McAfee™
Together is power.

5 принципов построения интеллектуального SOC

SOC·FORUM

Руслан Барбашин, CyberSecurity Territory Manager
Ruslans_Barbasins@mcafee.com

Обо мне

Образование

- Rigas Tehniska Universitate, Латвия
- University of Salford, Великобритания
- Sales Institute of Ireland, Ирландия

Карьера:

1995 – 2000 инженер телекоммуникаций
2000 – 2017 Прожект менеджер, BDM

2010- Territory Account Manager, McAfee Ireland Ltd.

9 лет в сфере ИБ

https://www.linkedin.com/in/ruslansbarbasins/

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.

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

McAfee Security Fusion Centre

Alert Details

Intel Update

Intel has two more identified vulnerabilities associated with the speculative execution. Speculative Store Bypass (SSB - known as variant 4) and Rogue System Register Read (RSRE - known as variant 3a). Both require local access. Lots of vendor bulletins too. OS updates are starting to roll.

More...

Computer Network Defence Alert State

VPNFilter	NetApp	strongSwan
Exploit	Patch	Patch
MicroFocus	Schneider	Linux
Patch	Patch	Patch

Click for alert details

COMPUTER NETWORK DEFENCE CND

Computer Network Defence Alert State

Wireshark	Novell	Huawei
+24hr	+24hr	+24hr
QNAP	ICS	Intel
+24hr	+24hr	Update

Click for alert details

Virus News

Troj/Fareit-EYG More...

Troj/Remcos-BV More...

COMPUTER NETWORK DEFENCE ALERT STATE Overall

COMPUTER NETWORK DEFENCE ALERT STATE VPNFilter

Security News

When Securing Customer Loyalty Becomes Critical

More...

Team Cymru Malicious Activity Map

Latest Tool Versions

Burp Suite	28Mar18	1.7.33
Kali-Linux	30Apr18	2018.2
Metasploit	06Dec17	4.14.2
Nessus	15May18	7.1.0
NetworkMiner	03Apr18	2.3
Nmap	14May18	7.70
Snort	04Jan18	2.9.11.1
Wireshark NEW	22May18	2.6.1

Latest IDS Signatures

Cisco IPS NEW	21May18	1018
Cisco Sourcefire NEW	22May18	05-21-001
Juniper IDP NEW	22May18	#3067
McAfee NSP NEW	22May18	9.8.22.2
Proventia NEW	17May18	3805.15183

Useful Links

McAfee Security Fusion Centre

SOC•FORUM

- Обеспечивает:

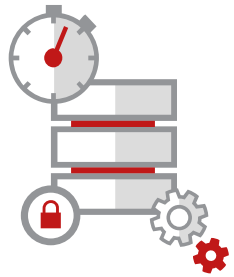
- Мониторинг, расследование и устранение инцидентов ИБ
- Физическая безопасность
- Федеральная безопасность
- Сбор и обмен данными Threat Intelligence

- 365/24/7

- Плано, Техас, США и Корк, Ирландия

Требования и задачи интеллектуального iSOC

SOC·FORUM

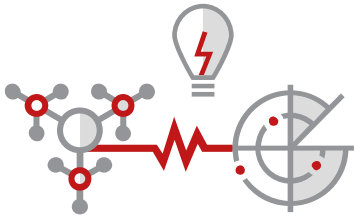


Использование большого объёма собираемых данных

Сбор из множества источников

Использование «сырых» данных для анализа

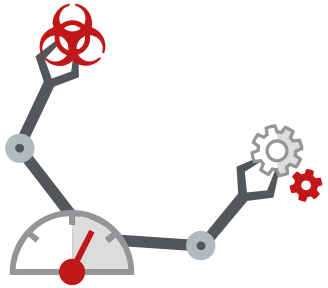
Быстрое распределение



Выделение сигнала из шума и выставление приоритетов

Предоставить аналитикам качественные данные в порядке их важности и приоритетов

Уменьшение false positives



Уменьшение времени на устранение инцидентов

Быстрое обнаружение

Быстрое блокирование

Быстрая ликвидация

Пять характеристик интеллектуального SOC от Gartner

Пять принципов построения интеллектуального iSOC

SOC·FORUM

SUMMARY

Security operations centers must be architected for intelligence, embracing an adaptive security architecture to become context-aware and intelligence-driven. Security leaders should understand how intelligence-driven SOCs use tools, processes and strategies to protect against modern threats.

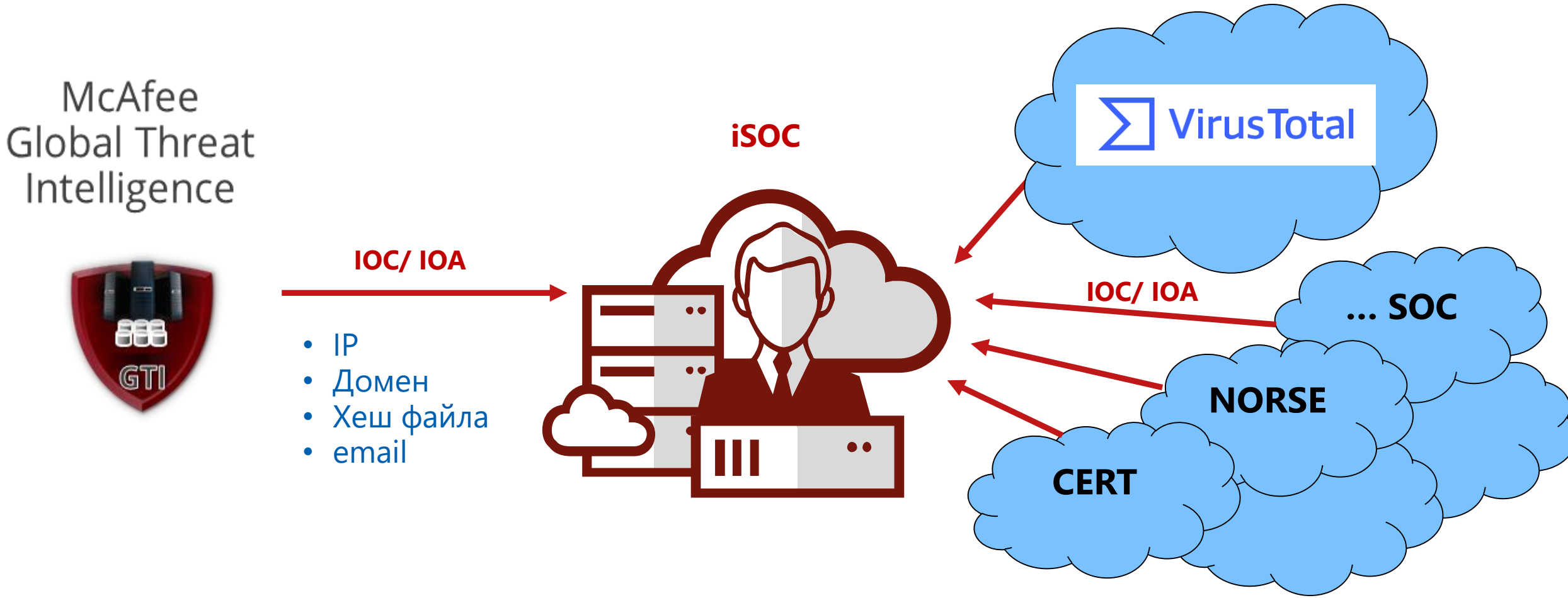
Вывод:

Центр мониторинга и реагирования на критические инциденты ИБ должен изначально проектироваться, как ***интеллектуальный***, и включать в себя ***архитектуру адаптивной безопасности*** и стать ***контекстно-ориентированным*** и с аналитическим управлением.

Пять принципов построения интеллектуального iSOC

SOC·FORUM

1. Использование множественных источников аналитики об угрозах/атаках, применяя их стратегически и тактически

