



5 принципов построения интеллектуального SOC



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>



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 Alert State

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

Click for alert details



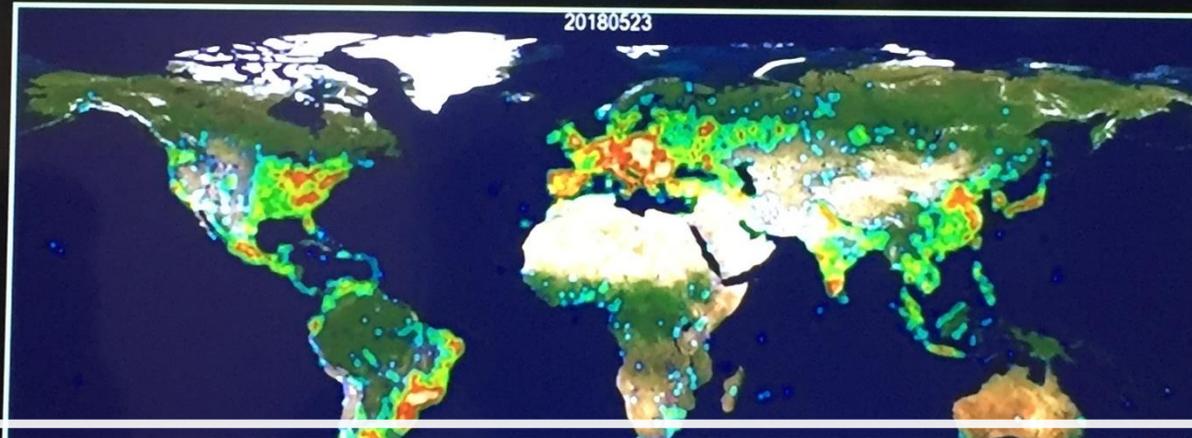
Virus News

Troj/Fareit-EYG [More...](#)

Troj/Remcos-BV [More...](#)

Troj/IDELI-EEV [More...](#)

Security News



McAfee Security Fusion Centre

When Securing Customer Loyalty Becomes Critical

[More...](#)

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	1048
Cisco Sourcefire	22May18	05-21-001
Sniper IDP	22May18	#3067
McAfee NSP	22May18	9.8.23.2
Proventia NEW	17May18	3805.15183

Team Cymru Malicious Activity Map

[Useful Links](#)



McAfee® Security Fusion Center

- Cybersecurity Operations
- Federal Security
- Physical Security
- Security Threat Intelligence

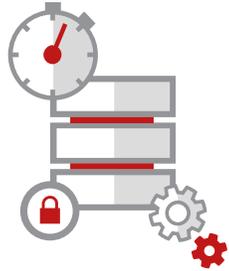


- Обеспечивает:
 - Мониторинг, расследование и устранение инцидентов ИБ
 - Физическая безопасность
 - Федеральная безопасность
 - Сбор и обмен данными Threat Intelligence
- 365/24/7
- Плано, Техас, США и Корк, Ирландия

Требования и задачи интеллектуального iSOC



SOC·FORUM

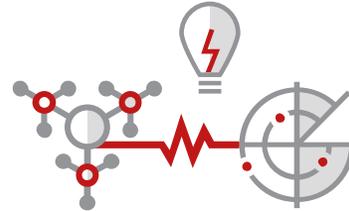


Использование
большого объёма
собираемых данных

Сбор из множества
источников

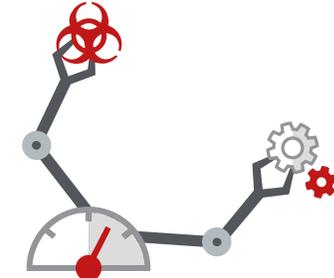
Использование «сырых»
данных для анализа

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

The Five Characteristics of an Intelligence-Driven Security Operations Center



ARCHIVED Published: 02 November 2015 ID: G00271231

Analyst(s): [Oliver Rochford](#) | [Neil MacDonald](#)

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 SOC's use tools, processes and strategies to protect against modern threats.

Table of Contents

- Introduction
- Analysis
 - Use Threat Intelligence Strategically and Tactically
 - Threat Intelligence Platforms (TIPs)
 - Use Advanced Analytics to Operationalize Security Intelligence
 - Technology Options
 - Automate Whatever and Whenever It Is Feasible

Already have a Gartner account?

Sign in to view this research document.

Enter Username

Enter Password

SIGN IN

Forgot [username](#) or [password](#)?

Purchase this Document

Price: \$1,295.00 USD (PAGES: 12)

To purchase this document, you will need to register or sign in above.

REGISTER NOW

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 SOC's 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

