexpose
✓	Обновление системных атрибутов в Aruba ClearPass (применение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



Ваши преимущества

OpenDXL открывает новые возможности

- Быстрое реагирование на инциденты ИБ
- Сокращение издержек на интеграцию, трудозатрат и сложностей при многовендорной интеграции
- Увеличение ценности от используемых Вами решений

Посетите www.opendxl.com для начала использования.

McAfee™
Together is power.

MONT
Group of companies

#CODEIB

Антон Тихонов
Ведущий инженер предпродажной подготовки решений McAfee
MONT (г.Москва)

atikhonov@mont.com
+7 966 184 31 64