

Единая платформа Security Intelligence как основа SOC



Олег Бакшинский

Security Intelligence Sales Representative R\CIS

Июнь 2016

Содержание

- Пять основных столпов построения успешного SOC
- Платформа Security Intelligence
- Новости IBM по теме SOC

Пять столпов успешного SOC

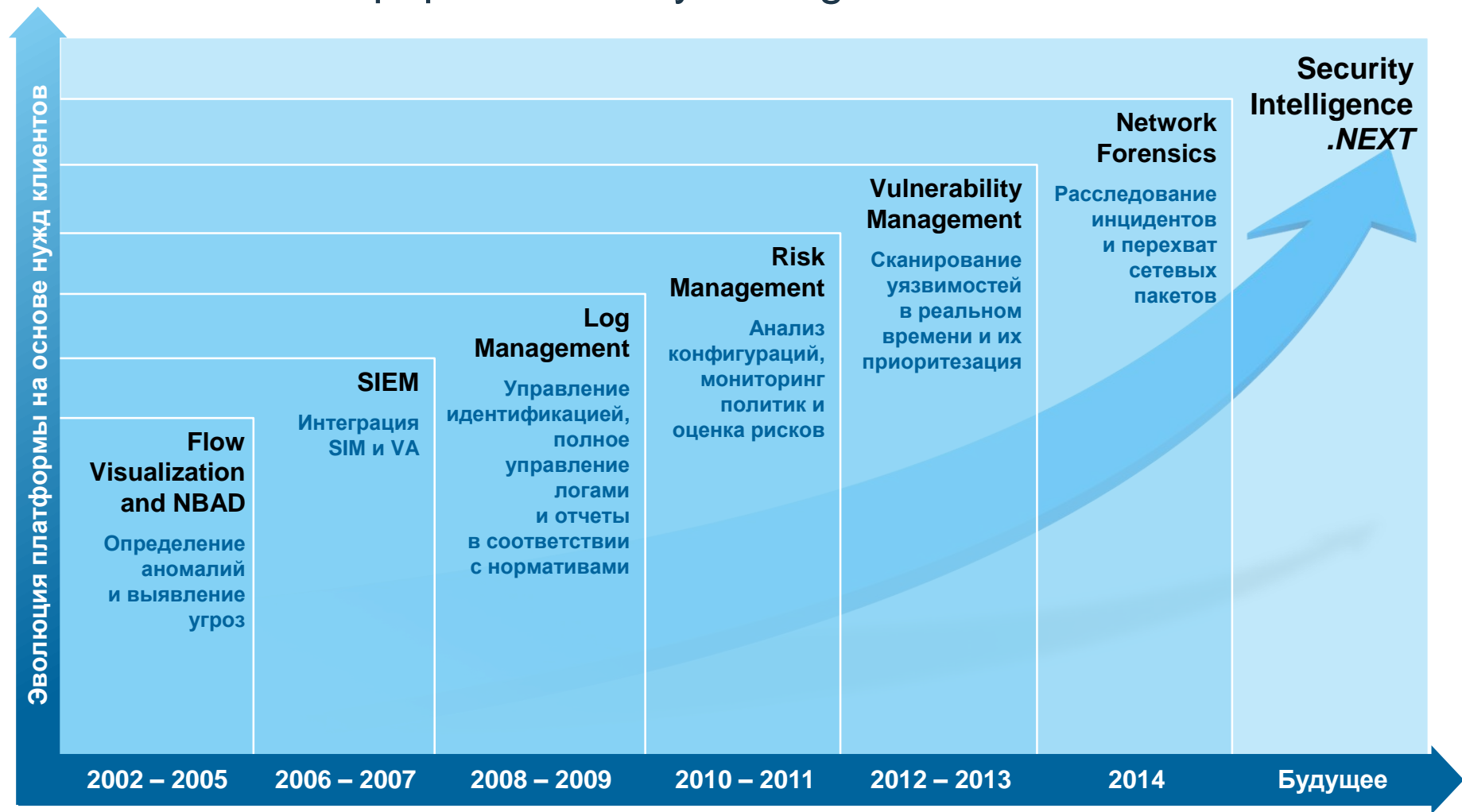
1. Определить и установить цели мониторинга
2. Найти правильную техническую конфигурацию
3. Собрать команду специалистов
4. Выстроить процессы реагирования на инциденты
5. Заручиться поддержкой ИТ и других департаментов