McAfee
Global Threat
Intelligence



IOC/ IOA

- IP
- Домен
- Хеш файла
- email

iSOC



VirusTotal

IOC/ IOA

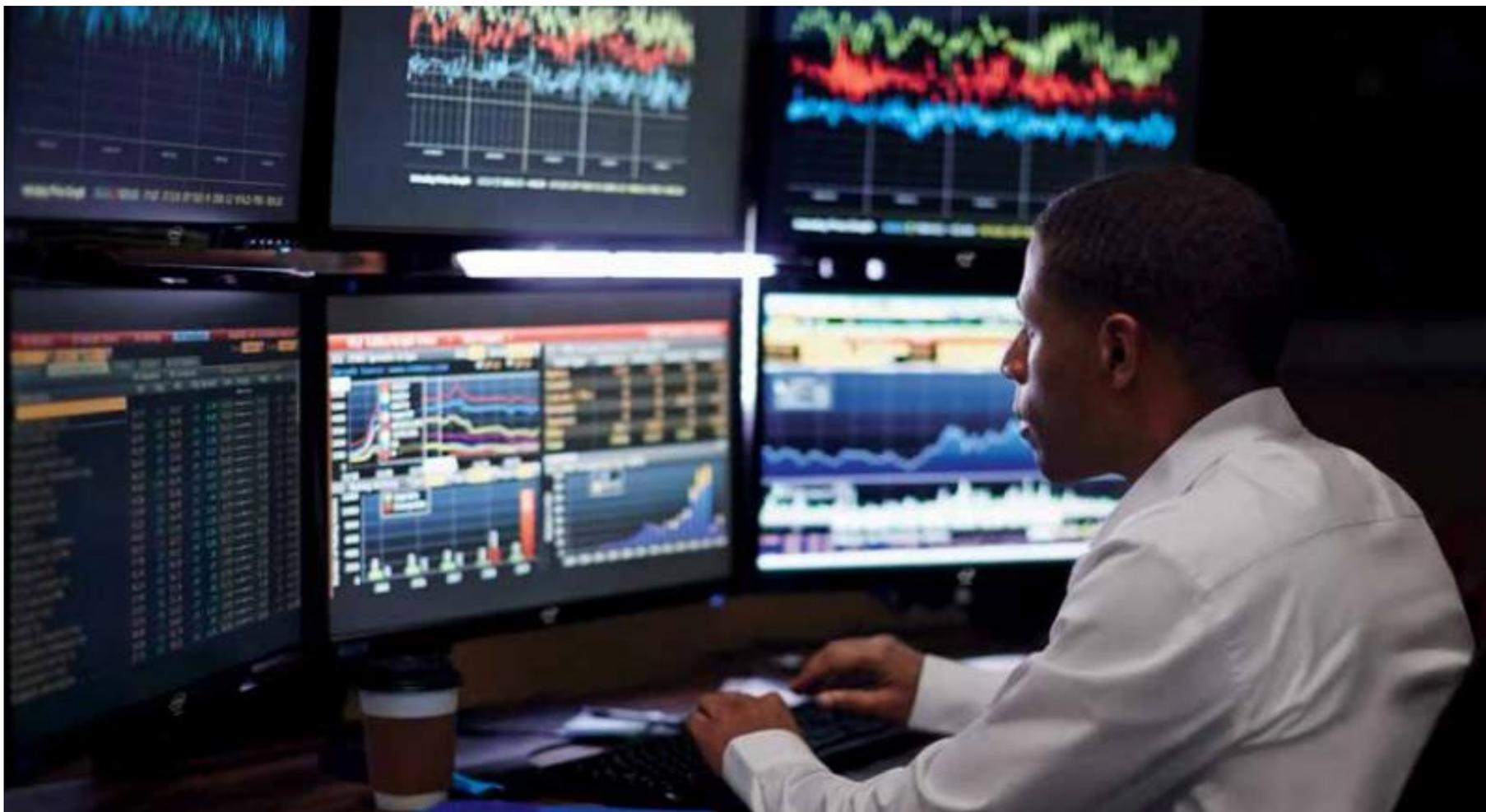
... SOC

NORSE

CERT

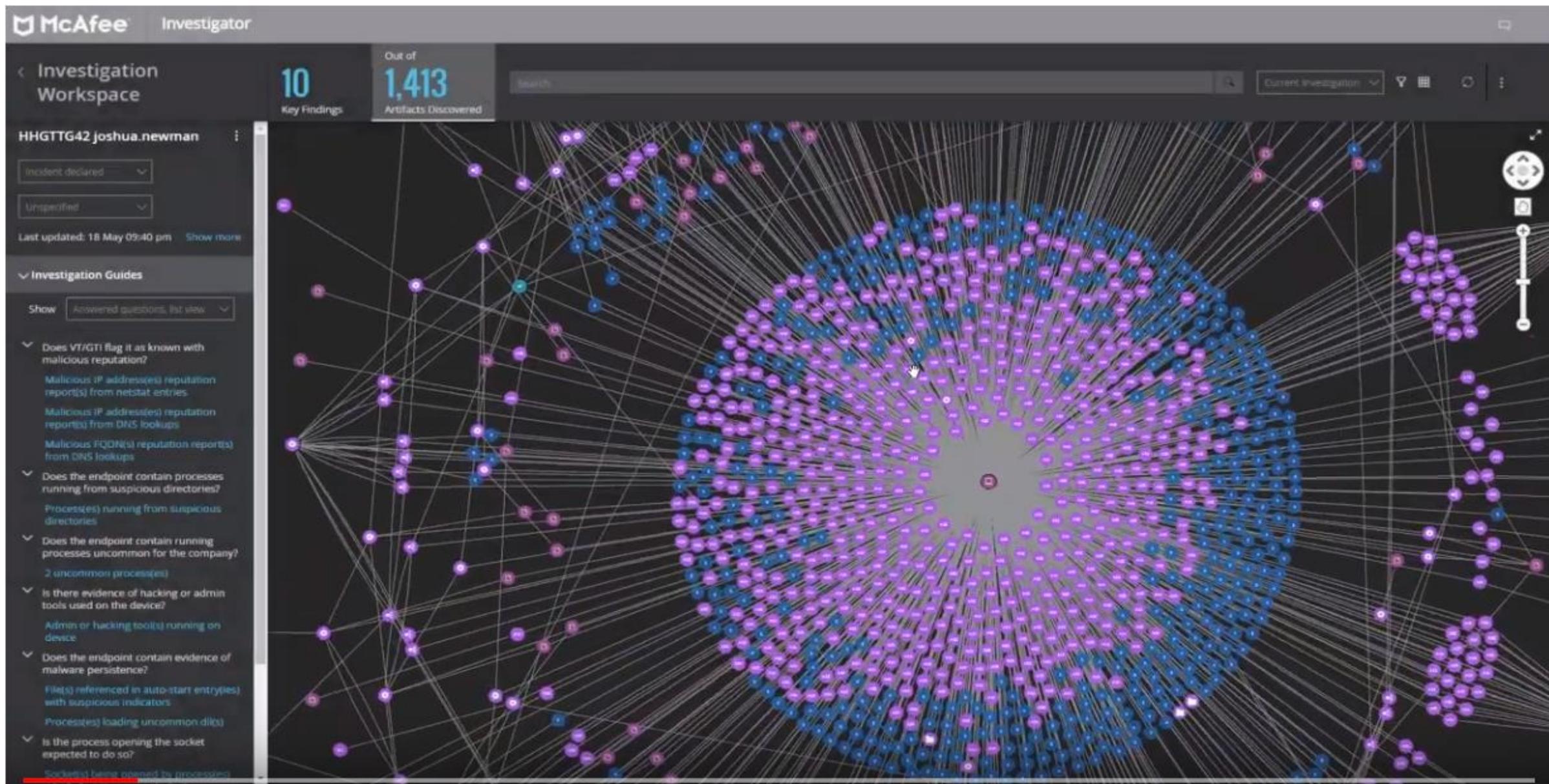
Пять принципов построения интеллектуального iSOC

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

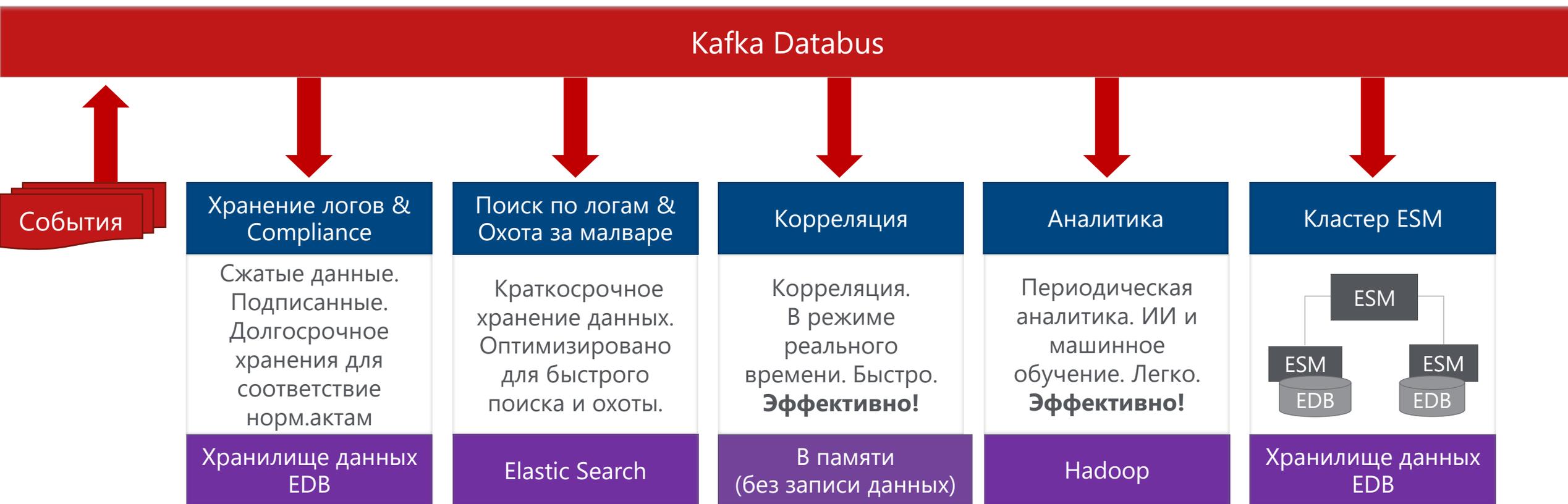
The screenshot displays the McAfee Investigator interface. At the top left, the McAfee logo and 'Investigator' are visible. The main workspace is titled 'Investigation Workspace' and shows '10 Key Findings' and '1,413 Artifacts Discovered'. A search bar and 'Current Investigation' dropdown are also present. The left sidebar contains 'Investigation Guides' with a 'Show' dropdown set to 'Answered questions'. Below this, there are sections for 'Analyst guide' and 'Malware alert triage'. The 'Malware alert triage' section is expanded, showing several questions and their corresponding answers, such as 'There is a security threat, we can confirm malicious activity' and 'Does the endpoint contain evidence of suspicious outbound network connections?'. The central area features a complex network diagram with various nodes and connections, including labels like 'ASD', 'run5dm', and 'ASD'. The right sidebar is titled 'Process Details' and shows 'No available actions'. Below this, it lists details for a process named 'ahxbnblq.exe', including 'processId: 6700', 'commandLine', 'publisher', 'description', 'product', 'version', 'fileVersion', 'createTime', and 'rawData'. There are also expandable sections for 'Suspicious indicator', 'Prevalence', and 'Evidence Notes'.

