IBM Security

IBM Security
Аналитика и когнитивные технологии для защиты

Дмитрий Ячевский
Руководитель направления интеллектуальной безопасности

IBM

Как было раньше…

А сейчас…

Человек не способен
анализировать млрд событий

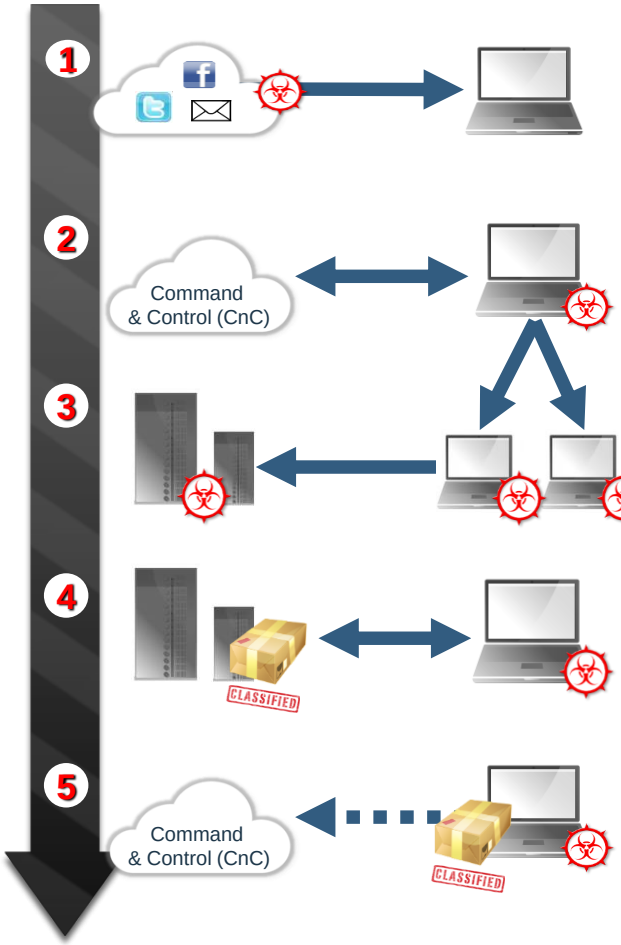
Advanced Persistent Threat

Как готовится атака такого типа?

- **Анализ доступной информации с сайта компании\новостей**
- **Поиск профилей на LinkedIn, Facebook и Twitter**
- **Анализ инфраструктуры**
  - Поиск слабых мест и потенциальных уязвимостей
  - Анализ информации из открытых источников

- **Кто работает с необходимой злоумышленнику информацией?**
  - Какова структура отчетности?
  - Кто у них в друзьях?

5 этапов современной атаки



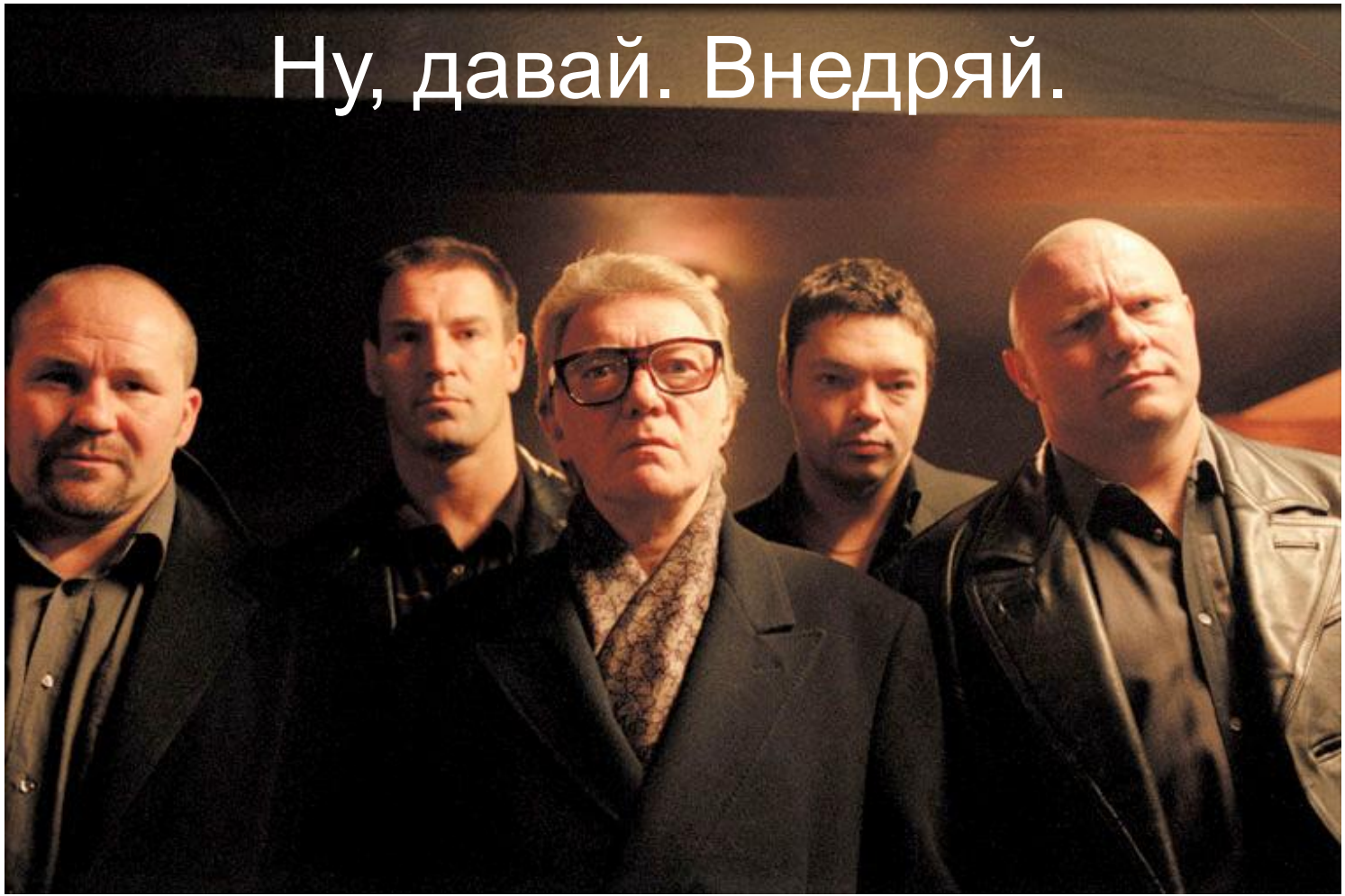
Разведка и Компрометация

Закрепление

Распространение

Сбор\Взлом

Выгрузка и Затирание


Ну, давай. Внедряй.


