IBM Security

IBM Security

Технологии защиты IBM и расследования

Арменак Аракелян
Руководитель технического направления IBM в группе компаний МОНТ

IBM

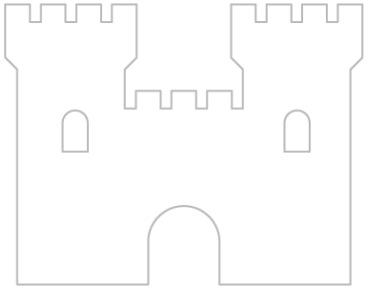
Вычислительные мощности

Сегодня

Безопасность

Будущее и настоящее.

До 2013

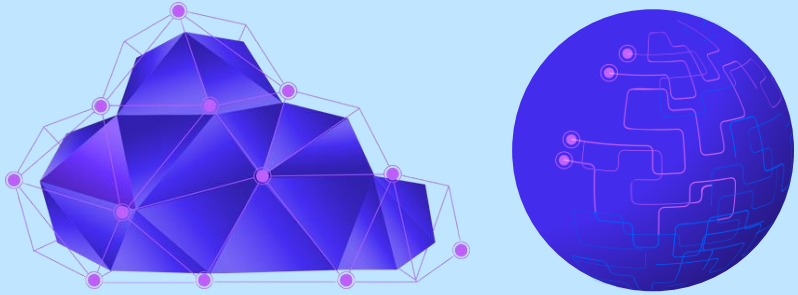


2013-2018

2019+

Connected security

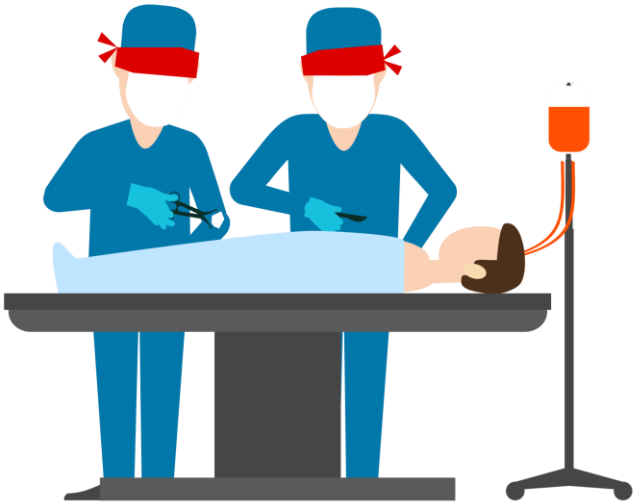
AI, ML