Платформа для обработки Big Data



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

SOC·FORUM



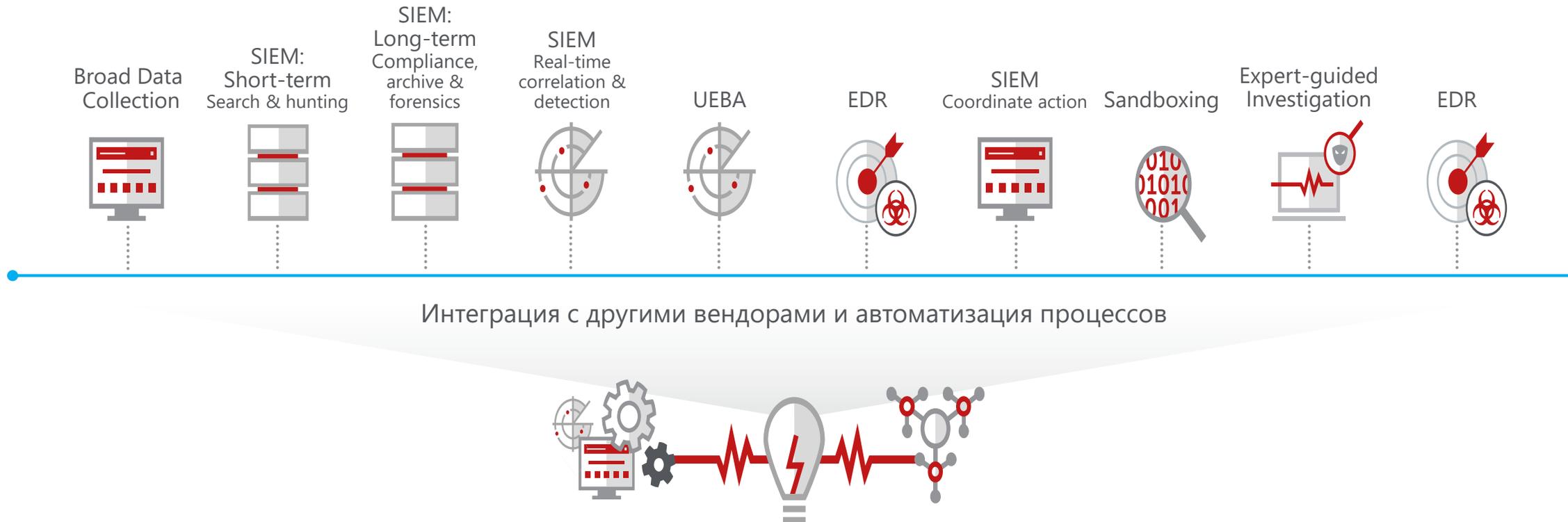
Пять принципов построения интеллектуального iSOC



SOC·FORUM

3. Автоматизация процессов

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



Примеры автоматизации (интеграция с openDXL и pxGrid)



SOC FORUM



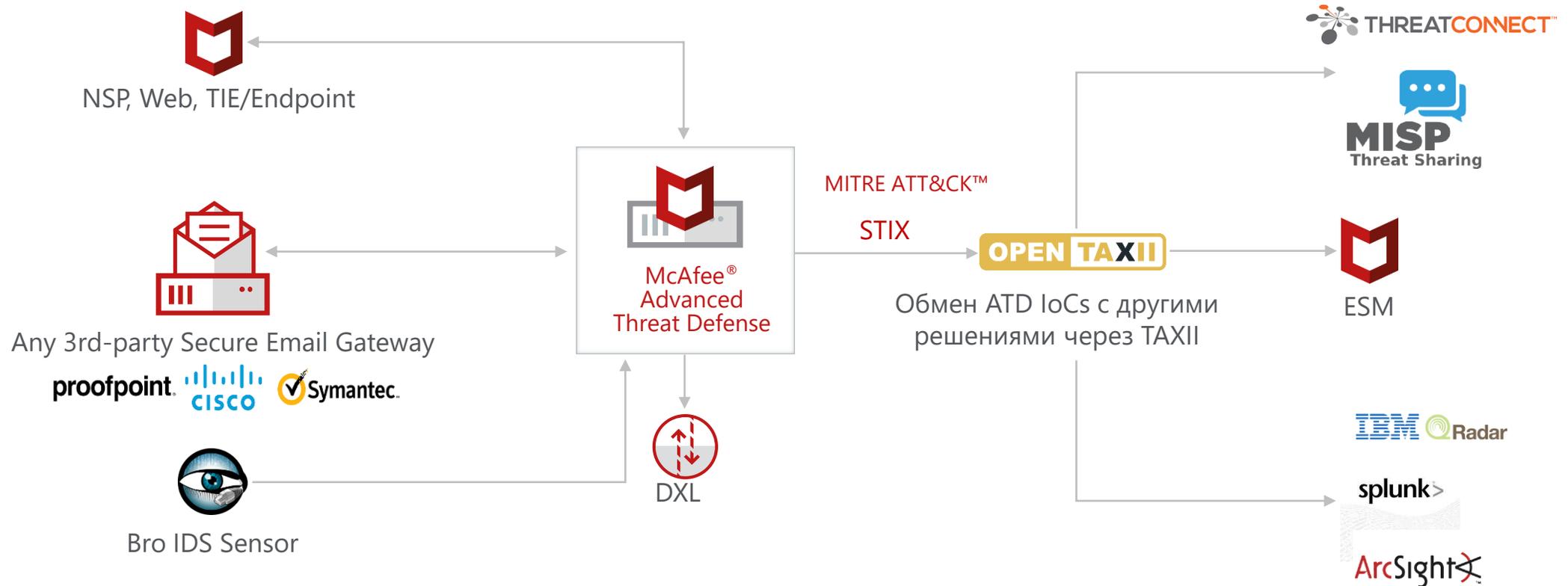
https://www.cisco.com/c/dam/m/en_us/products/security/technical-alliance-partners/core/assets/pxgrid-mcafee-opendxl-integration-aag.pdf