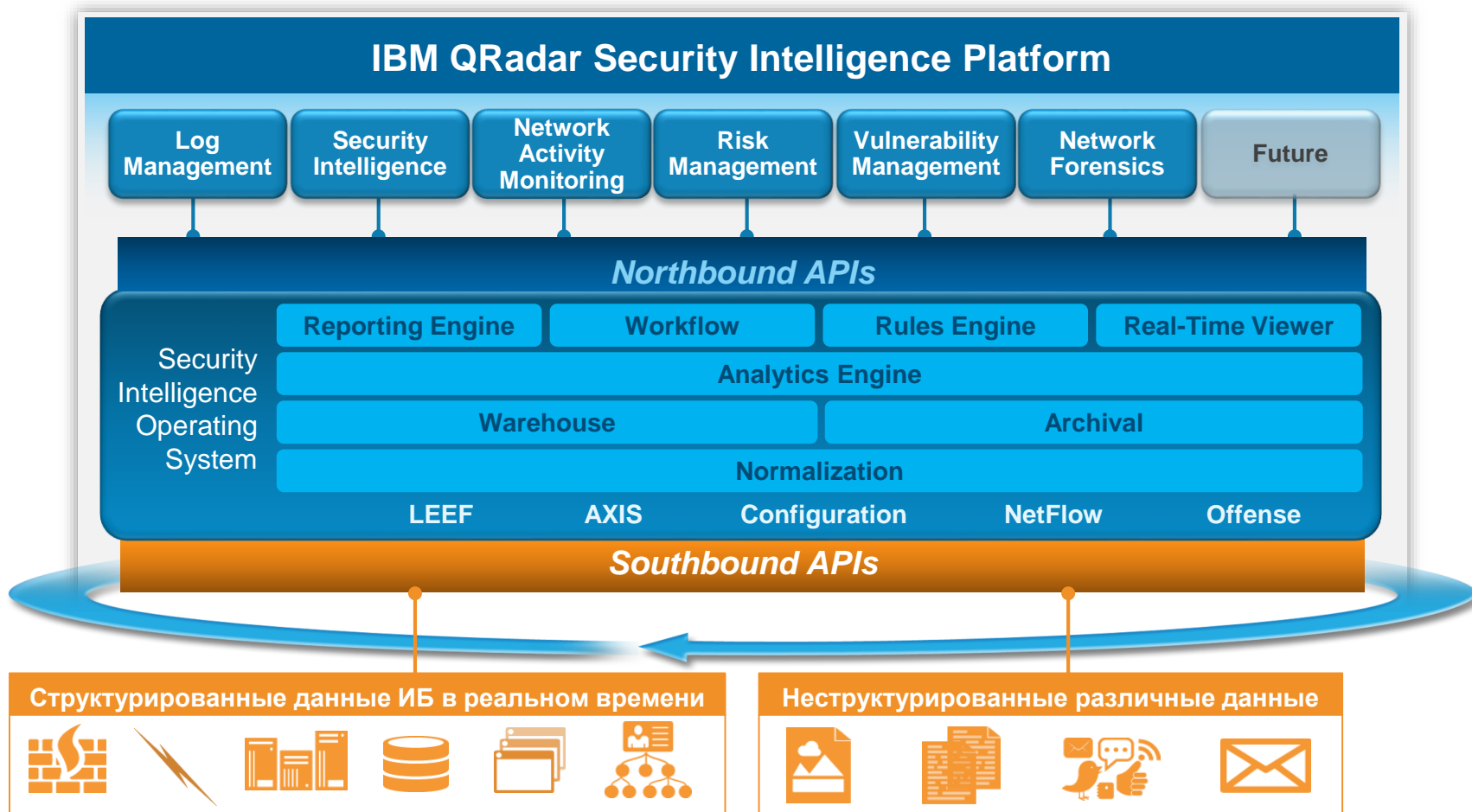
Платформа Security Intelligence



Развитие платформы Security Intelligence



Единая специализированная платформа



Интегрированная архитектура и единый интерфейс работы

Log
Management

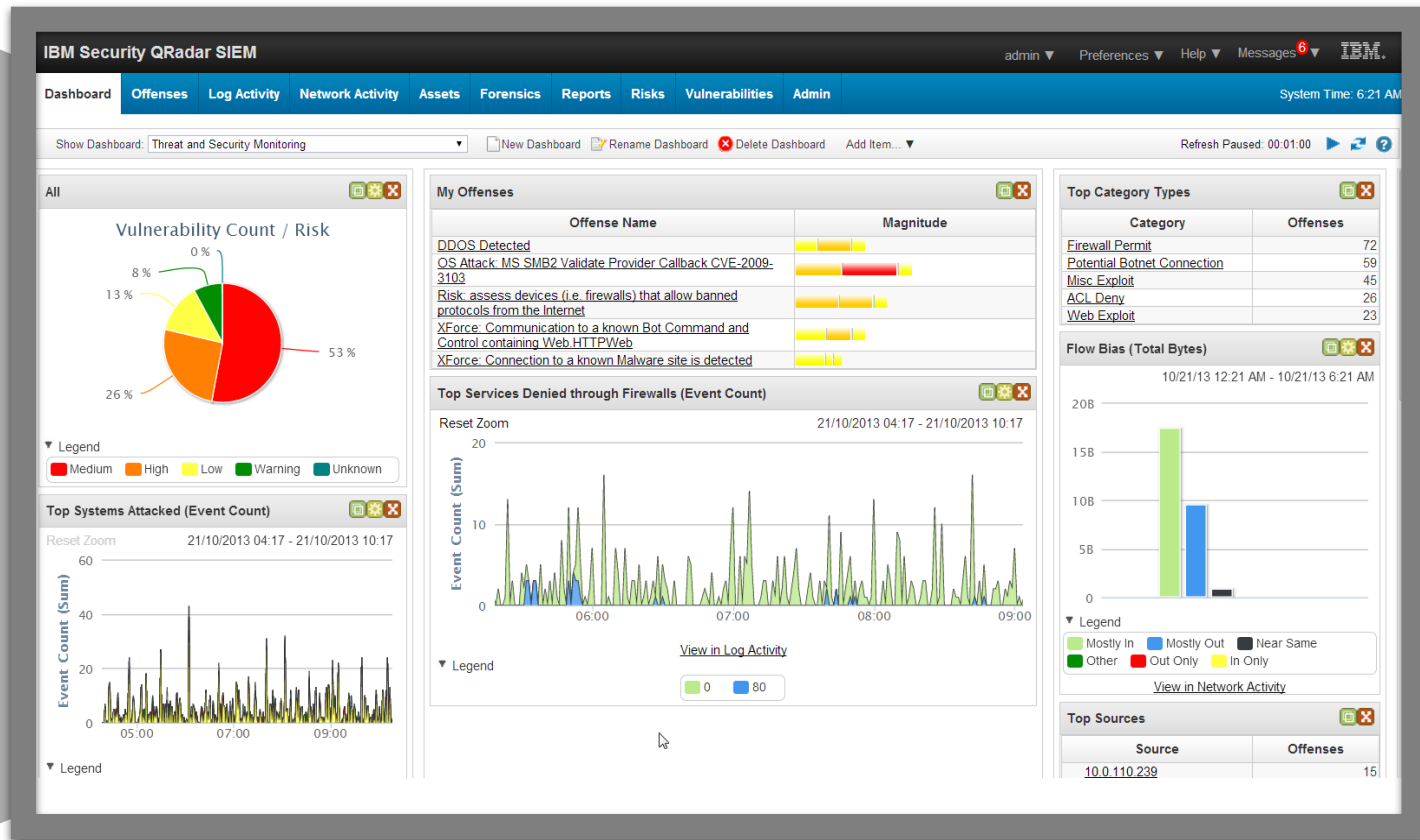
Security
Intelligence

Network
Activity
Monitoring

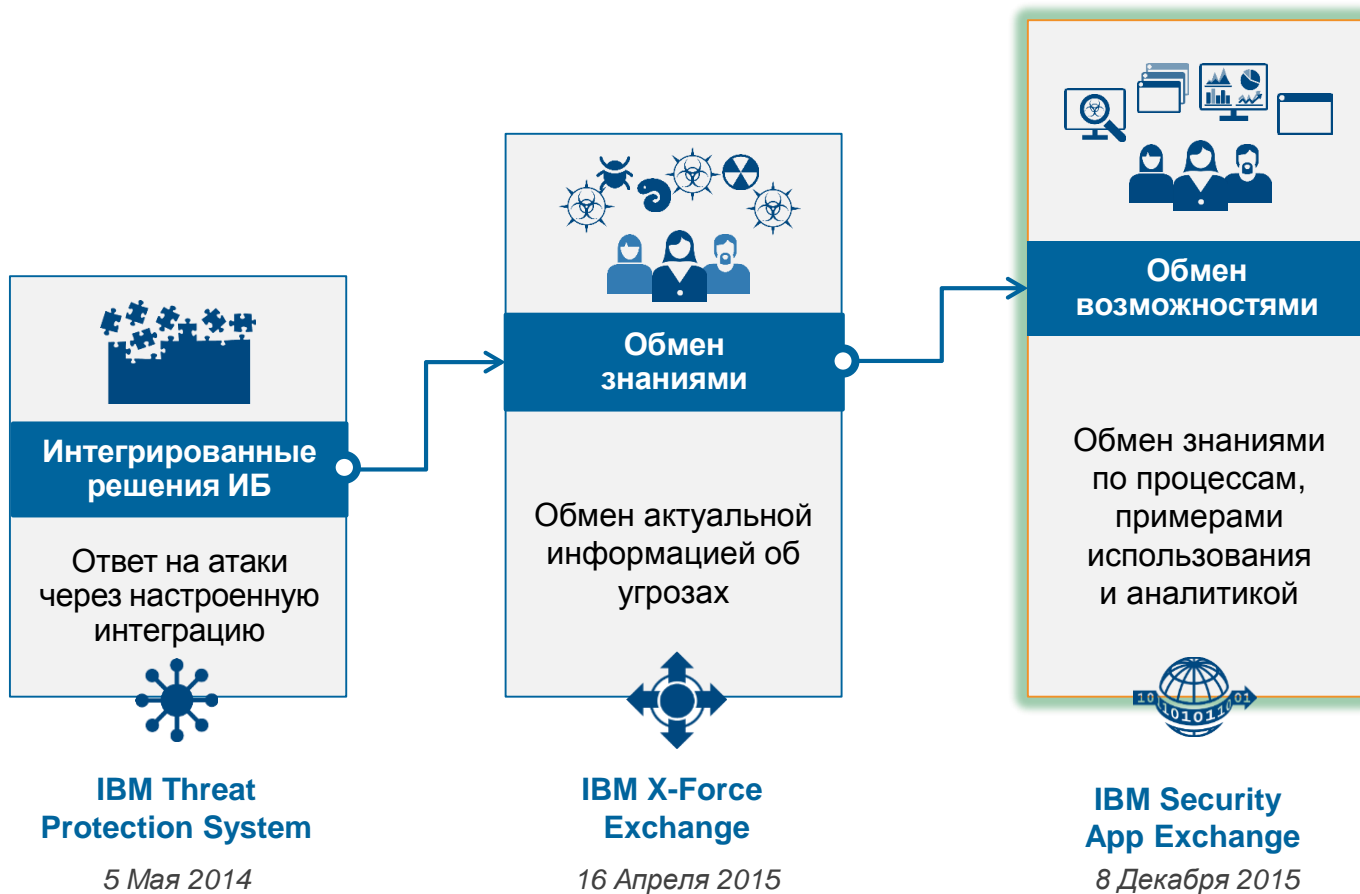
Risk
Management

Vulnerability
Management

Network
Forensics



IBM инвестирует в развитие коалиционной защиты



Платформа взаимодействия

NEW

IBM Security App Exchange

Сертифицированные приложения ИБ