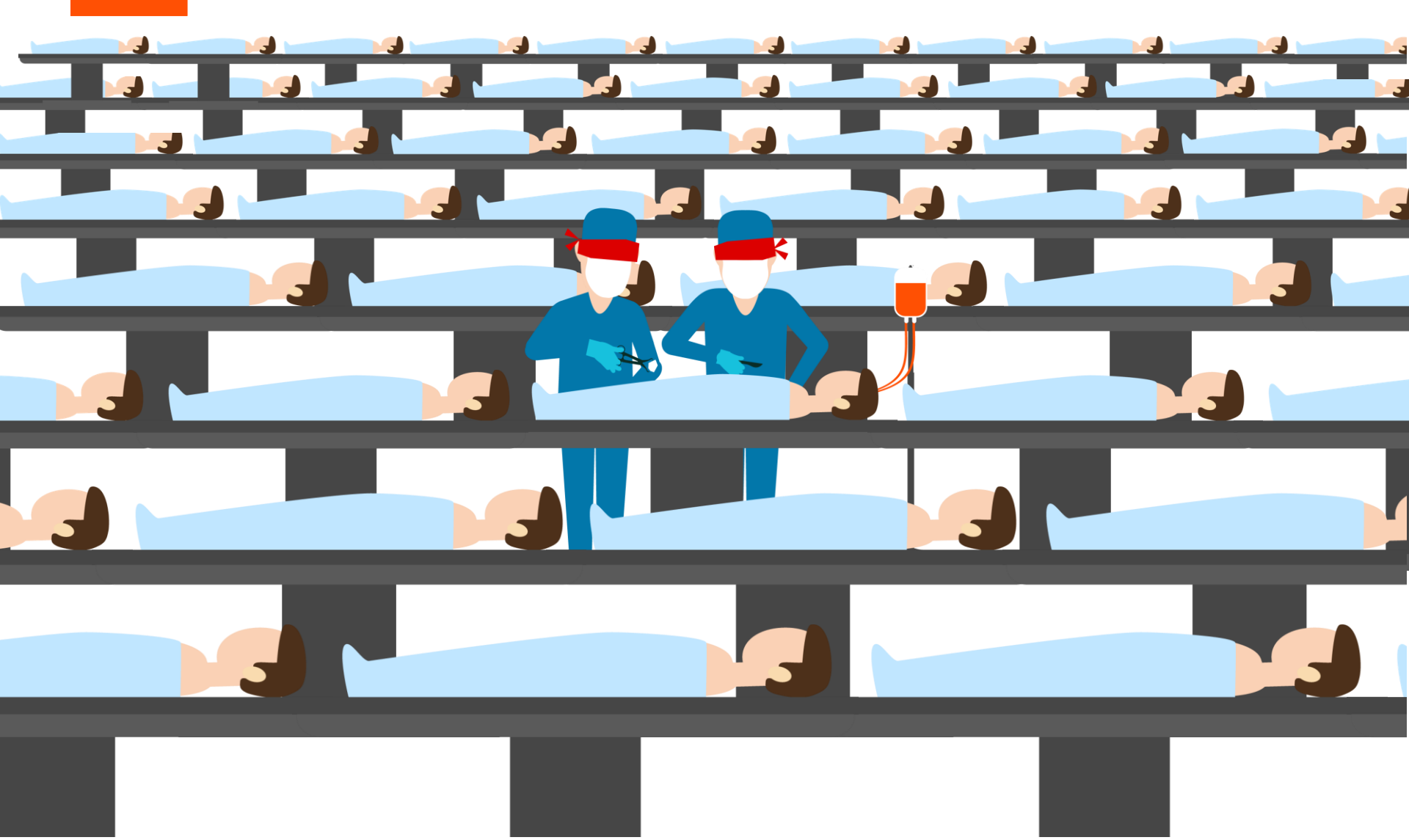


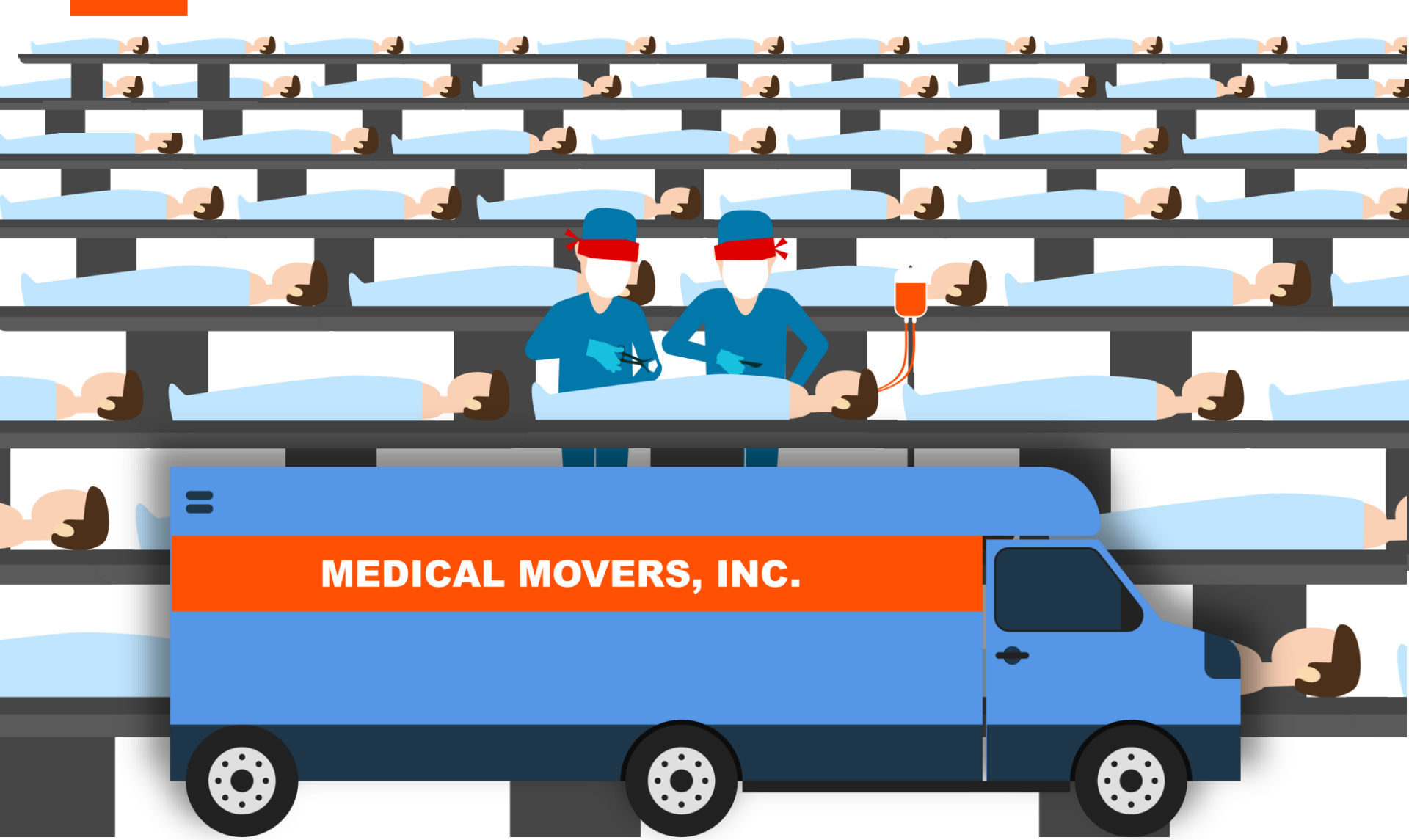
- **8,000+** сотрудников
- **17,500+** клиентов
- **133** страны
- **3,500+** патентов
- **Самый крупный Security Стартап**

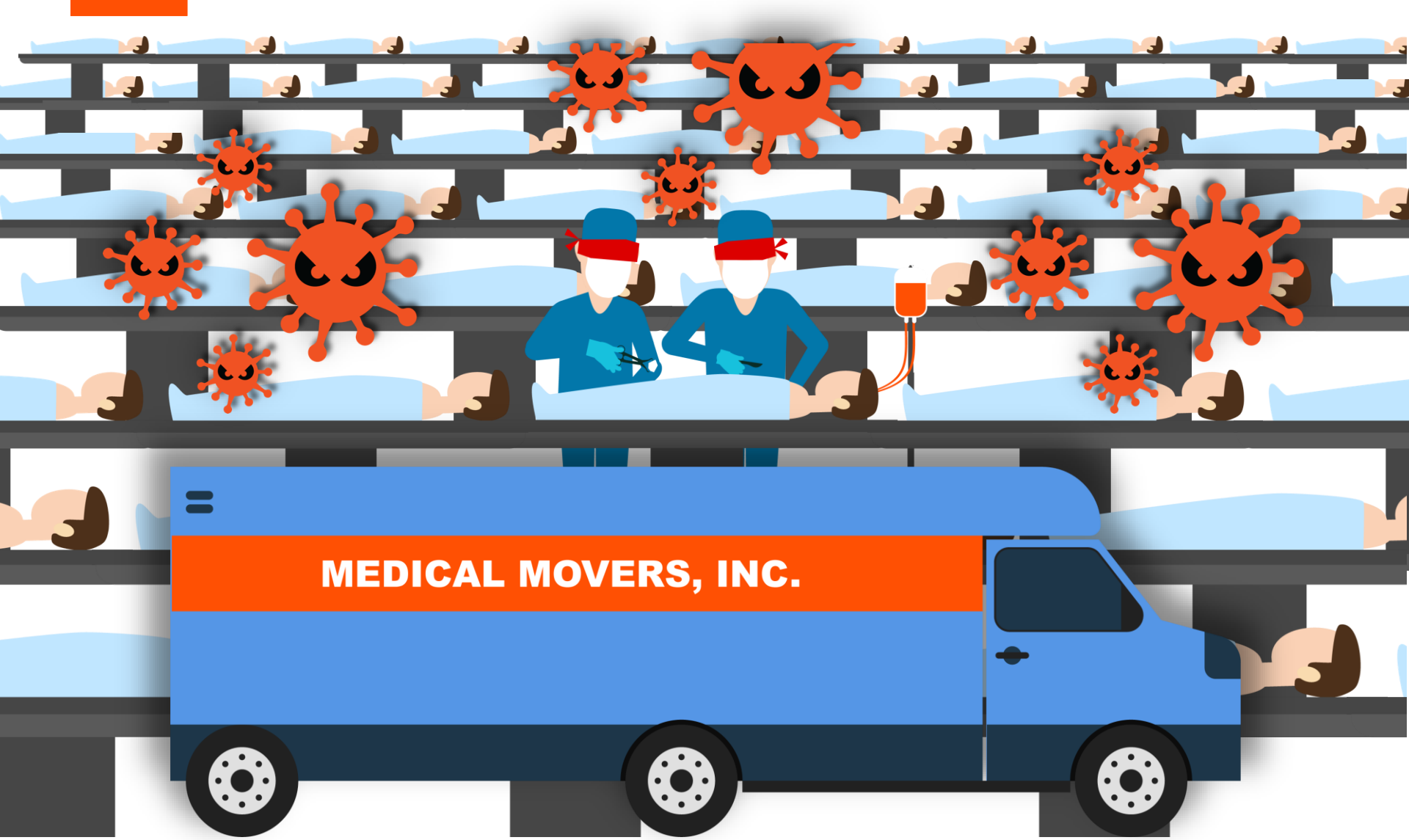
- **2 Представительства** в Казахстане
- **20+** партнеров
- Постоянные обучения

IBM Security

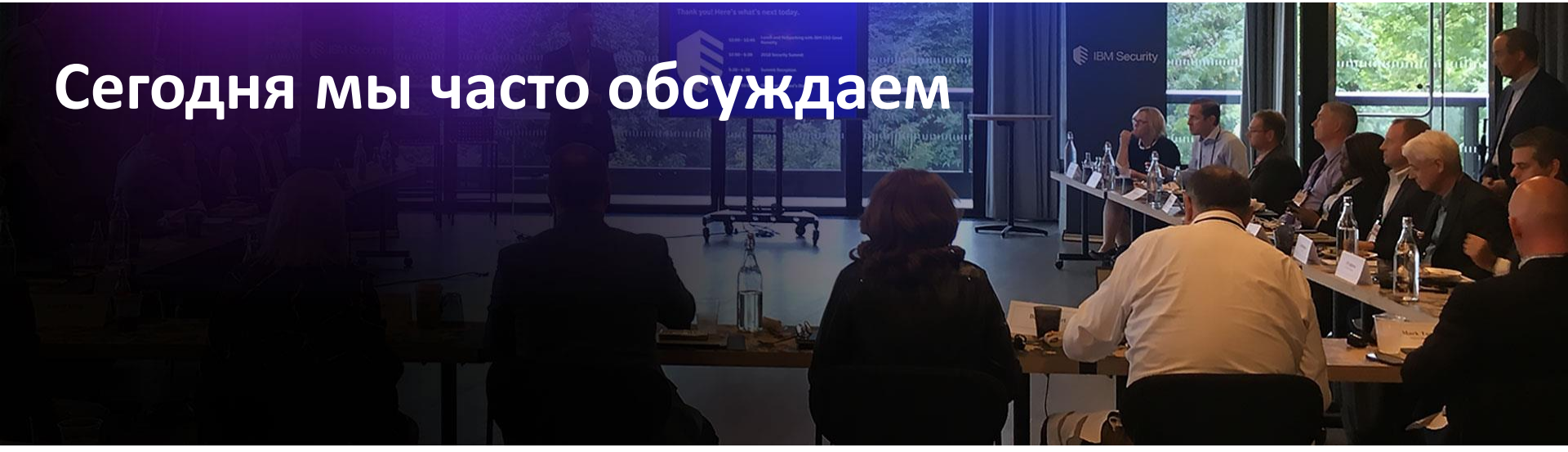





MEDICAL MOVERS, INC.


