Форум

"Современный подход к построению ИТ-инфраструктуры. Практика IBM."

17 марта 2015 года, Санкт-Петербург

Форум
"Современный подход
к построению ИТ-инфраструктуры.
Практика IBM."

17 марта 2015 года, Санкт-Петербург

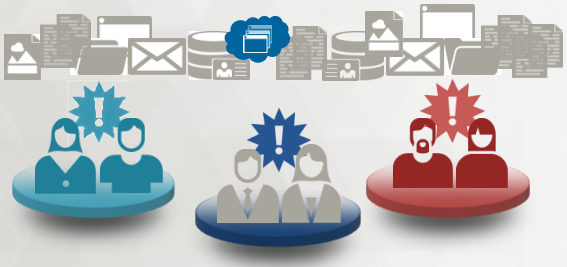
Алексей Воронцов, IBM Security

ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ

КАЖДЫЙ

из наших заказчиков сегодня – цель для злоумышленников

Три причины для “интеллектуальной безопасности”

Вы – под угрозой,	защита все сложнее	но знаний - не хватает.
		
• Изощренные методы атак • Исчезающий периметр • Использование уязвимостей в системах безопасности	• Постоянно изменяющаяся инфраструктура • Много продуктов от разных вендоров; дорого настраивать и управлять • Неадекватные и неэффективные инструменты	• Недостаток специалистов ИБ • Слишком много данных при ограниченных человеческих ресурсах и навыках управления ими • Управление и мониторинг – требования регуляторов

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Три основы “интеллектуальной безопасности”

- Аналитика
- Интеграция
- Экспертиза

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

1. Аналитика

Современный подход к построению
ИТ-инфраструктуры. Практика IBM.

Аналитика на службе информационной безопасности

Предсказывать и приоритезировать слабые элементы системы ИБ до того, как это сделают злоумышленники

IBM Security QRadar Security Intelligence Platform

Определять активности и аномалии в отличие от нормального поведения

Аналитика до атаки

Аналитика атаки в реальном времени

IBM Security QRadar Vulnerability and Risk Manager

IBM Security QRadar SIEM

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Выявлять бреши, прослеживать активности и закрывать уязвимости

Respond

Расследование инцидентов после атаки

Уменьшить время на полное расследование того, что и когда произошло

IBM Security QRadar Incident Forensics

Быстрая интеграция

Быстро охватить много областей ИБ защищая будущее

Интеграция решений платформы IBM Security

Emergency Response Services

Помочь подготовиться и противостоять атакам более эффективно

24x7

IBM Emergency Response Services

Автоматическое определение инцидентов

Extensive Data Sources

- Средства ИБ
- Сервера и мейнфреймы
- Сетевая активность и VM
- Активность СУБД
- Активность приложений
- Информация о конфигурациях
- Уязвимости и угрозы
- Пользователи и учетки
- Глобальная база угроз

Автоматическое формирование инцидентов ИБ

- Неограниченный сбор, хранение и анализ данных
- Встроенная классификация данных
- Автоматическое обнаружение активов, сервисов и пользователей
- Корреляция и аналитика угроз в реальном времени
- Автоматическое профилирование и выявление аномалий
- Обнаружение инцидентов

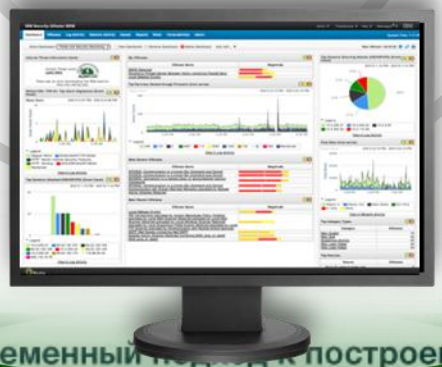
“из коробки”

