



Комплексная архитектура информационной безопасности

Взгляд McAfee на современные подходы ИБ

Николай Метёлкин | Представитель McAfee



О компании McAfee



- Обеспечивает безопасность более 250 млн конечных точек
 - Крупнейший в мире разработчик
 - Только кибербезопасность
 - McAfee GTI ежедневно появляется более 500 000 новых угроз
 - В компании McAfee работает более 7 500 опытных специалистов по кибербезопасности
 - Главный офис - Santa Clara, California
-
- Комплексность и эффективность
 - Открытая платформа
 - Портфолио
 - Лидирующие позиции

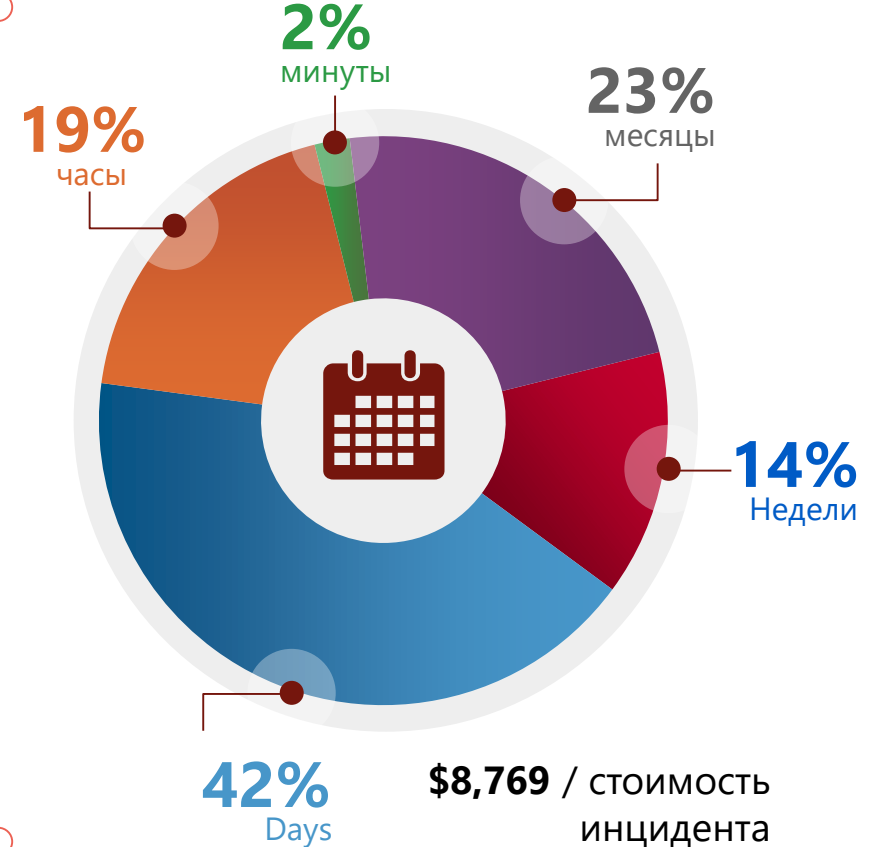
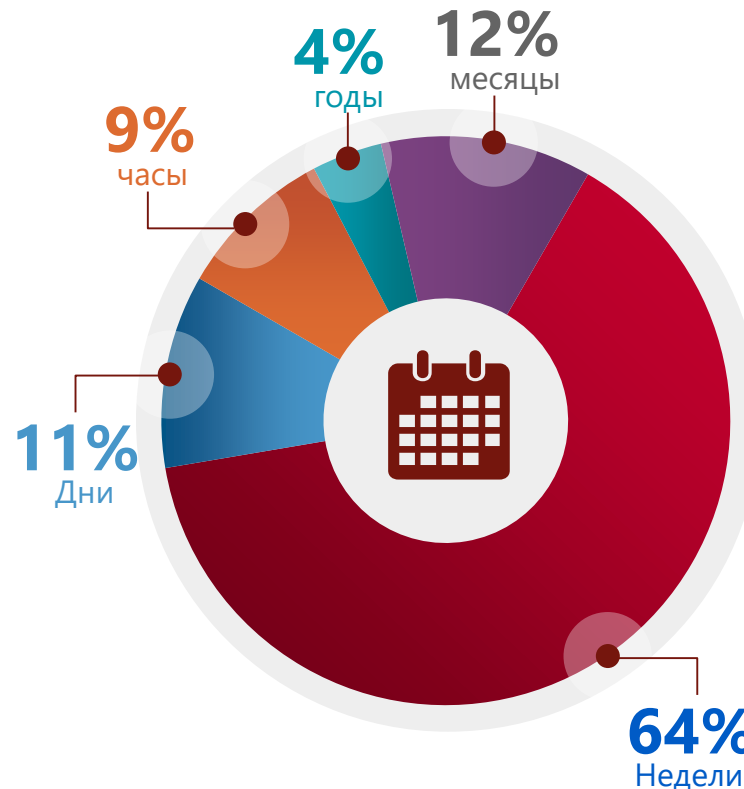
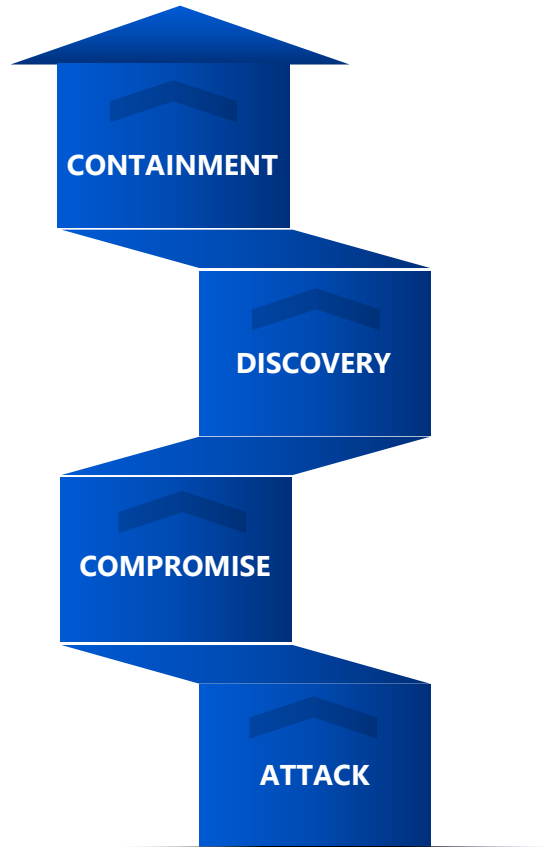
Проблематика