MEDICAL MOVERS, INC.

Сегодня мы часто обсуждаем



Нам нужны новые **контроли**

Нам не хватает **сотрудников**

Как нам защищать **IoT**?

Мы уходим в **облако**

Что делать с **регулятором**?

SOC – сердце инфраструктуры кибербезопасности

Как выиграть время при расследовании инцидентов ИБ?

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

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

Обнаружение IBM Qradar

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

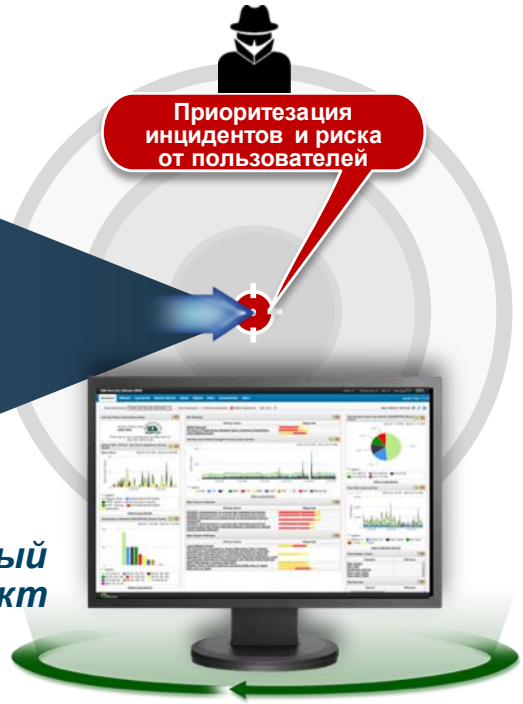
Пользователи и учетные записи

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

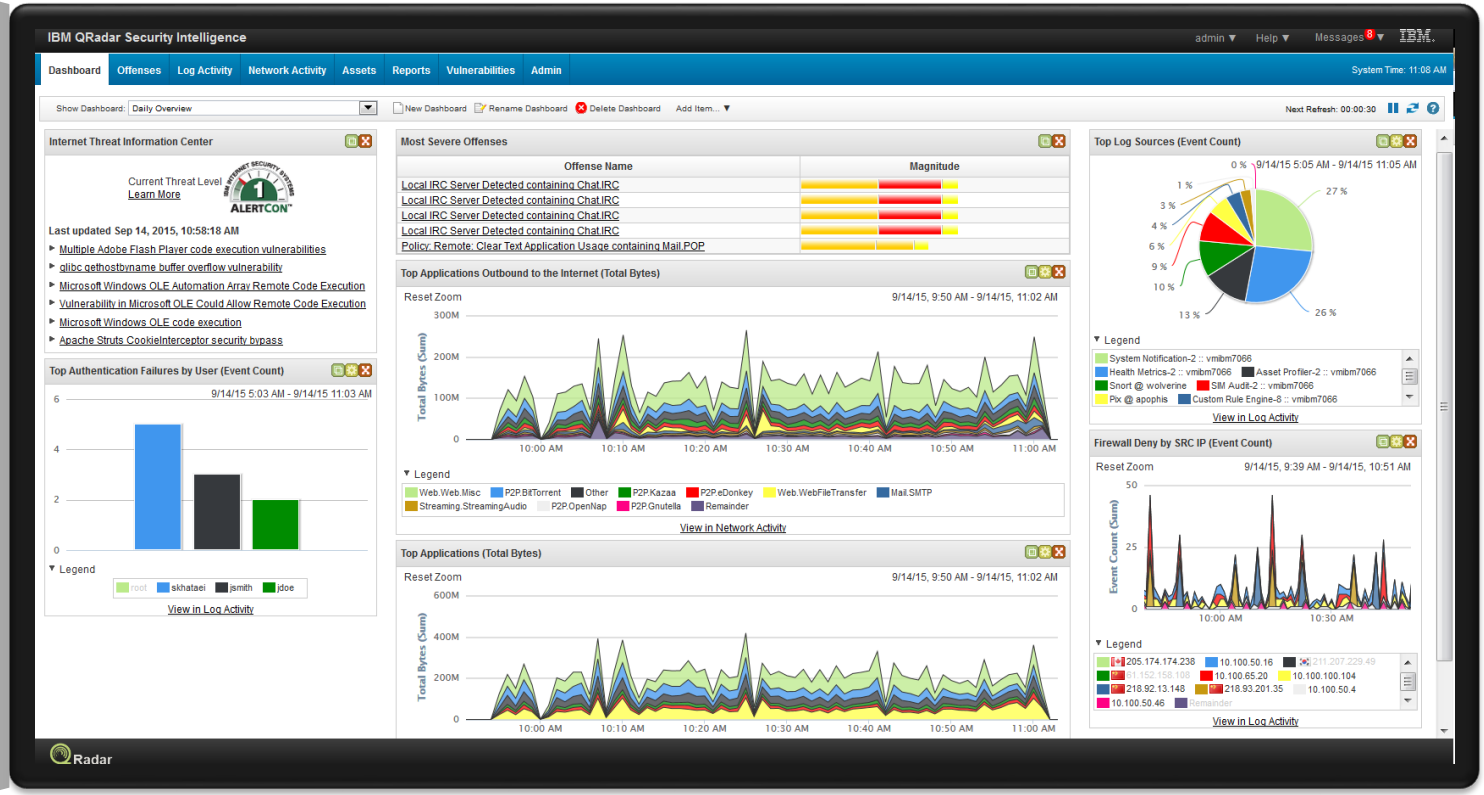


Встроенный Интеллект

Улучшенная аналитика для предотвращения, выявления и реагирования на угрозы

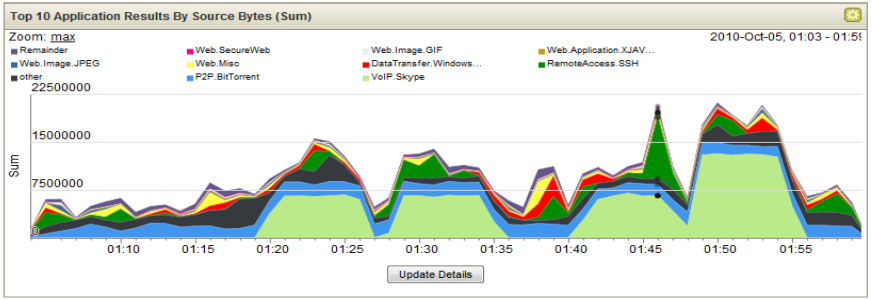
Интегрированная, унифицированная архитектура в одной web-консоли

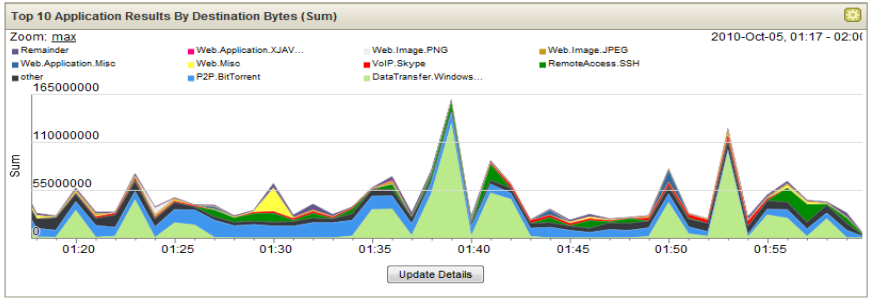
- **Log Management**
- **Security Intelligence and Sense Analytics**
- **Network Activity Monitoring**
- **Vulnerability and Risk Management**
- **Network Forensics**
- **Incident Response**