Интеллектуальная

Подозрительные инциденты

Приоритезированные

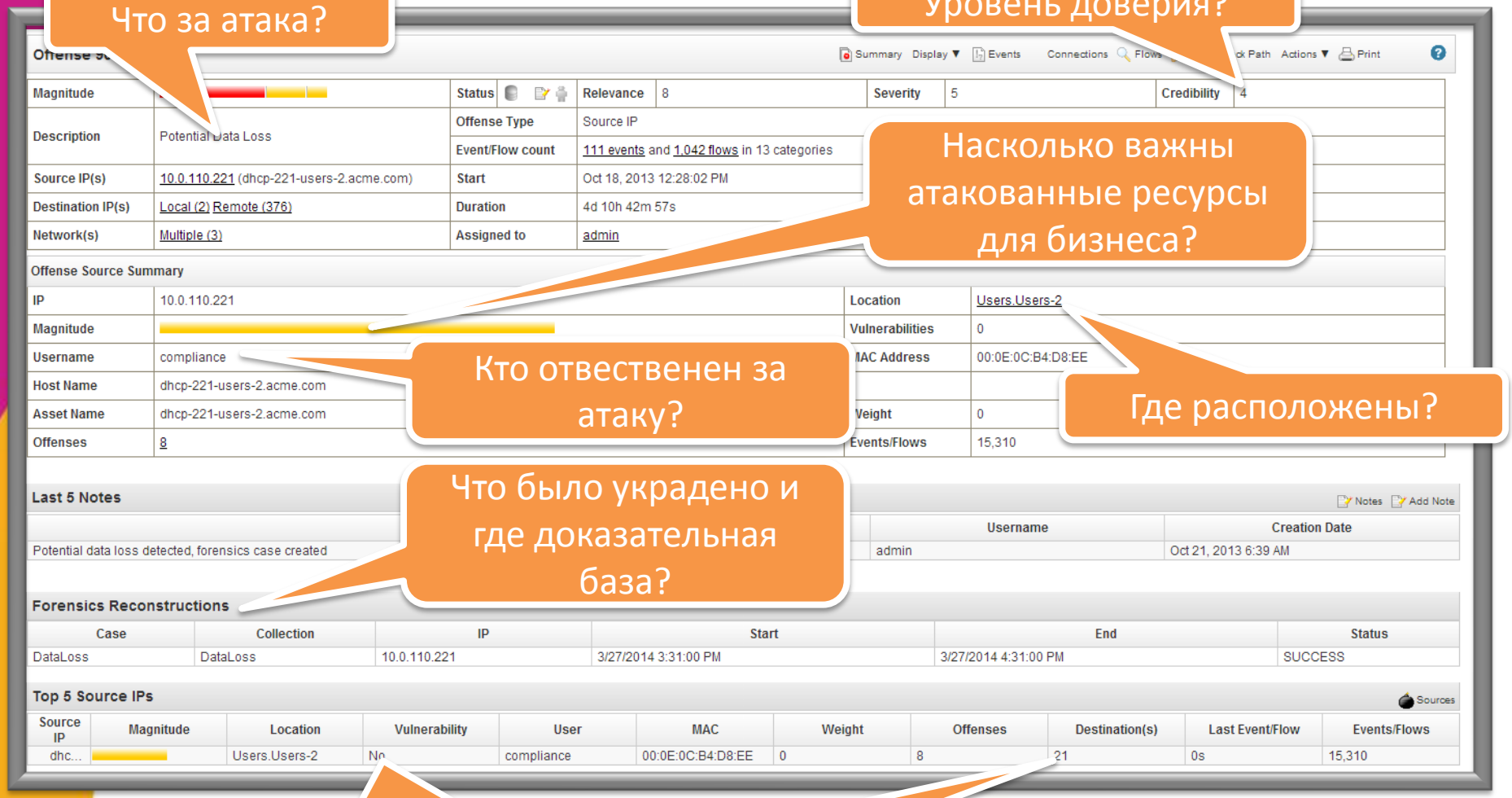
Встроенный интеллект



Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Аналитика – отвечая на все вопросы безопасника

Интегрированная



Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Простота и немедленный результат

Внедрение IBM QRadar почти в три раза быстрее по времени в сравнении с другими SIEM решениями.

