ОНЛАЙН-КОНФЕРЕНЦИЯ

Взаимодействие технологий и процессов при построении оперативных центров ИБ

Технологии оперативного *обнаружения* и *реагирования* на кибератаки

Руслан Барбашин

Территориальный менеджер
McAfee

McAfee

- Инженер телекоммуникаций
- Executive MBA
- 10 лет в ИБ
- 10 лет в McAfee

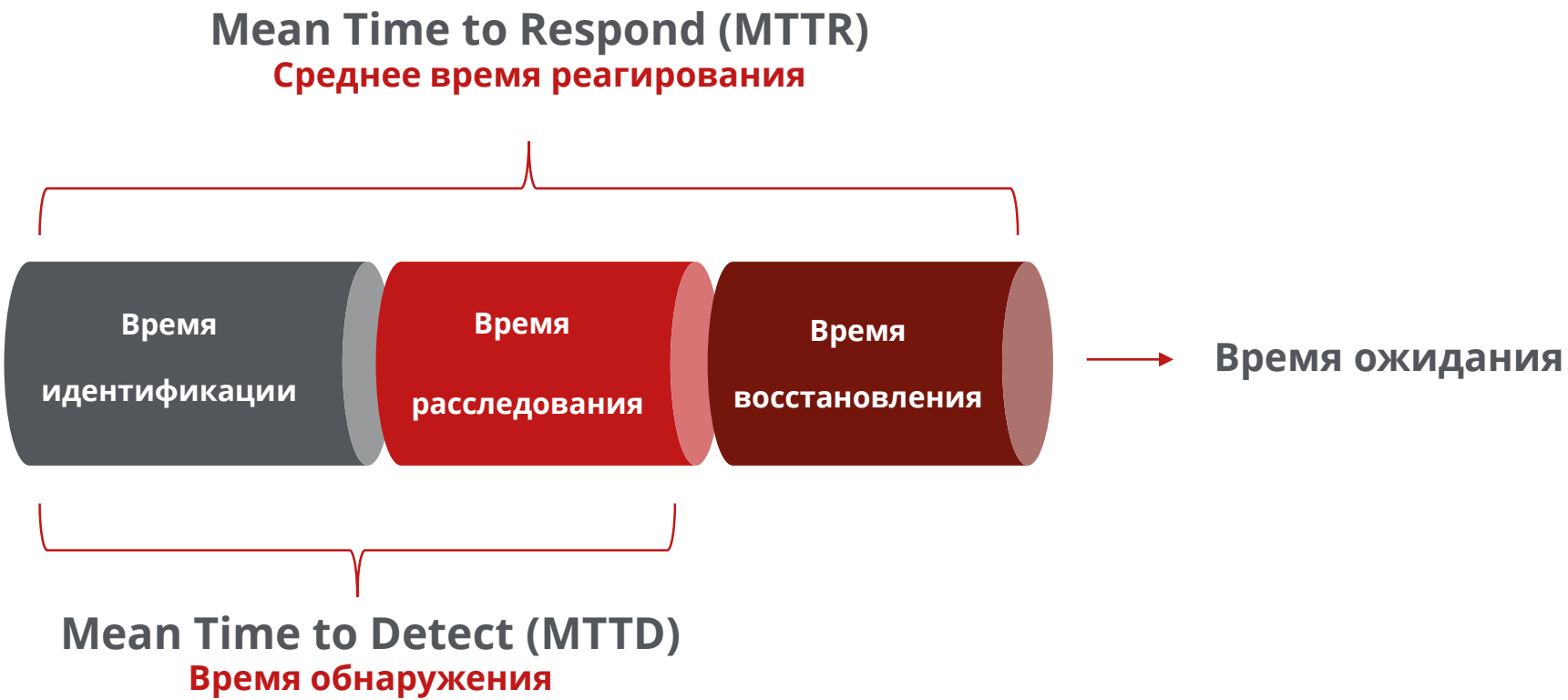
Руслан Барбашин
Territory Account Manager
Kazakhstan, Central Asia, Caucasus

Ruslans_Barbasins@McAfee.com
Ireland: +353 214672532
Kazakhstan: +7 727 350 5498

2000 City Gate, Mahon, Cork, Ireland

McAfee

Одна из ключевых задач при построении ОЦИБ



Среднее время обнаружения и время реагирования

Минимальное MTTR = 2+2 = 4 дня!