Анализ сетевой активности

- Определение атак нулевого дня, на которые не выпущены сигнатуры
- Мониторинг политик и детектирование серверов
- Видимость всех путей атак
- Пассивный мониторинг всей сети и создание профилей активов
- Решение проблемы видимости всего происходящего в сети





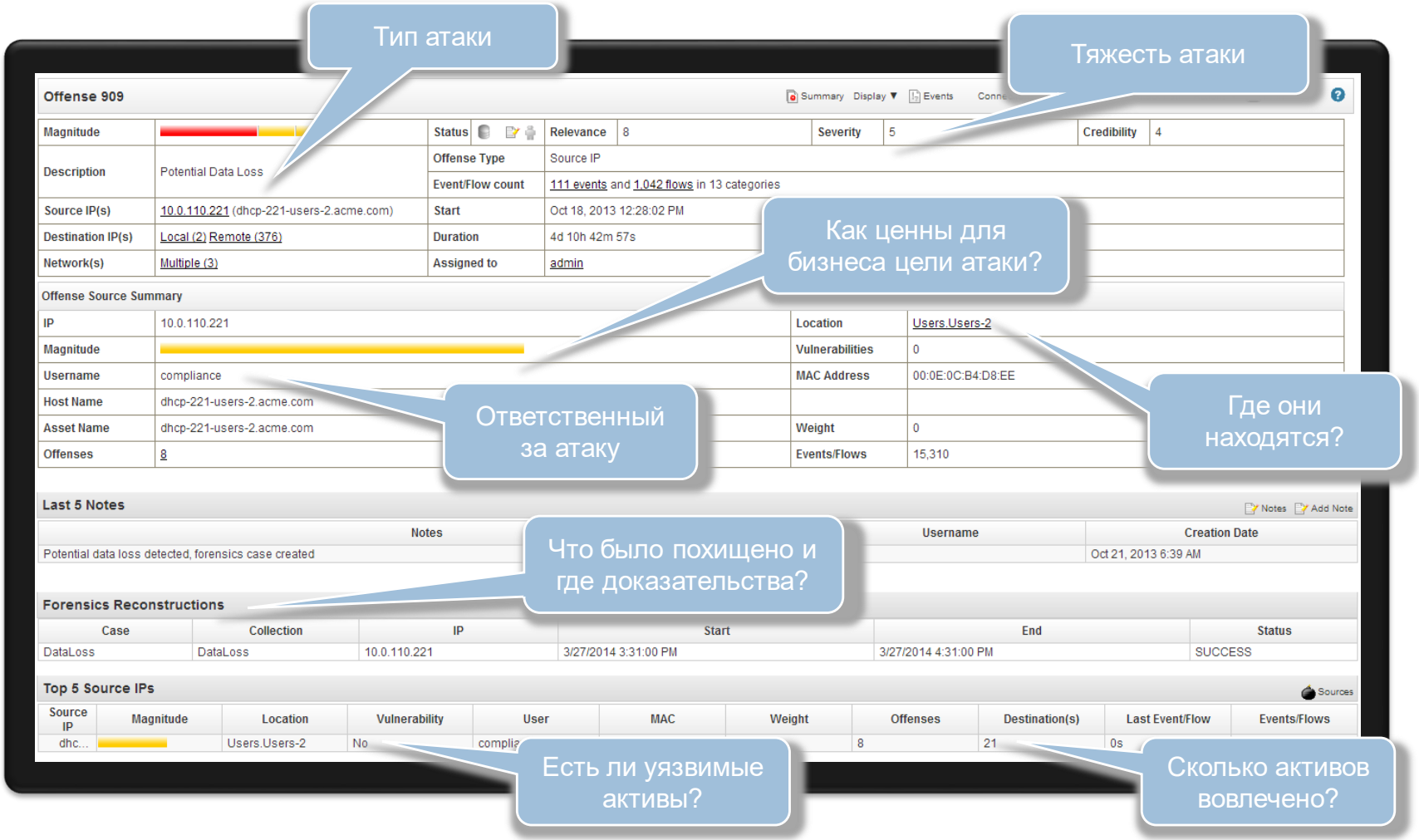
(Hide Charts)

Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708	547 851 023	178 629	390 655	569 284	123
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654	235 838 522	127 854	161 966	289 820	546
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101	206 151 800	93 672	228 533	322 205	6 810
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290	177 991 748	195 570	76 007	271 577	171
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020	149 113 136	101 404	261 727	363 131	122
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741	31 361 821	33 634	23 904	57 538	2 401
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267	23 780 010	8 193	15 674	23 867	89
Web.Image.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204	20 957 061	15 449	14 150	29 599	586
Web.Web.Misc	Multiple (16)	Multiple (4)	Multiple (152)	80	other	266 544	9 127 264	9 393 908	4 184	6 830	11 014	761

Displaying 1 to 40 of 64 items (Elapsed time: 0:00:00.106)

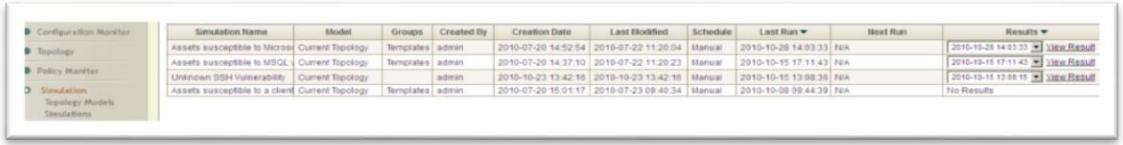
Page: 1 Go < 1 | 2

Выявление потенциальных угроз через аналитику

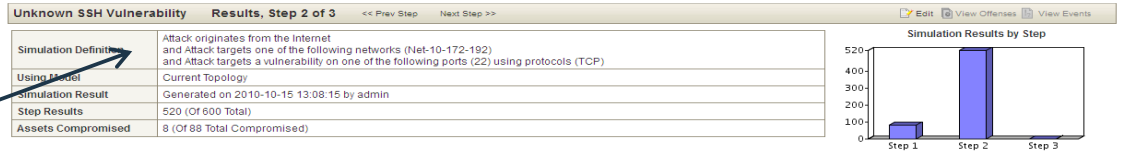


Симуляция атаки с помощью RiskManager

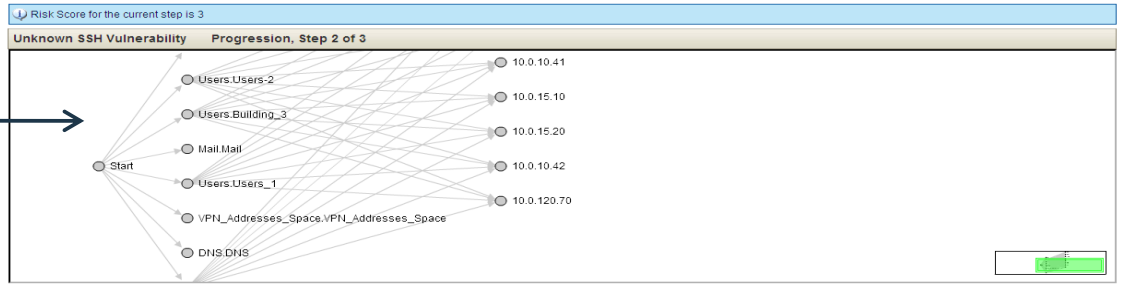
- Выбор симуляции
- Выбрать SSH vulnerabilities'
- Выбрать активы