Единая платформа для взаимодействия

Доступ к инновациям партнеров

Быстрое расширение функционала

IBM X-Force Exchange

Search by Application

Create IBM ID Log In

Refine By

All Applications

All Industries

Type

<input type="checkbox"/> Application	10
<input type="checkbox"/> Custom Properties	21
<input type="checkbox"/> Custom QID Map Entries	2
<input type="checkbox"/> Custom Rule	9

+ 7 More

Find. Download. Use.

Featured

StealthINTERCEPT

StealthINTERCEPT App for QRadar

STEALTHbits Technologies ...

Active Directory, File System, and Exchange Security

★★★★★

Bit9 + CARBON BLACK

Carbon Black App for IBM QRadar

Bit9 + Carbon Black

The Carbon Black App for IBM QRadar allows administrators to access to see, detect and take...

★★★★★

exabeam

Exabeam User Behavior Analytics

Exabeam

Exabeam is a user behavior analytics solution that leverages existing log data to quickly...

★★★★★

resilient

Resilient Systems Integration for QRadar

Resilient Systems, Inc.

Integrate the Resilient Incident Response Platform (IRP) with IBM QRadar to simplify and...

★★★★★

All Applications (34)

Sort By **Newest**

StealthINTERCEPT

b

iSIGHTPARTNERS

NEW

IBM инвестирует в развитие коалиционной защиты



- Больше гибкости, меньше сложности
- Экономические и операционные выгоды
- Понятная интеграция процессов
- Объединенные компоненты помогают в конкретных примерах использования

Компоненты QRadar API



Открытые API для быстрой разработки и внедрения инноваций

**Примеры
использования**



Insider Threats



Internet of Things



Incident Response

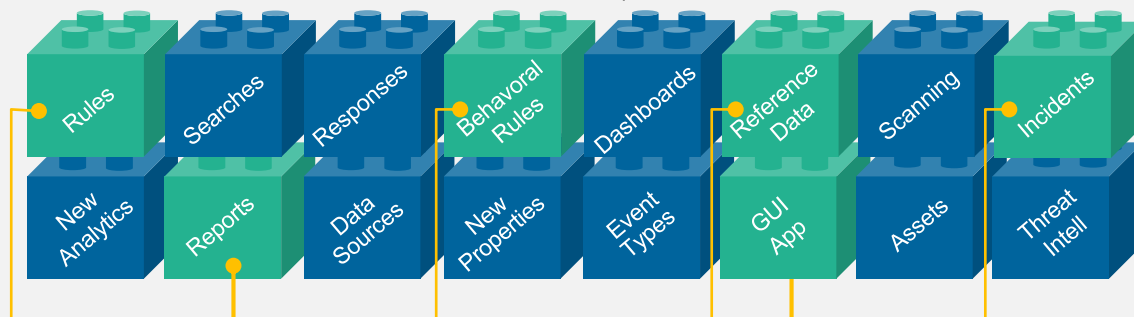
Пример использования: Угрозы от инсайдеров