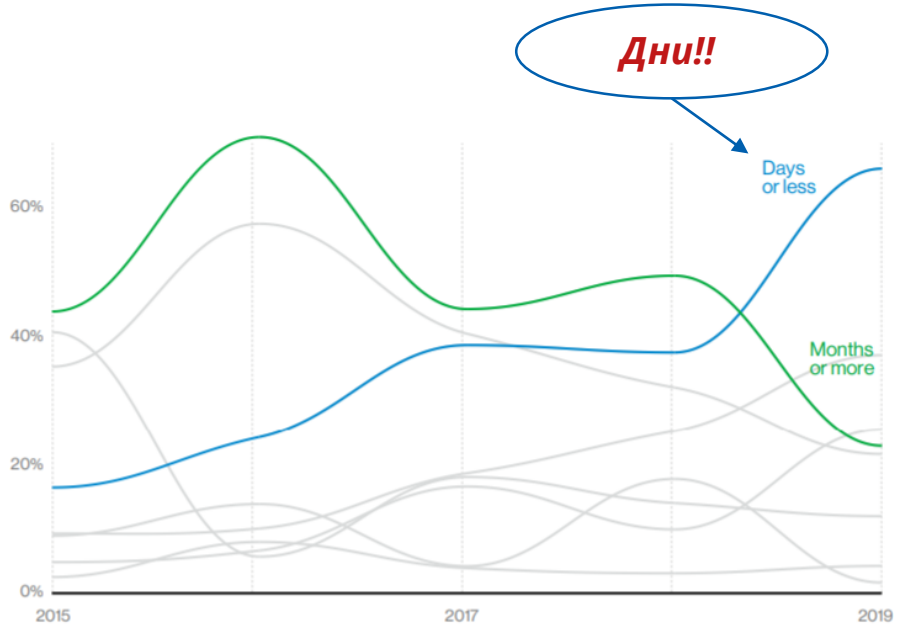


Figure 44. Discovery over time in breaches

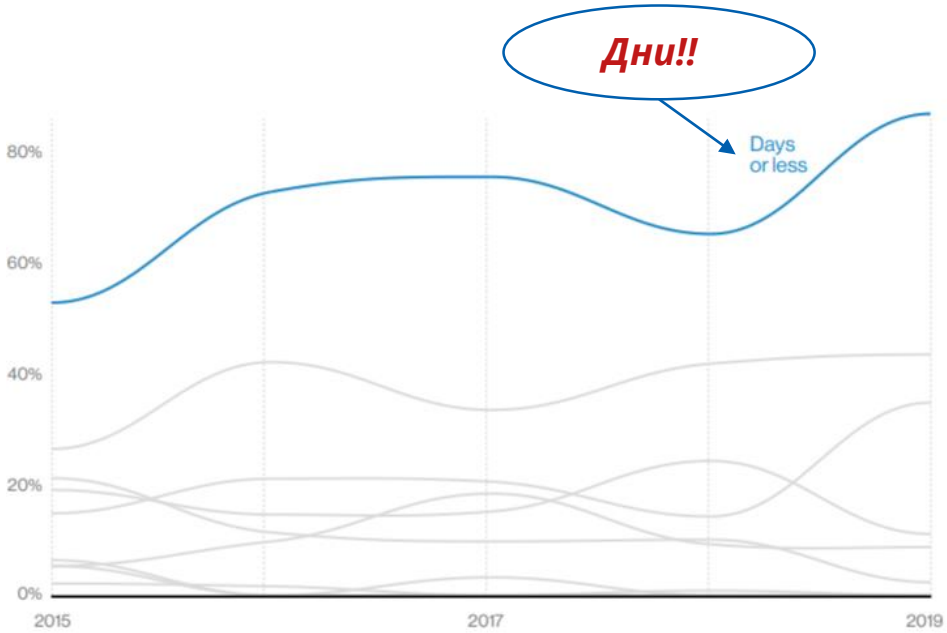


Figure 45. Containment over time in breaches

Verizon Data Breach Investigation Report 2020

Клиент McAfee:

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

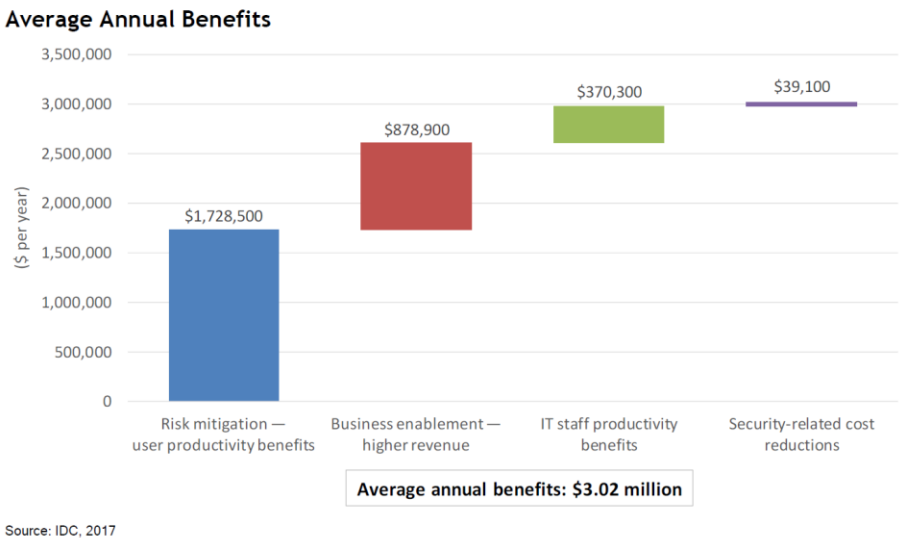
https://www.mcafee.com/enterprise/en-us/assets/case-studies/cs-idc-national-bank.pdf