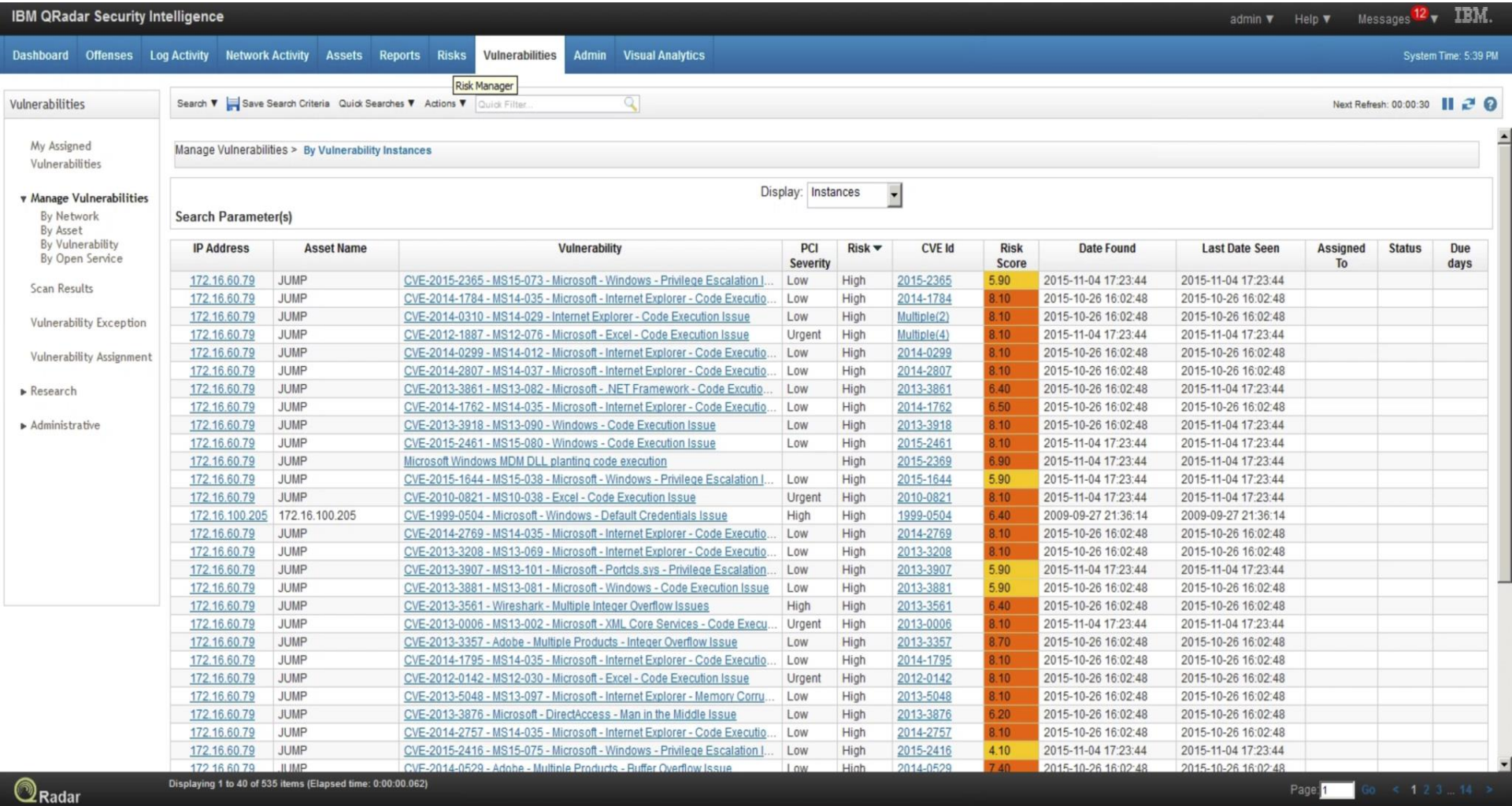
Визуализация…



- Путь атаки
- Распространение
- Мониторинг в режиме РВ

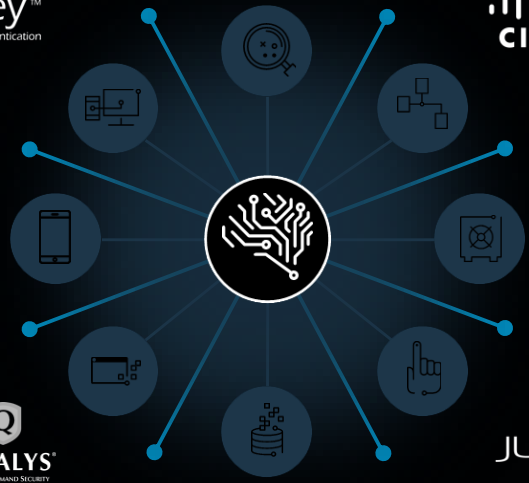


IBM Security Qradar Vulnerability Manager

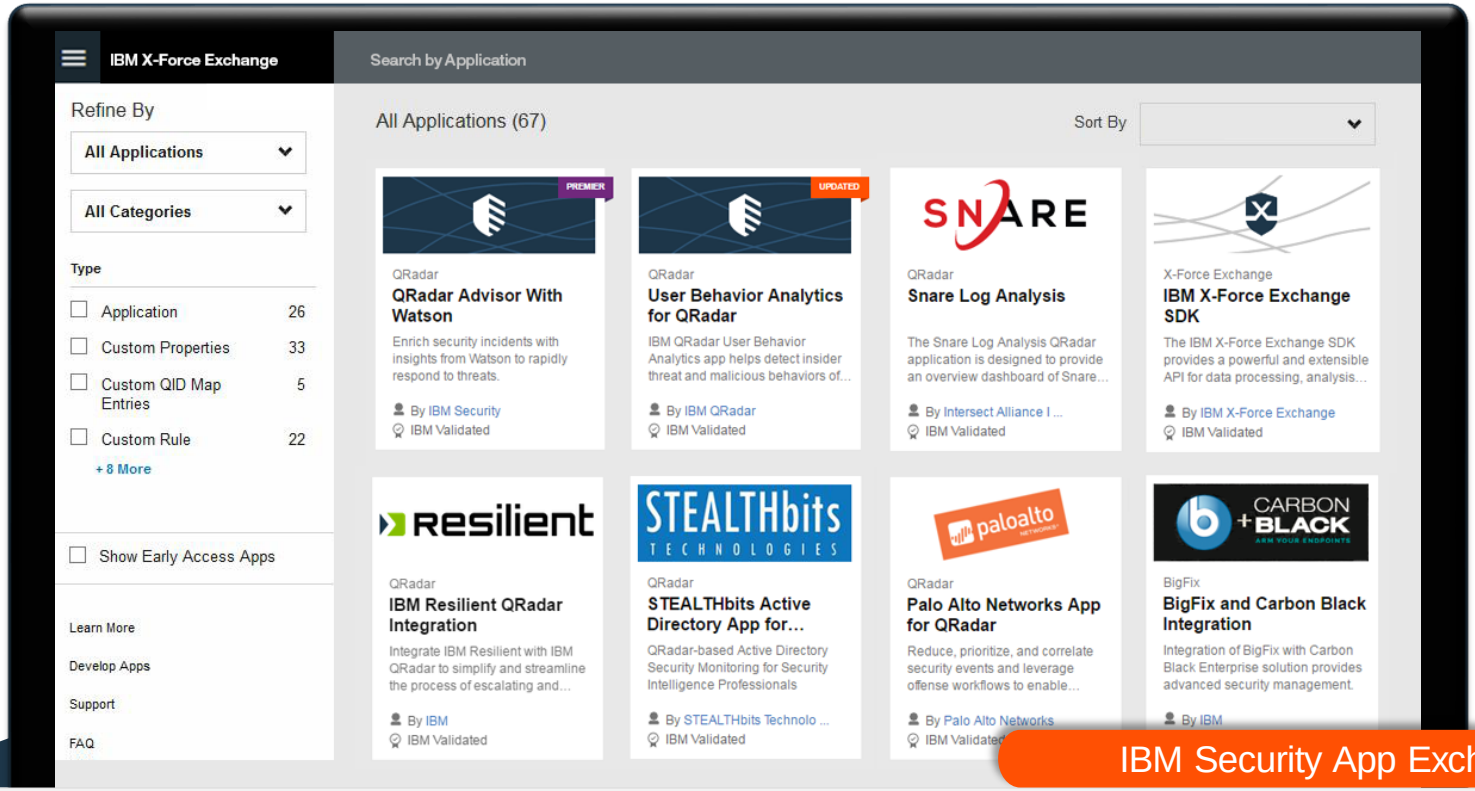


Экосистема технологических партнеров

- 200+ партнеров, 550+ QRadar интеграций



Экосистема защиты через сотрудничество