MYTH

Время серьезно посмотреть на портфель ваших решений по ИБ

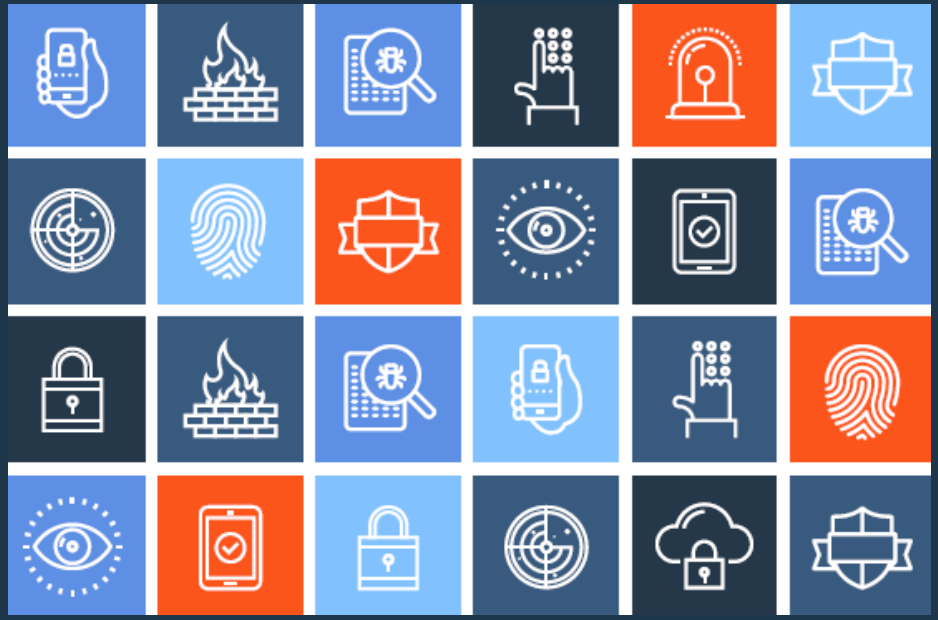
В среднем организации используют до

85

продуктов ИБ от более чем

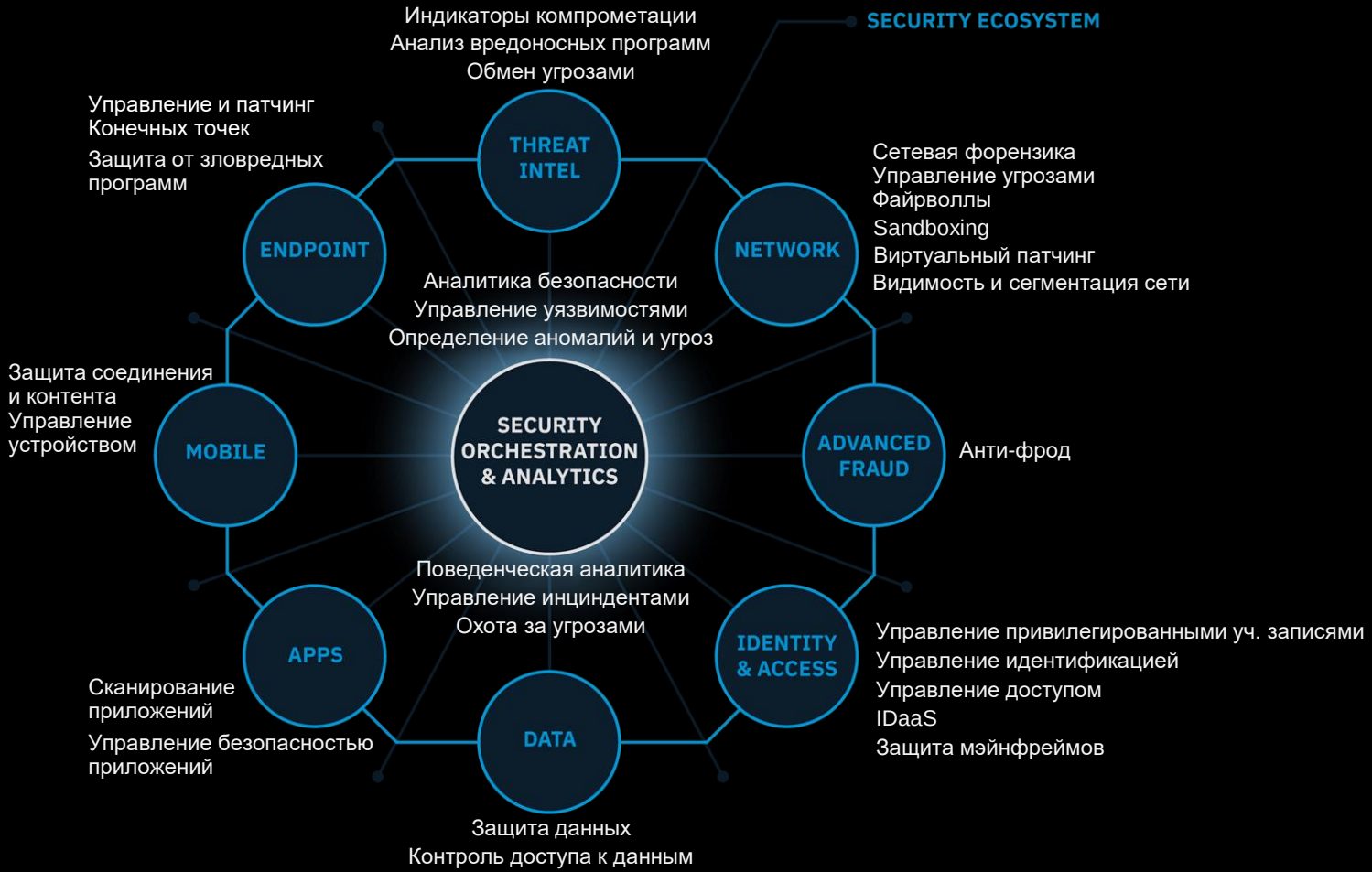
40

разных производителей – это очень дорогостоящий подход

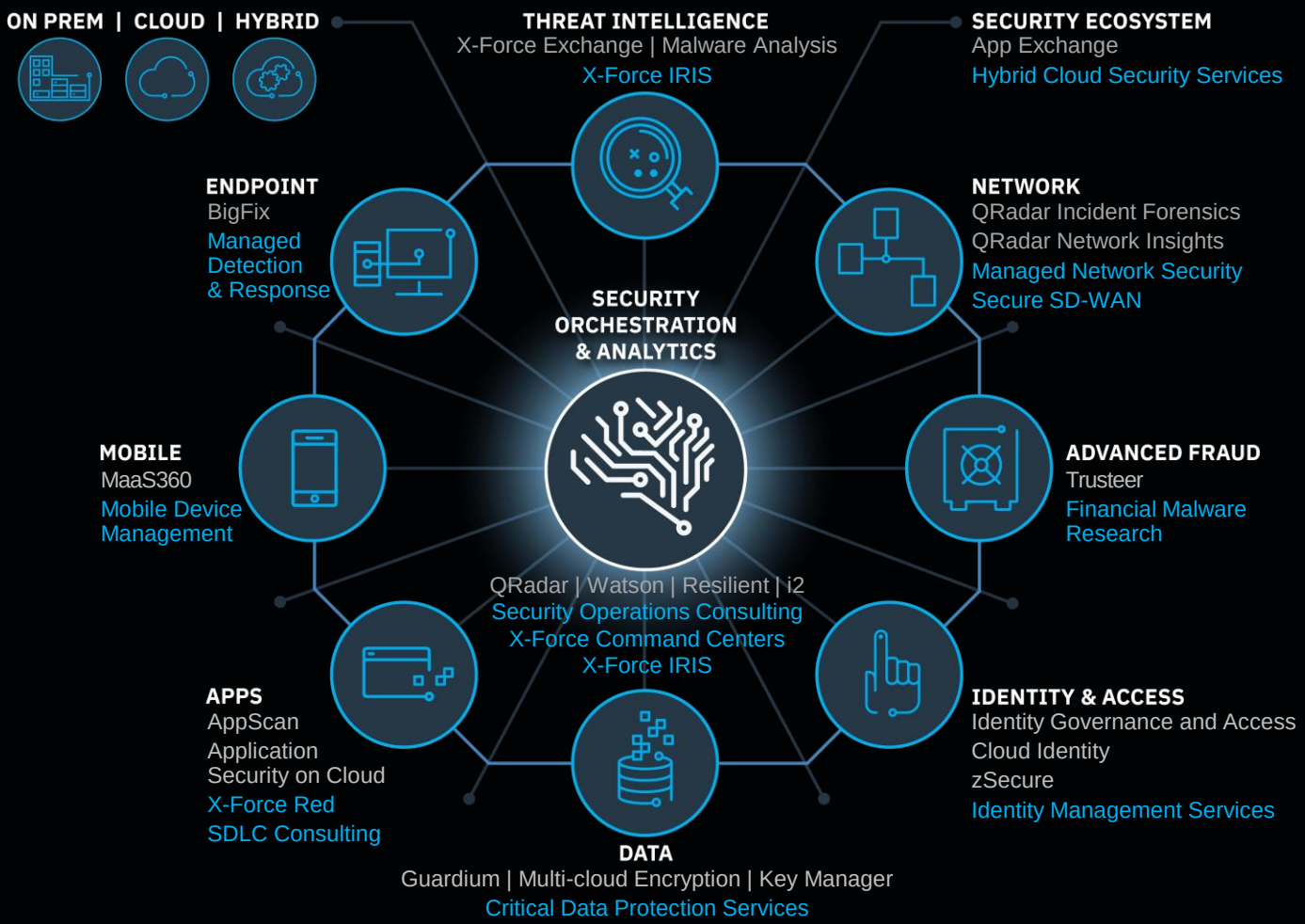


Работать будет, но насколько эффективно?

Сегменты информационной безопасности



IBM Security – портфель интегрированных решений



IBM Security: Лидер в 12 из 12 сегментов рынка ИБ

ОБЛАСТЬ	РАЗДЕЛ	СЕГМЕНТ РЫНКА / ОТЧЕТ	РЕЙТИНГИ АНАЛИТИКОВ
Security Operations and Response	Security Intelligence	Security Information and Event Management (SIEM)	**LEADER**
	Network & Endpoint Protection	Endpoint: Client Management Tools	**LEADER**
Information Risk and Protection	Identity Governance & Access Management	Identity and Access Governance	**LEADER**
		Access Management (worldwide)	**LEADER**
		Identity and Access Management as a Service (IDaaS)	**LEADER**
		Identity Provisioning Management	**LEADER**
	Data Security	Database Security	**LEADER**
	Application Security	Application Security Testing (dynamic and static)	**LEADER**
	Mobile Protection	Enterprise Mobility Management (MaaS360)	**LEADER**
	Fraud Protection	Web Fraud Detection (Trusteer)	**LEADER**