2014 Ponemon Institute, LLC
Independent Research Report

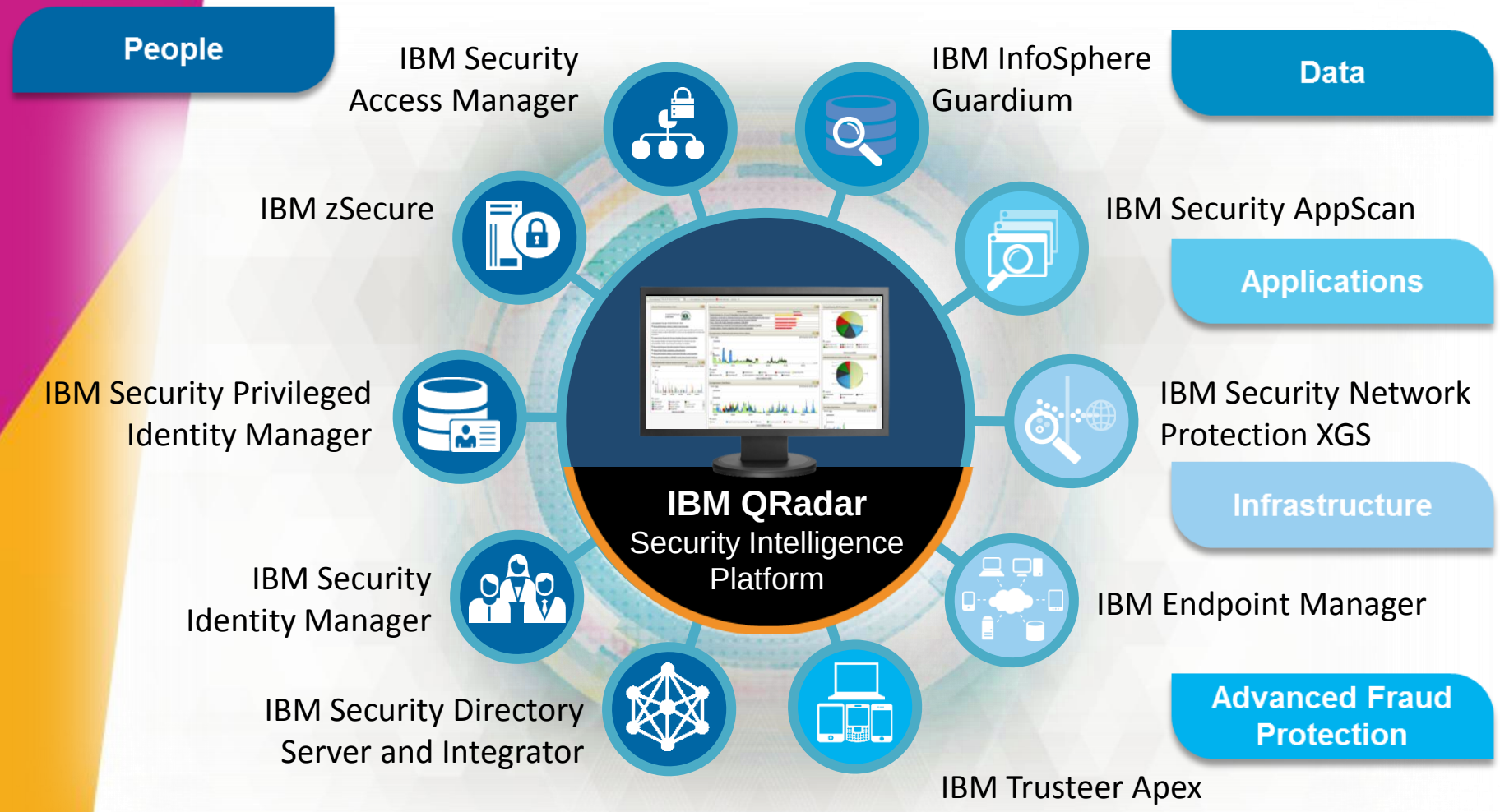
Простота установки и поддержки QRadar позволила уменьшить трудозатраты и освободить специалистов для других проектов.

Private U.S. University *with large online education community*

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

2. Интеграция

Центр интеграции IBM Security



Современный подход к построению ИТ-инфраструктуры. Практика IBM.

People: Управление учётными записями и правами доступа

Учётные записи и права доступа пользователей как новый периметр ИБ

Safeguard mobile, cloud and social access

Prevent advanced insider threats

Deliver actionable identity intelligence

Simplify cloud integrations and identity silos

Пример успеха

Большой российский банк, централизованная структура управления для

250000 сотрудников, контракторов и партнёров

150+ Бизнес приложений и сервисов

Решение IBM Security Systems:

- Access Manager for Web
- Access Manager for Mobile
- Federated Identity Manager
- Identity Manager
- Privileged Identity Manager
- zSecure Suite

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Data: Безопасность информации хранящейся в БД, включая Big Data

Найдите и защитите самые ценные активы вашей компании

Пример успеха

Крупная компания в области финансовых услух защитила более **2,000 критичных БД**