IDC 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



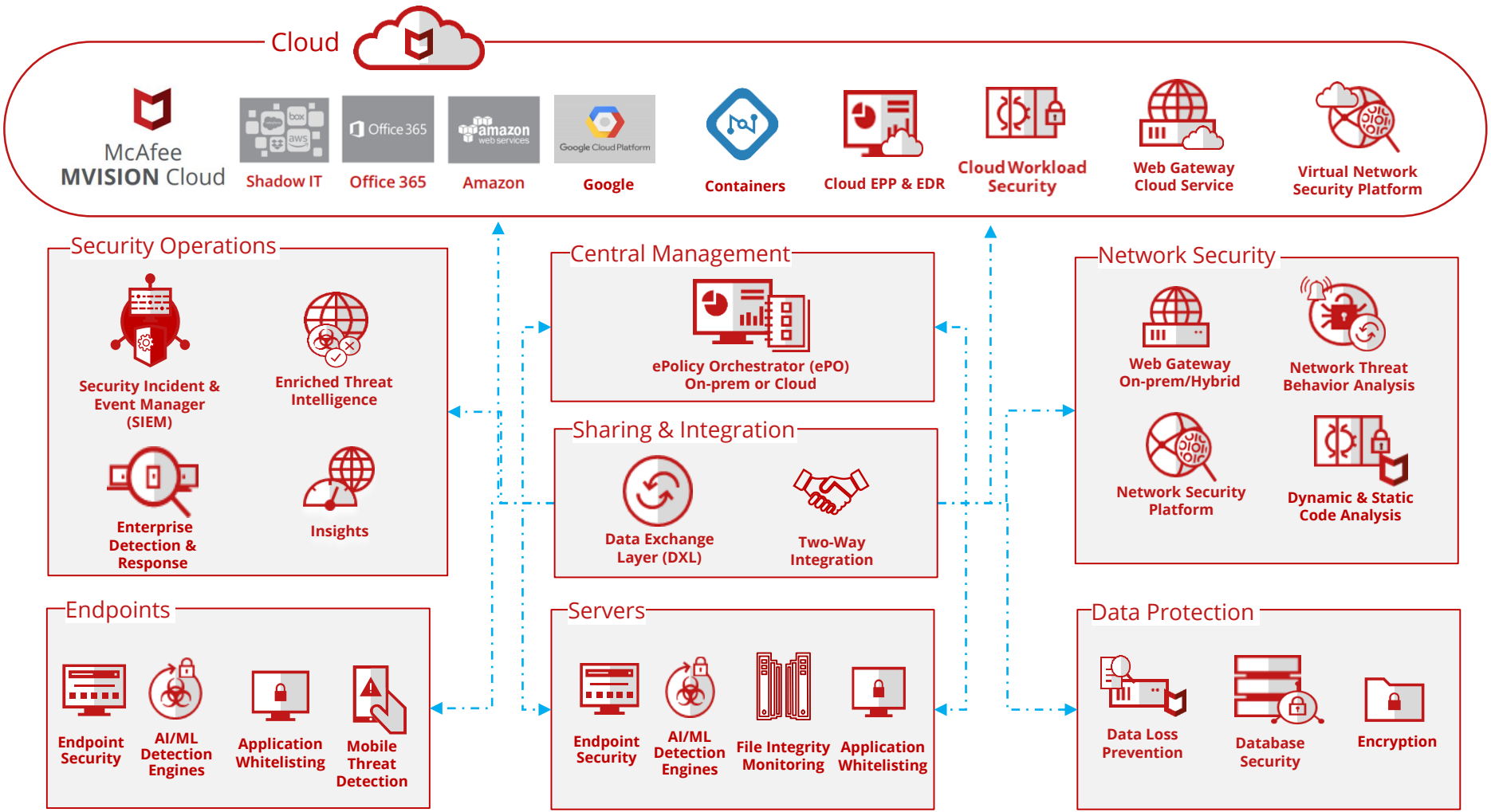
Source: IDC, 2017

- 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

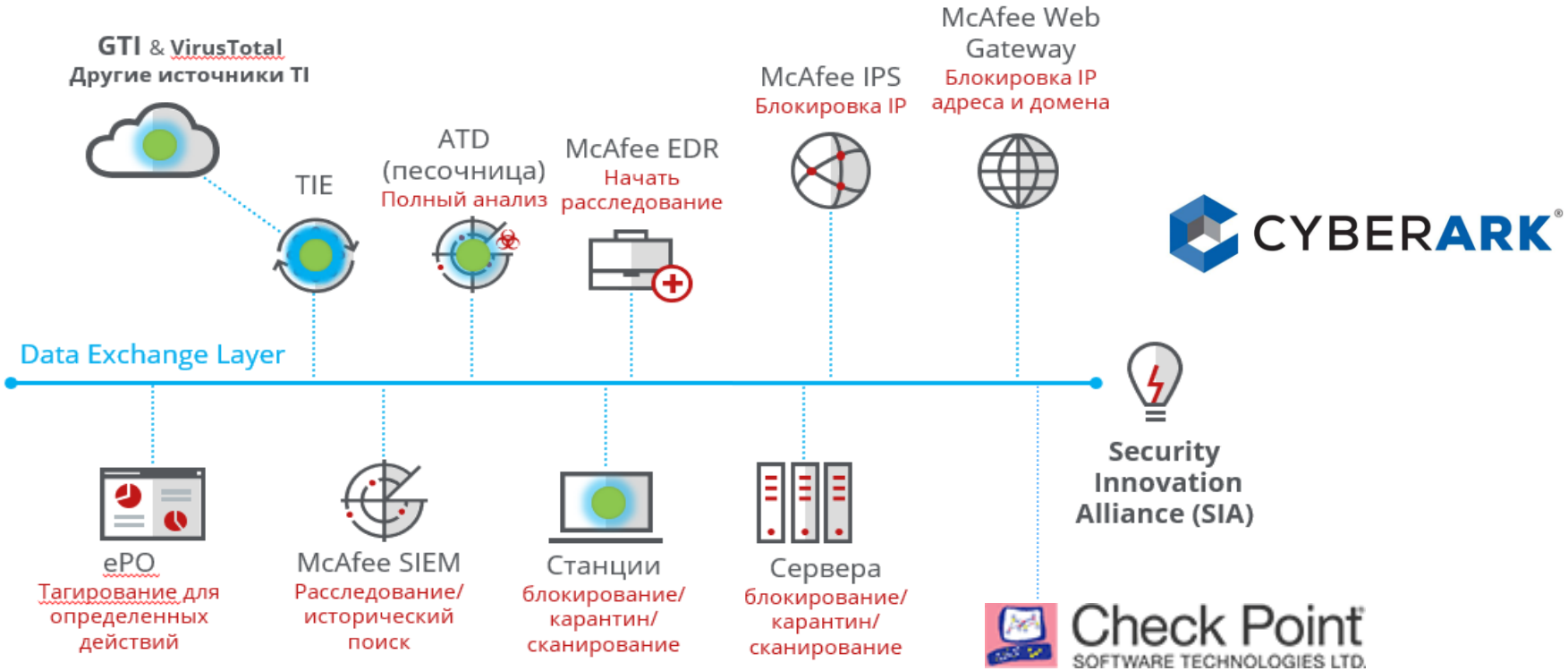
Как мы это делаем?