Security Transformation Services	Consulting and Managed Services	Managed Security Services (MSS)	**LEADER**
		Information Security Consulting Services	**LEADER**

Примечание: Данные собраны среди ведущих аналитических агентств, действительны на Ноябрь 2017

Международный лидер в области кибербезопасности

IBM Security

- **ЛИДЕР** в 12 из 12 сегментов рынка КБ
- **8.000+** сотрудников
- **17.500+** заказчиков
- **133** стран
- **3.500+** патентов КБ
- **20** поглощений с 2002 года

QRadar – платформа для построения единого ИБ решения

Security Intelligence + IBM Sense Analytics © resilient

Реагировать на изменения и определять угрозы раньше через анализ поведения и выявление аномалий

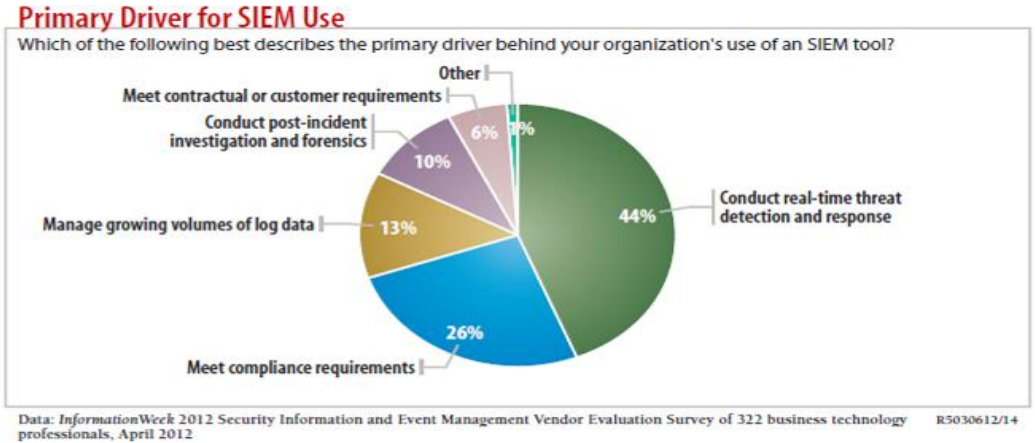
Radar®

SIEM
Мониторинг инцидентов

Уже давно не только SIEM

Что должны делать SIEM?

- Compliance
- Обработка и хранение большого объема журналов событий
- Инциденты
- Мошенничество
- Реагирование
- Отчеты
- SOC



SOC – сердце инфраструктуры кибербезопасности

Как выиграть время при расследовании инцидентов ИБ?

SOC – Security Operations Center
Центр оперативного реагирования на инциденты ИБ
Люди – Процессы – Технологии

Ключевое отличие – использование **аналитических** технологий для создания единого оперативного видения текущей ситуации в компании с точки зрения ИБ.