и сохранила более

$21M

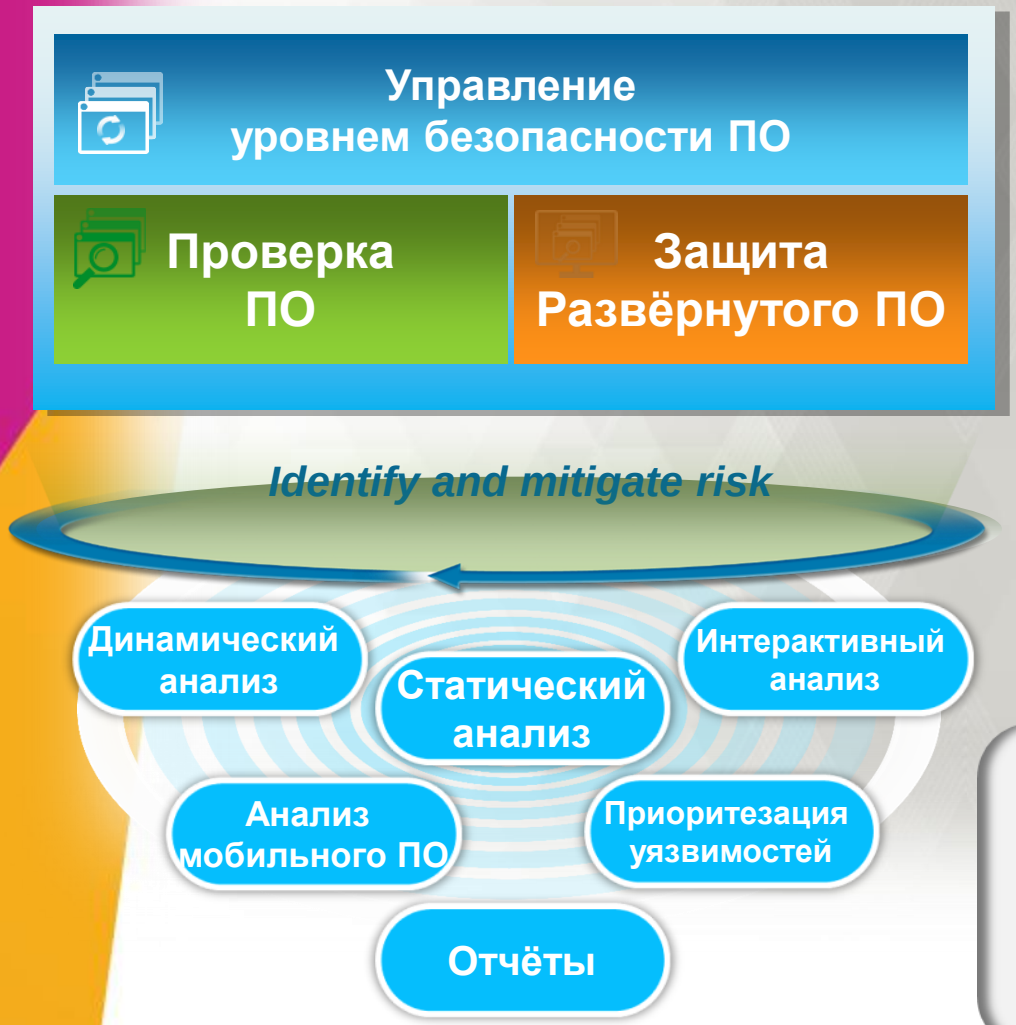
в затратах на комплайанс

Решения от IBM:

- Guardium Database Activity Monitoring
- Guardium Encryption Expert
- Guardium / Optim Data Masking
- Key Lifecycle Manager

Application: Безопасность на уровне приложений

Комлексные, интегрированные и гибкие решения для защиты приложений



Пример успеха

Сервисная IT компания обеспечивает контроль ИБ при разработке более

2,500 приложений

небольшой командой при

33%

сокращении количества найденных в продакшне уязвимостей

Решения IBM Security

- AppScan Source
- AppScan Enterprise / Standard
- DataPower Web Security Gateway
- Security Policy Manager

Infrastructure: Базовый уровень защиты

Глубинная защита сети, серверов, виртуальных серверов, мейнфреймов, APM и мобильных устройств