- Постоянная оценка рисков от пользователей
- Информирование об активностях регуляторов
- Выявление аномальных активностей через модели поведения
- Быстрое расследование активности пользователя
- Обмен информацией с другими системами и кадровыми подразделениями для лучшего контекста

Больше гибкости, меньше сложности

Компоненты QRadar API



**Примеры
использования**



Insider Threats



Internet of Things



Incident Response

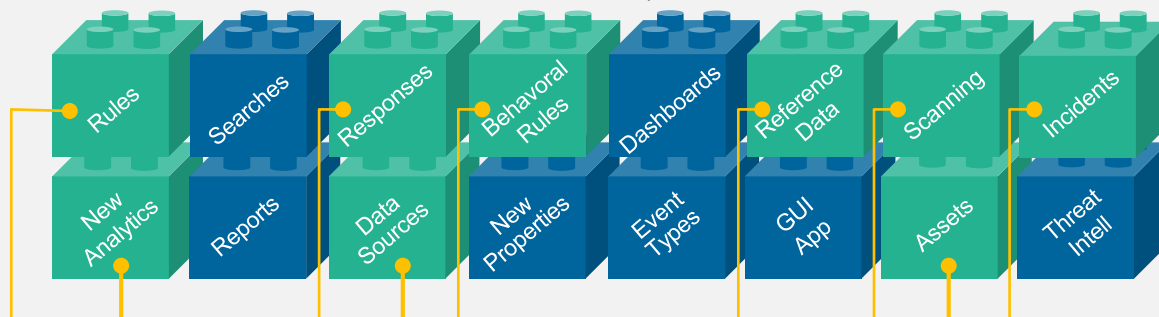
Пример использования: Интернет вещей



- Обнаружение и классификация новых “вещей”
- Особая визуализация сетей “вещей”
- Специальные атрибуты и консоли управления
- Построение поведенческих правил и цепочки последствий для выявления аномалий
- Интеграция новых источников данных и их свойств

Больше гибкости, меньше сложности

Компоненты QRadar API



**Примеры
использования**



Insider Threats



Internet of Things



Incident Response

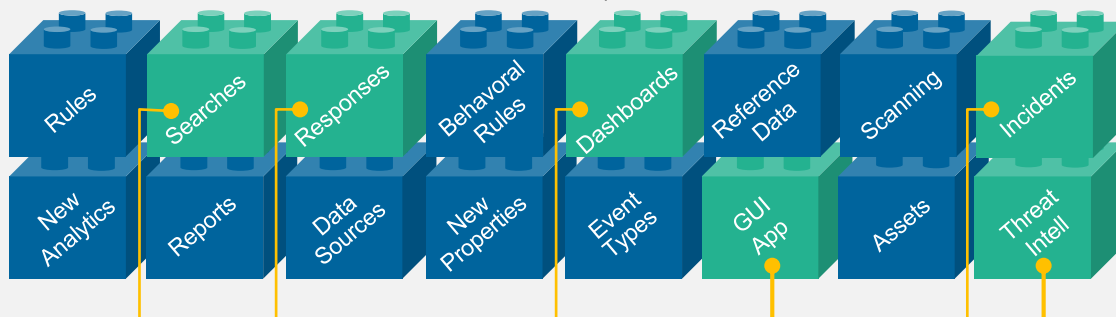
Пример использования: Реагирование на инциденты



- Полная уверенность в том, что выявленные инциденты находятся в процессе реагирования
- Автоматизация реагирования на инциденты и процедур
- Ассоциация доказательств из QRadar с открытым делом по инциденту
- Отслеживание прогресса в процессе реагирования и приоритезация