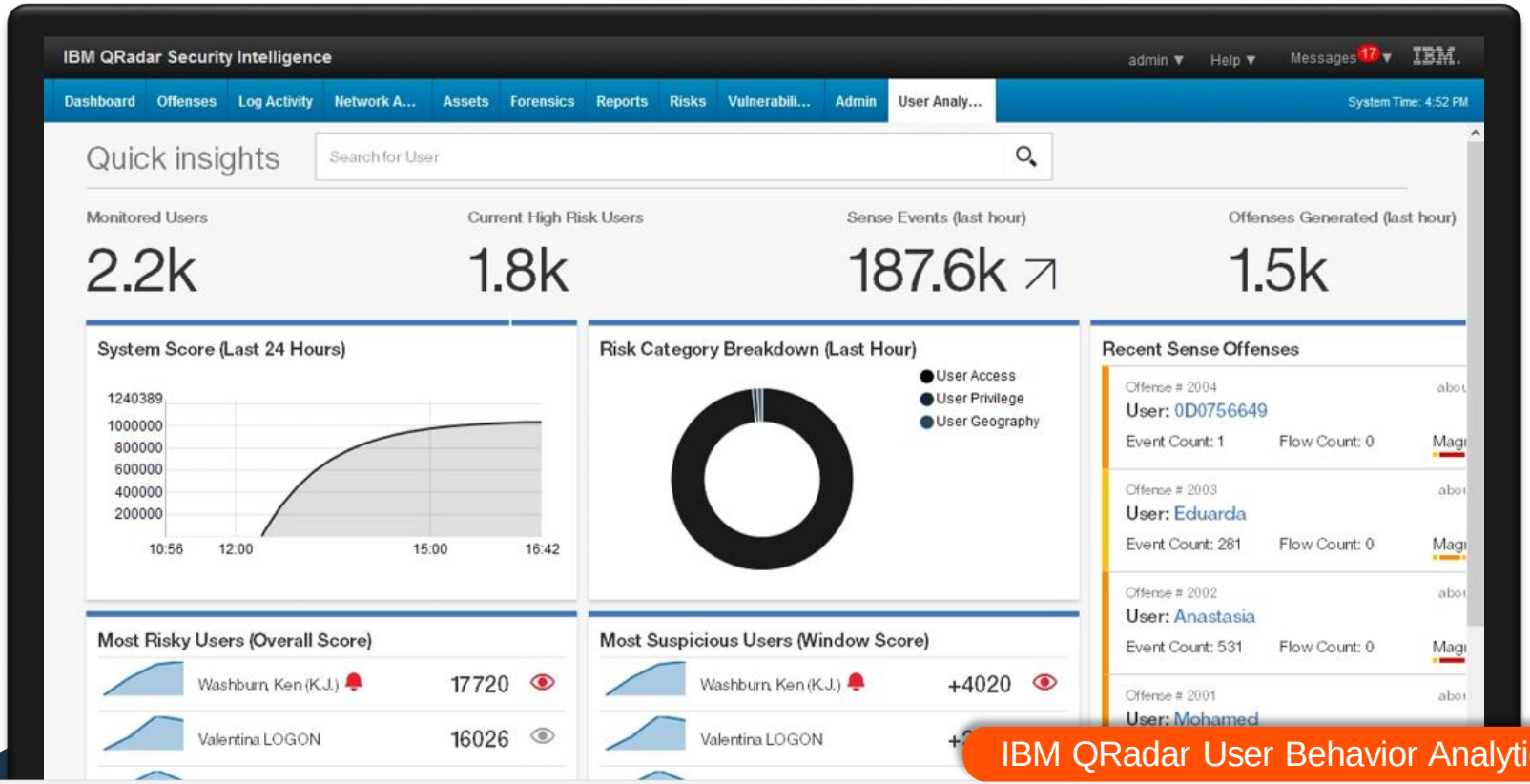
IBM Security App Exchange

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

Визуализация

Обнаружить аномальное поведение одним кликом



IBM QRadar User Behavior Analytics

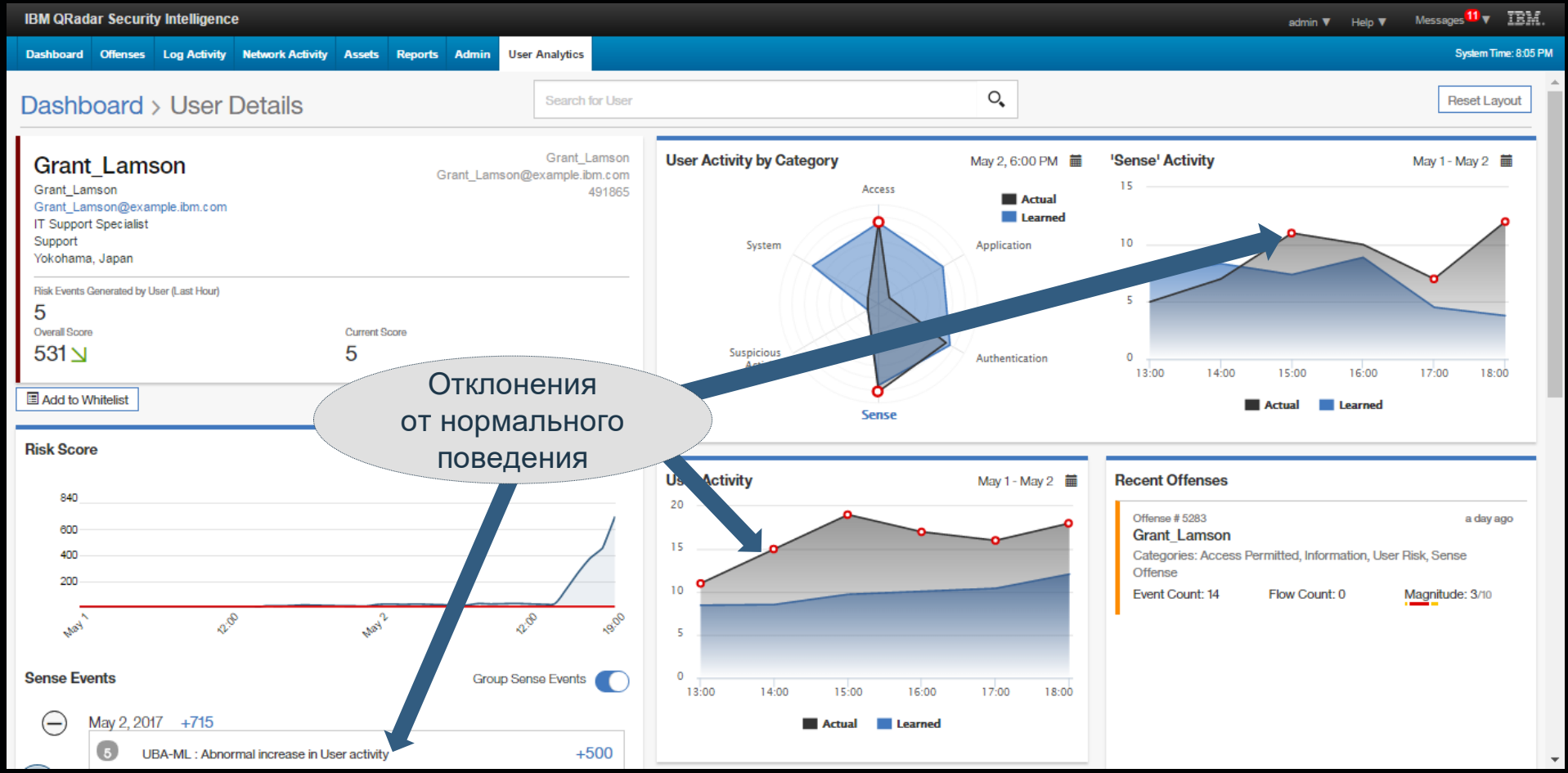
Приложение для визуализации действий каждого пользователя и выявления его аномального поведения