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
MDS Hash Identifier	E2CFE1CB9703352C42763E48459FC356		
SHA-1 Hash Identifier	FD384A9FCFF228F4C371EF3BCA693A9A336D64B7		
SHA-256 Hash Identifier	258E08D6193BCE5856A22482D9F6954911AD81D582ABAE95EBDF0BE578D8975		
	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

```

169 :00401001 3316          xor esi,esi
170 :00401003 397424 0c     cmp dword ptr ss:[esp+0c],esi
171 :00401007 57           push edi
172 :00401008 74 07       jz short 00401011
173 :0040100a 68 1ce04000 push 40e01c
174 :0040100f eb 05       jmp 00401016
175
176 :00401011 68 18e04000 push 40e018
177
178 :00401016 68 10e04000 push 40e010
179 :0040101b ff15 18814000 call dword ptr ds:[408118]
180
181 :00401021 8b f0       mov esi,eax
182 :00401023 59         pop ecx
183 :00401024 3b fe     cmp edi,esi
184 :00401026 59         pop ecx
185 :00401027 75 04     jnz short 0040102d
186 :00401029 33c0      xor eax,eax
187 :0040102b ab 34     jmp 00401061
188
189 :0040102d 397424 10     cmp dword ptr ss:[esp+10],esi
190 :00401031 57         push edi
191 :00401032 6a 01     push 1
192 :00401034 68 0c300000 push 30c
193 :00401039 ff7424 18     push dword ptr ss:[esp+18]
194 :0040103d 74 08     jz short 00401047
195 :0040103f ff15 14814000 call dword ptr ds:[408114]
196
197 :00401040
198 :00401040
199 :00401040
200 :00401040
201 :00401040
    
```

```

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