IBM QRadar Sense Analytics

МНОЖЕСТВО ИСТОЧНИКОВ

Устройства ИБ

Серверы и мейнфреймы

Сетевая и виртуальная активность

Активность БД

Активность приложений

Информация о конфигурации

Уязвимости и угрозы

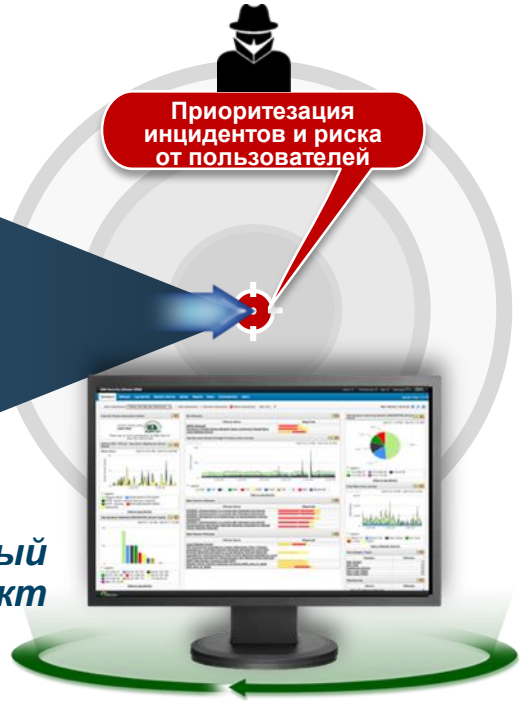
Пользователи и учетные записи

Глобальные базы угроз

QRadar Sense Analytics

Идентификация Инцидентов

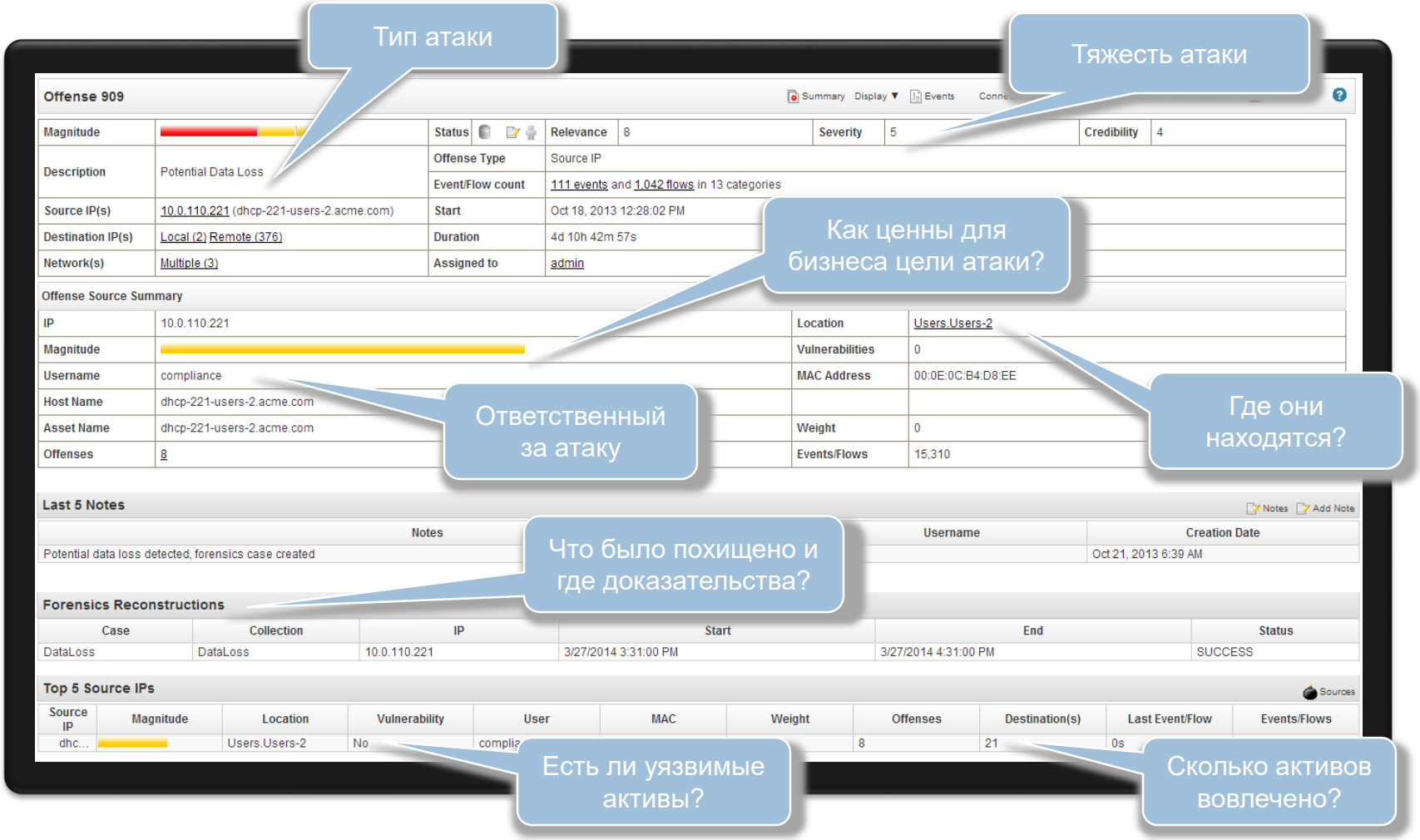
- Сбор данных, хранение и анализ
- Корреляция и анализ угроз в реальном времени
- Автоматическое определение и профилирование активов, сервисов и пользователей
- Базовые активности и выявление аномалий



Встроенный Интеллект

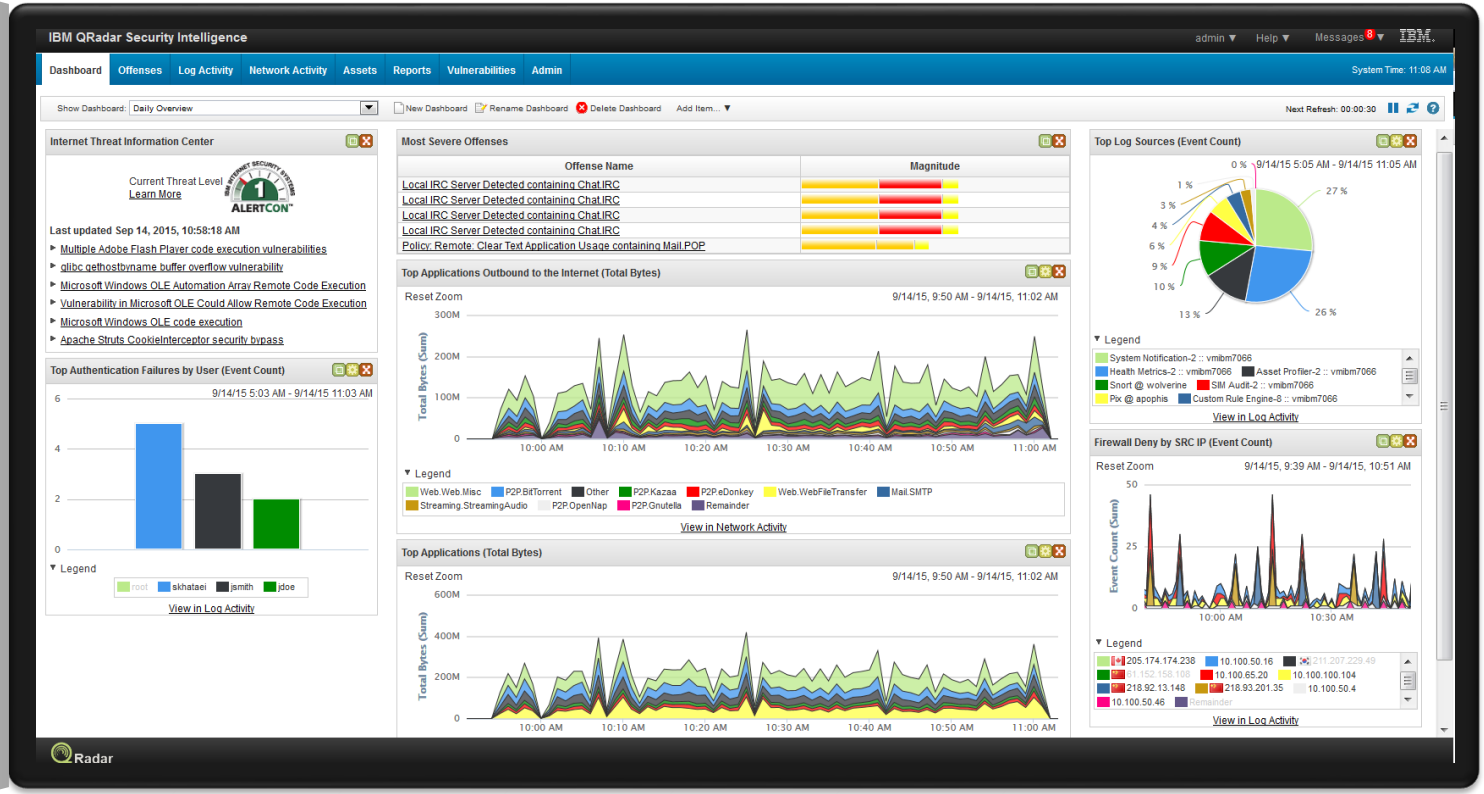
Улучшенная аналитика для предотвращения, выявления и реагирования на угрозы