Больше гибкости, меньше сложности

Компоненты QRadar API



**Примеры
использования**



Insider Threats



Internet of Things



Incident Response

Новый функционал от IBM Security

Визуализация инцидентов



Отслеживать угрозы

IBM Security: Incident Visualization

- Понимание цепи атаки
- Идентификация общего влияния угрозы
- Реакция быстрее через понимание движения данных
- Расследование для выявления сути атаки
- Связь между IPs вовлеченными в нарушение
- Контекст от других ИБ решений

Новый функционал от IBM Security

Threat Intelligence



Add Threat Feed + Create Rule Action +

Configured Threat Intelligence Feeds

<https://api.xforce.ibmcloud.com/taxii>

Collection: xfc.collections.public
Reference Set: Web Servers

Signatures received last poll

Enter credentials to connect to the TAXII server. Then click the "Discover" button to discover a collection to use.

TAXII Endpoint:

Authentication Method:

Username:

Password:

Discover

Collection:

Action Name:

Properties:

Discoverable Type:

Indicator Type:

Cancel Add action

IBM Security: Threat Intelligence

- Загрузка Threat Intelligence через открытые форматы STIX/TAXII
- Загрузка индикаторов угроз в наборах в QRadar Reference sets
- Использование Reference sets для корреляции, поиска, отчетов
- Создание ответных правил на появление новых угроз в наборе
- Пример использования:
Загрузить подозрительные IP-адреса из X-Force Exchange создать правило увеличения магнитуды любого нарушения с такими IP