MITRE ATT&CK™ mapping

McAfee MITRE ATT&CK mapping dashboard showing Tactics (8) and Techniques (24). The dashboard includes a table with columns for Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, and Command and Control. Each cell contains a color-coded icon representing a specific MITRE ATT&CK technique.

Threat Timeline

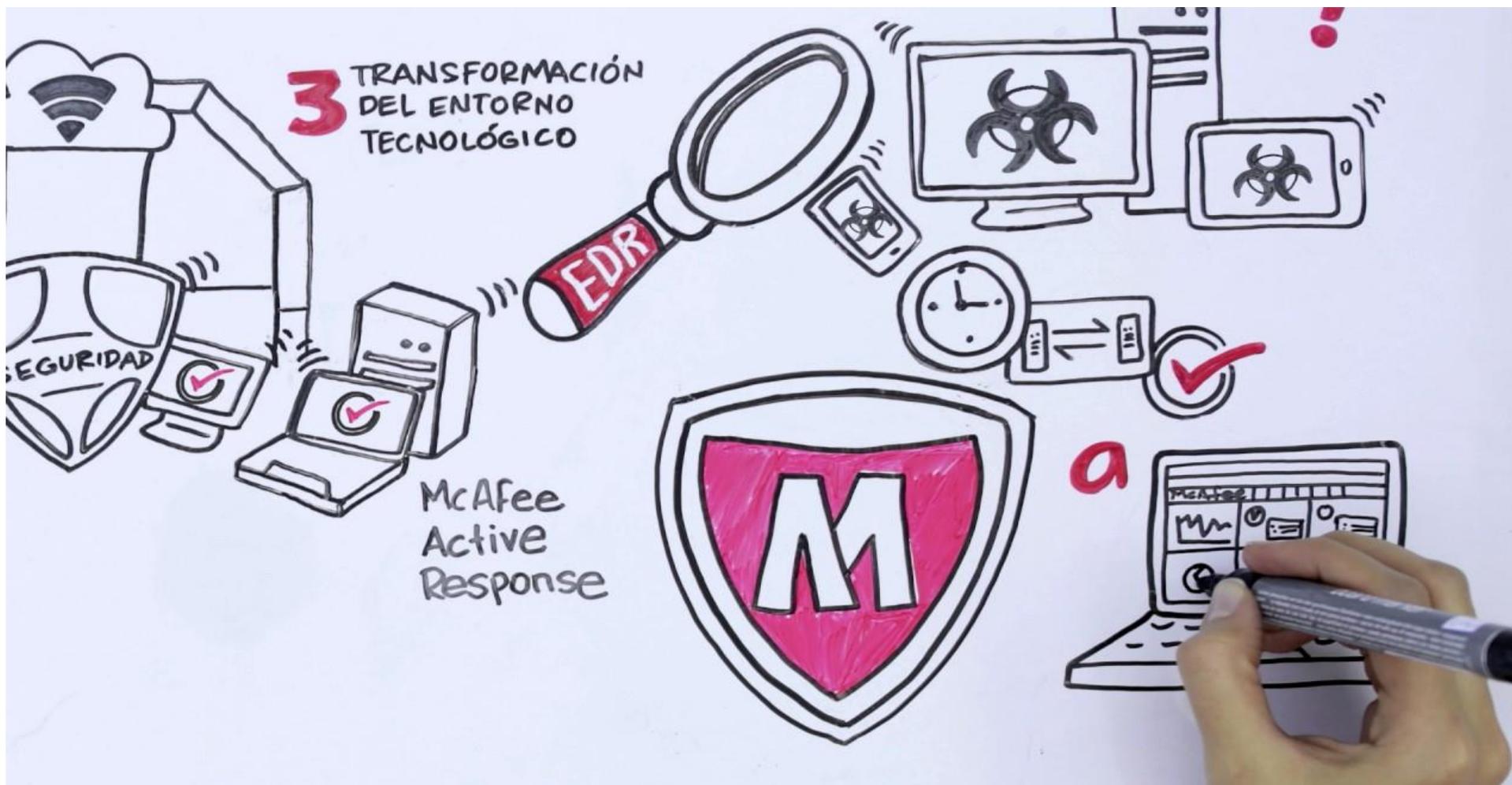
Threat Timeline chart showing Timeline Activity. The x-axis represents Offset in seconds (0 to 30). The y-axis shows various operations: Processes, Files, Registry Operations, Network Operations, and Multiple Operations. A prominent orange bar indicates a significant activity period between approximately 15 and 25 seconds.

Пять принципов построения интеллектуального iSOC



SOC-FORUM

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



MVISION EDR – поиск в режиме реального времени

The screenshot displays the McAfee MVISION EDR Real-time Search interface. At the top, there is a search bar with the text "Click Search to get results." Below the search bar, a dropdown menu is open, showing a list of search criteria options: "Processes", "Process history", "CurrentFlow process_id", "CurrentFlow process", "EnvironmentVariables process_id", "Files create_process_pid", and "Files create_process_sha256". The search query entered is "Processes name where Processes.threadcount greater than 3".