Пример успеха

Международная биржа обеспечивает доступность сервисов на уровне более

99.9%

при

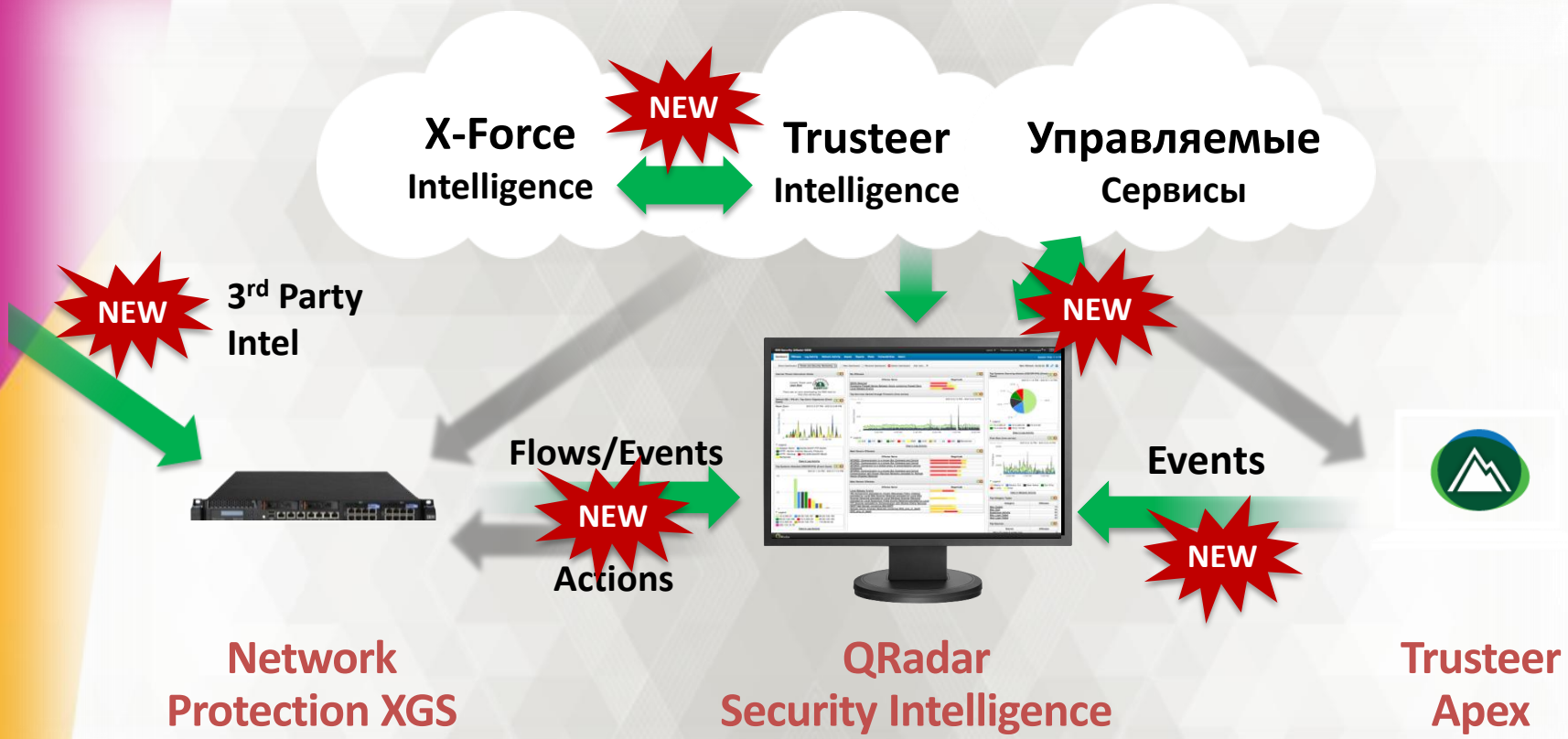
0

взломах за 3 последних года

Решения IBM Security

- Next Generation Network Protection (XGS)
- Network Intrusion Prevention (GX)
- SiteProtector Threat Mgmt
- QRadar Network Anomaly Detection
- Trusteer Apex
- Fiberlink MaaS360
- Endpoint Manager
- Host Protection
- zSecure

Новые типы интеграции между различными решениями



...и это только один из примеров интеграции в безопасности.

3. Экспертиза

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

IBM X-Force
Ведущая аналитическая команда в направлении ИБ в мире.

Покрытие

20,000+ устройств под управлением

3,700+ клиентов сервисов управления инфраструктуры ИБ

15млрд+ событий ИБ в день

133 страны под мониторингом (MSS)

1,000+ уникальных патентов в области ИБ

100млн+ конечных клиентов, защищённых от финансового мошенничества

Глубина

22млрд проверенных web страниц и сайтов

7млн спам & фишинг атак каждый день

73тыс документированных уязвимостей

860тыс подложных IP адресов

1000+ семплов вредоносного ПО в день

Миллионы уникальных вирусов

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Долгий путь IBM Security

1964

- IBM представляет ОС IBM System/360 с встроенными функциями ИБ. Развитие этого мейнфрейма до сих пор является одной из самых безопасных платформ, созданных когда-либо.

1968

- Лаборатория IBM Watson Laboratory (Йорктаун, США) начинает разработку стандарта DES (U.S. Data Encryption Standard).

1972

- IBM инвестирует первые $40 миллионов долларов за 5 лет в исследования в области ИБ.

1976

- IBM представляет технологию Resource Access Control Facility (RACF) для управления доступом и аудитом в мейнфреймах. Теперь нет необходимости реализовывать данные функции в каждом из приложений.

1978

- IBM анонсирует банкомат 3624 A.T.M. использующий DES.

1995

- IBM начинает разработку технологий безопасности и Java.

1996

- IBM запускает SecureWay Key Management Framework — коллекцию приложений, сервисов и крипто-движков для обеспечения безопасности электронной коммерции.
- IBM учавствует в разработке протокола Secure Electronic Transaction (SET), для обеспечения безопасности транзакций банковских карт через интернет.
- Исследователи IBM разрабатывают критографический стандарт keyed-hash message authentication code (HMAC), основу протоколов безопасности Интернет.
- IBM выпускает первый LDAP сервер энтерпрайз уровня.