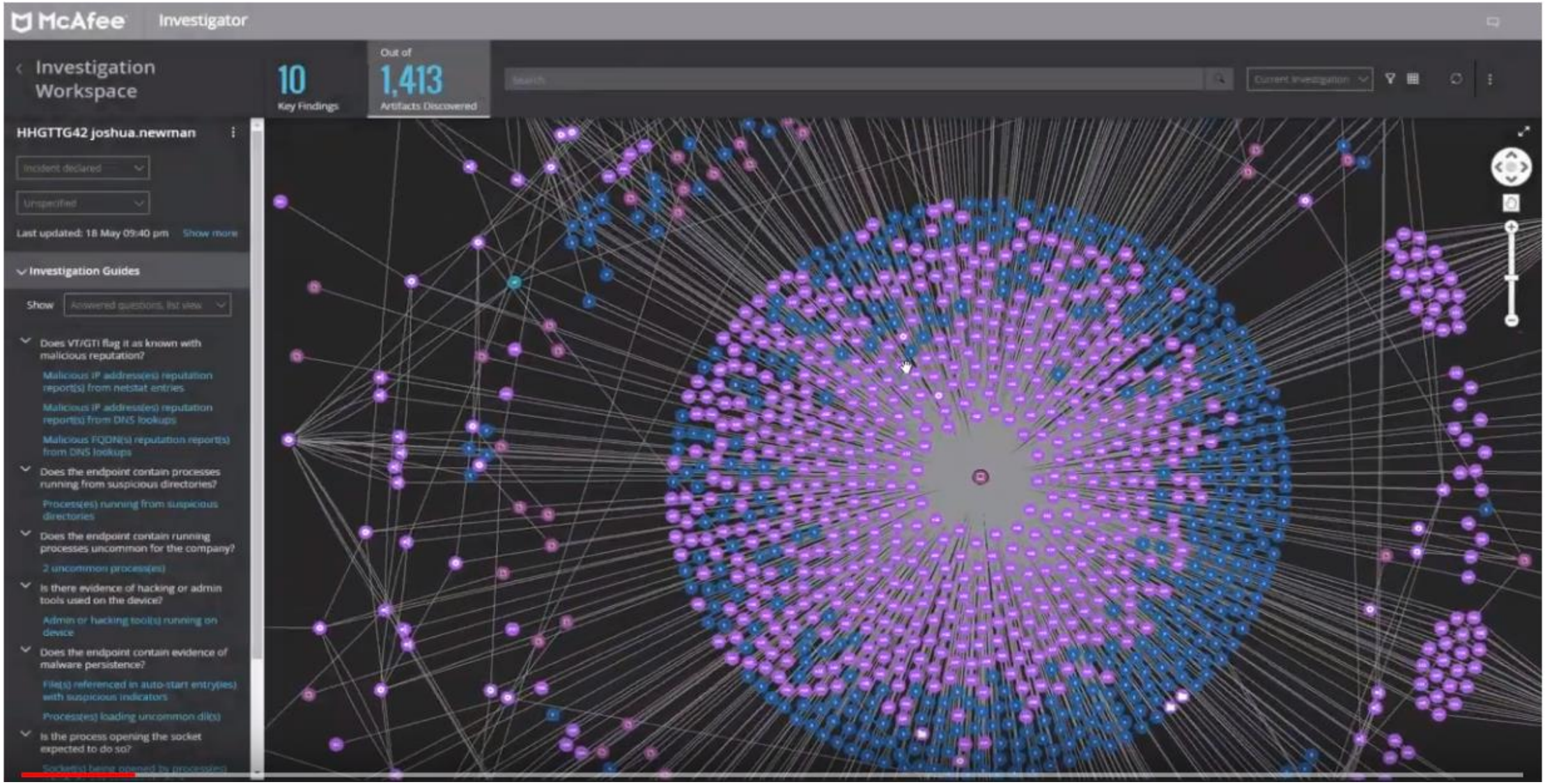


Пять принципов построения интеллектуального iSOC

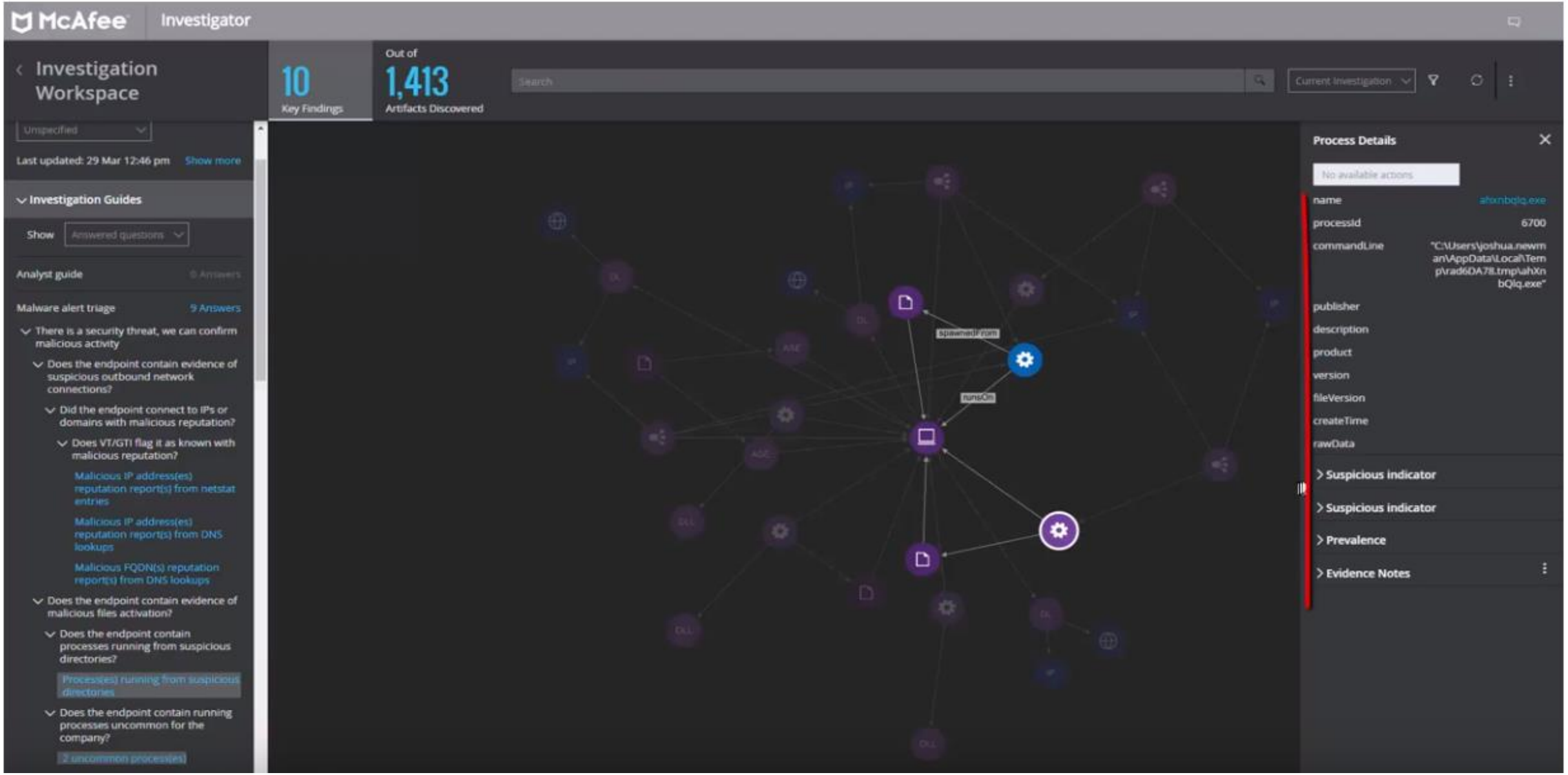
2. Использование современных методов анализа (статистический, машинное обучение, data mining, оптимизация, нормализация и т.д)

SOC·FORUM

Пять принципов построения интеллектуального iSOC



Пять принципов построения интеллектуального iSOC



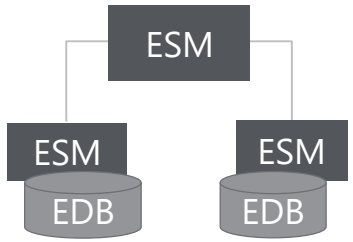
Платформа для обработки Big Data

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

SOC·FORUM

Kafka Databus

События

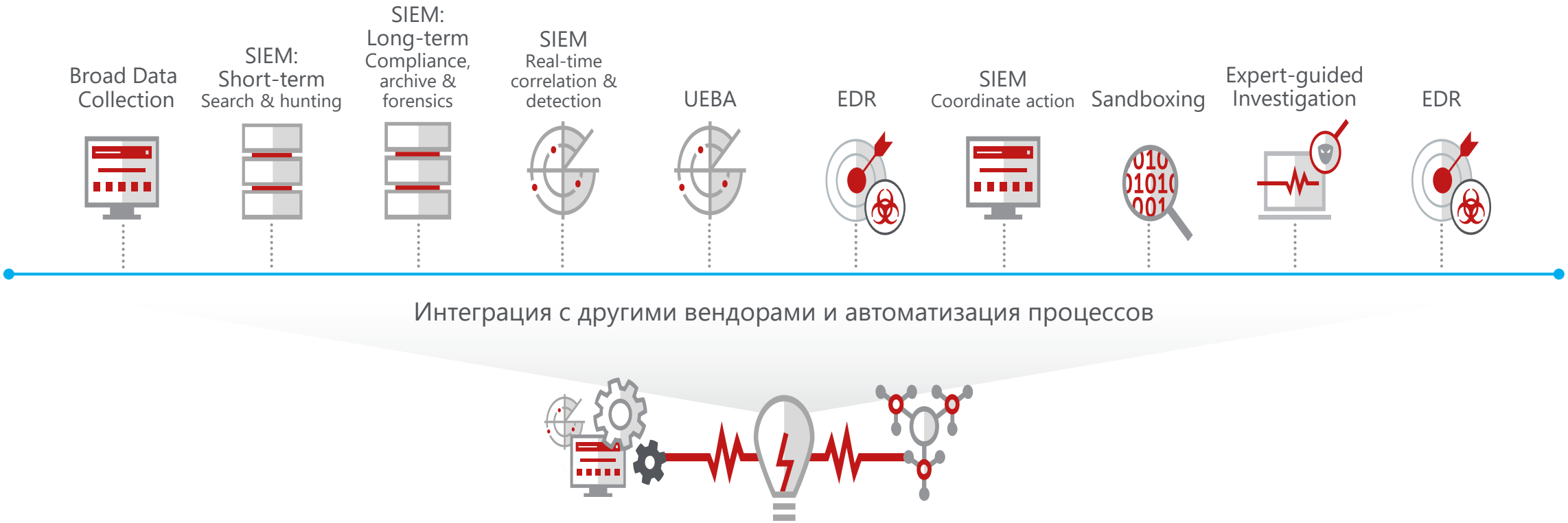
Хранение логов & Compliance	Поиск по логам & Охота за малваре	Корреляция	Аналитика	Кластер ESM
Сжатые данные. Подписанные. Долгосрочное хранения для соответствие норм.актам	Краткосрочное хранение данных. Оптимизировано для быстрого поиска и охоты.	Корреляция. В режиме реального времени. Быстро. **Эффективно!**	Периодическая аналитика. ИИ и машинное обучение. Легко. **Эффективно!**	
Хранилище данных EDB	Elastic Search	В памяти (без записи данных)	Hadoop	Хранилище данных EDB

Пять принципов построения интеллектуального iSOC

SOC·FORUM

3. Автоматизация процессов

«Все что можно автоматизировать, должно быть автоматизировано!» - Gartner



Примеры автоматизации (интеграция с openDXL и pxGrid)