Консоль User Behavior Analytics является интегрированной частью консоли QRadar

UBA: Выявляя аномальные отклонения

- Мониторинг пользователей по отклонениям от нормального поведения:
  - множество разных категорий событий
  - временной анализ
  - анализ временных рядов
- Предсказание диапазона в который должна укладываться активность
- Примеры аномальных активностей выявленных этими алгоритмами:
  - Изменение в активности (во времени)
  - Изменения в авторизации или активности доступа
  - Отклонения от нормального риск-профиля

UBA: Алгоритмы машинного обучения



Отклонения от нормального поведения

Совместное использование базы 800TB+ данных об угрозах

0$

IBM Security X-Force Exchange

Доступ к интегрированной базе угроз в режиме реального времени

- **15Млрд+** мониторинг событий ИБ в день
- Данные о вредоносных угрозах с **270Млн+** конечных точек
- **1Млн+** вредоносных IP-адресов
- **1000+** сэмплов финансовых вредоносов в день

Данные от более 2000 организаций среди 16 индустрий

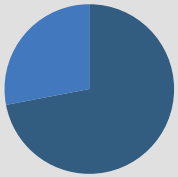
Resilient Incident Response
Автоматизированное реагирование на инциденты

На чём мы должны быть сфокусированы?

Предотвращение

Обнаружение

Реагирование

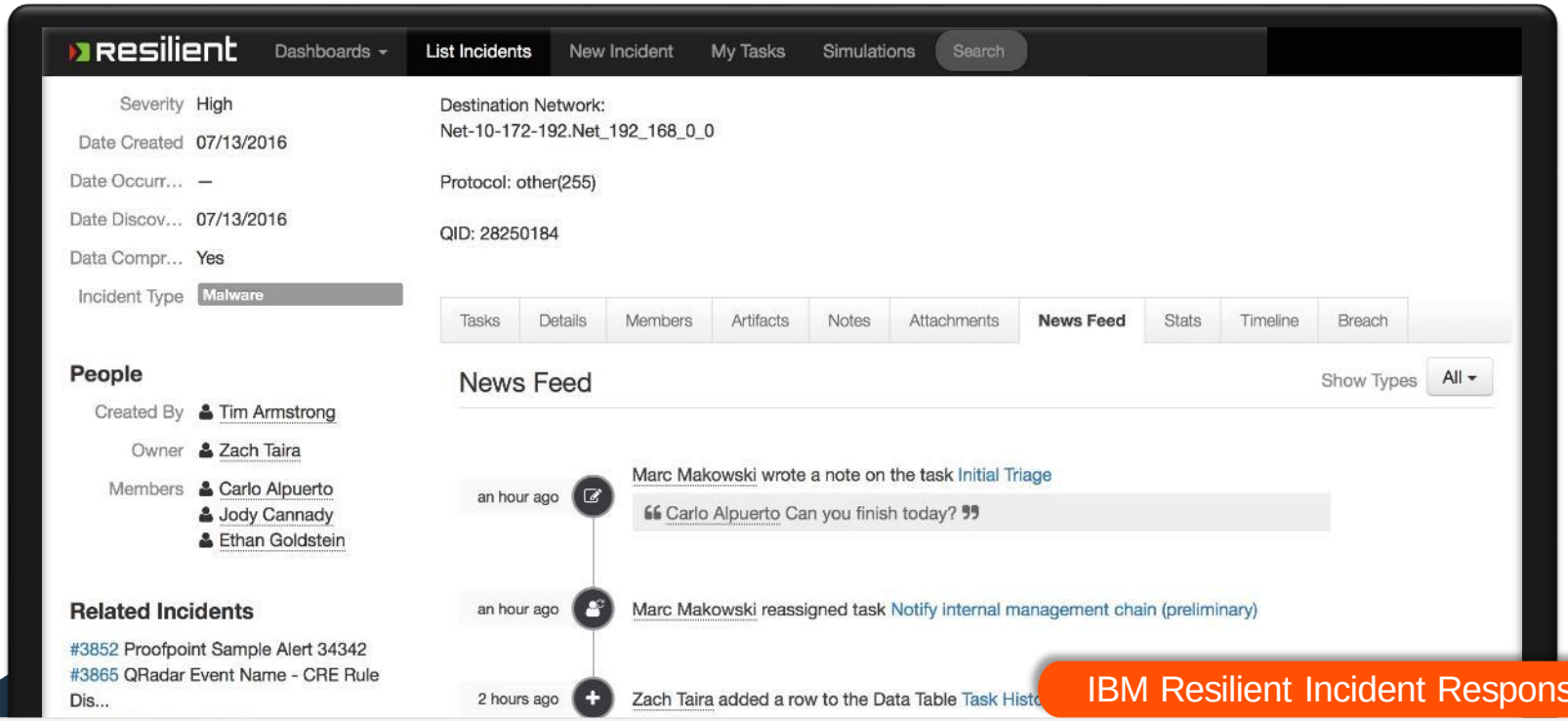


72%
предотвращение

Что мы пытаемся обнаружить?

Реагирование

Автоматизированное реагирование на инциденты



Организовать реагирование на инциденты из единой консоли объединяя людей, процессы и технологии

- Организовать и автоматизировать реагирование на инциденты
- Сбор индикаторов компрометации с использованием глубокого расследования
- Внедрение процедур реагирования и экспертизы

QRadar + Resilient = SIEM + 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

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

Сбор контекста и назначение задач
- Сбор дополнительных доказательств
- Применение требований 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