1999

- IBM приобретает компанию Dascom, основу текущего портфолио решений по управлению доступом ISAM.
- Исследователи IBM учавствуют в разработке стандарта TLS 1.0 для шифрования интернет трафика.

2000

- IBM назначает первого Chief Privacy Officer.

2002

- IBM приобретает компанию Access360, ставшую основой решения по управлению УЗ Identity Manager.
- IBM приобретает MetaMerge, основу продукта Directory Integrator.

2005

- IBM представляет первый ноутбук ThinkPad с интегрированным считывателем отпечатков пальцев, обеспечивая безпренцидентный уровень безопасности для мобильного устройства.

2006

- IBM приобретает Internet Security Systems, Inc., основу сегодняшней исследовательской группы **IBM X-Force®** и текущих решений в области защиты сети.
- IBM первой выводит на рынок ленточные библиотеки с встроенной функцией шифрования.

2007

- IBM приобритает Consul, основу портфеля решений zSecure для обеспечения безопасности мейнфреймов.
- IBM приобритает Princeton Softech, интегрируя в свои продукты её решения для архивирования данных, менеджмента данных, безопасности, классификации и обнаружения типов данных.
- IBM приобретает Watchfire, интегрируя их технологии в линейку решений IBM AppScan.
- Исследователи IBM сыграли ключевую роль в разработке стандарта шифрования при хранении данных в рамках IEEE 1619.

2008

- IBM приобретает Encentuate, ставшую основой для продукта Enterprise Single-sign-on (ESSO).

2009

- IBM приобритает Ounce Labs, компанию специализировавшуюся на анализе исходного кода ПО, и интегрирует её технологии в линейку IBM AppScan.
- IBM приобритает **Guardium**, лидера в направлении реал-тайм мониторинга и защиты баз данных.
- Исследователи IBM researchers первые используют технологии Big Data для решения проблем кибербезопасности.

2010

- IBM приобретает Big Fix, основу текущих технологий по управлению конечными точками Endpoint Manager.
- IBM Research разрабатывает Fully Homomorphic Encryption.

2011

- Создано подразделение IBM Security Systems.
- IBM приобретает Q1 Labs, с решением по аналитике ИБ Qradar для усиления позиции в данном направлении.
- IBM запускает облачные сервисы Mobile Security Services, IBM Hosted Mobile Device Security Management.

2012

- Создано сервисное подразделение IBM Security Services.
- IBM выпускает некст-ген систему обнаружения вторжения, ПАК по управлению доступом и технологию управления привелегированными УЗ.
- IBM анонсирует 25 новых продуктовых релизов в области ИБ.
- IBM представляет технологии тестирования кода Android приложений.