Целенаправленные атаки – новая реальность

APT

Обнаружение

устранение



\$8,769 / стоимость инцидента
\$3,840,988 / в год

Sources: Verizon Data Breach Investigations Report. Securosis Malware Analysis Quant Metrics Model

Проблематика

Целенаправленные атаки – новая реальность

АРХИТЕКТУРА

АВТОМАТИЗАЦИЯ

ИНТЕГРАЦИЯ

ТЕХНОЛОГИИ

ПРОЦЕССЫ

ЛЮДИ



Проблематика

Дефицит кадров в сфере кибербезопасности на уровне эпидемии

Нехватка профессионалов в области кибербезопасности влияет на возможности организаций управлять безопасностью своих все более усложняющихся информационных сетей.

82%

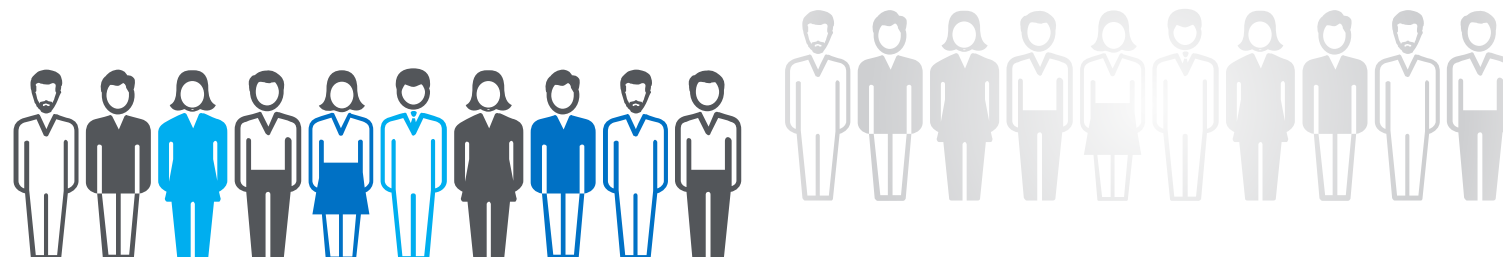
респондентов со всего мира сообщили о дефиците специалистов по кибербезопасности в своей организации *

71%

признали, что из-за недостатка кадров организации становятся более уязвимыми для злоумышленников. *

1,8 Млн.