Below the search bar, a table of search results is displayed. The table has columns for "md5", "sha256", "sha1", and "count". The results list various system processes and their corresponding hashes and counts.

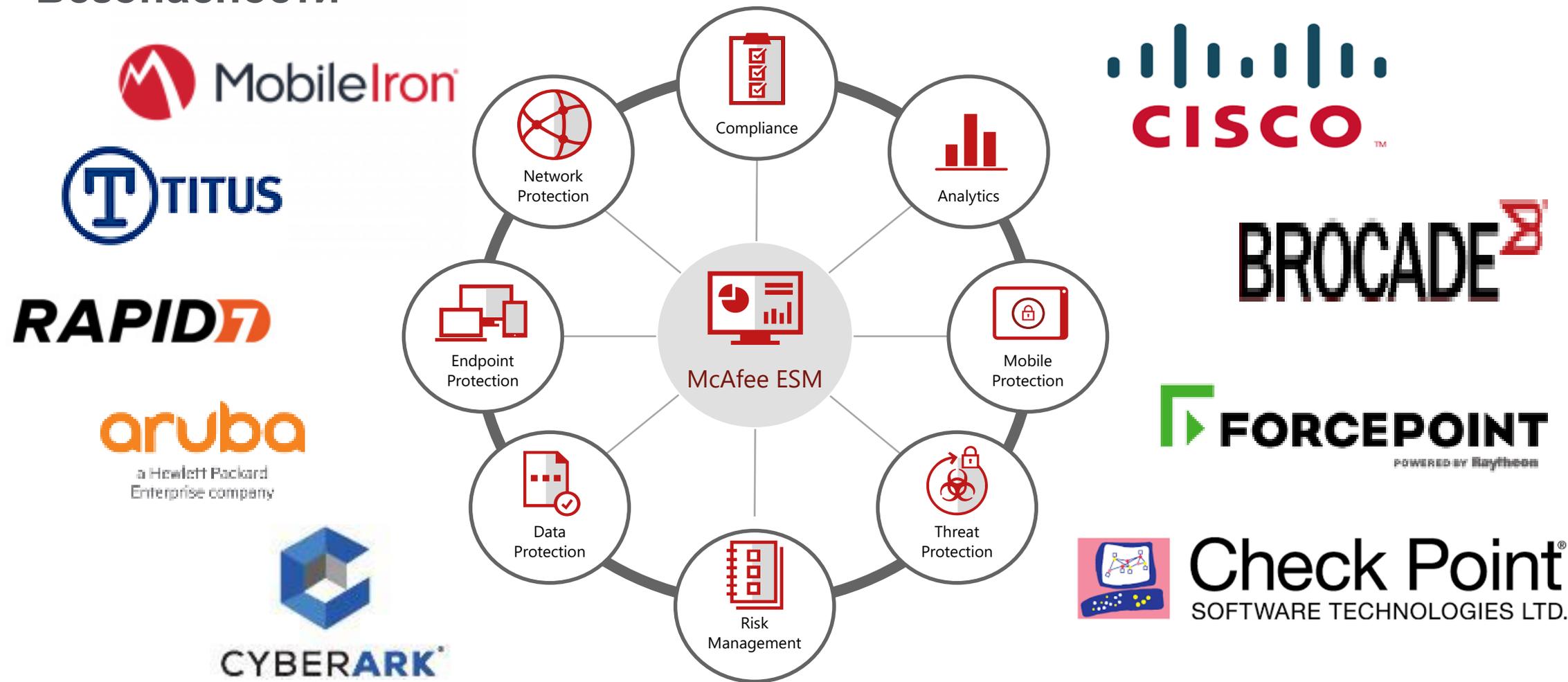
md5	sha256	sha1	count
C7E3684A5D9E6AC600D07AD60052D4C5	5C3AC5C17B10C47EFFFF95687B629877E	12124C44EC062C966FF72E4FB7C5E6782E	12
2A4058E70F07924628EF26F7C8323515	CA910C559714F29E065C141533251C0FF	62BF7713E837532CEFD8C5A8D76FB0FC3E	4
90568EF05C6AEF3D05877707029F85F8C	D8FF3595F3E3C43C84F400AF47A187227C	04CDD04EE996FA2CDE5481E41B12D9E3E	4
F759228C5934E98F330BAA188F33873A	8E57CC1186FE66FC94CAD09F093715616C	278533C2A1CBF84E81F2560B47006F1E81	4
A41E8CE3717A4B0FA145C67616A9E98E	38CFBF9913346CE067F23006909BD211DC	6FC15FCE13E0E9E92803C1FE43D258882A	4
B443AE3895A6E3886820703607B886CB	D7707881E5C36D04E00DF3F49F68B43B	E91C8858D0868217617402EE7111758408	3
773670E7F1D33CF1223F60793A805441	5A3A50AF7698DF0CC3AF00F838C584F	B31CD468734C88246827037D4C17E8F7F	3
62887353A86E3C6DC8D013CDE710922B	4FFB6354776FE651226E4ACFC7CC97A55	38C7D454EC686D60EBAE33EC999C8A02C	3
		[SYSTEM PROCESS]	3
90568EF05C6AEF3D05877707029F85F8C	D8FF3595F3E3C43C84F400AF47A187227C	04CDD04EE996FA2CDE5481E41B12D9E3E	3
FF59CBFB210F6C7550CF22239228A15	1793608817FE948B3E21E052C96C01AC37	DDAF6A751D187792CC5E31ABF71FDAB4F	3
3614BE6974877C5D7D85D96E36D76042	A484F3017C7D7E732228FED9A8A06CC5D0	E55C113A451B31BFD3858CEB82195E88C	3
		SYSTEM	3