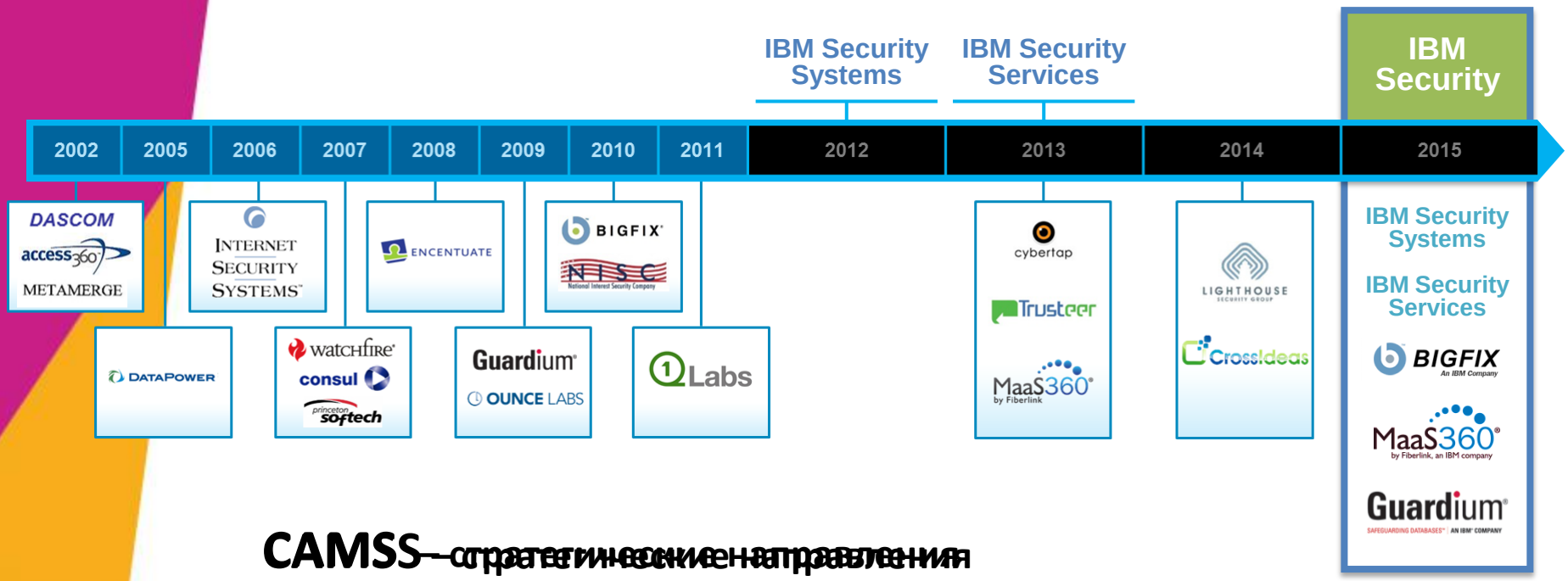
2013

- IBM анонсирует прорыв в комбинации технологий Security Intelligence и Big Data.
- IBM анонсирует сканер уязвимостей QRadar Vulnerability Manager .
- IBM анонсирует ПО безопасности MobileFirst для улучшения безопасности мобильного ПО без ухудшения скорости разработки.
- На текущий момент IBM получает более 3,000 патентов в области ИБ.
- IBM приобретает компанию Trusteer

- Примеры технологий ИБ, разработанных IBM : DES, Java Security SET HMAC, TLS, IPSEC и IKE.
- Более 4к клиентов находятся на аутсорсе ИБ компанией IBM.
- Каждый день IBM мониторит более 15миллиардов событий ИБ.

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

…текущие шаги



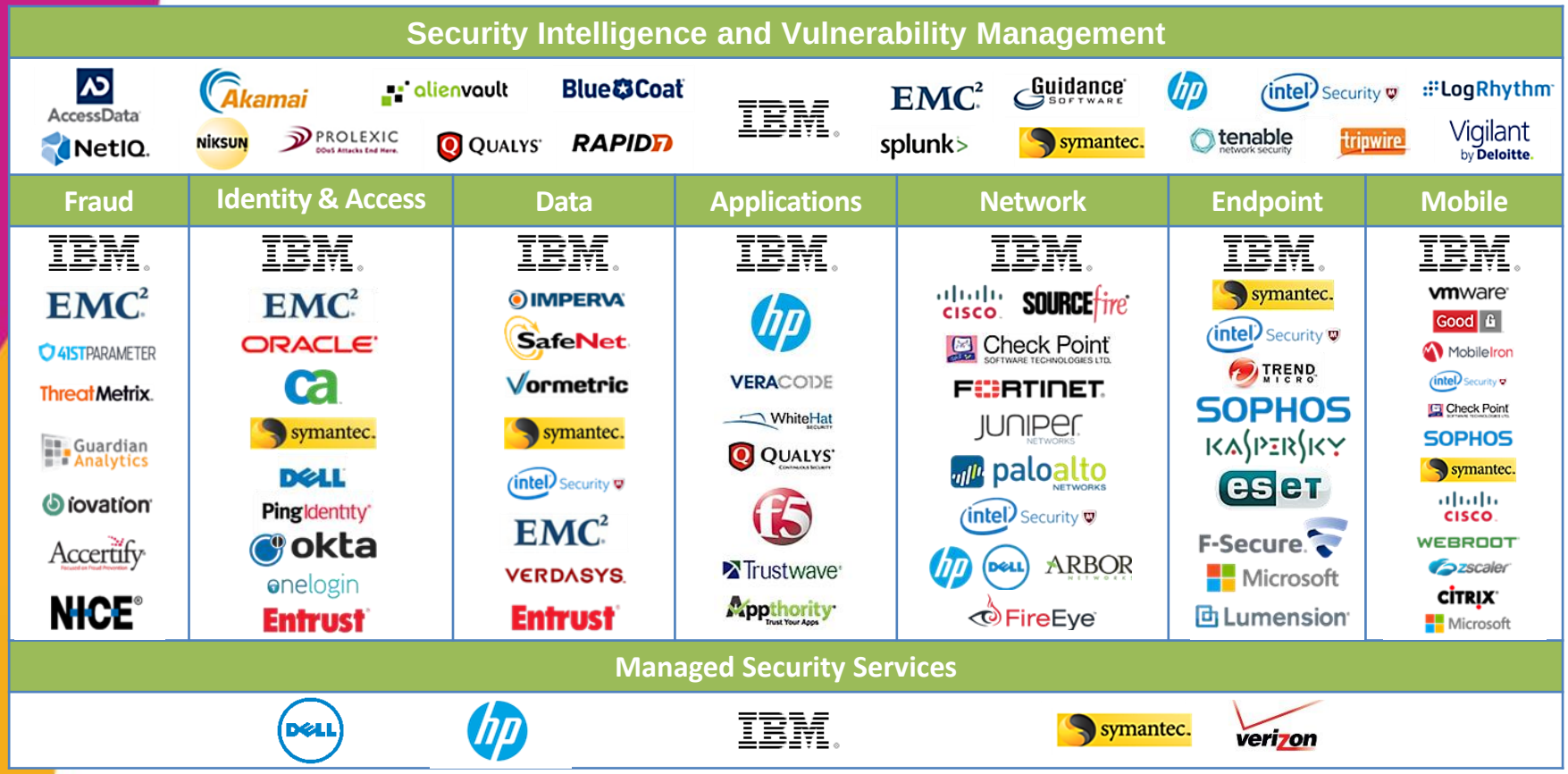
CAMSS – стратегические направления развития бизнеса IBM Corporation