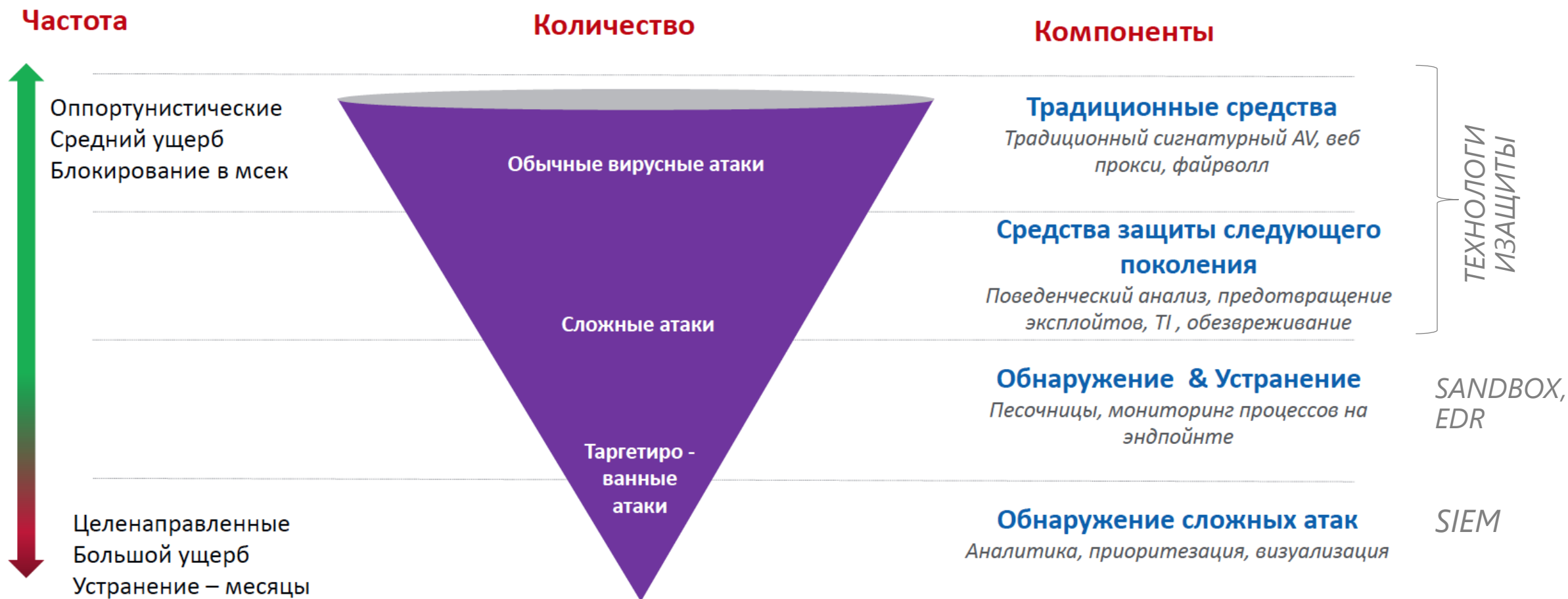
к 2022 году нехватка специалистов может достичь 1,8 миллиона человек **



- * Исследование McAfee и Центра стратегических и международных исследований (CSIS — Center for Strategic and International Studies), Hacking the Skills Shortage (Нехватка специалистов как уязвимость)
- ** Global Information Security Workforce Study, проведенный организацией (ISC)2

Стратегические инвестиции: взгляд на угрозы

Соответствие вложений сложности атаки



Позиция McAfee соответствует рекомендациям ведущих аналитиков

Verizon Report Recommendations

- Eliminate unnecessary data
- Collect, analyze, share
 - Incident data
 - Threat intelligence
- Focus on better and faster detection
- Evaluate threat landscape

What can we do about it?

- ✓ Eliminate unnecessary data; keep tabs on what's left.
- ✓ Ensure essential controls are met; regularly check that they remain so.
- ✓ Collect, analyze and share incident data to create a rich data source that can drive security program effectiveness.
- ✓ Collect, analyze, and share tactical threat intelligence, especially Indicators of Compromise (IOCs), that can greatly aid defense and detection.
- ✓ Without deemphasizing prevention, focus on better and faster detection through a blend of people, process, and technology.
- ✓ Regularly measure things like "number of compromised systems" and "time to detection" in networks, them to drive security practices.
- ✓ Evaluate the threat landscape to prioritize a treatment strategy, buy into a "one-size fits all" approach to security.
- ✓ If you're a target of espionage, underestimate the tenacity of an adversary. Nor should you underestimate the intelligence and tools at your disposal.

Picking over the remains of breach picture of our current state, but it's have said before—we have the tools and using them in the right way. To that end, we're convinced of the value of understanding your enemy. If it is your business, then there's a number of controls on which you can focus. Knowing the attack patterns (and sharing them) can make that work more fruitful. Take steps to better understand your threat landscape and deal with it accordingly. See the Conclusion for tips on threat-centric control prioritization.

We strongly recommend readers consider the detection of failures (in a reasonable time frame) as a success. The security industry has long been overly focused on prevention.