Выявление потенциальных угроз через аналитику



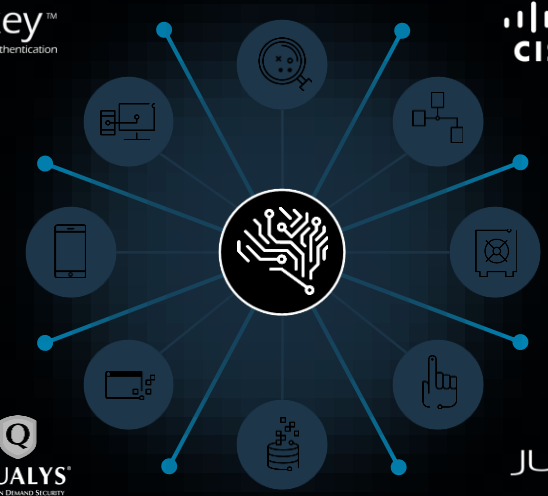
Интегрированная, унифицированная архитектура в одной web-консоли

- **Log Management**
- **Security Intelligence and Sense Analytics**
- **Network Activity Monitoring**
- **Vulnerability and Risk Management**
- **Network Forensics**
- **Incident Response**

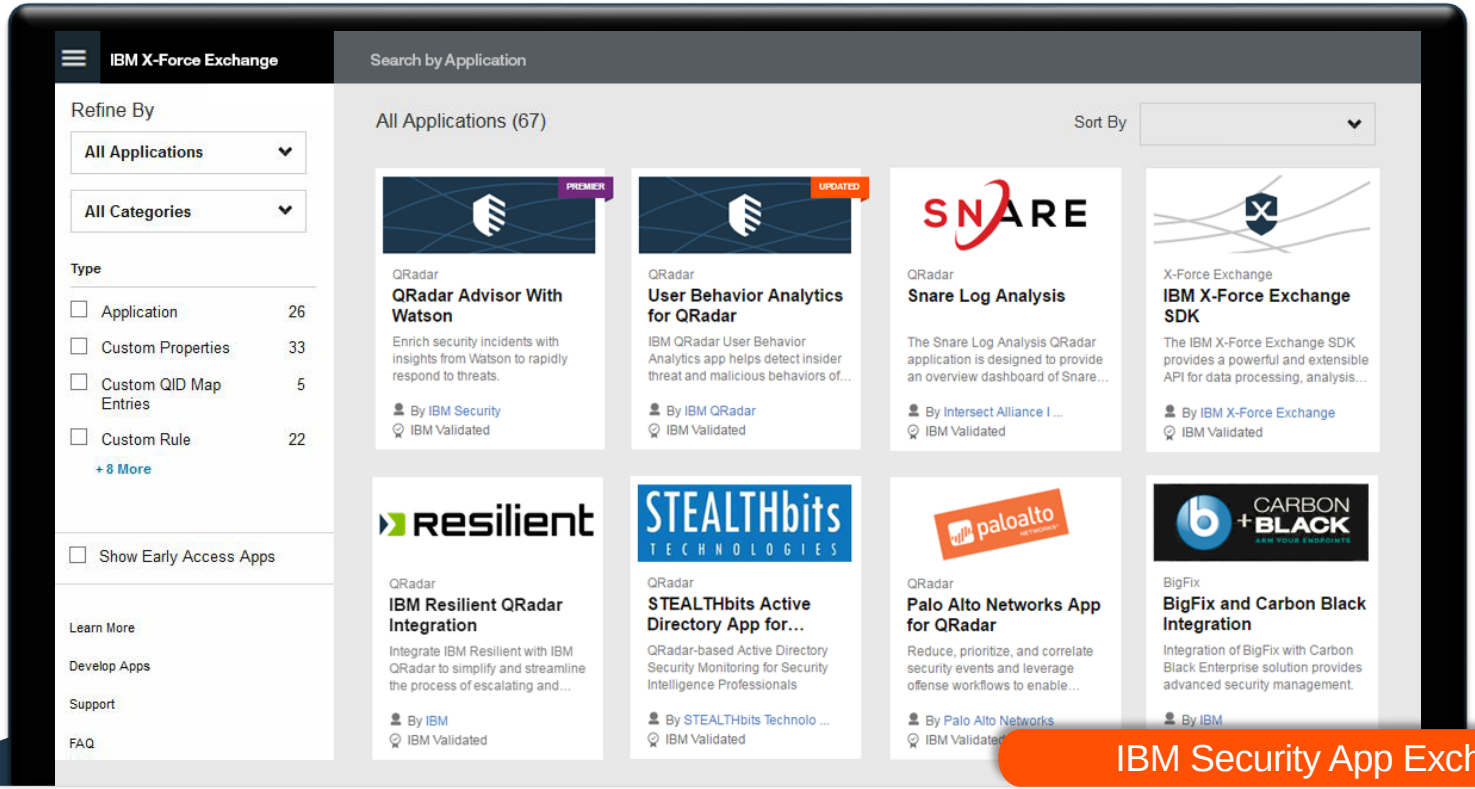


Экосистема технологических партнеров

- 200+ партнеров, 550+ QRadar интеграций



Экосистема защиты через сотрудничество

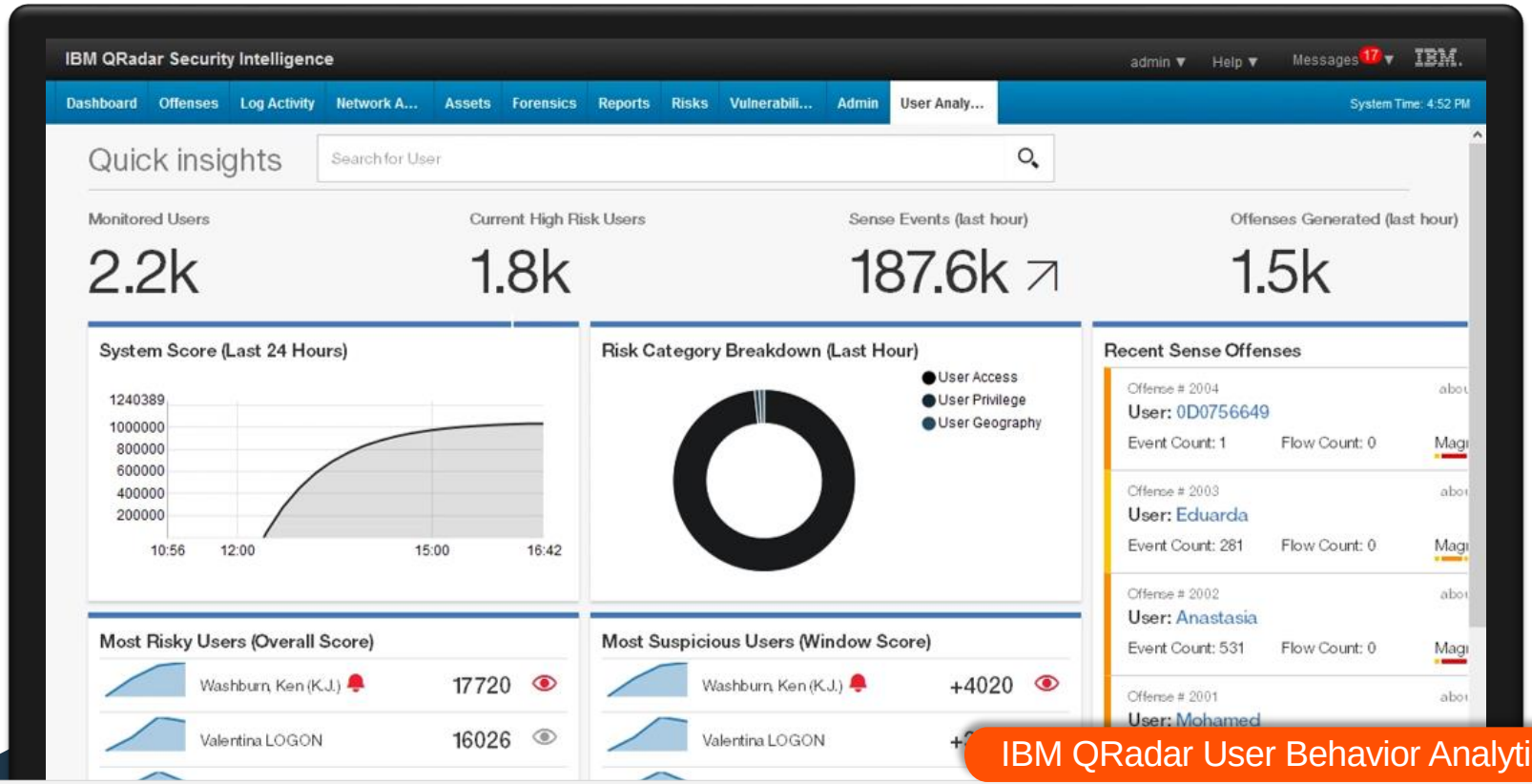


IBM Security App Exchange

Создавайте и используйте приложения на основе технологий IBM security

- **100+ приложений** созданных IBM и партнерами
- **49K+** посещений
  28K+ скачиваний приложений
  с момента начала работы в Декабре 2015