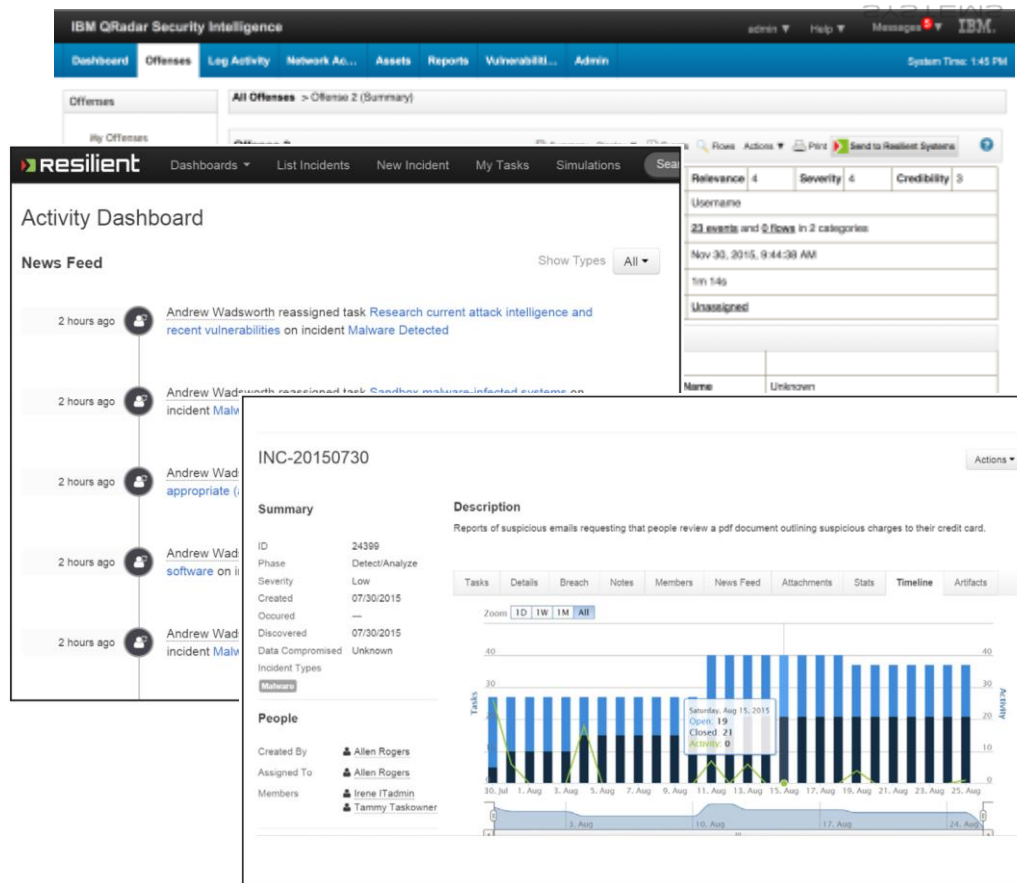
Интеграция QRadar и Resilient

Единый центр выявления угроз и реагирования на них

- Автоматизированная и ручная связь между инцидентами Resilient и QRadar
- Ассоциация QRadar доказательств по инциденту с данными в Resilient
- Автоматическая синхронизация статуса и записей по инциденту

Преимущества

- Уменьшение времени принятия ответного решения
- Контроль над процессом реагирования
- Выполнение требований регуляторов
- Позволяет персоналу использовать время более эффективно
- Наполняет процесс реагирования на инциденты информацией от бизнеса и аналитикой



QRadar + Incident Response

QRadar
Приоритезация информации из Logs, Flows, Vulns, User, Config Data и т.п.

Процесс реагирования SOC на инцидент ИБ для ответа на угрозы, дыры, уязвимости

ИСТОЧНИКИ ДАННЫХ

Security devices
Servers and mainframes
Network and virtual activity
Data activity
Application activity
Configuration information
Vulnerabilities and threats
Users and identities
Global threat intelligence



QRadar Sense Analytics™

- Extensive data collection, storage, and analysis
- Real-time correlation and threat intelligence
- Automatic asset, service and user discovery and profiling
- Activity baselining and anomaly detection

Встроенный Интеллект



Prioritized incidents

Создание инцидента

- Присвоение типа (напр. уязвимость)
- Присвоение бизнес характеристики в зависимости от типа (напр. Риск)

Сбор контекста и назначение задач

- Сбор дополнительных доказательств
- Применение требования регуляторов
- Назначение задач ответственным

Восстановление и Закрытие

- Постановка задач восстановления команде
- Подтверждение восстановления
- Закрытие инцидента
- Отчет/Уведомление

База всех инцидентов ИБ

Отчет по инциденту и уведомление

Постоянная аналитика ИБ

Три этапа инцидента ИБ

Улучшение процесса выявления инцидентов

Новости IBM по теме SOC



IBM помогает строить самый большой SOC в РФ

Разработчиком Центра информационной безопасности Сбербанка выбрана IBM

*Выбор подрядчика

В апреле 2016 года [IBM](#) была выбрана консультантом [Сбербанка](#) по развитию единого операционного центра информационной безопасности (Security Operation Center, SOC).

В рамках проекта американская корпорация проведет обследование и анализ процессов управления и обеспечения, реализованных в существующем SOC Сбербанка, обследование ИТ и ИБ – инфраструктуры внешнего и внутреннего сетевых сегментов банка, проверку и анализ текущего состояния системы управления инцидентами ИБ (SIEM).

Срок оказания услуг составляет 3 месяца с даты заключения договора. В результате IBM должна будет спроектировать целевую модель SOC на основе «лучших мировых практик» и предоставить Сбербанку детальную дорожную карту поэтапного развития SOC.

Консультанта по развитию центра Сбербанк выбирал с декабря 2015 года^[1]. Максимальная цена контракта составляла 60,9 млн рублей, IBM согласился выполнить работу за 56,9 млн.

Заявки на участие в конкурсе также подавали [Microsoft Россия](#), [Accenture](#) и [Deloitte](#). Самое большое снижение максимальной цены контракта предлагала Microsoft: компания готова была

- покупка компани
- "БОСС Гонвар
- Softline данные центра
- Утвержд СпецТс надежн
- Подвод систем девело
- Омега I миллис



СПАСИБО

FOLLOW US ON:



ibm.com/security



securityintelligence.com



xforce.ibmcloud.com



[@ibmsecurity](https://twitter.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.