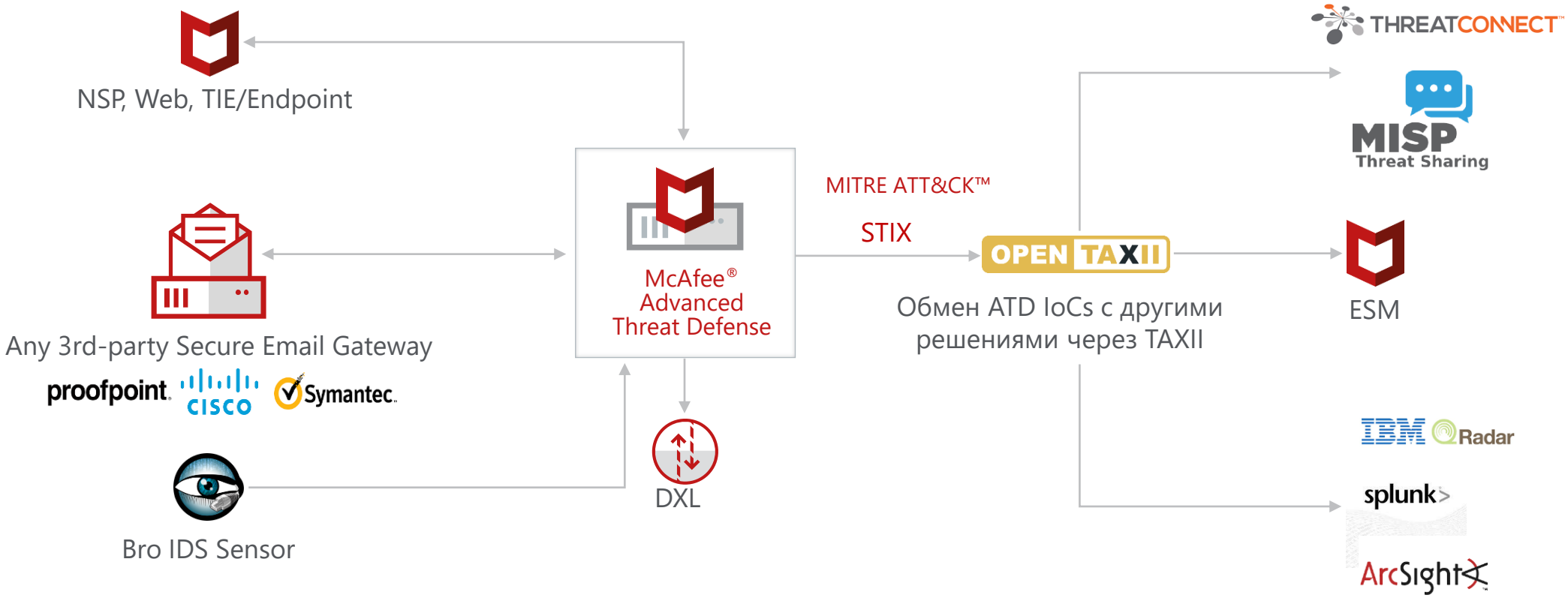
SOC·FORUM

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

Примеры автоматизации (обмен IOC)

SOC·FORUM

Автоматизация действий по защите и детектированию, интеграция через открытую платформу



Детализированные отчеты и выдача их в стандартизированном виде

SOC·FORUM

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 11:06:28	Processing Time	17 seconds
File Size	45,056 bytes	Sandbox Replication	9 seconds
Show More	Hash Values	File Details	Environment
MD5 Hash Identifier	E2CFE1C89703352C42763E4B458FC356		
SHA-1 Hash Identifier	FD384A9FCFF228F4C371EF3BCA693A9A336D6AB7		
SHA-256 Hash Identifier	258E08D6193BCE55856A22482D9F6954911AD81D582ABAE95EBDFDBE578D8975		
	Hide hash values		
File Type	PE32 executable (console) Intel 80386		
Digital Signature Verified	Unsigned		
Publisher	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		

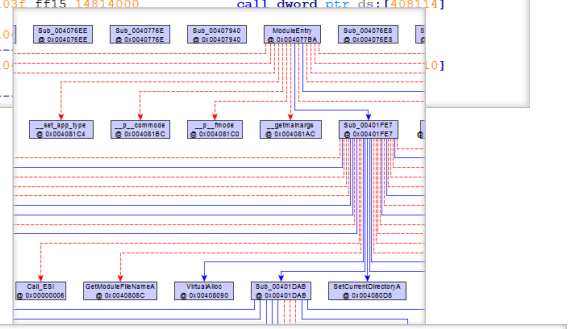
Microsoft Windows XP Professional Service Pack 3 (build 2600, version 5.1.2600)

Internet Explorer version: 6.0.2900.5512

Microsoft Office version: 2003

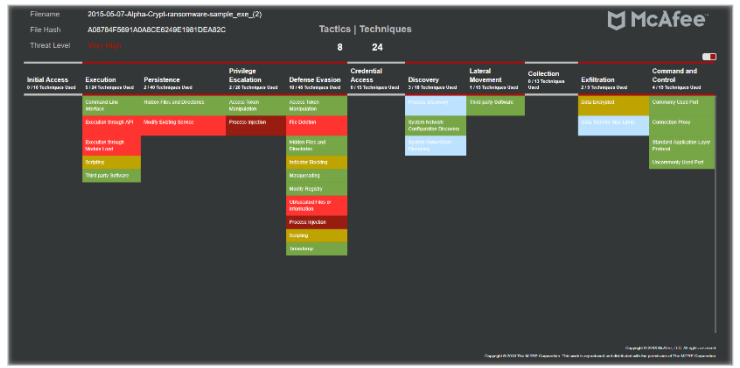
Assembly Code, Graph Analysis, and Indicators of Compromise

```
:00401001 33f6                  xor esi,esi
:00401003 397424 0c             cmp dword ptr ss:[esp+c],esi
:00401007 57                    push edi
:00401008 74 07                 jz short 00401011
:0040100a 68 1ce04000           push 40e01c
:0040100f eb 05                 jmp 00401016
-------->
:00401011 68 18e04000           push 40e018
-------->
:00401016 68 10e04000           push 40e010
:0040101b ff15 18814000         call dword ptr ds:[408118]
                          ;;call MSVCRT.fopen
:00401021 8bf8                  mov edi,eax
:00401023 59                    pop ecx
:00401024 3bfe                  cmp edi,esi
:00401026 59                    pop ecx
:00401027 75 04                 jnz short 0040102d
:00401029 33c0                  xor eax,eax
:0040102b eb 34                 jmp 00401061
-------->
:0040102d 397424 10             cmp dword ptr ss:[esp+10],esi
:00401031 57                    push edi
:00401032 6a 01                 push 1
:00401034 68 0c030000           push 30c
:00401039 ff7424 18             push dword ptr ss:[esp+18]
:0040103d 74 08                 jz short 00401047
:0040103f ff15 14814000         call dword ptr ds:[408114]
```

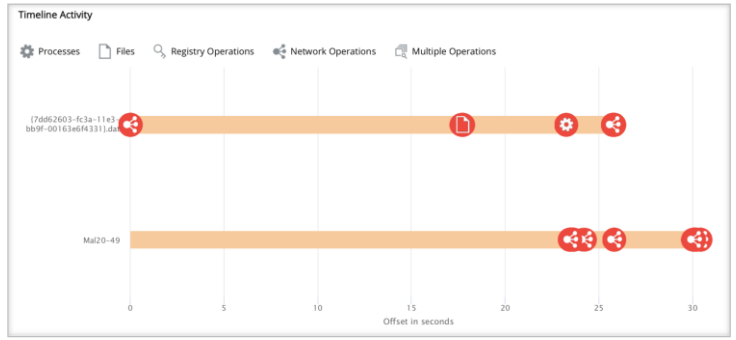


```
"Dropped Malware Files": [
    {
        "Name": "@WanaDecryptor@.exe",
        "factor": "100.00"
    }
```

MITRE ATT&CK™ mapping



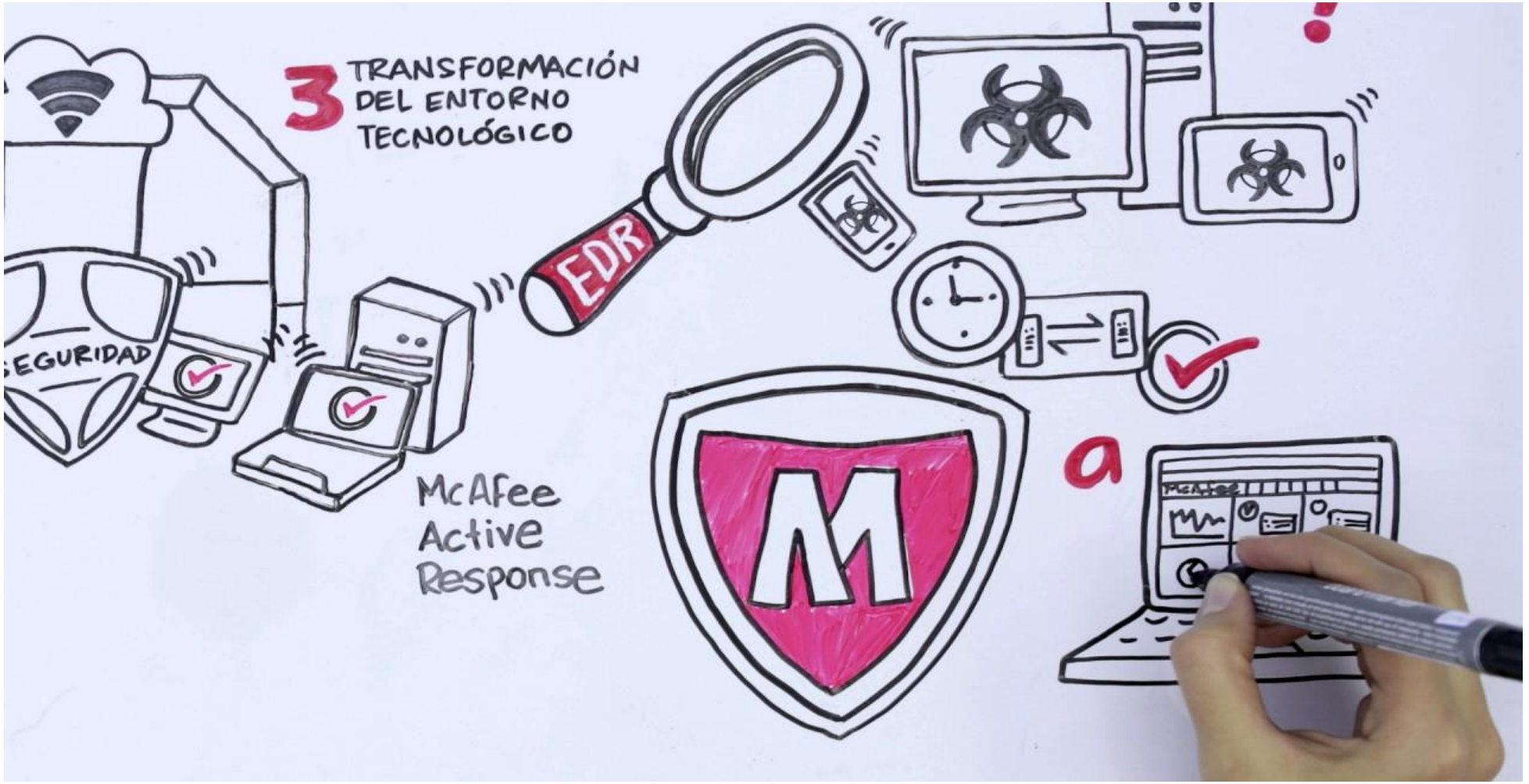
Threat Timeline



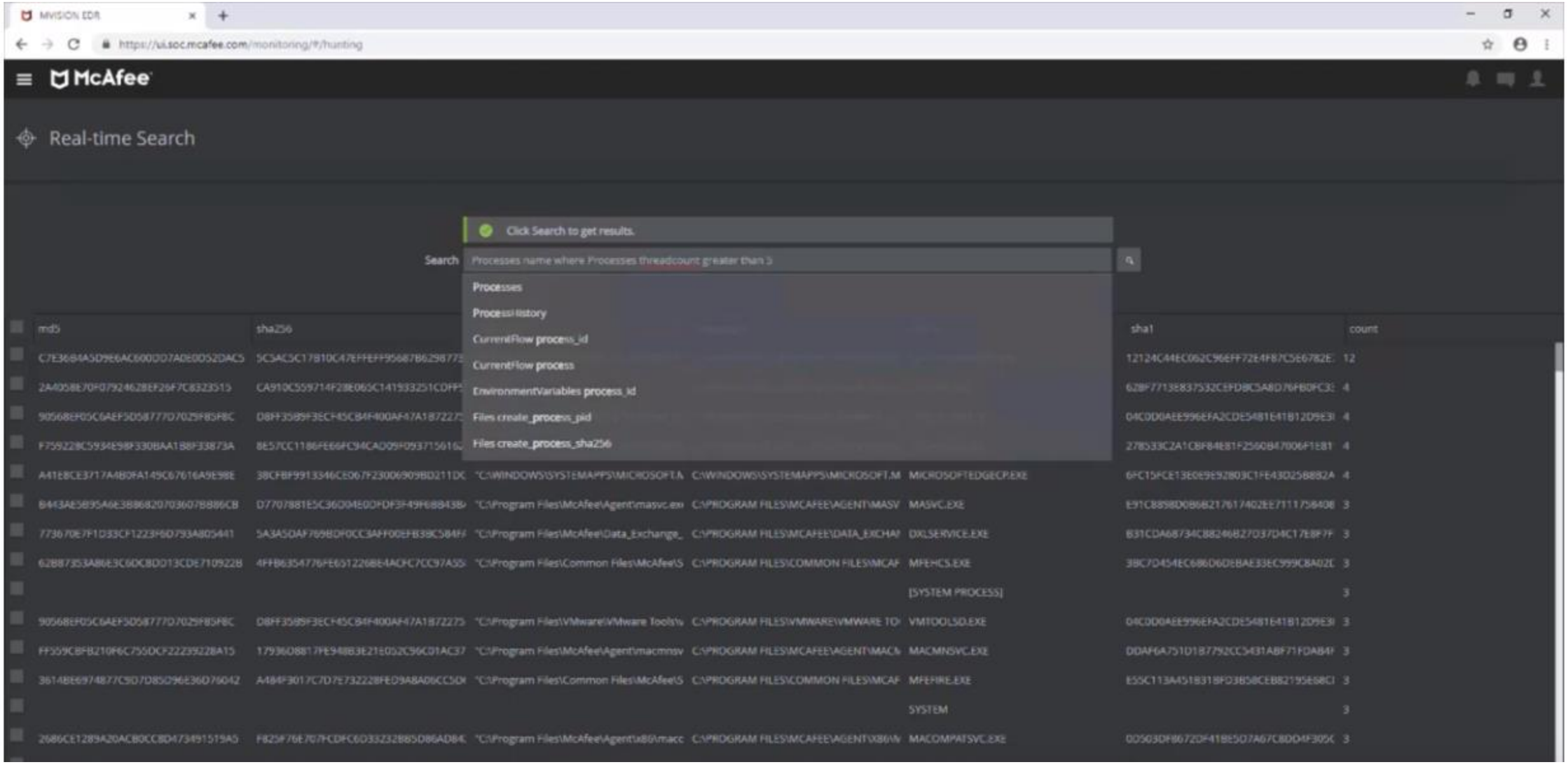
Пять принципов построения интеллектуального iSOC

SOC·FORUM

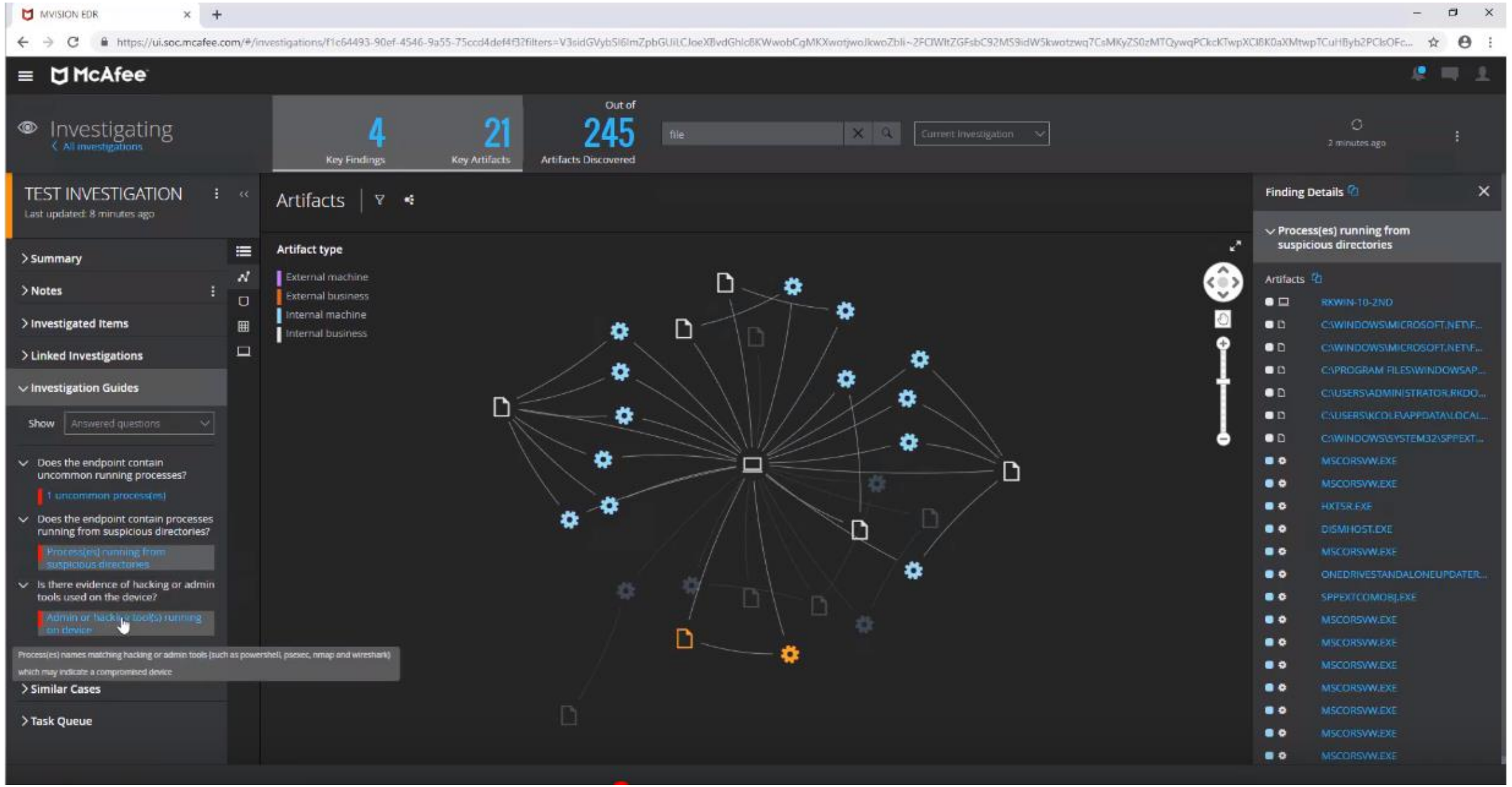
4. Активная охота за вредоносами (Threat Hunting) и расследование вредоносной активности



MVISION EDR – поиск в режиме реального времени



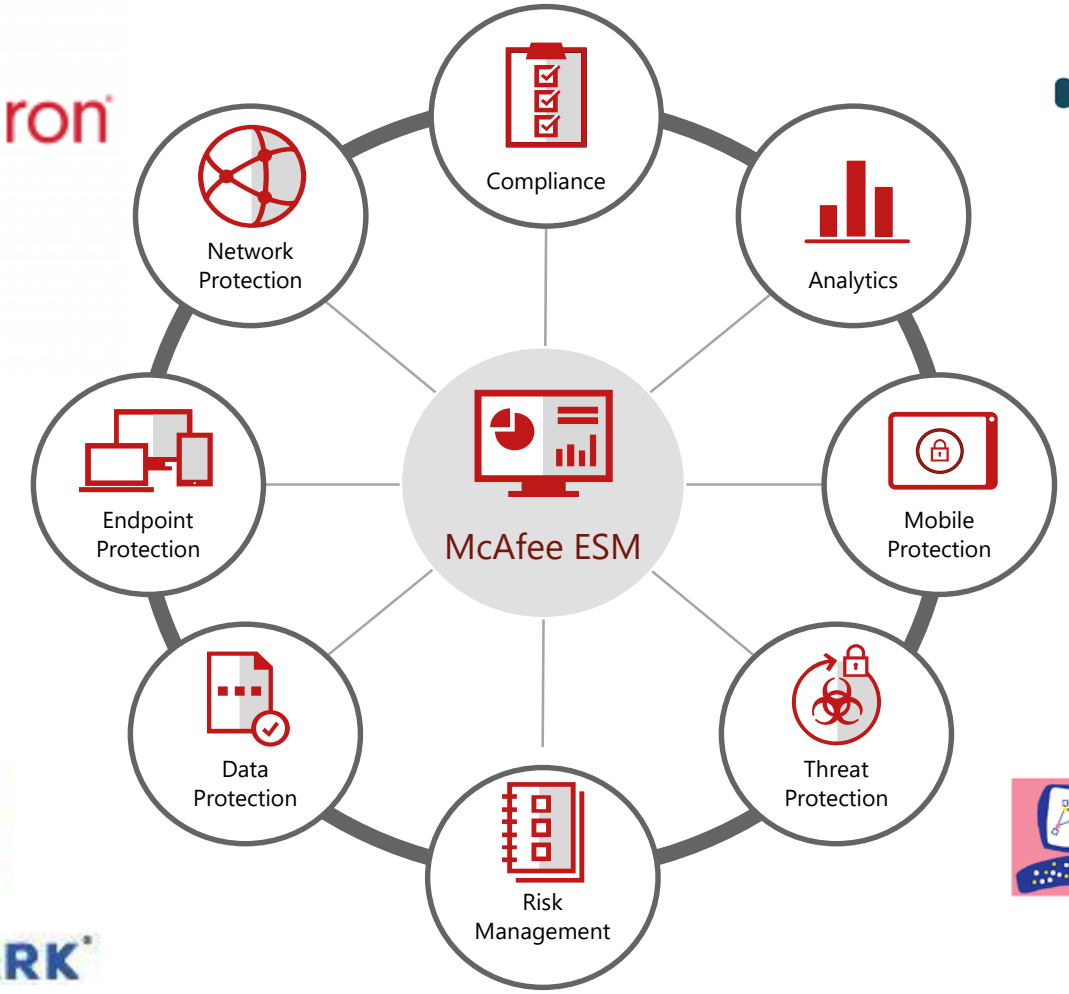
MVISION EDR – инструмент для расследований



Пять принципов построения интеллектуального iSOC

5. Построение и использование Архитектуры Адаптивной Безопасности

SOC·FORUM



MobileIron

TITUS

RAPID7

aruba
a Hewlett Packard Enterprise company

CYBERARK

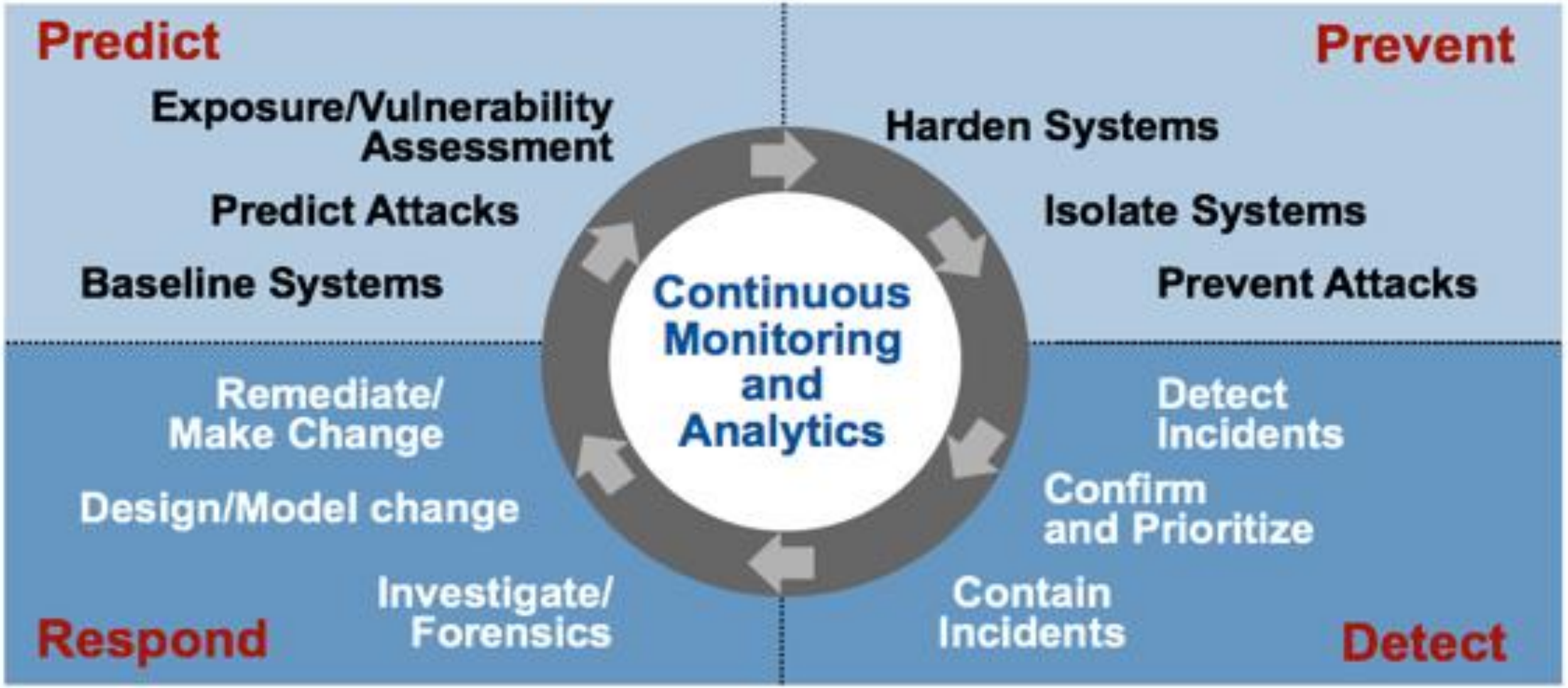
CISCO

BROCADE

FORCEPOINT
POWERED BY Raytheon

Check Point
SOFTWARE TECHNOLOGIES LTD.

The Adaptive Security Architecture: Twelve Critical Capabilities of Security



Gartner

Краткие выводы от Gartner:

SOC·FORUM

- 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:

SOC·FORUM

- 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.

Экосистема McAfee

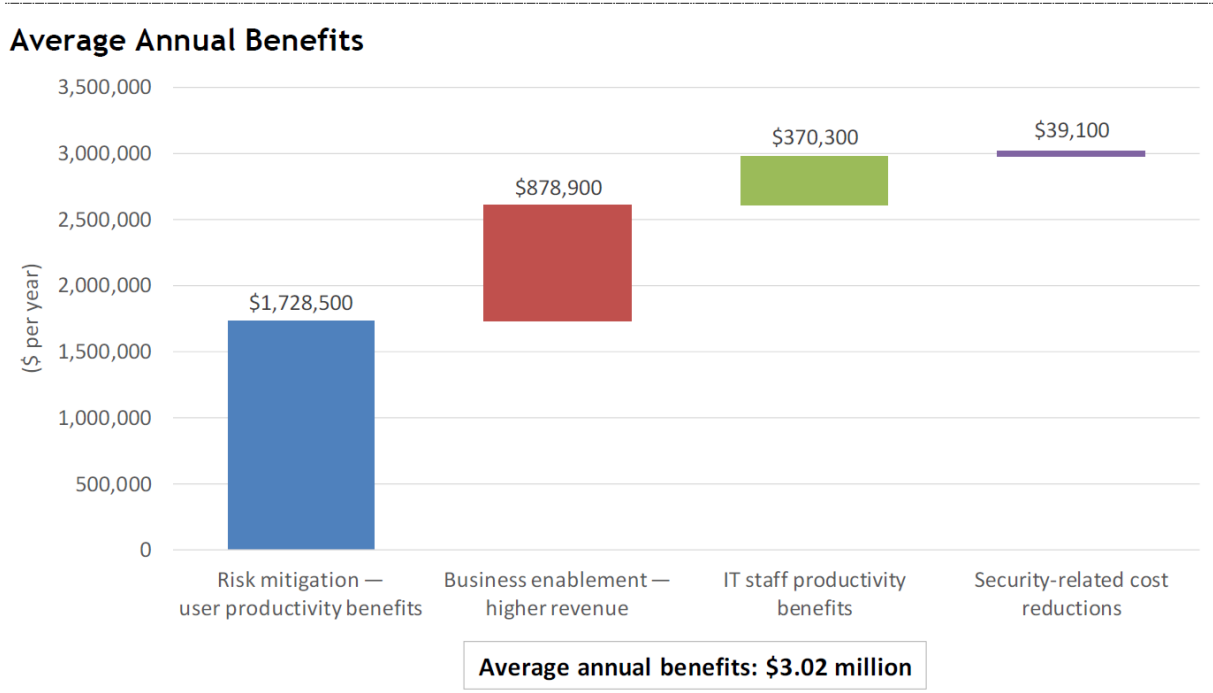
IDC ExpertROI Spotlight Top 100 US FDIC Bank

SOC·FORUM

"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



Source: IDC, 2017

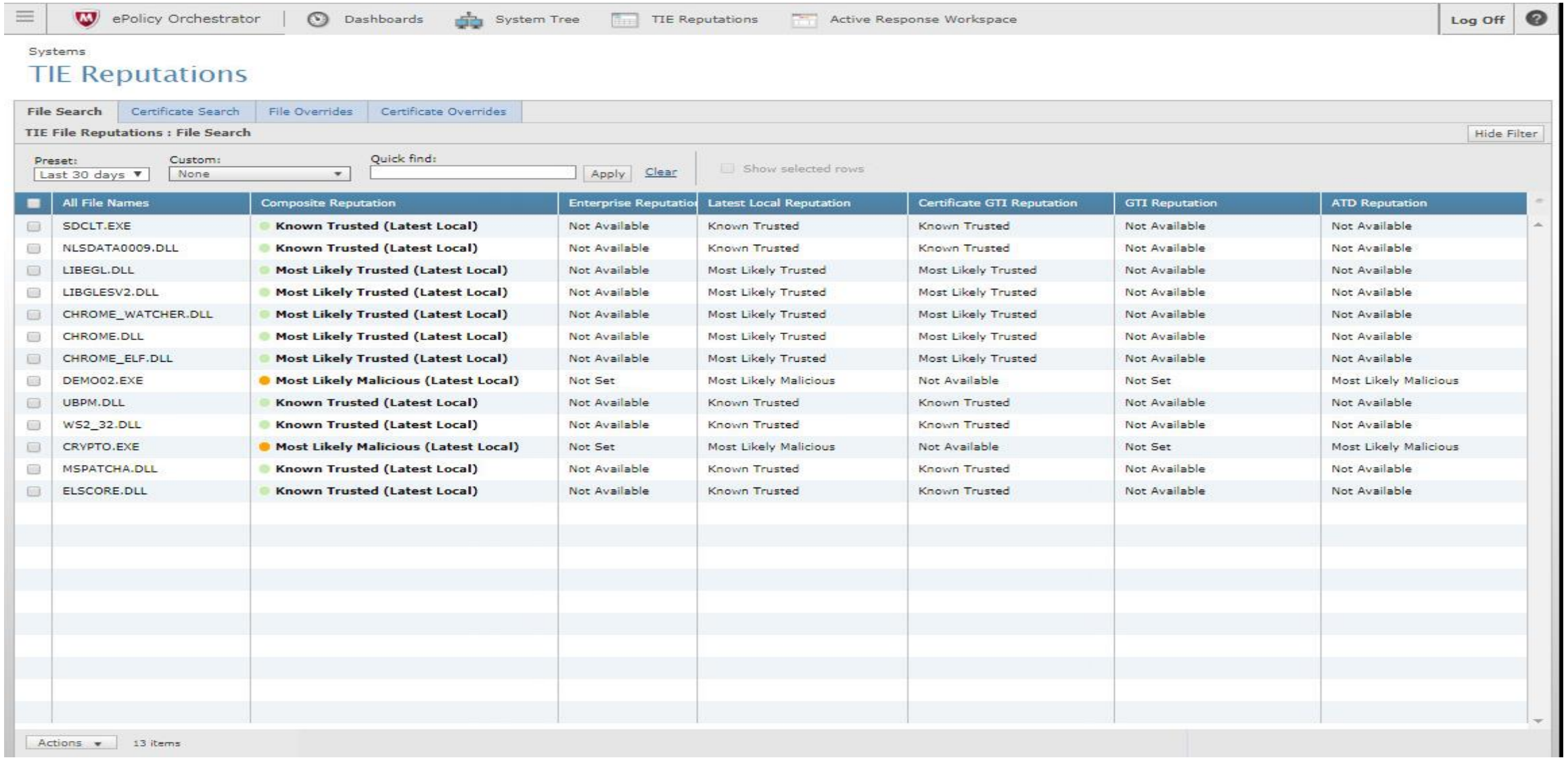
- Экономия средств **$3.02 M** в год
- **ROI 208%** в течении 4 лет
- Период окупаемости **20** месяцев
- На **90%** быстрее расследование инцидентов
- На **77%** меньше инцидентов с причиненным ущербом
- На **98%** меньше времени снижение продуктивности из-за инцидентов ИБ
- **$5-10 миллионов** дополнительная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

Source: http://idcdocserv.com/US42210917

SOC·FORUM

McAfee Threat Intelligence Exchange DXL

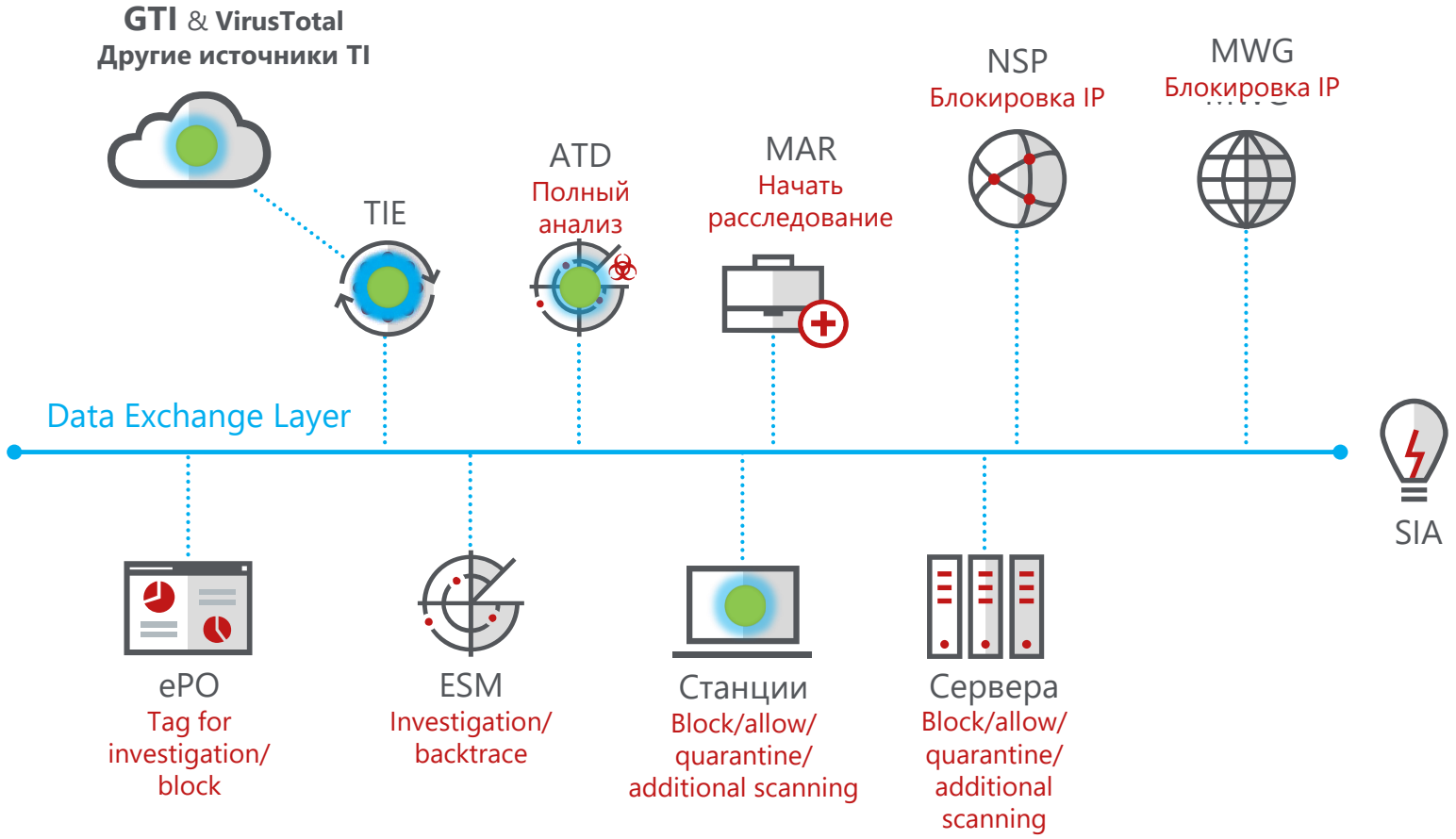
McAfee Threat Intelligence Exchange



McAfee Adaptive Security Architecture

Постоянный обмен репутациями (IOC) по всей экосистеме

SOC·FORUM



Extreme® Connect Beyond the Network

RAPID7

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

JUNIPER NETWORKS

Интеграция по шине DXL

SOC·FORUM

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
aruba a Hewlett Packard Enterprise company	▪ ClearPass integration with DXL and ePO ▪ Publishing Topics: IOC Information, New Asset Discovery Information ▪ Subscribing Topics: IOC information, Threat Event
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

Примеры интеграции с openDXL

SOC•FORUM

OpenDXL-ATD-Cisco-ASA

License Apache 2.0

This integration is focusing on the automated threat response with McAfee ATD, OpenDXL and Cisco ASA Firewalls. McAfee Advanced Threat Defense (ATD) will produce local threat intelligence that will be pushed via DXL. An OpenDXL wrapper will subscribe and parse IP indicators ATD produced and will automatically update Firewall rules.

Component Description

McAfee Advanced Threat Defense (ATD) is a malware analytics solution combining signatures and behavioral analysis techniques to rapidly identify malicious content and provides local threat intelligence. ATD exports IOC data in STIX format and DXL. https://www.mcafee.com/in/products/advanced-threat-defense.aspx

Cisco ASA Firewalls are security devices protecting corporate networks and data centers of all sizes. It provides users with highly secure access to data and network resources - anytime, anywhere, using any device. https://www.cisco.com/c/en/us/products/security/adaptive-security-appliance-asa-software/index.html

https://github.com/mohlcyber/OpenDXL-ATD-Cisco-ASA

Примеры интеграции с openDXL

SOC·FORUM

OpenDXL-ATD-Fortinet

This integration is focusing on the automated threat response with McAfee ATD, OpenDXL and Fortinet Firewalls. McAfee Advanced Threat Defense (ATD) will produce local threat intelligence that will be pushed via DXL. An OpenDXL wrapper will subscribe and parse IP indicators ATD produced and will automatically update Firewall rules.

Component Description

McAfee Advanced Threat Defense (ATD) is a malware analytics solution combining signatures and behavioral analysis techniques to rapidly identify malicious content and provides local threat intelligence. ATD exports IOC data in STIX format in several ways including the DXL. https://www.mcafee.com/in/products/advanced-threat-defense.aspx

Fortinet Firewalls provide high performance network security protection platform. https://www.fortinet.com/products/next-generation-firewall.html

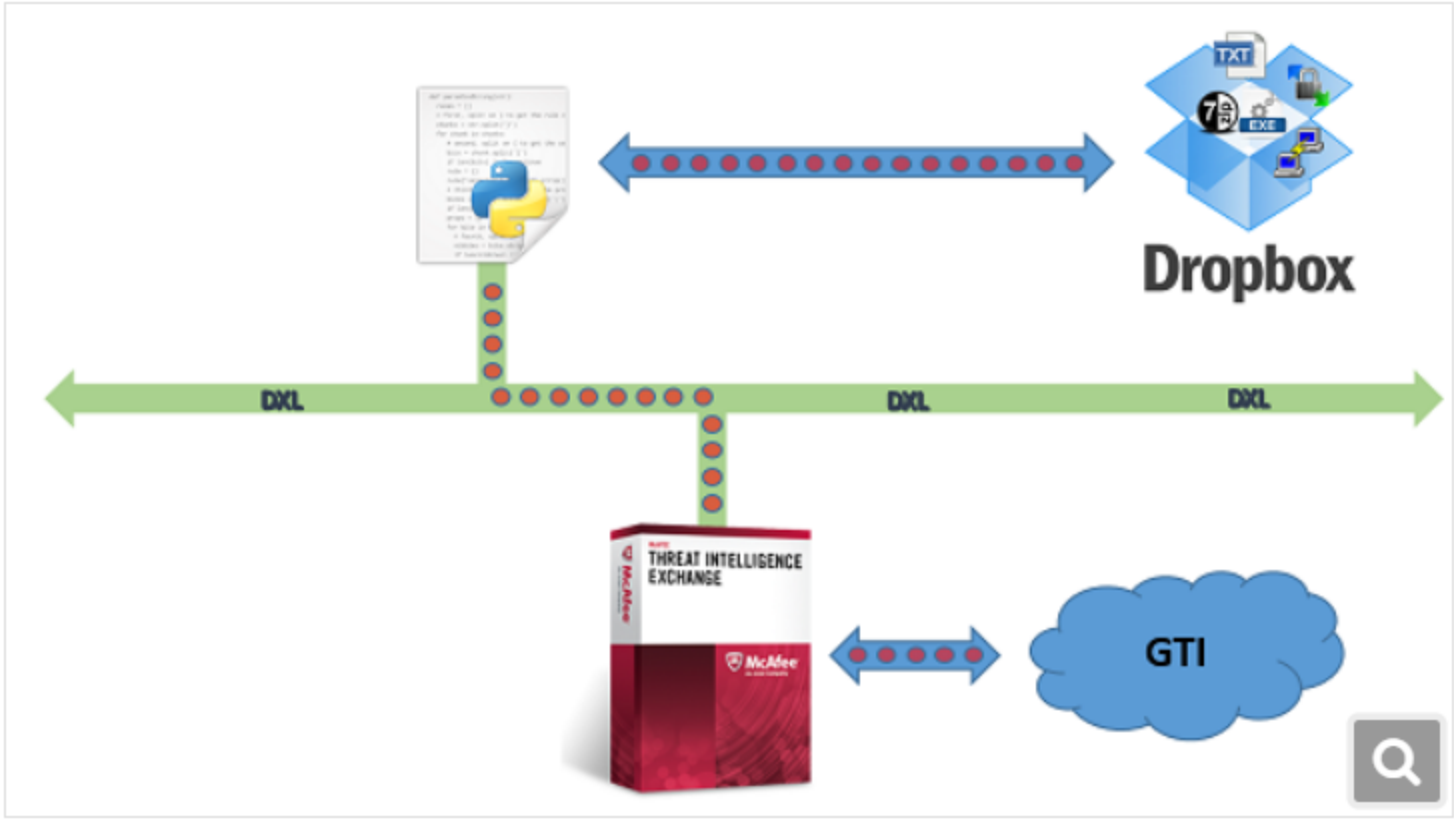
Примеры интеграции с openDXL

SOC·FORUM

Website

https://github.com/filippostz/OpenDXL-TIE-Dropbox

Software that scans every file within a DropBox folder structure and will check against the McAfee Threat Intelligence Exchange ser

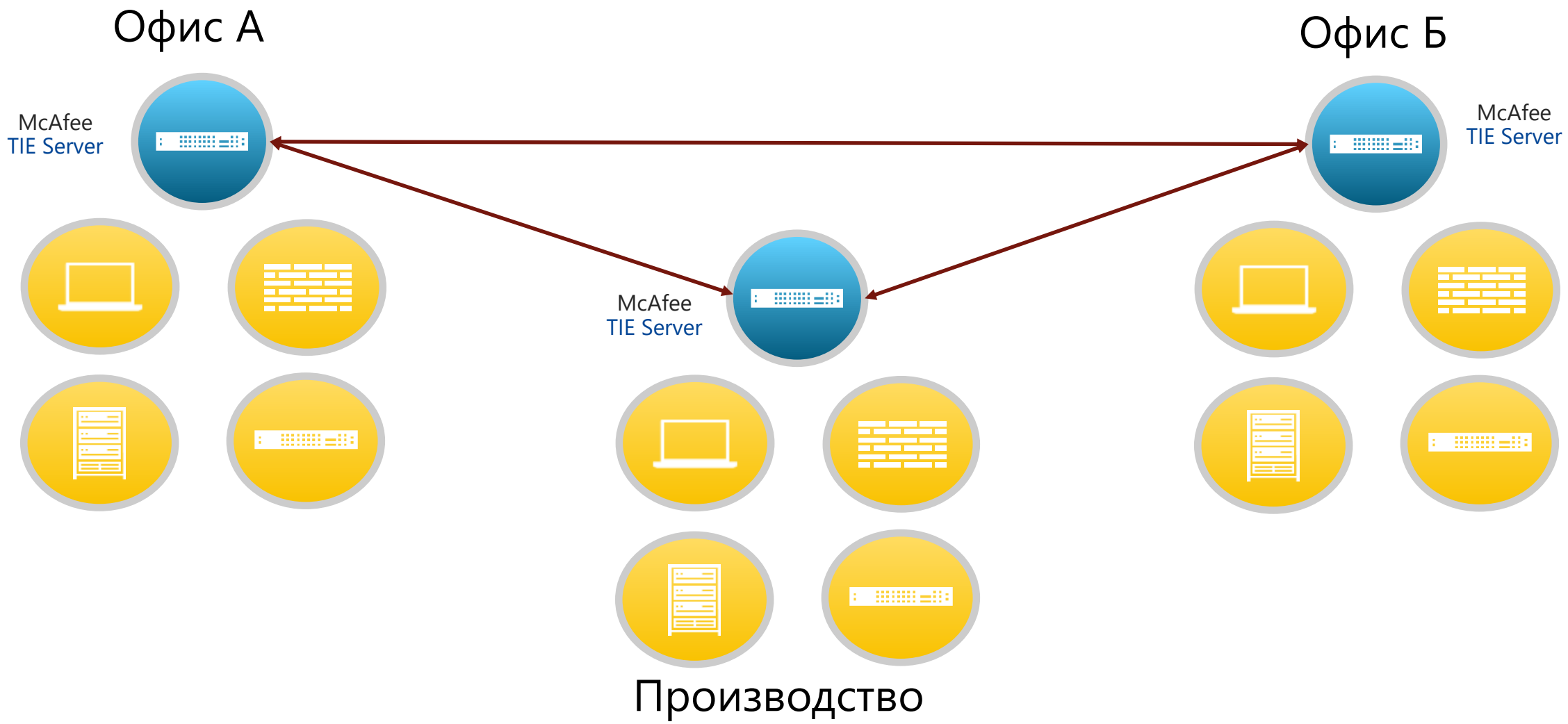


Адаптивная безопасность для корпораций и государства

Защита корпорации

SOC·FORUM

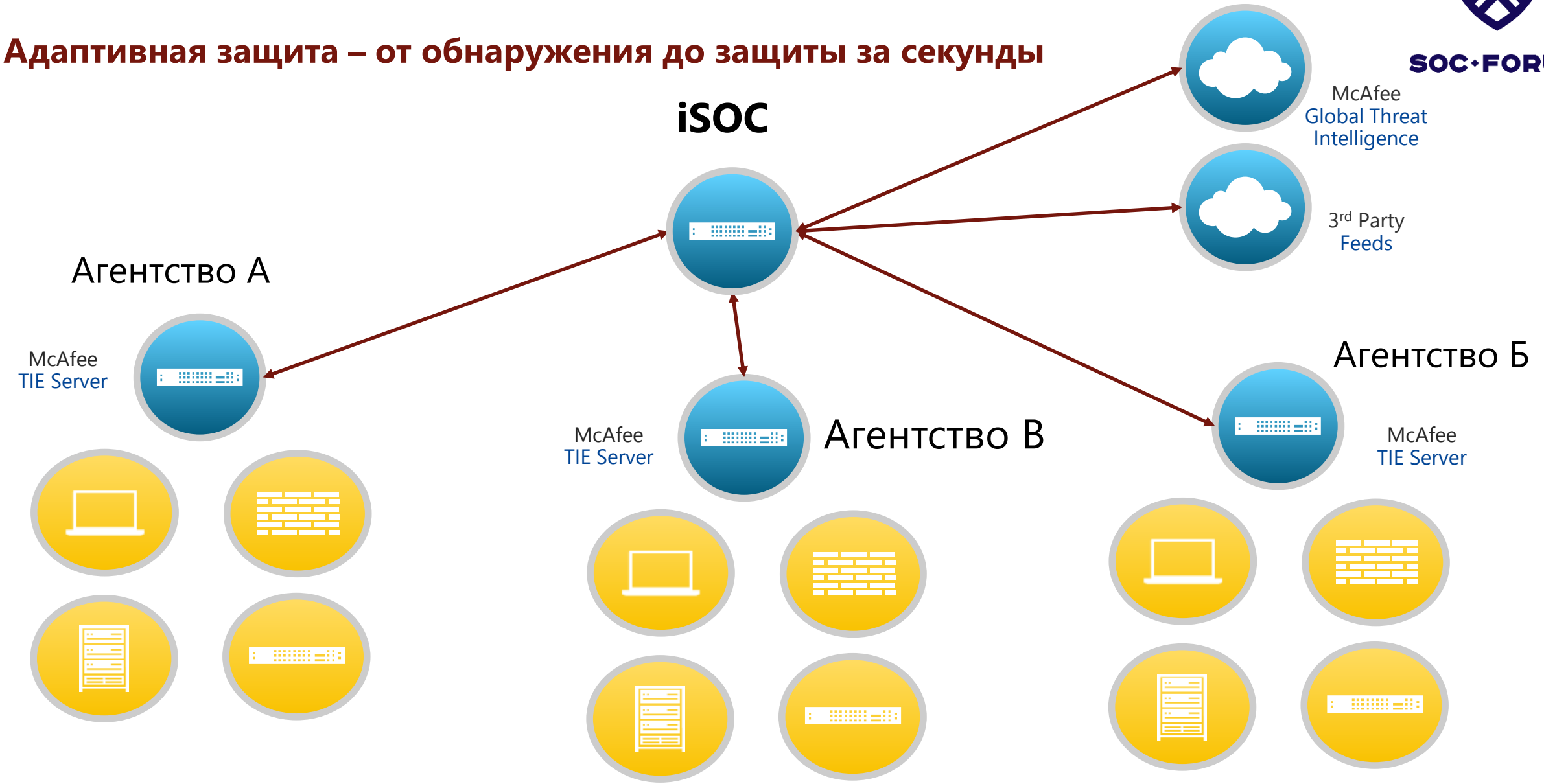
Адаптивная защита – от обнаружения до защиты за секунды



Защита для всего государства

SOC·FORUM

Адаптивная защита – от обнаружения до защиты за секунды



Solution Architecture

Advanced Threat Intel Use Case

Threat Intelligence and Orchestration Platforms

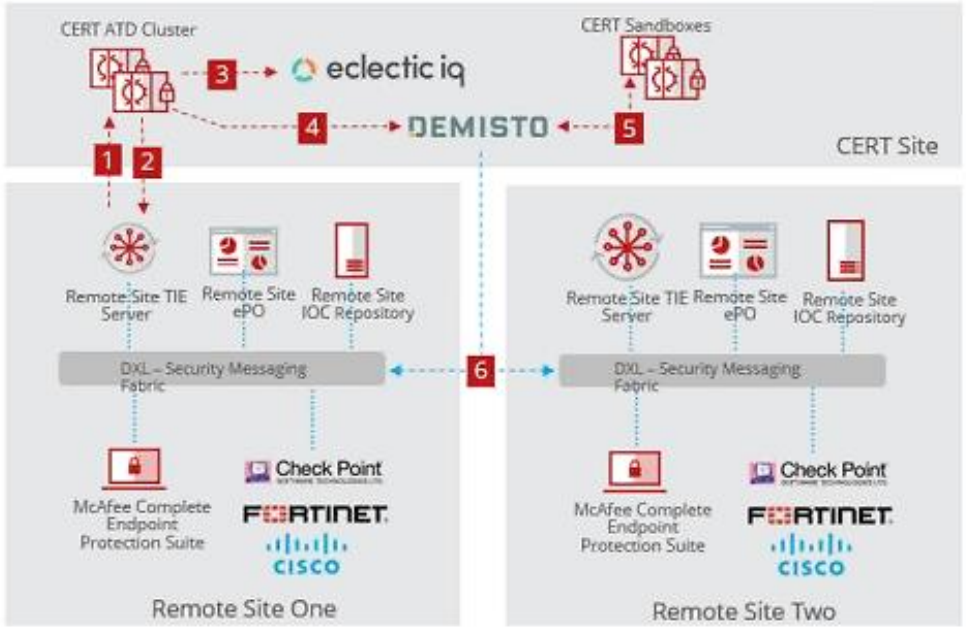
- Open Source and Commercial
- Used to extend Sec Ops solutions
- Improve the value of our Endpoint solutions

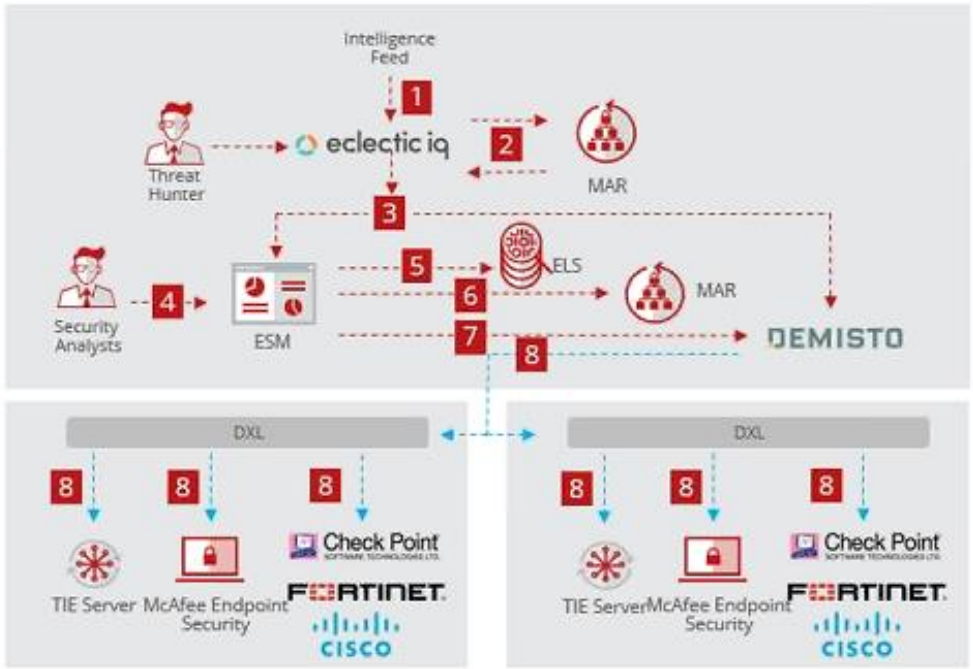
Multi-Agency Threat Intel Sharing

- National CERT
- Large Government or Enterprise customers
- MSSP

External Asset Locations

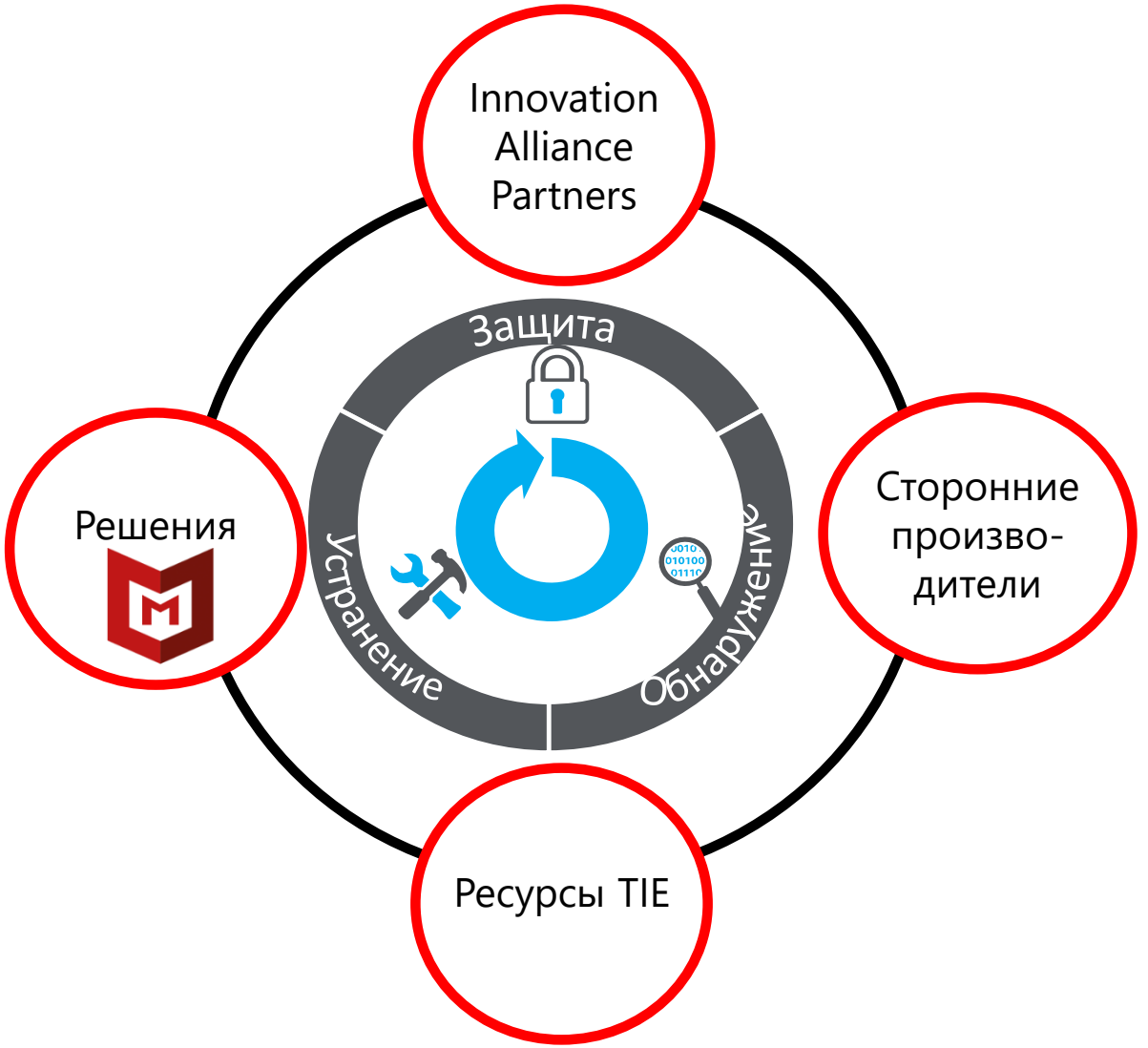
https://github.com/mohlcyber/OpenDXL-ATD-Demisto





Видение экосистемы «Адаптивная Архитектура Безопасности»

Новая эра в безопасности, где все компоненты объединяются, чтобы работать как единая сплоченная система, независимо от поставщика или базовой архитектуры



Присоединяйтесь!

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