Обнаружить аномальное поведение одним кликом

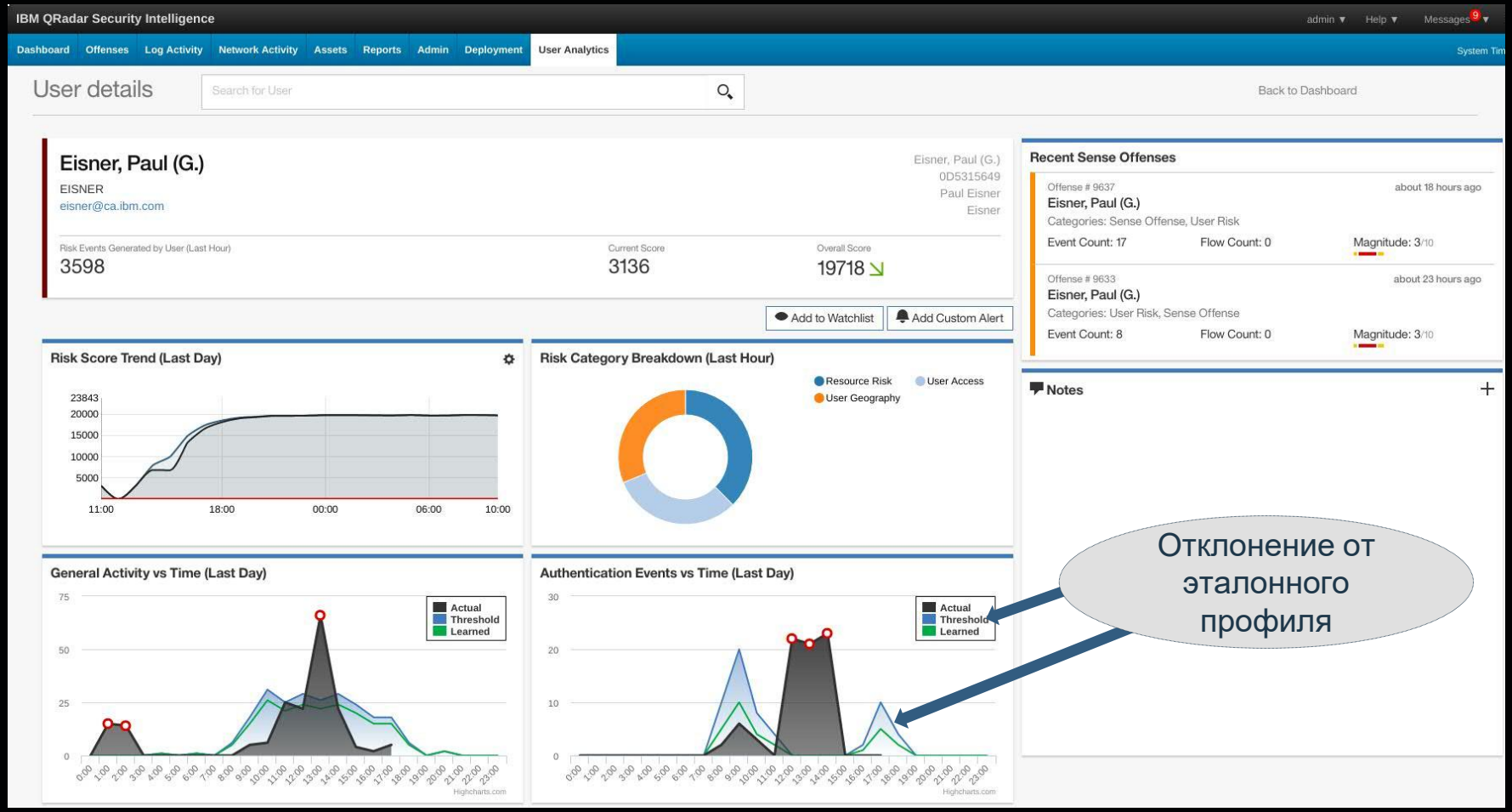


IBM QRadar User Behavior Analytics

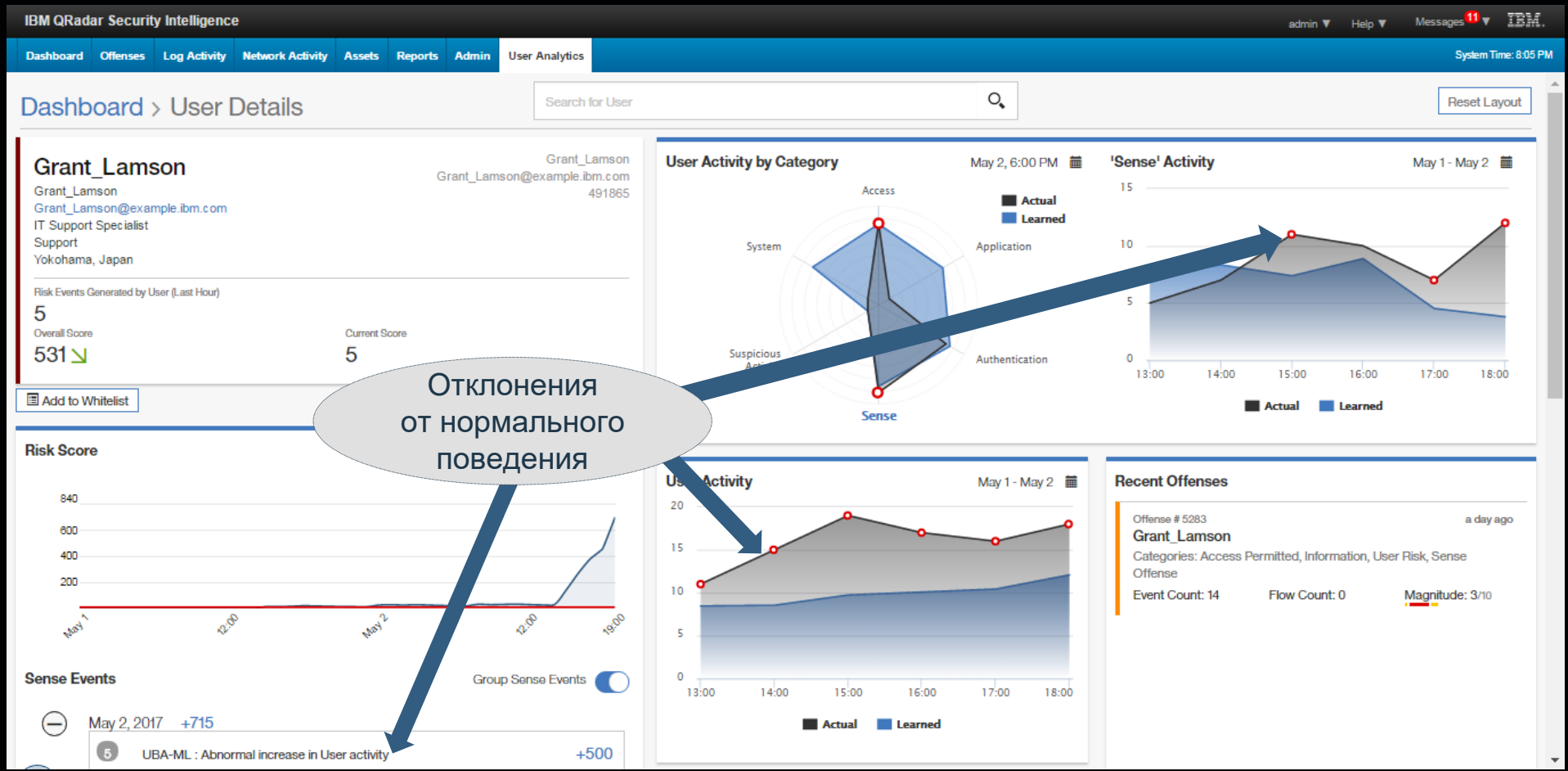
Приложение для визуализации действий каждого