2686CE1289A20ACB0CC8D473491519A5	F825F76E707CDFC6D33232885D86ADB4	0D5G3DF8672DF418E5D7A67CBDD4F305C	3

Пять принципов построения интеллектуального iSOC

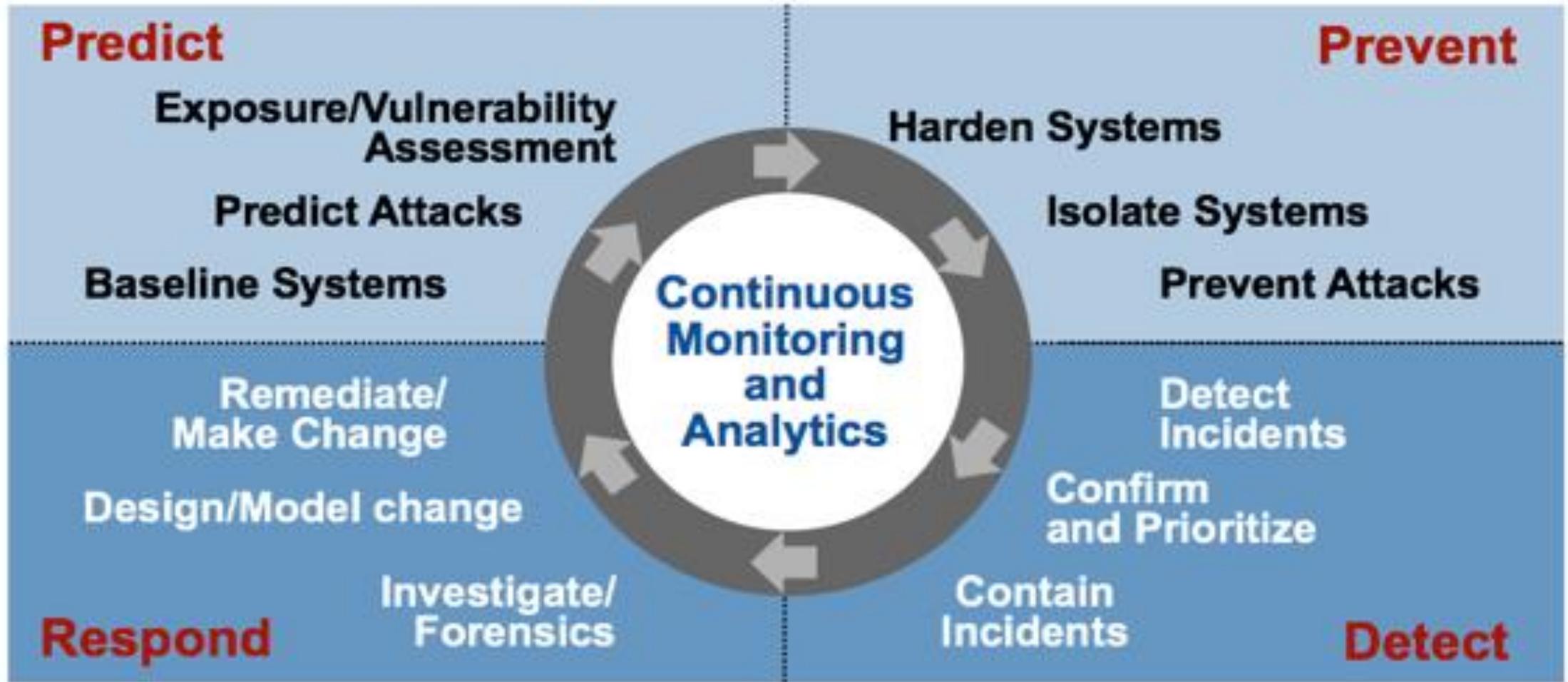


SOC-FORUM

5. Построение и использование Архитектуры Адаптивной Безопасности



The Adaptive Security Architecture: Twelve Critical Capabilities of Security



Gartner.



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.

Экосистема McAfee



IDC ExpertROI Spotlight Top 100 US FDIC Bank



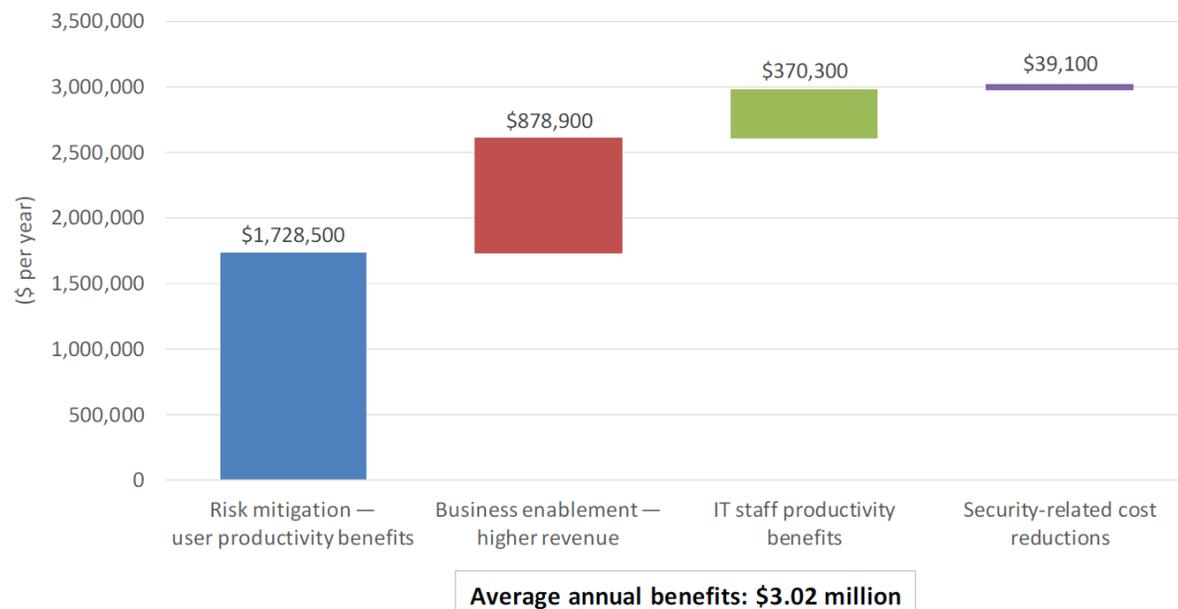
SOC-FORUM

“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

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



SOC-FORUM



McAfee Threat Intelligence Exchange DXL

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

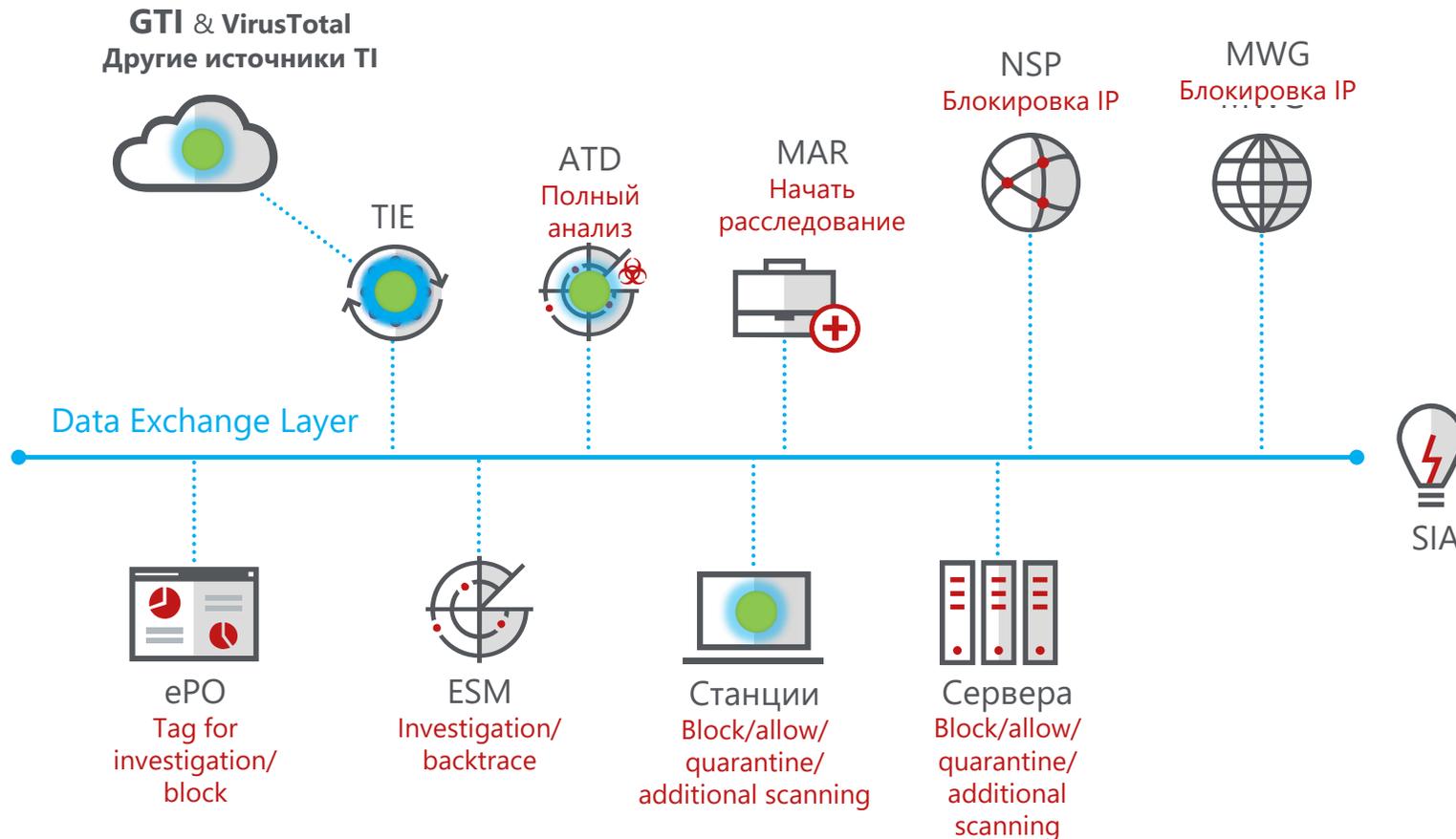
Actions | 13 items

McAfee Adaptive Security Architecture

Постоянный обмен репутациями (IOC) по всей экосистеме



SOC-FORUM



Интеграция по шине DXL



SOC-FORUM

SIA
Partners



- SandBlast integration with DXL, TIE and ePO
- Publishing Topics: File Reputation, IOC, Threat Event Data, Mobile
- Subscribing Topics: IOC, File Reputation Updates



- ClearPass integration with DXL and ePO
- Publishing Topics: IOC Information, New Asset Discovery Information
- Subscribing Topics: IOC information, Threat Event



- Nexpose integration with DXL, TIE and ePO
- Publishing Topics: IOC, Vulnerability, New Asset Discovery Information
- Subscribing Topics: IOC, File Reputation, Threat Event, Vulnerabilities



- Deception Grid integration with DXL, TIE and ePO
- Publishing Topics: File Reputation, IOC, Threat Event Data
- Subscribing Topics: IOC, File Reputation, Threat Event



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

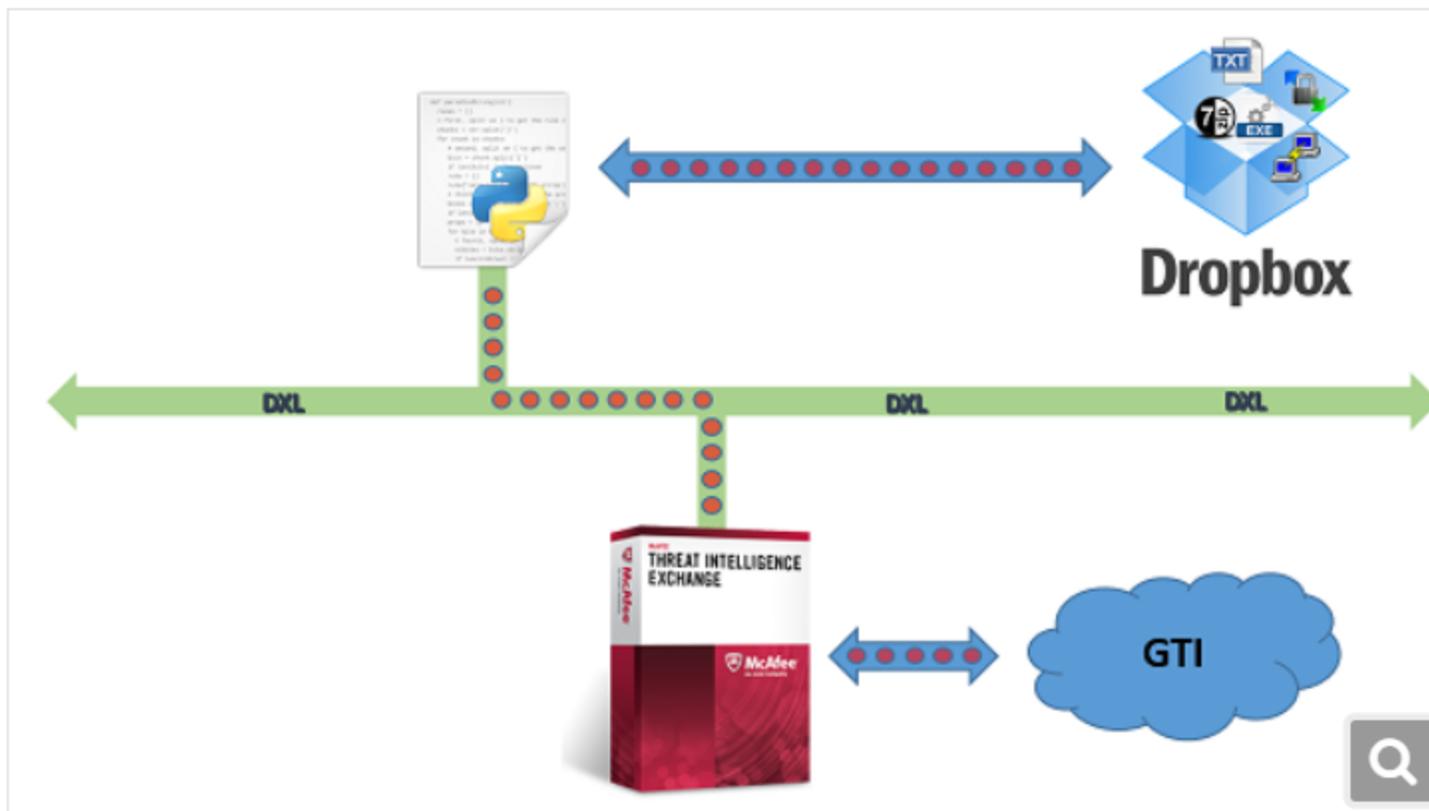


SOC-FORUM

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



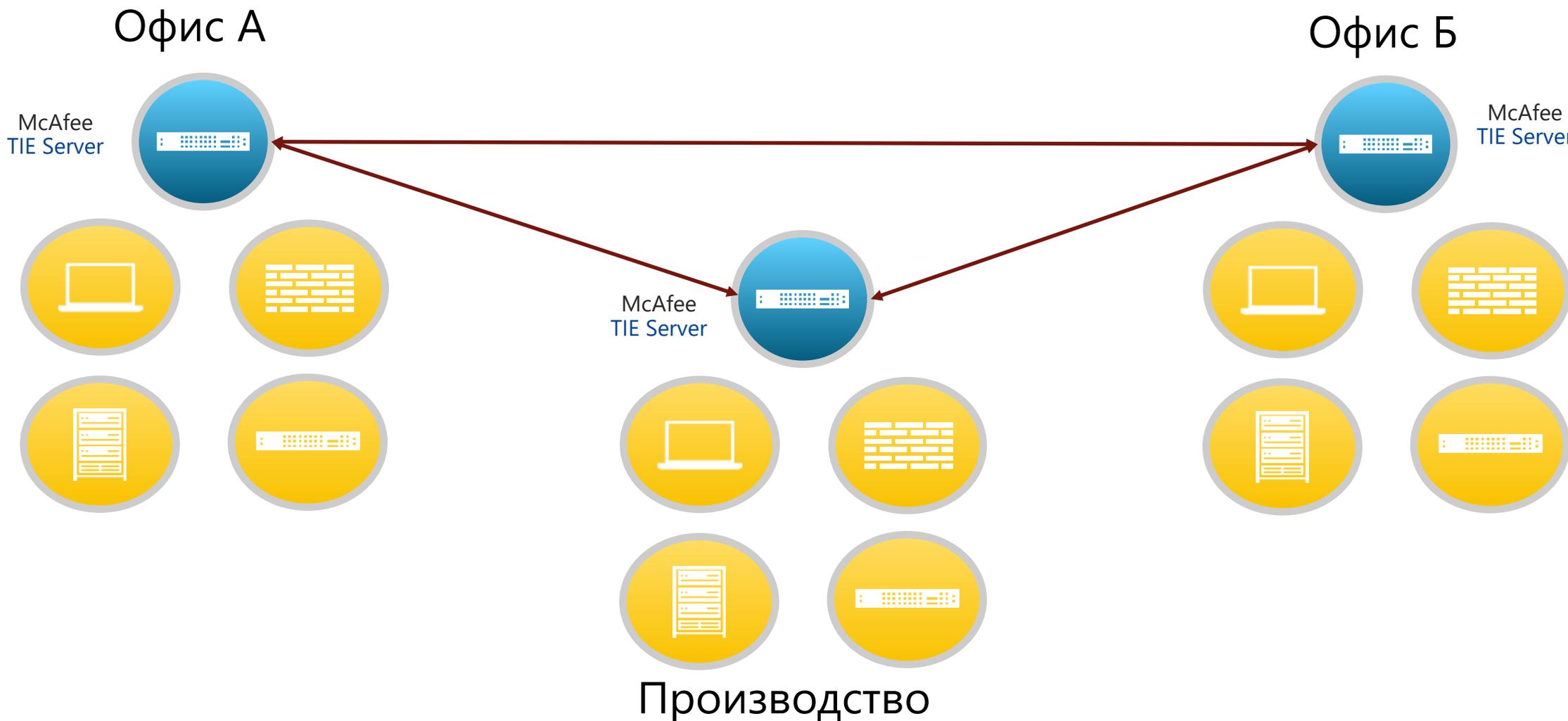
Адаптивная безопасность для корпораций и государства

Защита корпорации



SOC FORUM

Адаптивная защита – от обнаружения до защиты за секунды

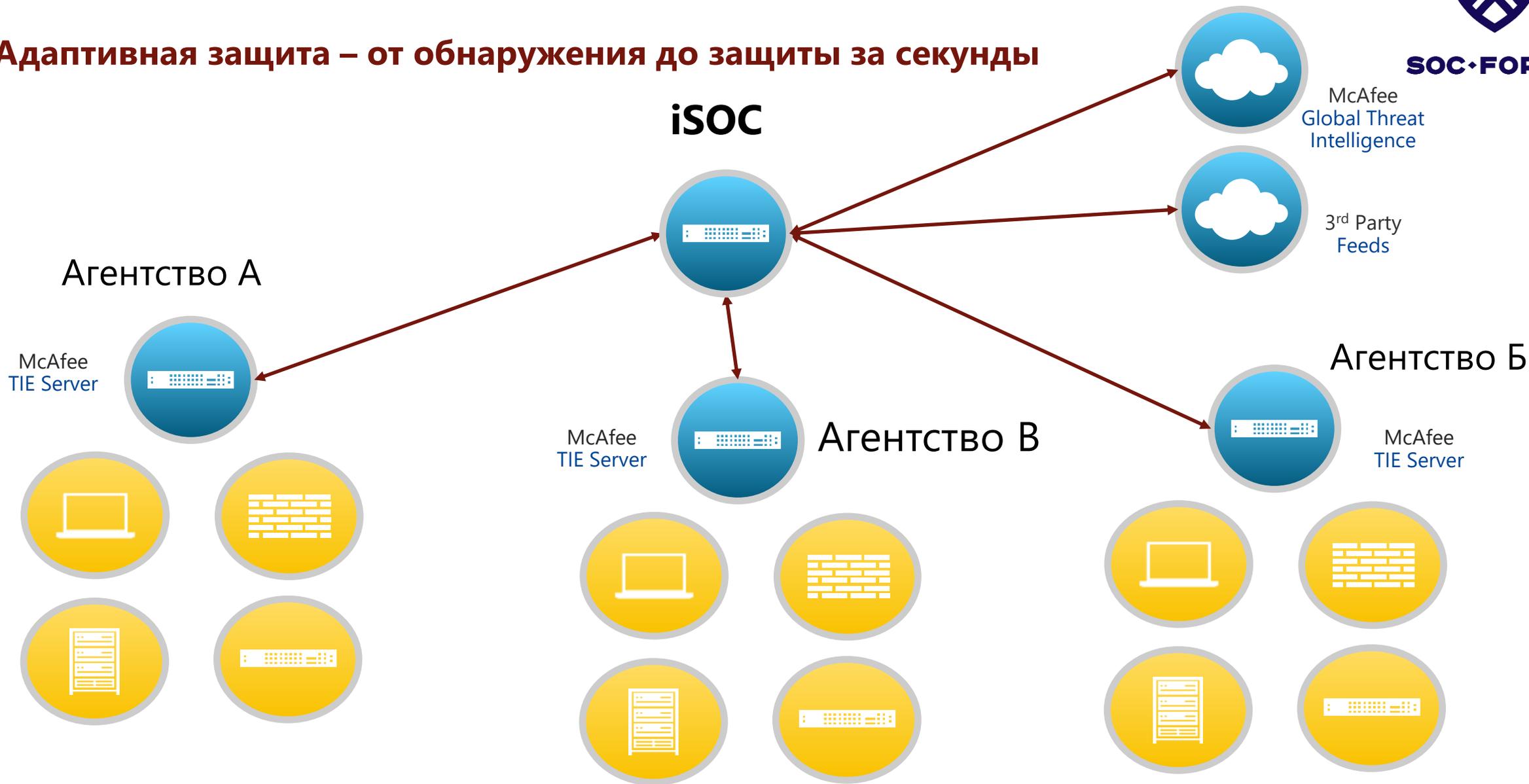


Защита для всего государства



SOC-FORUM

Адаптивная защита – от обнаружения до защиты за секунды



Solution Architecture

Advanced Threat Intel Use Case

Threat Intelligence and Orchestration Platforms

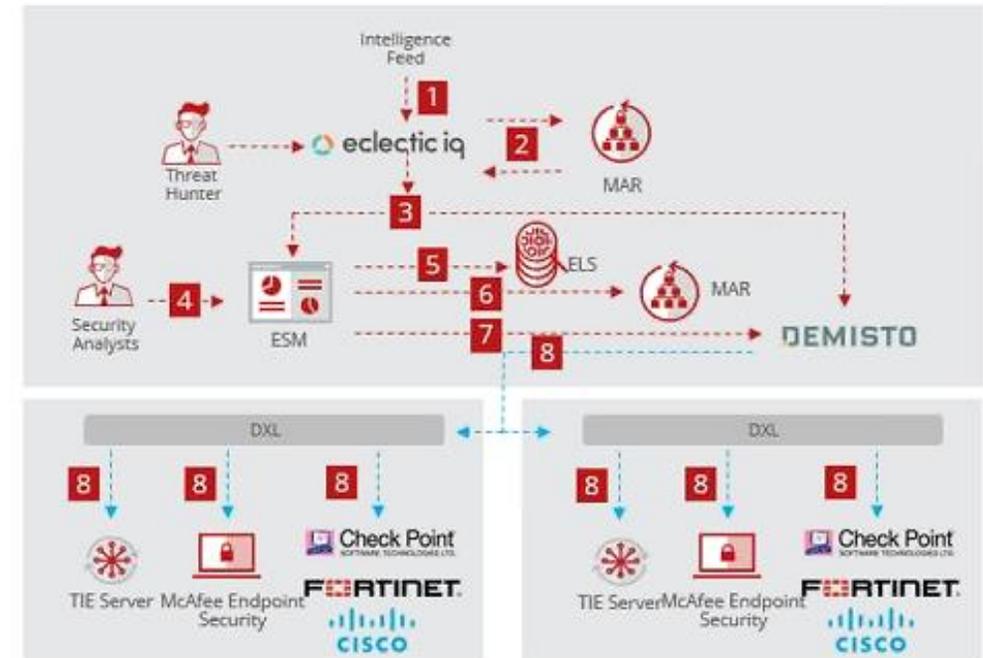
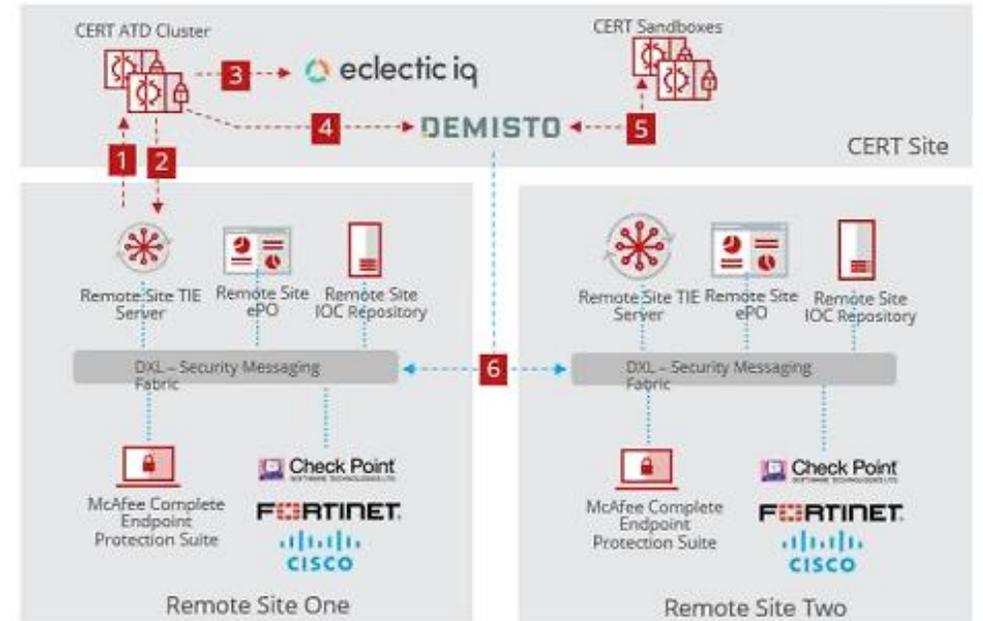
- Open Source and Commercial
- Used to extend Sec Ops solutions
- Improve the value of our Endpoint solutions

Multi-Agency Threat Intel Sharing

- National CERT
- Large Government or Enterprise customers
- MSSP

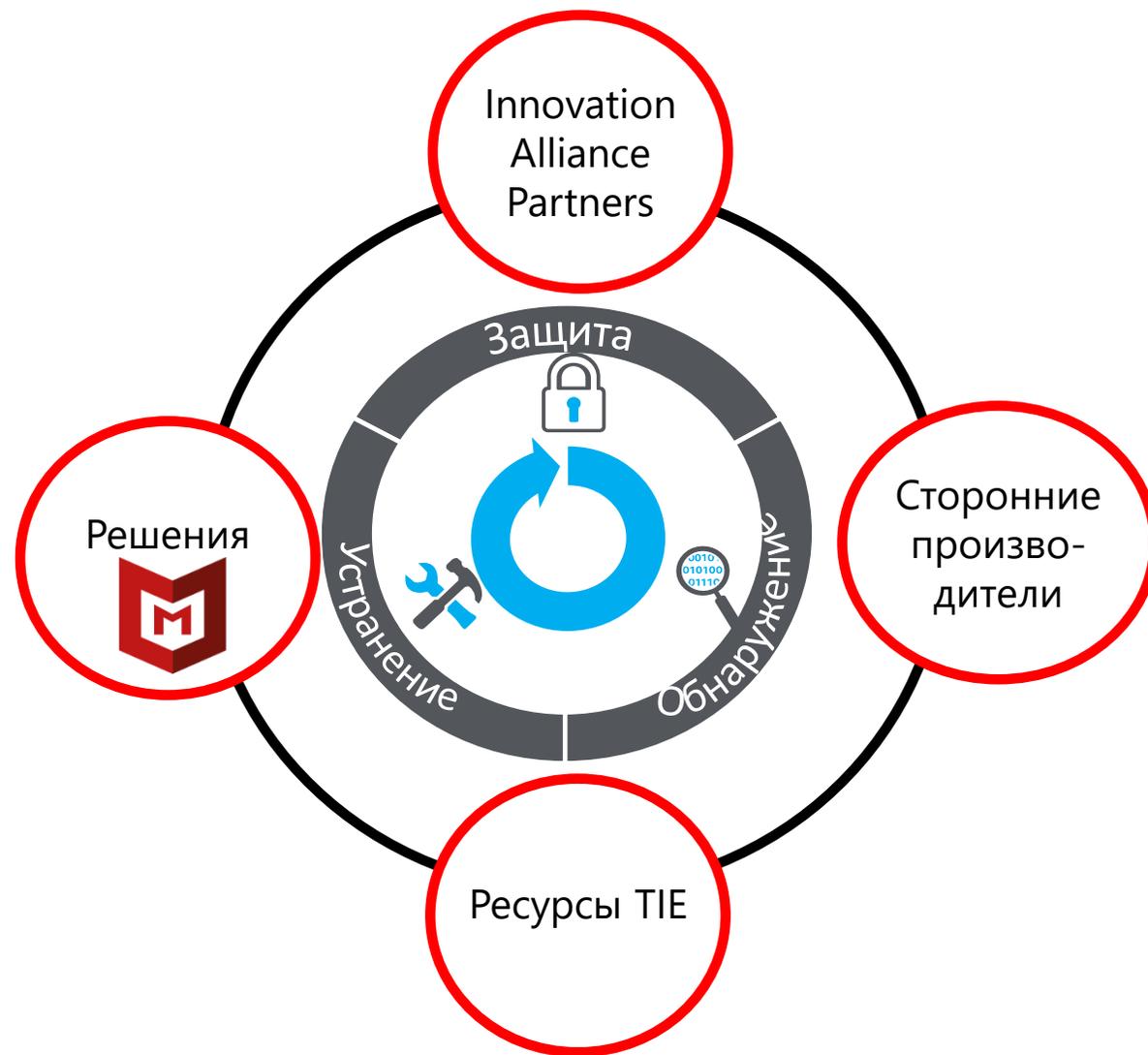
External Asset Locations

<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”***





McAfee, the McAfee logo and [insert <other relevant McAfee Names>] 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.