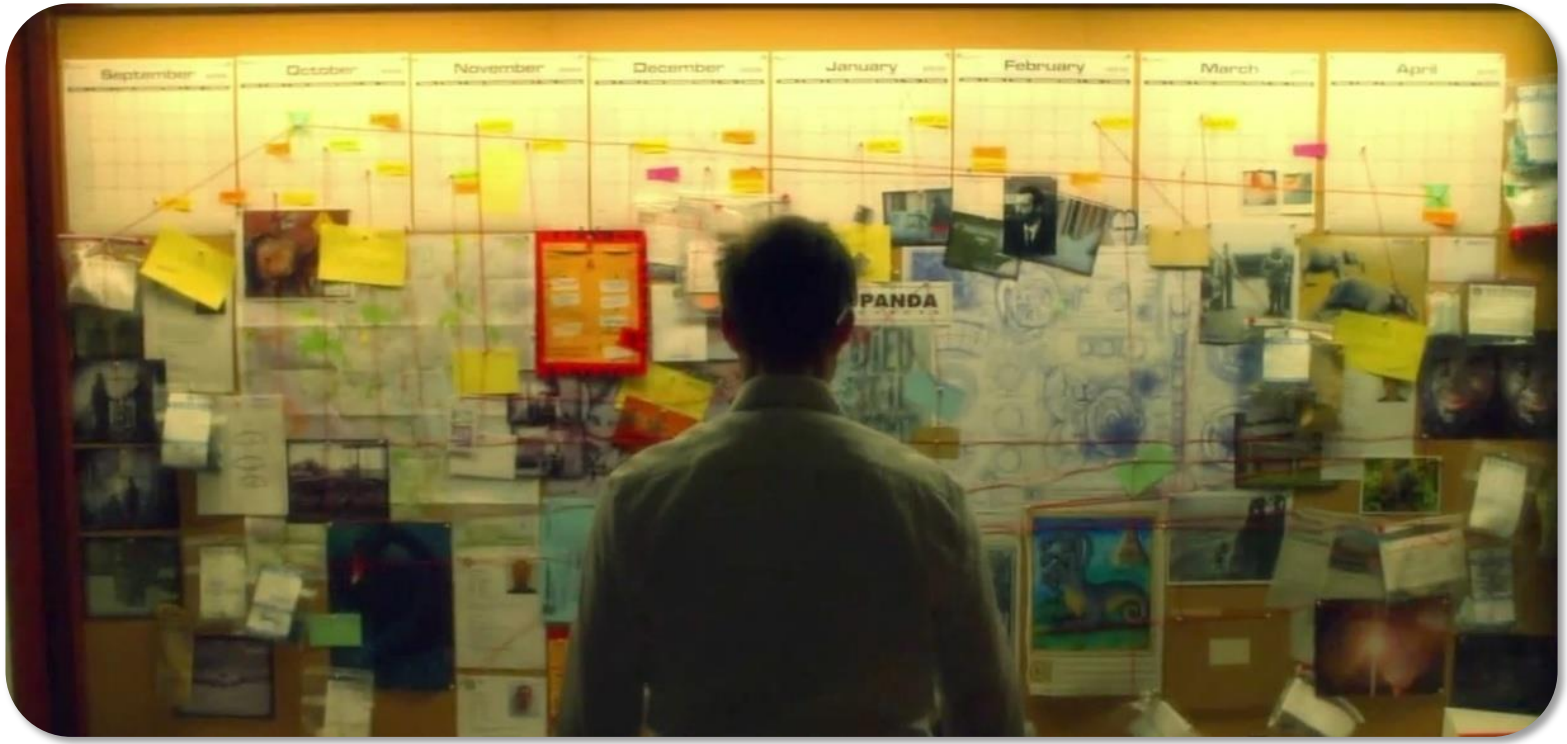
Три этапа инцидента ИБ

Улучшение процесса выявления инцидентов

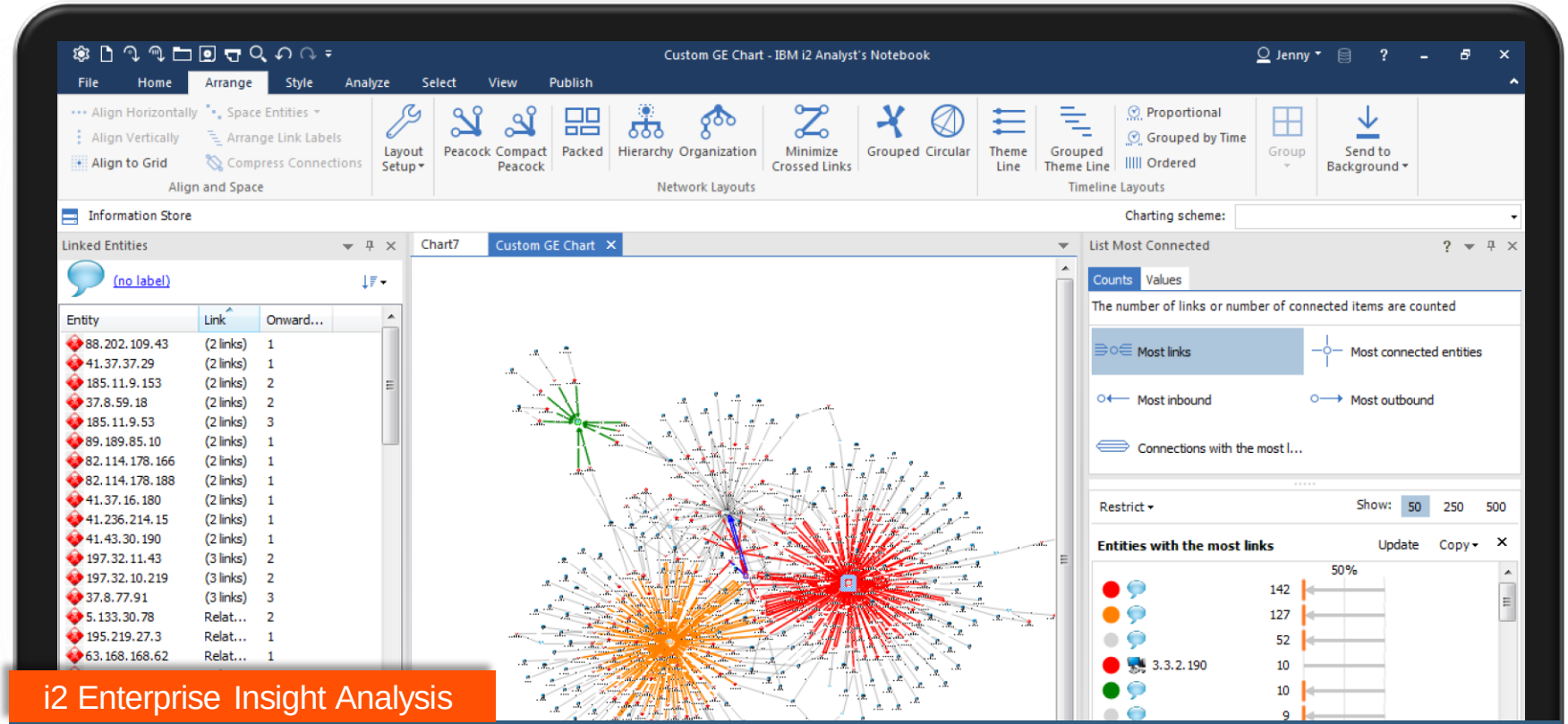
i2 Enterprise Insight Analysis

Анализ и расследование киберпреступелений и мошенничества

IBM i2


September
October
November
December
January
February
March
April
PANDA

Анализ рисков через поиск взаимосвязей сущностей



i2 Enterprise Insight Analysis

Анализ и расследование киберпреступлений и мошенничества

- Помощь аналитику в выявлении скрытых связей между мошенниками
- Легко комбинировать структурированные и неструктурированные данные

Guardium

Data Protection
Полный мониторинг и защиты

Не только БД, но и файловые хранилища

Зачем нужен Guardium?

Угрозы

- Неавторизованные изменения
- Предотвращение утечек данных

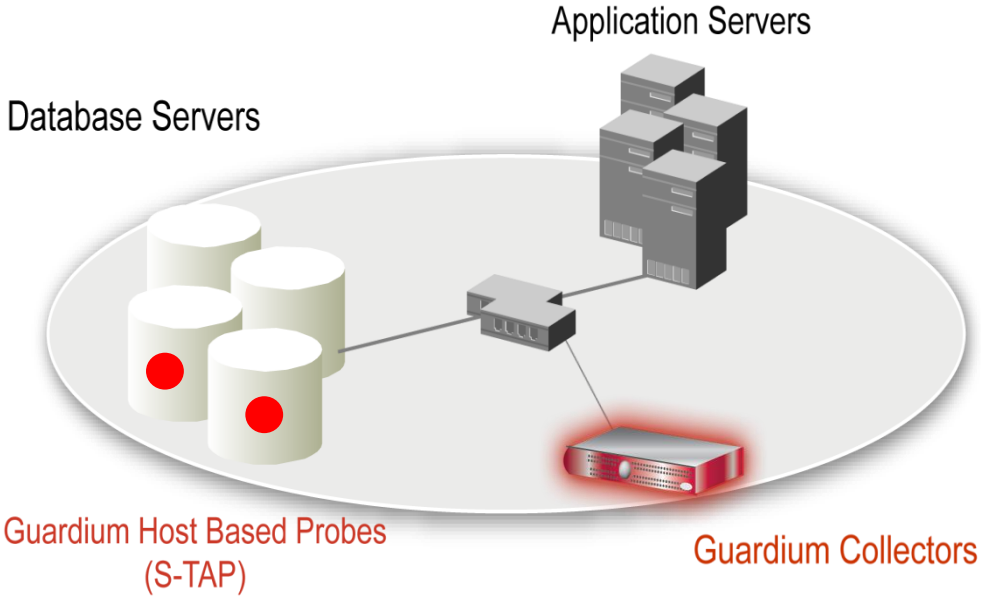
Нормативные требования

- Упрощение процессов
- Сокращение затрат

Уменьшение нагрузки на СУБД

- Замена нативного аудита
- Сокращение затрат !!!

Мониторинг БД в реальном времени



- Продуманная архитектура
- Универсальное решение для разных СУБД
- 100% контроля, включая локальный доступ DBA

- Не полагается на логи в БД, которые могут быть стерты
- Детальные политики и аудит
- Автоматическая отчетность (SOX, PCI, NIST, и т.д.)

IBM Security

СПАСИБО

FOLLOW US ON:

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

IBM