- Cloud
- Analytics
- Mobile
- Social
- Security

NEW

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Результат:
куда обратиться за безопасностью?



Современный подход к построению ИТ-инфраструктуры. Практика IBM.

А что считают аналитики?

Domain	Market Segment / Report	Gartner Magic Quadrant	Forrester Wave	IDC Market Share / Scape
Security Intelligence	Security Information and Event Management (SIEM)	**Leader** *2014*		**Leader** *2013*
Fraud Protection	Web Fraud Detection *(Trusteer)*	**Leader** *2013*		
Identity and Access Management	Federated Identity Management and Single Sign-On			**Leader** *2013*
	Identity and Access Governance	**Leader** *2015*	**Strong Contender** *2013*	
	Role Management and Access Recertification		**Contender** *2011*	
	Web Access Management (WAM)	**Leader** *2013 MarketScope*		
	Mobile Access Management	**Leader,** *2014 Customer Value, Frost & Sullivan*		
	Identity Provisioning Management	**Leader,** *2014 Leadership Compass, KuppingerCole*		
Data Security	Database Auditing and Real-Time Protection		**Leader** *2011*	
	Data Masking	**Leader** *2014*		
Application Security	Application Security Testing *(dynamic and static)*	**Leader** *2014*	**Leader** *2014*	**Leader** *2013*
Network, Endpoint and Mobile Security	Network Intrusion Prevention Systems (NIPS)	**Challenger** *2014*		
	Endpoint: Client Management Tools	**Leader** *2014*		
	Endpoint Protection Platforms (EPP)	**Visionary** *2014*	**Strong Performer** *2013*	
	Mobile Security *(Fiberlink)*	**Leader** *2014*	**Leader** *2014*	
Consulting and Managed Services	Managed Security Services (MSS)	**Leader** *2014 (AP, NA, WW)*	**Leader** *2014 (NA)*	**Leader** *2014*
	Information Security Consulting Services		**Leader** *2013*	
	Public Cloud Service Providers' Security (IBM Bluemix)		**Strong Contender** *2014*	

**по состоянию на январь 2015*

Ключевые инновации 2014

IBM Threat Protection System

IBM Dynamic Cloud Security

Наиболее заметные события

- *QRadar Incident Forensics*
- QRadar Advanced Search
- QRadar Data Nodes
- Управляемые сервисы SIEM
- Расширение мониторинга мошенничества и Apex
- Сервис защиты “ключевых систем”
- *Identity Governance*
- Access Manager for DataPower
- Cloud Identity Services
- *AppScan 9.0 и облачные анализаторы в IBM BlueMix*
- Новые модели XGS, *интеграция с QRadar*, в том числе на основе репутаций X-Force®

И на последок о сложном: сертификация средств ИБ в РФ

Сейчас:

- Guardium
  - НДВ, ТУ
- QRadar SIEM

NEW ТУ, сертификат №3354 от 3 марта 2015г

В процессе (+ пол года):

- Identity Manager
- Access Manager for Web
- XGS Appliance (NG-IPS)

Повышайте свою экспертизу в области ИБ!

http://www.ibm.com/security/xforce/downloads.html

Современный подход к построению ИТ-инфраструктуры. Практика IBM.

Подписывайтесь на
@ibmsecurity и @ibmxforce

Подписывайтесь на
оповещения безопасности
группы X-Force по адресам
http://iss.net/rss.php или
http://blogs.iss.net/rss.php

Подпишитесь на канал IBM
о решениях в области ИБ
www.youtube.com/ibmsecuritysolutions

Спасибо за внимание