Gartner.
WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT

MCAFEE INTEGRATED THREAT DEFENSE SOLUTION

Essential Capabilities for Analyzing and Protecting Against Advanced Threats

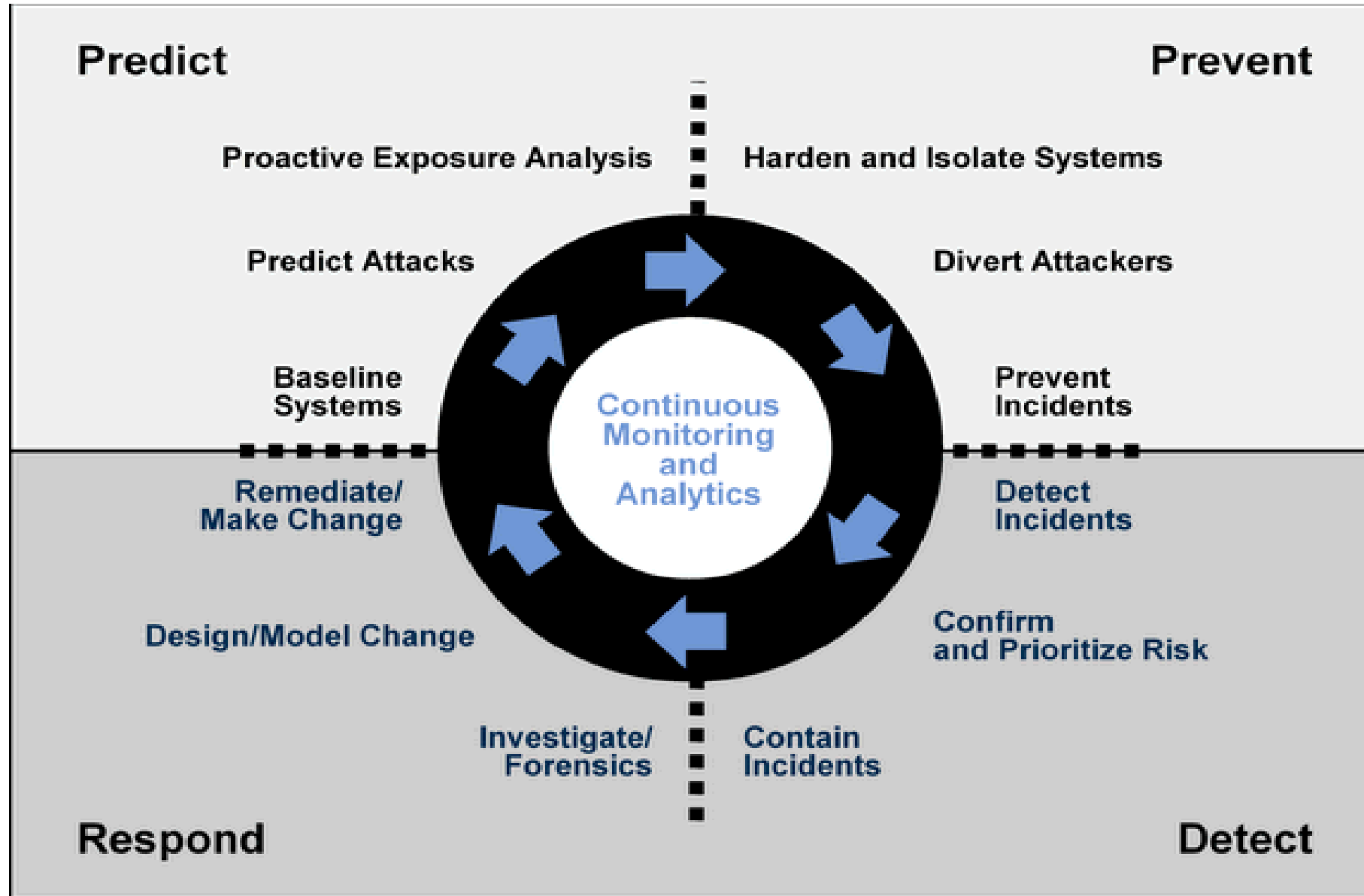
IDC Lab Validation Report

By Rob Ayoub, CISSP, IDC Security Products Team
Sponsored by McAfee | March 2017



The Five Characteristics of an Intelligence-Driven Security Operations Center

Архитектура Адаптивной безопасности



Экосистема McAfee – комплексная архитектура



Сертификация (ДССЗЗІ) продуктов McAfee в Украине

- ЗАЩИТА РАБОЧИХ СТАНЦИЙ
- ЗАЩИТА СЕРВЕРОВ
- РЕШЕНИЕ КЛАССА «ПЕСОЧНИЦА» (SANDBOX)
- ЗАЩИТА ВЕБ ТРАФИКА (Web Gateway)
- РЕШЕНИЕ КЛАССА EDR (Endpoint Detect and Response)
- УПРАВЛЕНИЕ СОБЫТИЯМИ БЕЗОПАСНОСТИ (SIEM)
- ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ И АТАК (IPS)
- ЗАЩИТА ОТ УТЕЧКИ ДАННЫХ (DLP)
- ЗАЩИТА БАЗ ДАННЫХ
- ЛОКАЛЬНЫЙ СЕРВЕР (БАЗА) РЕПУТАЦИЙ

McAfee Insights

The screenshot displays the McAfee Mvision Insights dashboard. At the top, the 'Campaigns & Threats' section features several widgets: 'SECURITY POSTURE SCORE' (74%), 'CAMPAIGNS BY THREAT LEVEL' (7), 'DEVICE STATUS' (7), 'CAMPAIGN DETECTIONS' (5), and 'CAMPAIGNS TRENDING GLOBALLY'. A red callout box points to the 'DEVICE STATUS' widget with the text: 'Вы можете СПРОГНОЗИРОВАТЬ, остановят ли принимаемые вами контрмеры эту угрозу.' Below this, the 'Threats' tab is active, showing 'Requiring Attention (2)' and 'All threats (24)'. A second red callout box points to the 'Requiring Attention (2)' link with the text: 'Вы можете ОПРЕДЕЛИТЬ угрозы, на которые вам следует обратить первостепенное внимание.' The main content area shows a table of threats, with 'Covid-19' selected. A third red callout box points to the 'Actions' column in the table with the text: 'Вы можете ДАТЬ точные указания по корректировке ваших контрмер.' The detailed view for 'Covid-19' includes a 'Severity' of HIGH, a 'Description' of the threat, 'Detected hashes', and a table of 'Detections'.

Threats	Infection Rate	You	Software	Canada	Global	Campaign?	Your Devices	Requiring Iso...	Insufficient Cov...	Last detected
Covid-19						Covid-19		4 !	3 !	a day ago

Severity	Global prevalence	Associated Campaign	Detection type
HIGH	Brazil, China, France, Germany, Italy, Japan + 2 more	Covid-19	Zero-Day

Devices	RealProtect sensitivity	Covered?	Actions
3	Low	Yes	None
2	High	Yes	None
2	Med	No	Enable RealProtect Cloud now

# of detections	Devices	Status	Actions

Threat Intelligence Exchange

Системы
TIE Reputations

File Search Certificate Search File Overrides Certificate Overrides

TIE File Reputations : File Search Скрыть фильтр

Встроенные: All
 Пользовательские: Нет
 Быстрый поиск:
Применить
Очистить
 Показать выбранные строки

<input type="checkbox"/>	All File Names	Company Name	Product Name	File Version	Composite Reputation	Enterprise Reputation	Certificate Enterprise Rep	Latest Local Reputation	Certificate GTI Reputation	GTI Reputation	ATD Reputation	MWG Reputation	External Reputation
<input type="checkbox"/>	AdobeARM.exe	Adobe Inc.	Adobe Reader and Acroba	1.824.39.9311	🟢 Most Likely Trusted (Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	mozavcodec.dll	Mozilla Foundation	Firefox	81.0	🟢 Most Likely Trusted (Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	mozavutil.dll	Mozilla Foundation	Firefox	81.0	🟢 Most Likely Trusted (Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	xul.dll	Mozilla Foundation	Firefox	81.0	🟢 Most Likely Trusted (Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	mozglue.dll	Mozilla Foundation	Firefox	81.0	🟢 Most Likely Trusted (Not Available	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	libEGL.dll		SwiftShader libEGL Dynan	4.1.0.7	⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	libGLESv2.dll		SwiftShader libGLESv2 Dy	4.1.0.7	⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	ffmpeg.dll				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	System.Threading.Tasks.n	Microsoft Corporation	Microsoft® .NET Framewo	4.8.3752.0	🟢 Most Likely Trusted (Not Available	Not Available	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	System.Runtime.InteropServices	Microsoft Corporation	Microsoft® .NET Framewo	4.8.3752.0	🟢 Most Likely Trusted (Not Available	Not Available	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	System.Runtime.ni.dll	Microsoft Corporation	Microsoft® .NET Framewo	4.8.3752.0	🟢 Most Likely Trusted (Not Available	Not Available	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	WinStore.Preview.dll				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	WinStore.App.dll	Microsoft Corporation	Windows Store	12010.1001.2.0	⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	WinStoreTasksWrapper.dll				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.Notifications.di				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.SharedContent				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.Calling.WinRT.c				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.Messaging.Win				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhoneControls.dll				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.Devices.WinRT				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.ScreenMirrorin				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	setup.exe				🟢 Most Likely Trusted (Not Set	Not Set	Most Likely Trusted	Most Likely Trusted	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.Views.dll				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.dll	Microsoft Corporation	Microsoft Your Phone	1.20092.108.0	⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.exe	Microsoft Corporation	Microsoft Your Phone	1.20092.108.0	⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available
<input type="checkbox"/>	YourPhone.AppCore.WinRT				⚪ Unknown (Latest Loc	Not Set	Not Available	Unknown	Not Available	Not Available	Not Available	Not Available	Not Available

Действия Элементов: 5567

Открытая платформа (Open DXL)

- Работа шины на передачу/получение
- Возможность интеграции с другими решениями ИБ
- Обмен ИОС между решениями разных производителей
- MQTT, TLS 1.2, PKI, двухсторонняя СВЯЗЬ

The screenshot shows the OpenDXL Security Intelligence Sharing interface. It features a header with the OpenDXL logo and a navigation menu. Below the header, there are sections for 'Solutions' and 'Filter by Price'. The 'Solutions' section lists various integrations, including 'TheHive DXL' and 'OpenDXL ATD'. The 'Filter by Price' section has buttons for 'All', 'Free', and 'Commercial'. The 'Categories' section is also visible. The main content area displays two solution cards: 'OpenDXL-ATD-Cisco-ASA' and 'OpenDXL-ATD-Fortinet'. Each card includes a 'README.md' link, a license type (Apache-2.0), a description of the integration, a component description, prerequisites, and a diagram showing the flow of data between the components.



Партнеры SIA (Security Innovation Alliance)

Крупнейшая в индустрии интеграционная платформа – McAfee SIA – более 130 партнеров



DXL – уникальное преимущество

Global Threat Intelligence

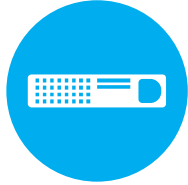


virusTotal

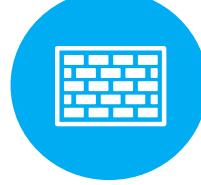
TIE Server



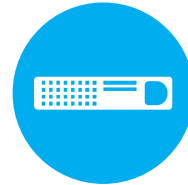
SANDBOX



NGFW



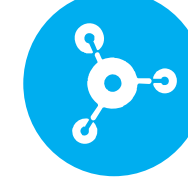
IPS



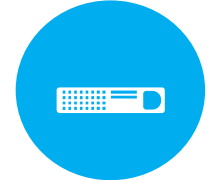
Web Gateway



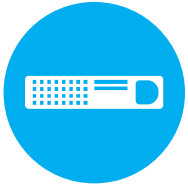
3rd Party Solutions



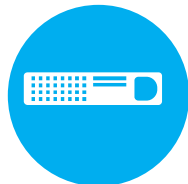
SIEM



Data Exchange Layer



Консоль управления ePO



EDR



MOVE



Application Control



Mail Security



DLP



Endpoint Protection

- ✓ Возраст файла скрыт
- ✓ Подписано с отозванным сертификатом
- ✓ Создано ненадежным процессом

Trust Level: Low
Action: Block

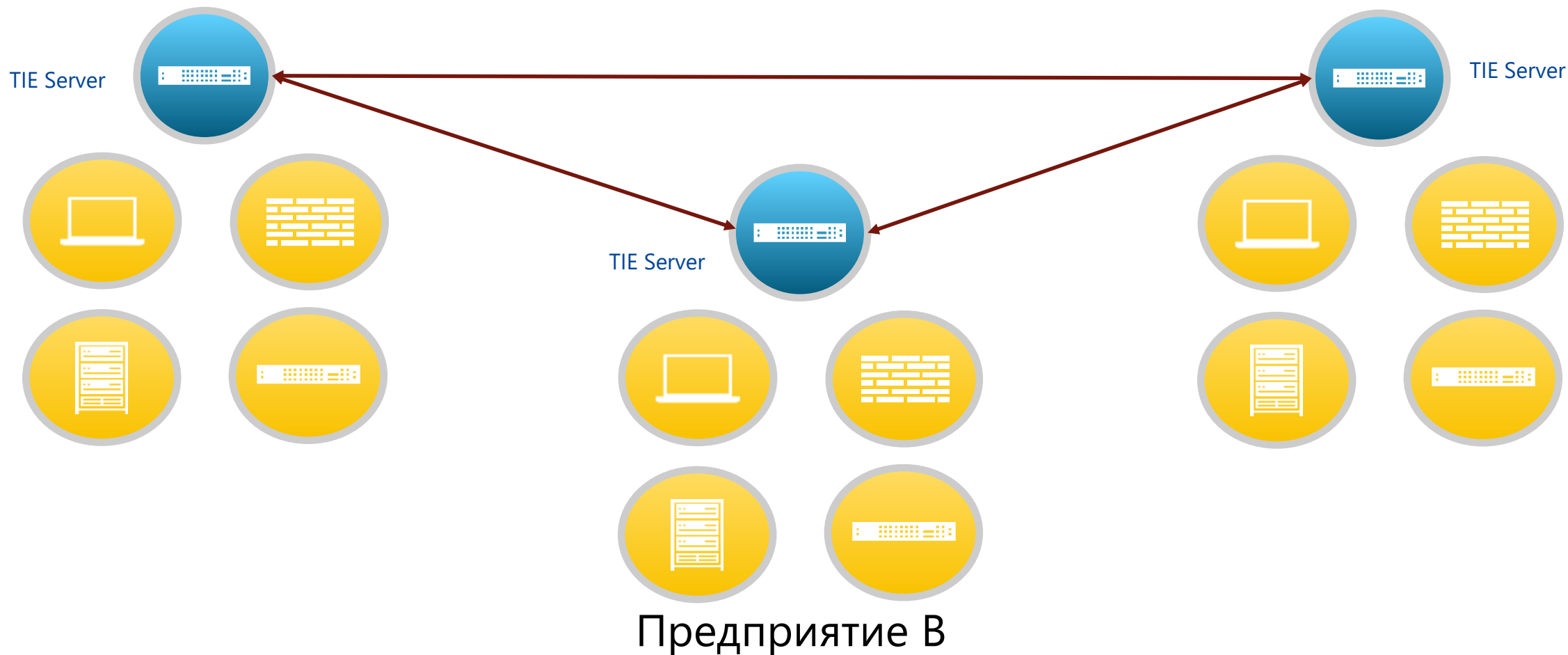
Мгновенный обмен аналитическими данными об угрозе и анализ на связь в прошлом