пользователя и выявления его аномального поведения

Консоль User Behavior Analytics является интегрированной частью консоли QRadar

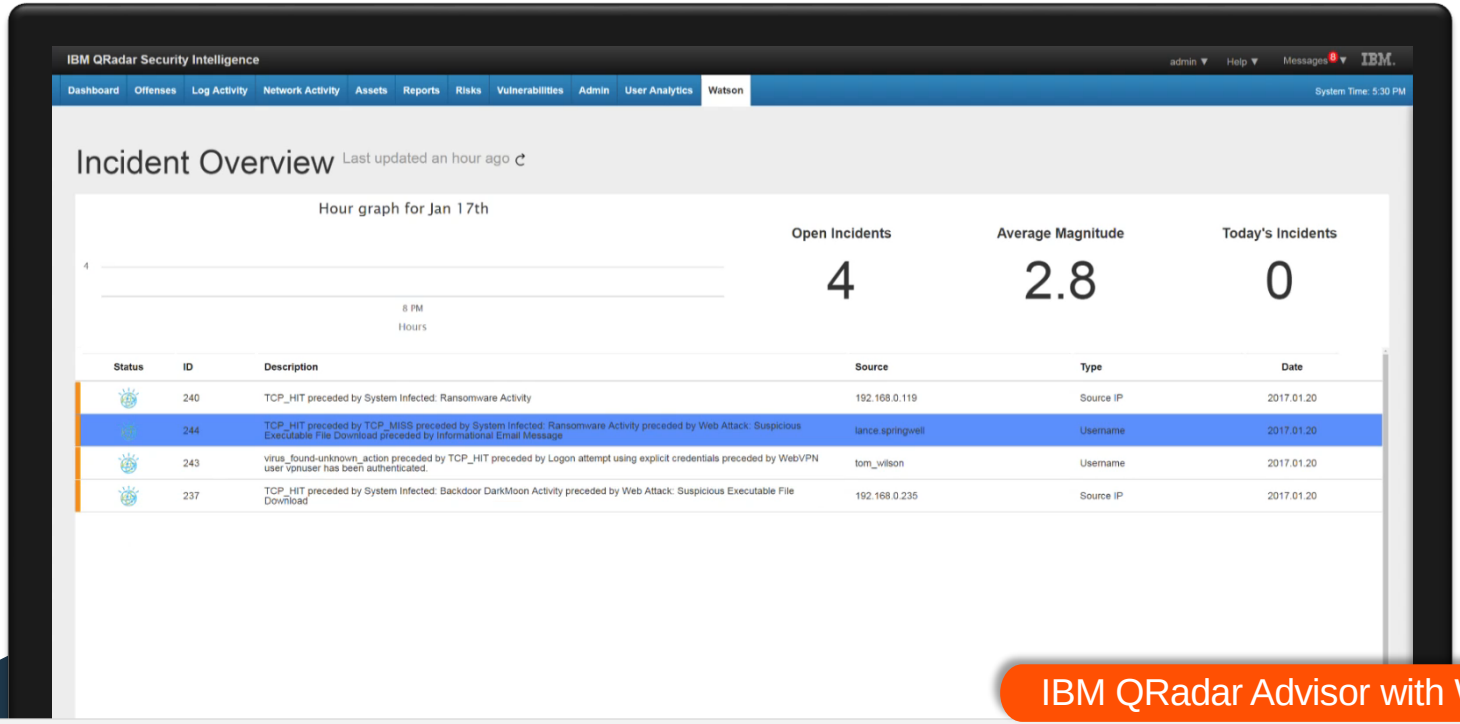
Эталон поведения (порог срабатывания)