McAfee


Cloud
McAfee MVISION Cloud
Shadow IT
Office 365
Amazon
Google
Containers
Cloud EPP & EDR
Cloud Workload Security
Web Gateway Cloud Service
Virtual Network Security Platform
Security Operations
Security Incident & Event Manager (SIEM)
Enriched Threat Intelligence
Enterprise Detection & Response
Insights
Central Management
ePolicy Orchestrator (ePO) On-prem or Cloud
Sharing & Integration
Data Exchange Layer (DXL)
Two-Way Integration
Network Security
Web Gateway On-prem/Hybrid
Network Threat Behavior Analysis
Network Security Platform
Dynamic & Static Code Analysis
Endpoints
Endpoint Security
AI/ML Detection Engines
Application Whitelisting
Mobile Threat Detection
Servers
Endpoint Security
AI/ML Detection Engines
File Integrity Monitoring
Application Whitelisting
Data Protection
Data Loss Prevention
Database Security
Encryption

McAfee Adaptive Security Architecture

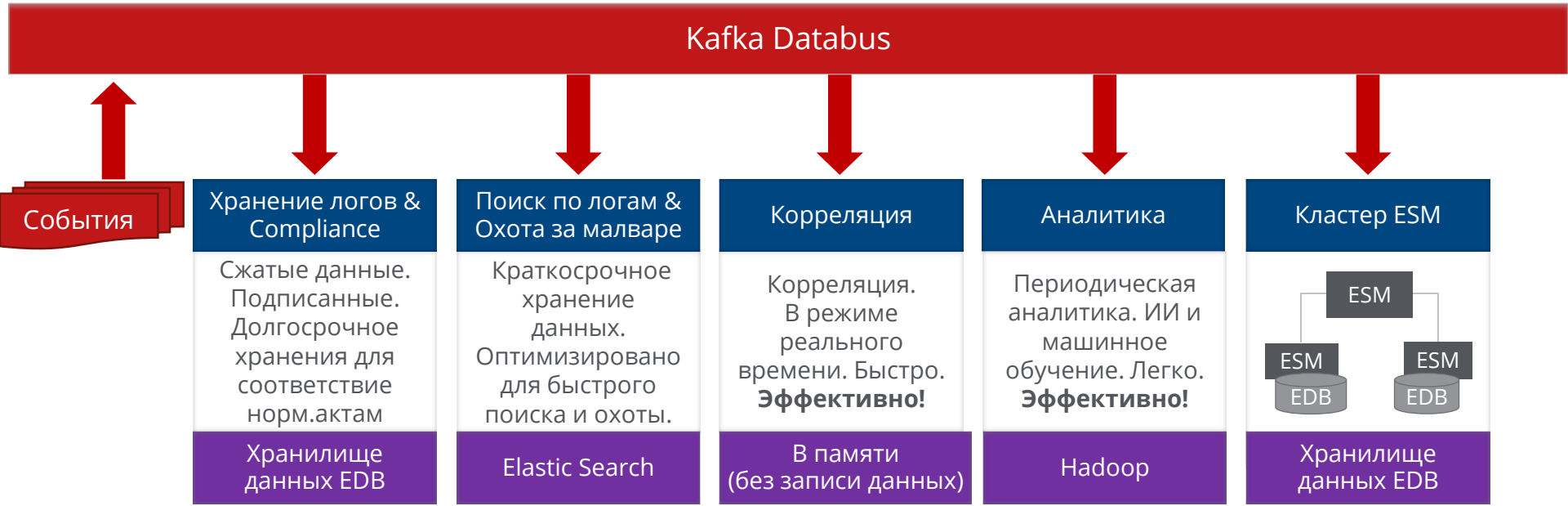
Постоянный обмен репутациями (IOC) по всей экосистеме



McAfee SIEM - Платформа для обработки Big Data –

ESM 11 = Высокая производительность. Низкая стоимость владения

И никаких компромиссов !!!



Это мощно! 500 000 (EPS) ивентов в секунду !!!

Industry News
September 18, 2019

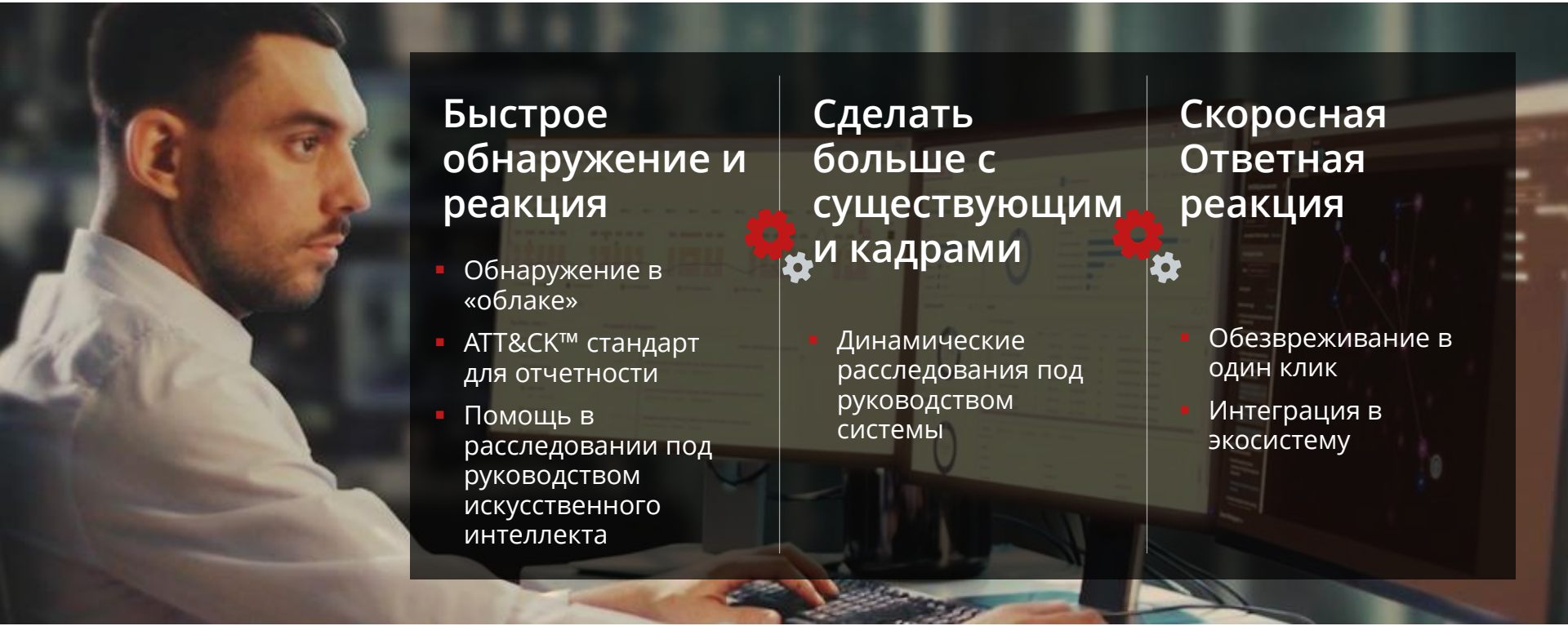
Share

McAfee and Oracle deliver SIEM performance capabilities in the cloud

McAfee, the device-to-cloud cybersecurity company, announced an extended relationship with Oracle to deliver security incident and events management (SIEM) performance capabilities in the cloud.

- **Record breaking performance**. McAfee ESM on Oracle Cloud Infrastructure will offer more than 16 times increase in the rate of events ingested versus on-premises deployments, designed to deliver up to 500,000 events per second across 600,000 data sources.

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

Рақмет!