Обмен информацией о угрозах в режиме реального времени

Адаптивная защита – от обнаружения до защиты за миллисекунды

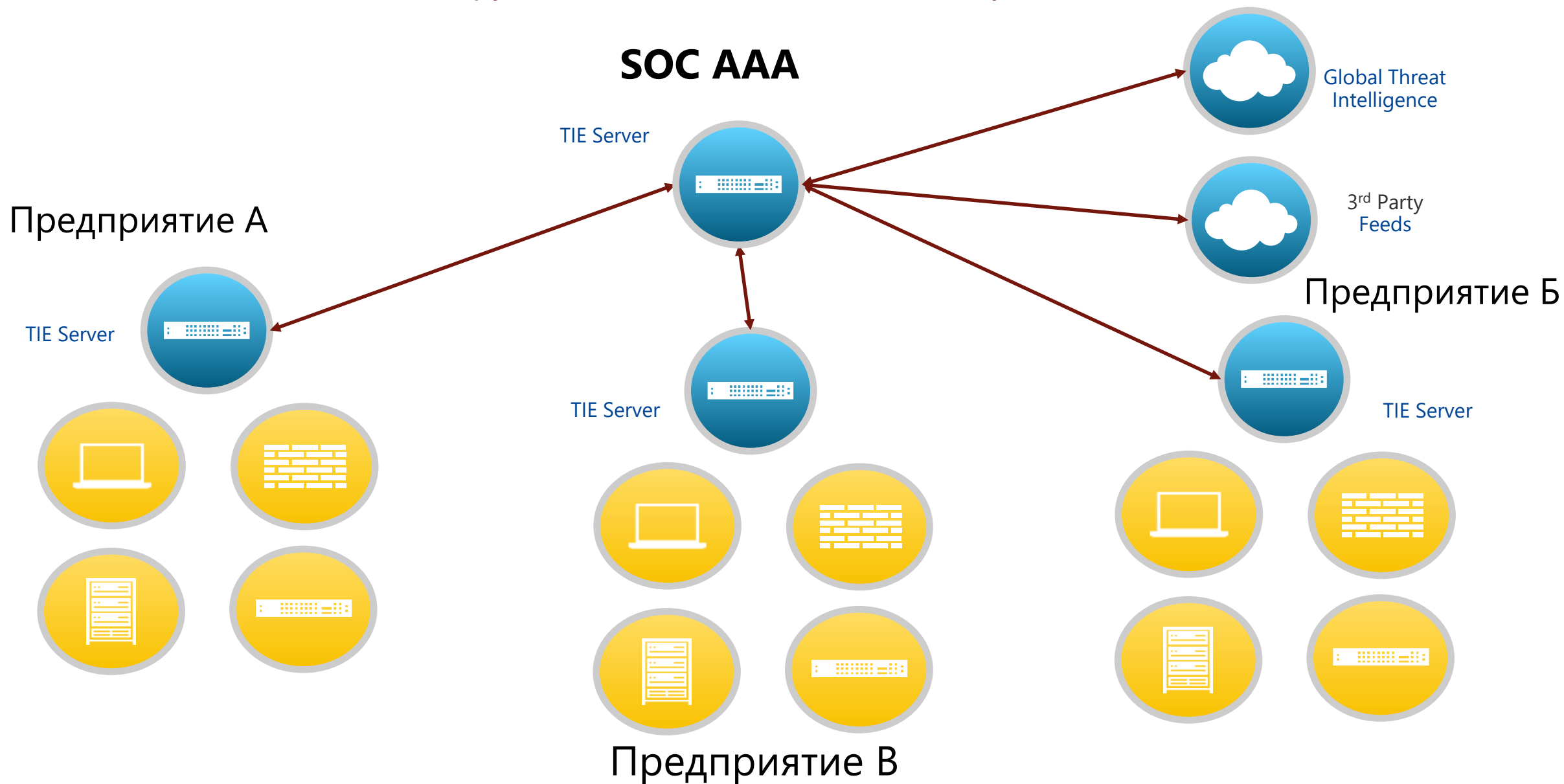
Предприятие А

Предприятие Б



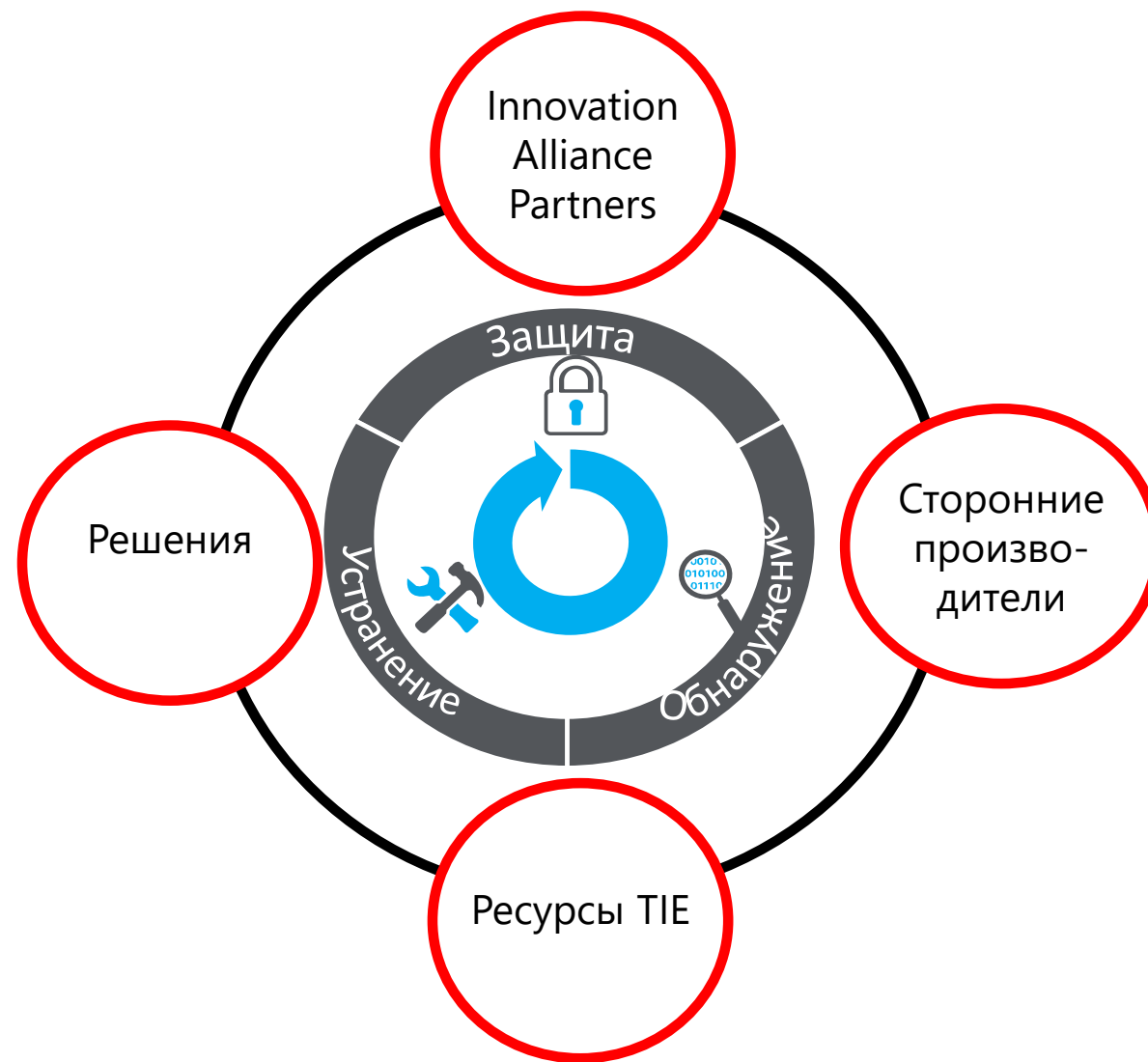
Обмен информацией о угрозах в режиме реального времени

Адаптивная защита – от обнаружения до защиты за миллисекунды



Преимущества единой экосистемы

- Снижение нагрузки на ИБ благодаря централизованному управлению
- Повышение эффективности по отражению сложных и целенаправленных атак
- Автоматизация процессов ИБ
- Снижение расходов на эксплуатацию
- Снижение репутационных и финансовых рисков



Благодарю за внимание!