UBA: Алгоритмы машинного обучения



Революционное изменение в работе аналитиков ИБ



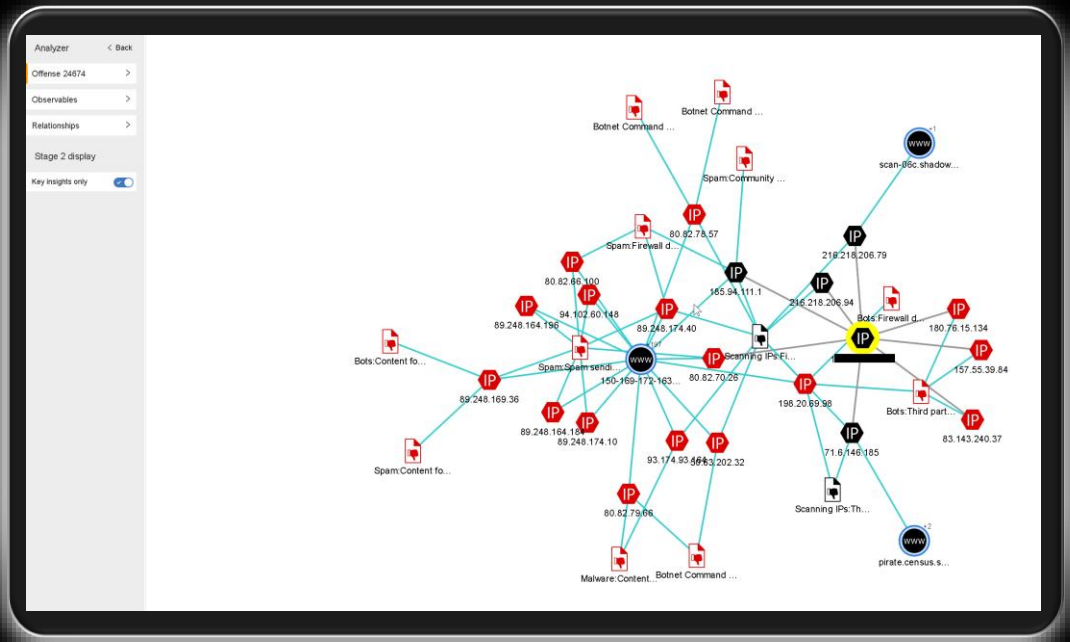
IBM QRadar Advisor with Watson

Автоматически раскрывает новый контекст ИБ и полную картину инцидента

- **2.3 Млн+** документов ИБ
- **10 Млрд+** элементов данных ИБ
- **80 тыс+** новых документов читается каждый день
- **250 тыс+** расследований проведено за последние 6 месяцев

Внешнее сканирование

Ключевые Индикаторы Watson

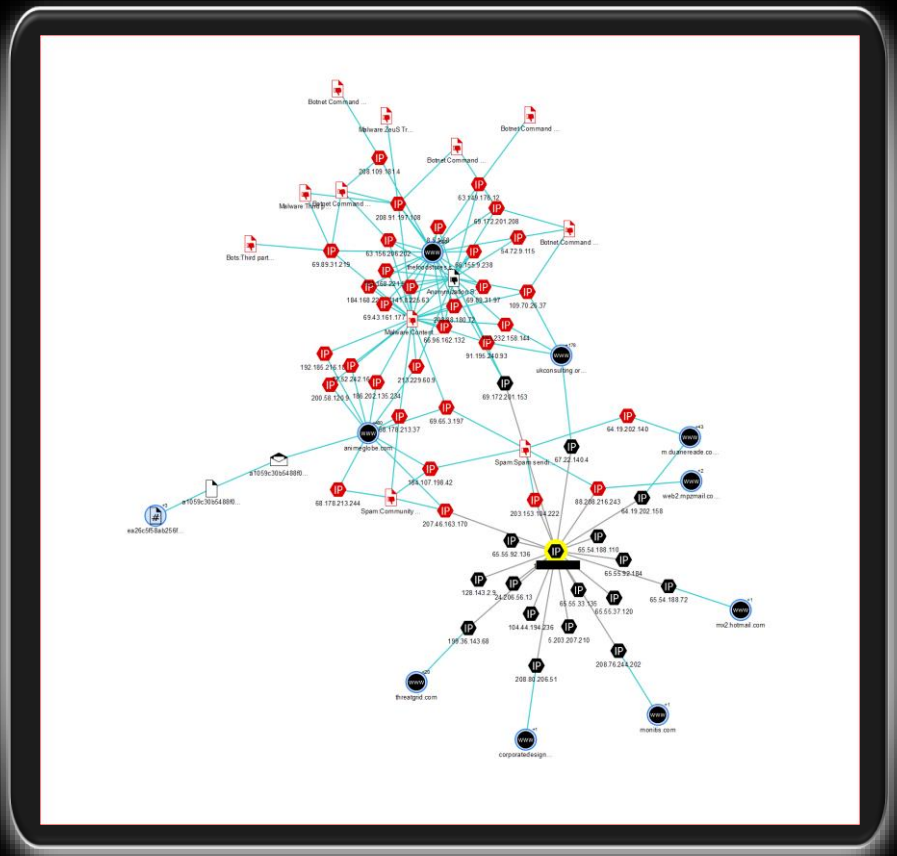


Нарушение – внешнее сканирование

- Внешнее сканирование
- Выглядит как Shodan
  - Аналитик отметил лишь факт
- Watson наполнил инцидент дополнительной информацией
  - Сервер управления Botnet
  - СПАМ-сервера
  - Распространитель вредоносного ПО

Клиент выходит на связь с Botnet IP

Индикаторы Watson



Botnet IP

- QRadar завел инцидент при попытке пользователя выйти на связь с botnet IP
  - Аналитик вручную нашел 5 связанных индикаторов пока мы ждали результат от Watson
- Watson показал расширенную картину угрозы с более чем 50 индикаторами, включая
  - Хэши эл.почты
  - Хэши файлов
  - IP-адреса
  - Домены

IBM Security

СПАСИБО

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM