

IBM Security

Технологии защиты IBM и расследования



Арменак Аракелян

Руководитель технического направления IBM в группе компаний МОНТ

1959



Вычислительные мощности

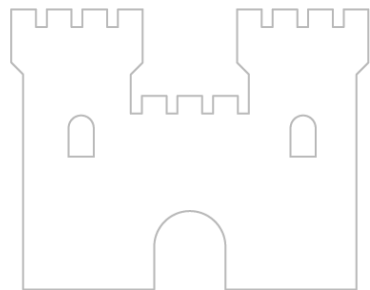
Сегодня



Безопасность

Будущее и настоящее.

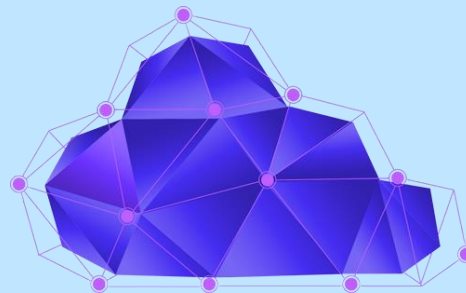
До 2013



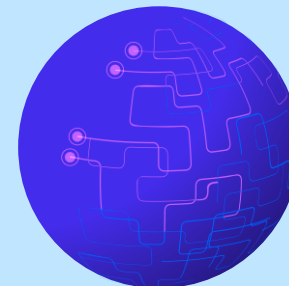
2013-2018



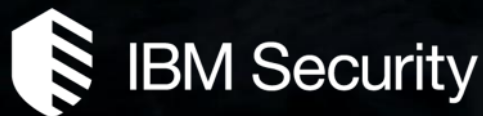
2019+
Connected security



AI, ML



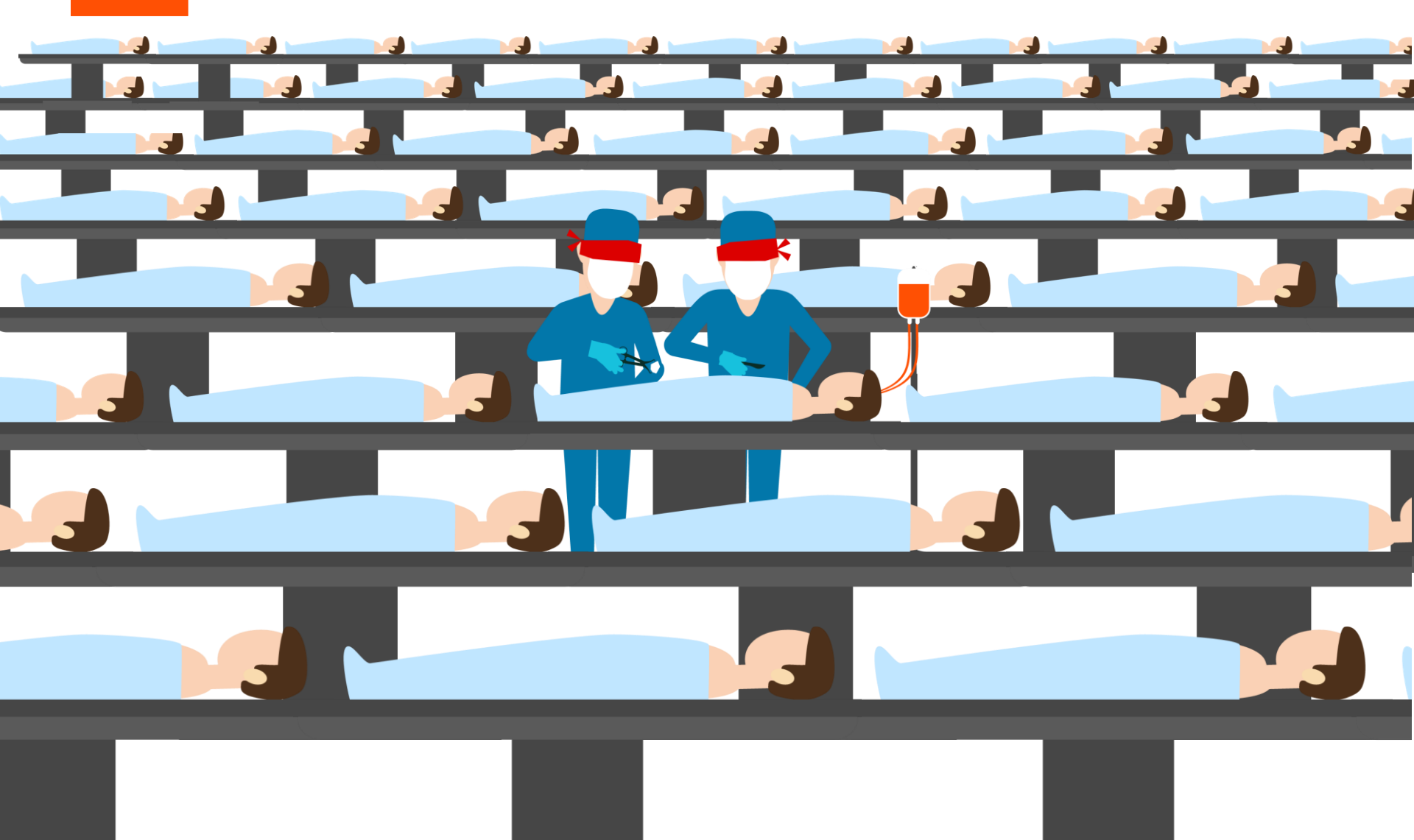
- **8,000+** сотрудников
- **17,500+** клиентов
- **133** страны
- **3,500+** патентов
- **Самый крупный Security Стартап**
- **2 Представительства в Казахстане**
- **20+** партнеров
- **Постоянные обучения**

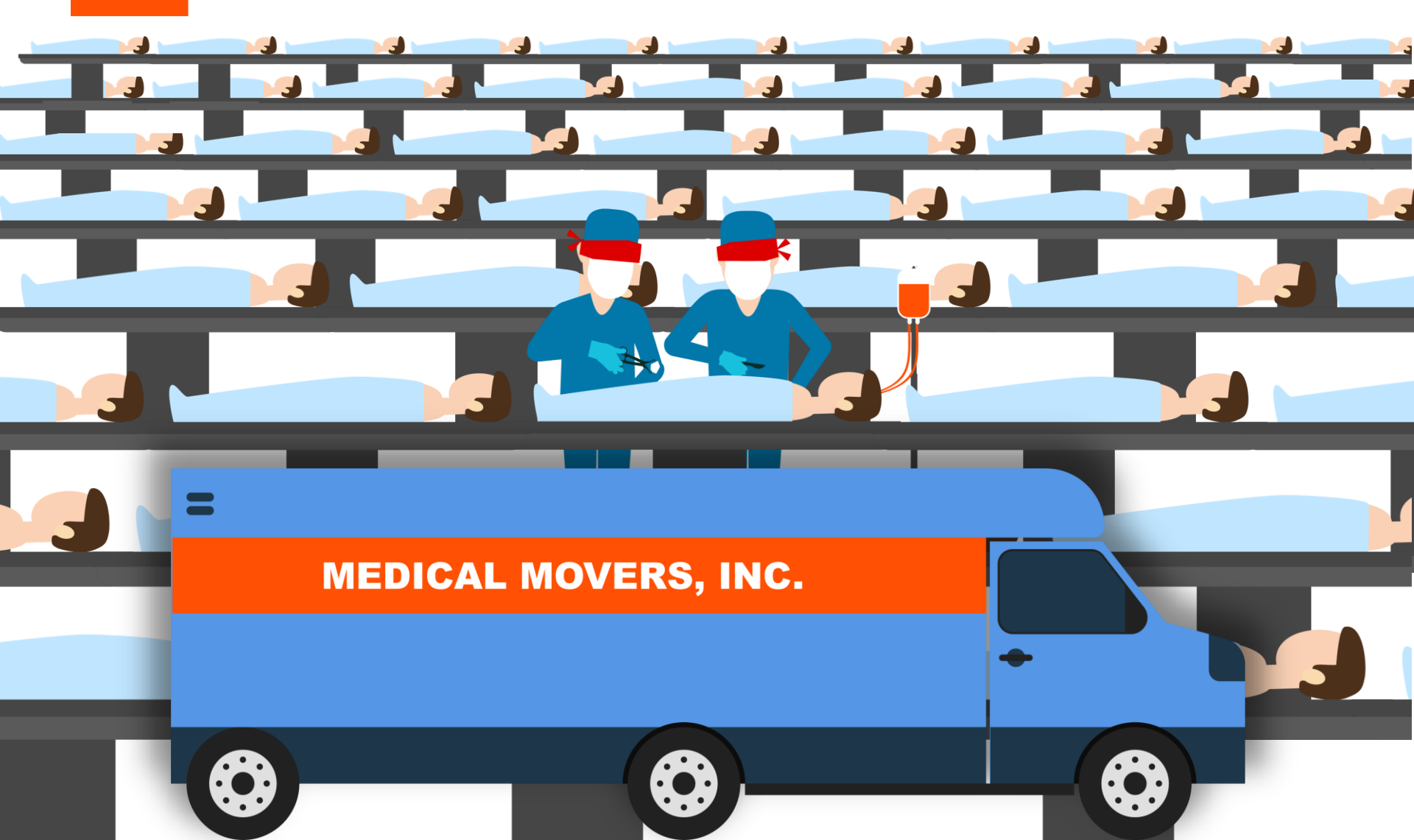




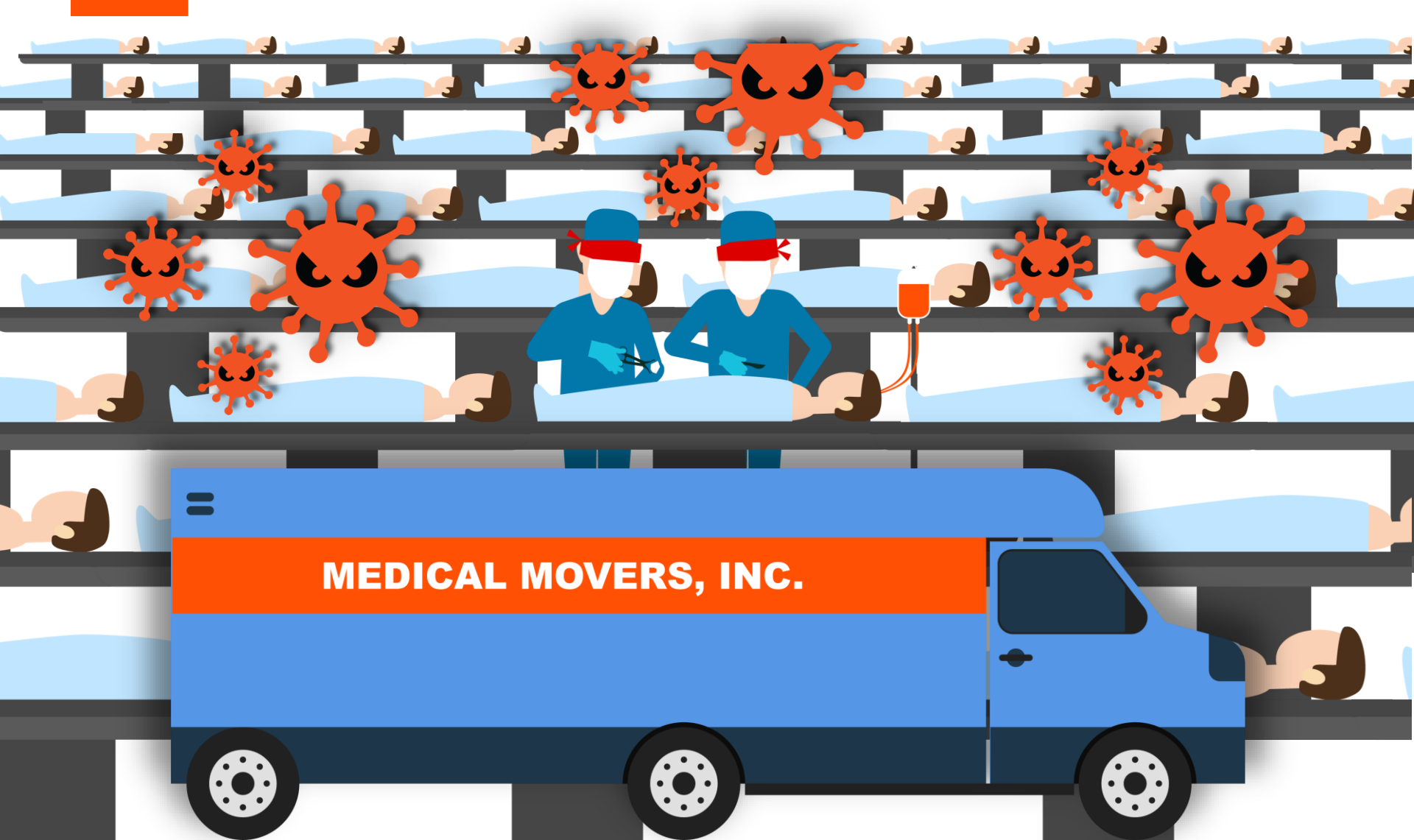








MEDICAL MOVERS, INC.



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**



**Приоритезация
инцидентов и риска
от пользователей**



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

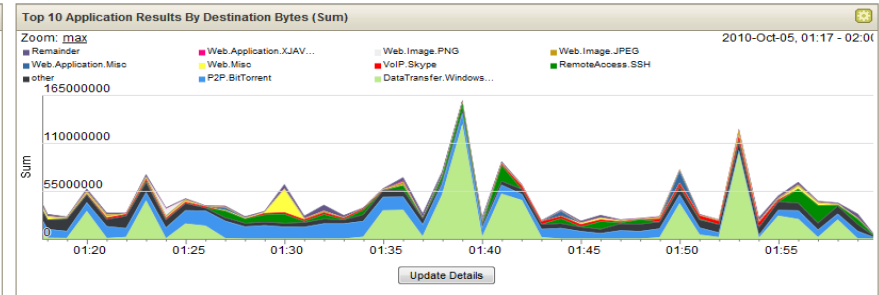
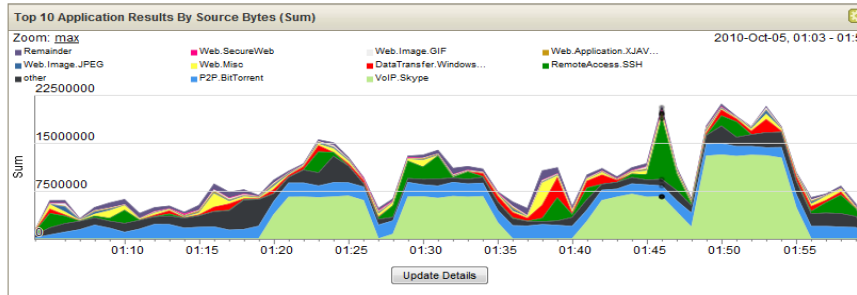
Network Forensics

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)	44 216 888	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.JPG	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 (162)	80	other	266 541	0 427 364	0 283 088	4 484	6 820	11 044	764

Выявление потенциальных угроз через аналитику

Offense 909

Magnitude		Status		Relevance	8	Severity	5	Credibility	4
Description	Potential Data Loss	Offense Type	Source IP	EventFlow count	111 events and 1,042 flows in 13 categories				
Source IP(s)	10.0.110.221 (dhcp-221-users-2.acme.com)	Start	Oct 18, 2013 12:28:02 PM	Duration	4d 10h 42m 57s				
Destination IP(s)	Local (2) Remote (376)	Assigned to	admin						
Network(s)	Multiple (3)								

Offense Source Summary

IP	10.0.110.221	Location	Users.Users-2
Magnitude		Vulnerabilities	0
Username	compliance	MAC Address	00:0E:0C:B4:D8:EE
Host Name	dhcp-221-users-2.acme.com	Weight	0
Asset Name	dhcp-221-users-2.acme.com	Events/Flows	15,310
Offenses	g		

Last 5 Notes

Notes	Username	Creation Date
Potential data loss detected, forensics case created		Oct 21, 2013 6:39 AM



Forensics Reconstructions

Case	Collection	IP	Start	End	Status
DataLoss	DataLoss	10.0.110.221	3/27/2014 3:31:00 PM	3/27/2014 4:31:00 PM	SUCCESS

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
dhc...		Users.Users-2	No	compli...			8	21	0s	




Симуляция атаки с помощью RiskManager

-  Выбор симуляции
-  Выбрать SSH vulnerabilities'
-  Выбрать активы



Simulation Name	Model	Groups	Created By	Creation Date	Last Modified	Schedule	Last Run	Next Run	Results
Assets susceptible to Micros...	Current Topology	Templates	admin	2010-07-20 14:52:54	2010-07-22 11:20:04	Manual	2010-10-28 14:03:33	FEA	2010-10-28 14:03:33 View Result
Assets susceptible to MSOL...	Current Topology	Templates	admin	2010-07-20 14:37:10	2010-07-22 11:20:23	Manual	2010-10-15 17:11:43	FEA	2010-10-15 17:11:43 View Result
Unknown SSH Vulnerability	Current Topology	Templates	admin	2010-10-23 13:42:16	2010-10-23 13:42:16	Manual	2010-10-15 13:08:16	FEA	2010-10-15 13:08:16 View Result
Assets susceptible to a client	Current Topology	Templates	admin	2010-07-20 15:01:17	2010-07-23 09:45:34	Manual	2010-10-08 09:44:39	FEA	No Results

Визуализация...

-  Путь атаки
-  Распространение
-  Мониторинг в режиме RB



Unknown SSH Vulnerability Results, Step 2 of 3 << Prev Step Next Step >> [Edit](#) [View Offenses](#) [View Events](#)

Simulation Definition	Attack originates from the internet and Attack targets one of the following networks (Net-10-172-192) and Attack targets a vulnerability on one of the following ports (22) using protocols (TCP)
Using Model	Current Topology
Simulation Result	Generated on 2010-10-15 13:08:16 by admin
Step Results	520 (Of 600 Total)
Assets Compromised	9 (Of 88 Total Compromised)

Simulation Results by Step

Risk Score for the current step is 3

Unknown SSH Vulnerability Progression, Step 2 of 3

IBM Security Qradar Vulnerability Manager

IBM QRadar Security Intelligence

admin Help Messages 12 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Visual Analytics

System Time: 5:39 PM

Risk Manager

Search Save Search Criteria Quick Searches Actions Quick Filter

Next Refresh: 00:00:30

Vulnerabilities

Manage Vulnerabilities > By Vulnerability Instances

Display: Instances

Search Parameter(s)

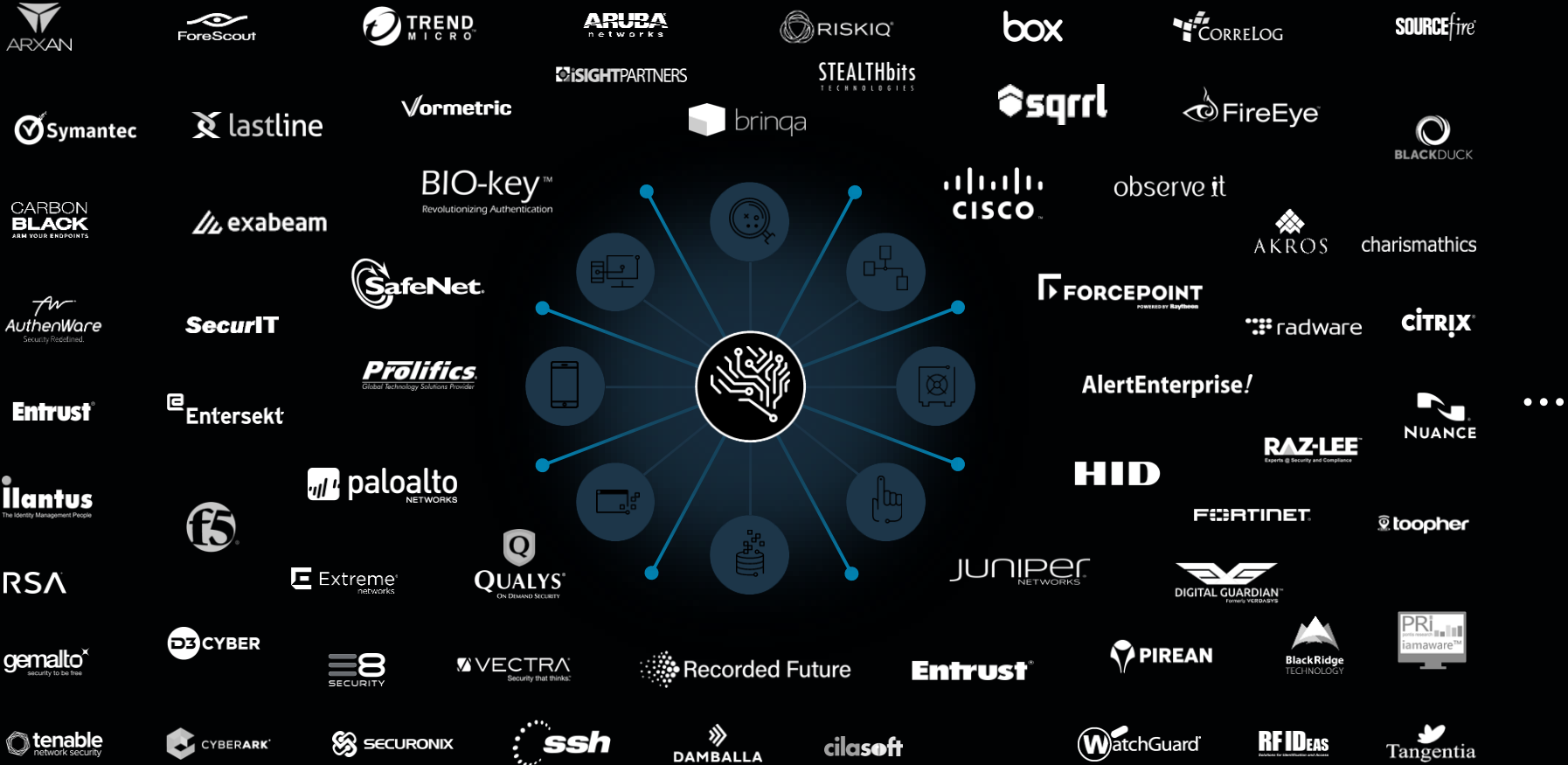
IP Address	Asset Name	Vulnerability	PCI Severity	Risk	CVE Id	Risk Score	Date Found	Last Date Seen	Assigned To	Status	Due days
172.16.60.79	JUMP	CVE-2015-2365 - Microsoft - Windows - Privilege Escalation I...	Low	High	2015-2365	5.90	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2014-1784 - MS14-035 - Microsoft - Internet Explorer - Code Executio...	Low	High	2014-1784	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2014-0310 - MS14-029 - Internet Explorer - Code Execution Issue	Low	High	Multiple(2)	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2012-1887 - MS12-076 - Microsoft - Excel - Code Execution Issue	Urgent	High	Multiple(4)	8.10	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2014-0299 - MS14-012 - Microsoft - Internet Explorer - Code Executio...	Low	High	2014-0299	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2014-2807 - MS14-037 - Microsoft - Internet Explorer - Code Executio...	Low	High	2014-2807	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-3861 - MS13-082 - Microsoft - .NET Framework - Code Executio...	Low	High	2013-3861	6.40	2015-10-26 16:02:48	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2014-1762 - MS14-035 - Microsoft - Internet Explorer - Code Executio...	Low	High	2014-1762	6.50	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-3918 - MS13-090 - Windows - Code Execution Issue	Low	High	2013-3918	8.10	2015-10-26 16:02:48	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2015-2461 - MS15-080 - Windows - Code Execution Issue	Low	High	2015-2461	8.10	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	Microsoft Windows MDM DLL planting code execution		High	2015-2369	6.90	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2015-1644 - MS15-038 - Microsoft - Windows - Privilege Escalation I...	Low	High	2015-1644	5.90	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2010-0821 - MS10-038 - Excel - Code Execution Issue	Urgent	High	2010-0821	8.10	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.100.205	172.16.100.205	CVE-1999-0504 - Microsoft - Windows - Default Credentials Issue	High	High	1999-0504	6.40	2009-09-27 21:36:14	2009-09-27 21:36:14			
172.16.60.79	JUMP	CVE-2014-2769 - MS14-035 - Microsoft - Internet Explorer - Code Executio...	Low	High	2014-2769	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-3208 - MS13-069 - Microsoft - Internet Explorer - Code Executio...	Low	High	2013-3208	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-3907 - MS13-101 - Microsoft - Portcls.sys - Privilege Escalation...	Low	High	2013-3907	5.90	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2013-3881 - MS13-081 - Microsoft - Windows - Code Execution Issue	Low	High	2013-3881	5.90	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-3561 - Wireshark - Multiple Integer Overflow Issues	High	High	2013-3561	6.40	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-0006 - MS13-002 - Microsoft - XML Core Services - Code Execu...	Urgent	High	2013-0006	8.10	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2013-3357 - Adobe - Multiple Products - Integer Overflow Issue	Low	High	2013-3357	8.70	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2014-1795 - MS14-035 - Microsoft - Internet Explorer - Code Executio...	Low	High	2014-1795	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2012-0142 - MS12-030 - Microsoft - Excel - Code Execution Issue	Urgent	High	2012-0142	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-5048 - MS13-097 - Microsoft - Internet Explorer - Memory Corru...	Low	High	2013-5048	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2013-3876 - Microsoft - DirectAccess - Man in the Middle Issue	Low	High	2013-3876	6.20	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2014-2757 - MS14-035 - Microsoft - Internet Explorer - Code Executio...	Low	High	2014-2757	8.10	2015-10-26 16:02:48	2015-10-26 16:02:48			
172.16.60.79	JUMP	CVE-2015-2416 - MS15-075 - Microsoft - Windows - Privilege Escalation I...	Low	High	2015-2416	4.10	2015-11-04 17:23:44	2015-11-04 17:23:44			
172.16.60.79	JUMP	CVE-2014-0529 - Adobe - Multiple Products - Buffer Overflow Issue	Low	High	2014-0529	7.40	2015-10-26 16:02:48	2015-10-26 16:02:48			

Displaying 1 to 40 of 535 items (Elapsed time: 0:00:00.062)

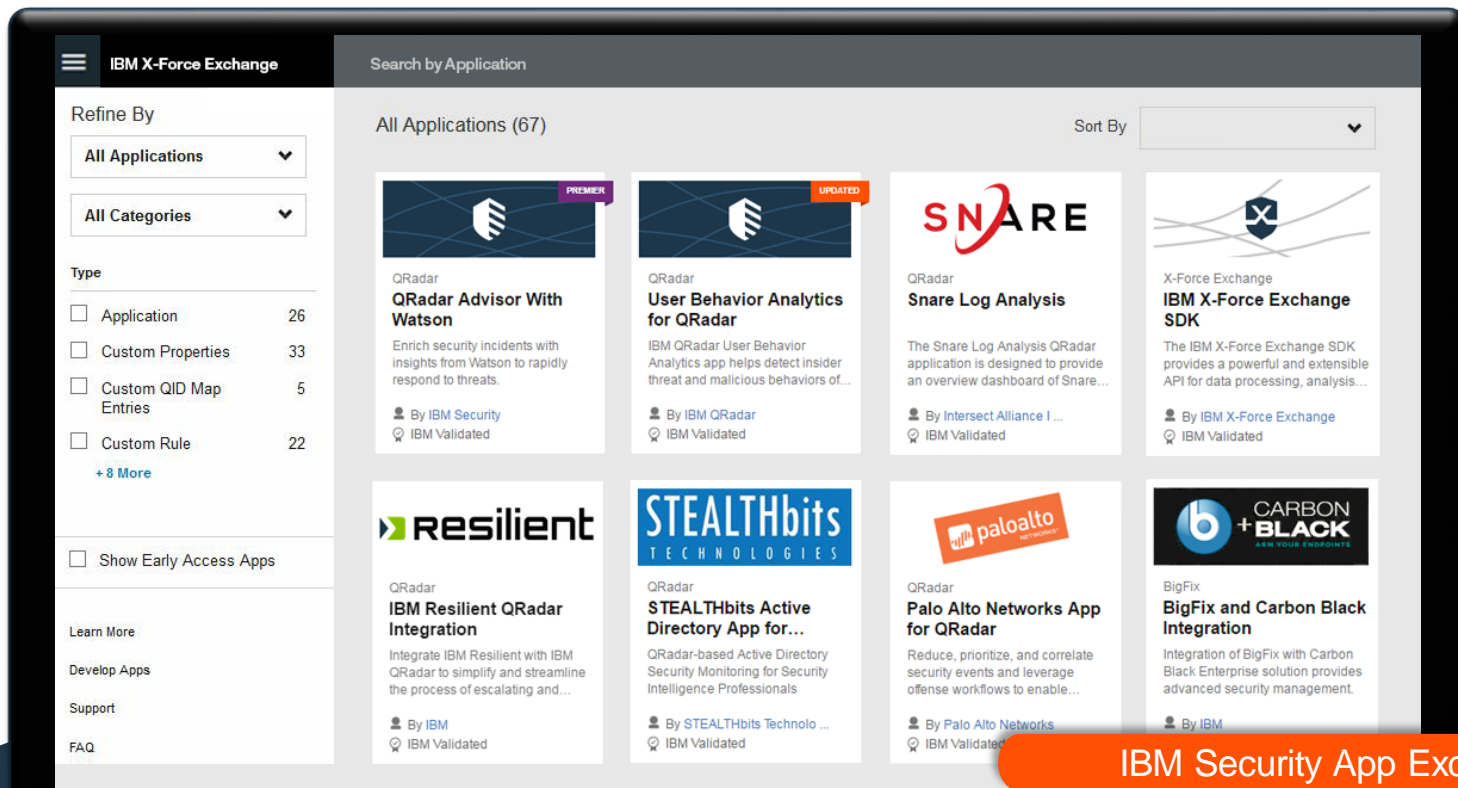


Экосистема технологических партнеров

- 200+ партнеров, 550+ QRadar интеграций



Экосистема защиты через сотрудничество



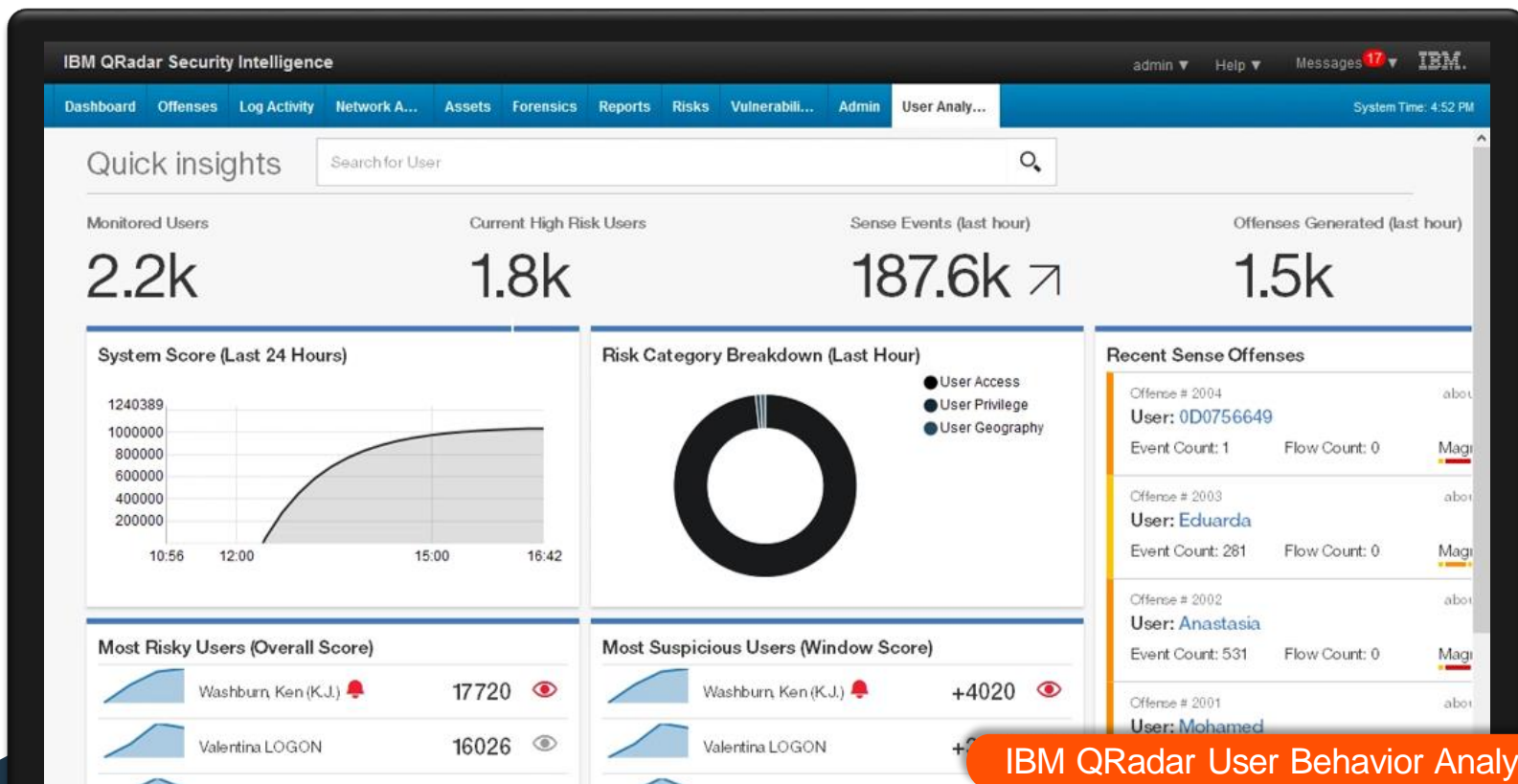
Создавайте и используйте приложения на основе технологий IBM security

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

Визуализация



Обнаружить аномальное поведение одним кликом



Приложение для визуализации действий каждого пользователя и выявления его аномального поведения

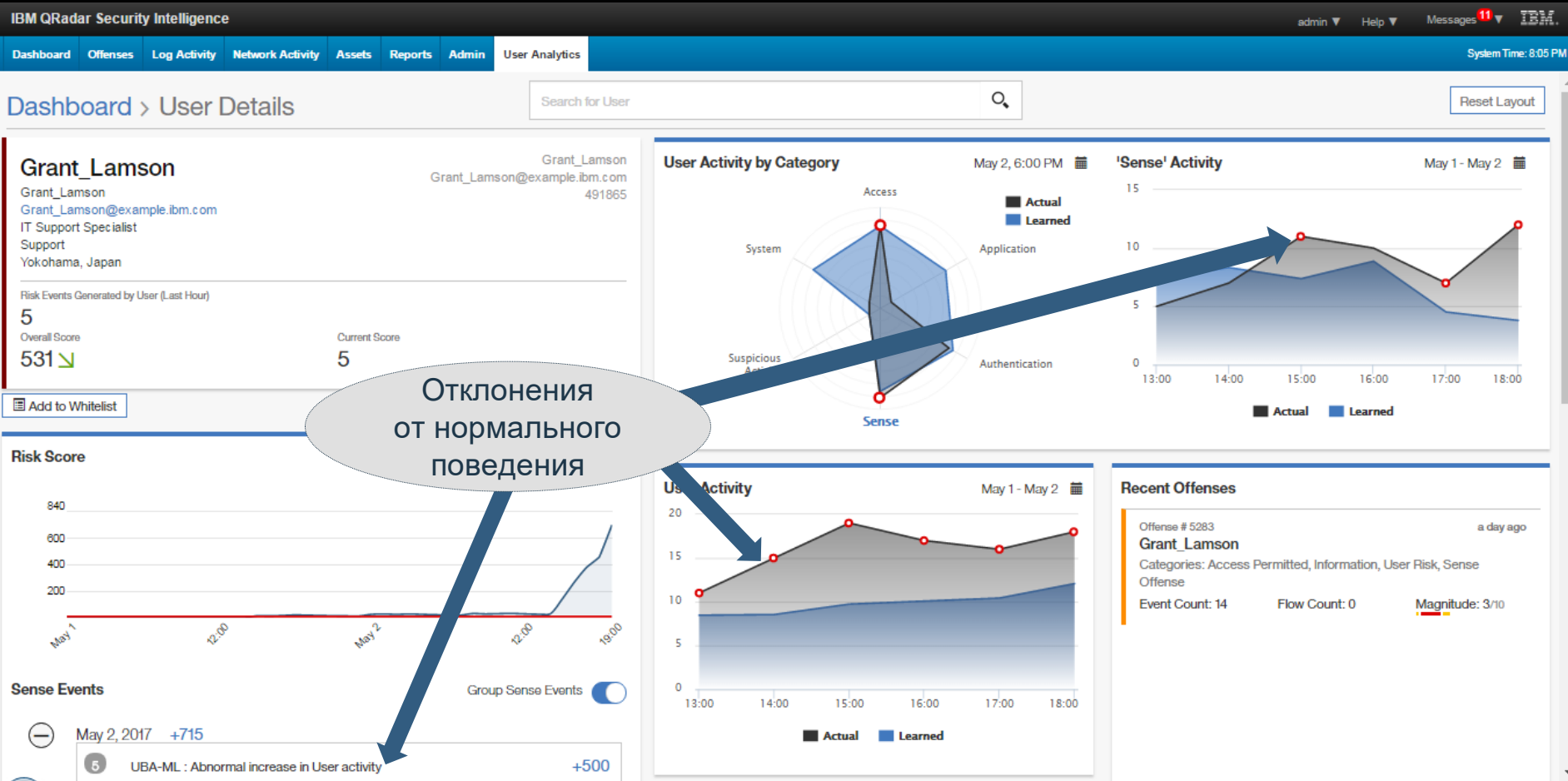
Консоль User Behavior Analytics является интегрированной частью консоли QRadar

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

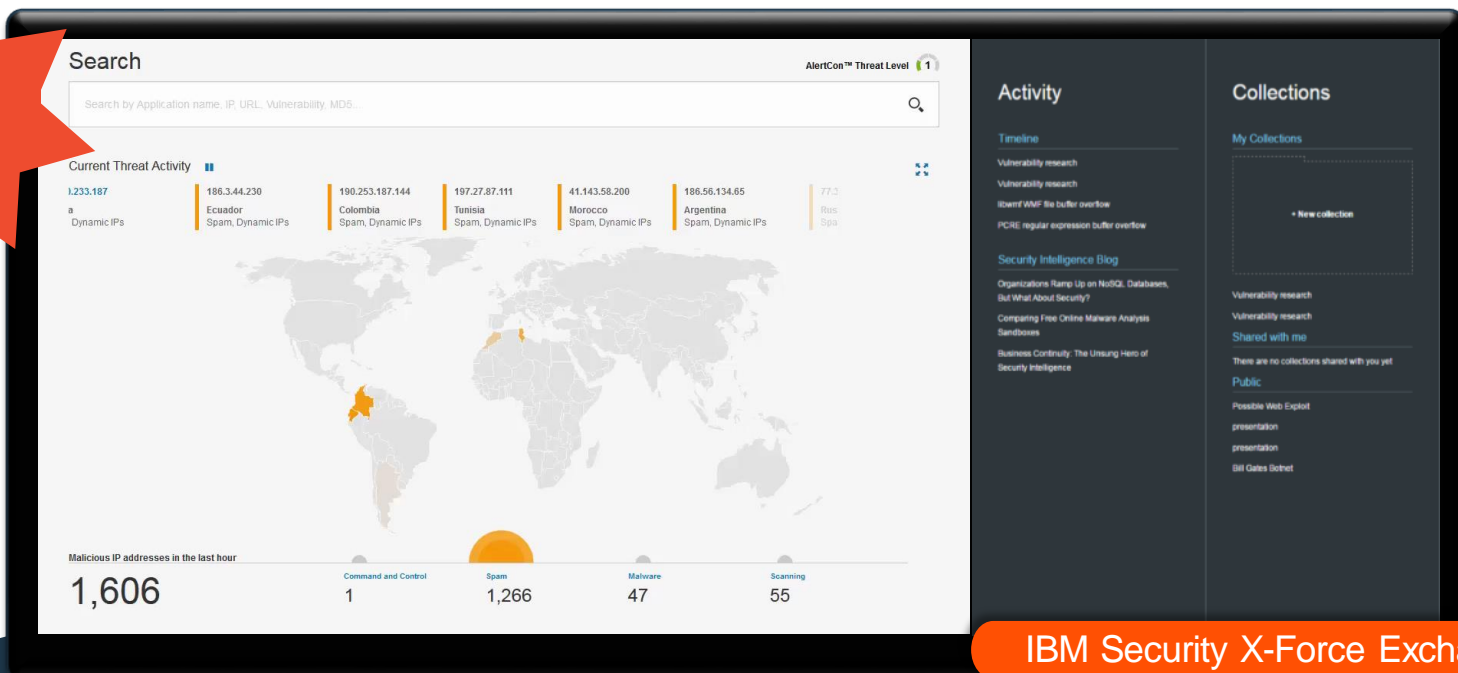


UBA: Алгоритмы машинного обучения



Совместное использование базы 800ТВ+ 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 вредоносных в день

Данные от более 2000 организаций среди 16 индустрий



Resilient Incident Response

Автоматизированное реагирование на инциденты



На чём мы должны быть сфокусированы?



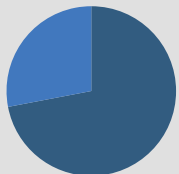
Предотвращение



Обнаружение



Реагирование



72%
предотвращение



Что мы пытаемся
обнаружить?

Реагирование



Автоматизированное реагирование на инциденты

The screenshot displays the IBM Resilient Incident Response dashboard. At the top, there is a navigation bar with the 'resilient' logo, a 'Dashboards' dropdown, and buttons for 'List Incidents', 'New Incident', 'My Tasks', 'Simulations', and a search bar. The main content area shows incident details for a 'Malware' incident. On the left, a 'People' section lists the incident's creator (Tim Armstrong), owner (Zach Taira), and members (Carlo Alpuerto, Jody Cannady, and Ethan Goldstein). Below this is a 'Related Incidents' section with links to other incidents. The central 'News Feed' shows a timeline of activity: an hour ago, Marc Makowski wrote a note on the task 'Initial Triage', followed by a quote from Carlo Alpuerto asking 'Can you finish today?'. Another hour ago, Marc Makowski reassigned the task 'Notify internal management chain (preliminary)'. Two hours ago, Zach Taira added a row to the 'Data Table Task Histo...'. A tabbed interface at the top of the main content area includes 'Tasks', 'Details', 'Members', 'Artifacts', 'Notes', 'Attachments', 'News Feed' (which is active), 'Stats', 'Timeline', and 'Breach'. An orange banner at the bottom right of the screenshot reads 'IBM Resilient Incident Response'.

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

ИСТОЧНИКИ ДАННЫХ

Устройства ИБ

Сервера и мейнфреймы

Сетевая и виртуальная среда

Активности БД

Работа приложений

Конфигурации устройств

Уязвимости и угрозы

Пользователи и учетки

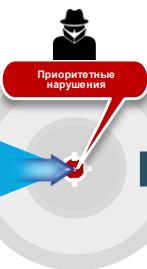
Глобальные базы угроз



QRadar Sense Analytics™

- Сбор, хранение и анализ данных
- Автоопределение источников, сервисов и пользователей и их профилирование
- Корреляция событий в реальном времени
- Определение аномалий активностей

Встроенный Интеллект



Приоритетные нарушения

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

Постоянная аналитика ИБ

Три этапа инцидента ИБ

База всех инцидентов ИБ

Отчет по инциденту и уведомление

Улучшение процесса выявления инцидентов



i2 Enterprise Insight Analysis

Анализ и расследование
киберпреступлений и мошенничества



IBM i2



Анализ рисков через поиск взаимосвязей сущностей

The screenshot displays the IBM i2 Analyst's Notebook interface. The main window shows a complex network graph with numerous nodes and edges, color-coded by clusters. The interface includes a top menu bar with options like File, Home, Arrange, Style, Analyze, Select, View, and Publish. Below the menu is a toolbar with various layout and analysis tools. On the left, the 'Information Store' panel shows a list of 'Linked Entities' with columns for Entity, Link, and Onward... On the right, the 'List Most Connected' panel provides filters for 'Counts' and 'Values', and a table titled 'Entities with the most links' showing top entities and their link counts.

Entity	Link	Onward...
88.202.109.43	(2 links)	1
41.37.37.29	(2 links)	1
185.11.9.153	(2 links)	2
37.8.59.18	(2 links)	2
185.11.9.53	(2 links)	3
89.189.85.10	(2 links)	1
82.114.178.166	(2 links)	1
82.114.178.188	(2 links)	1
41.37.16.180	(2 links)	1
41.236.214.15	(2 links)	1
41.43.30.190	(2 links)	1
197.32.11.43	(3 links)	2
197.32.10.219	(3 links)	2
37.8.77.91	(3 links)	3
5.133.30.78	Relat...	2
195.219.27.3	Relat...	1
63.168.168.62	Relat...	1

Entity	Link Count
3.3.2.190	142
	127
	52
	10
	10
	9

i2 Enterprise Insight Analysis

Анализ и расследование киберпреступлений и мошенничества

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



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

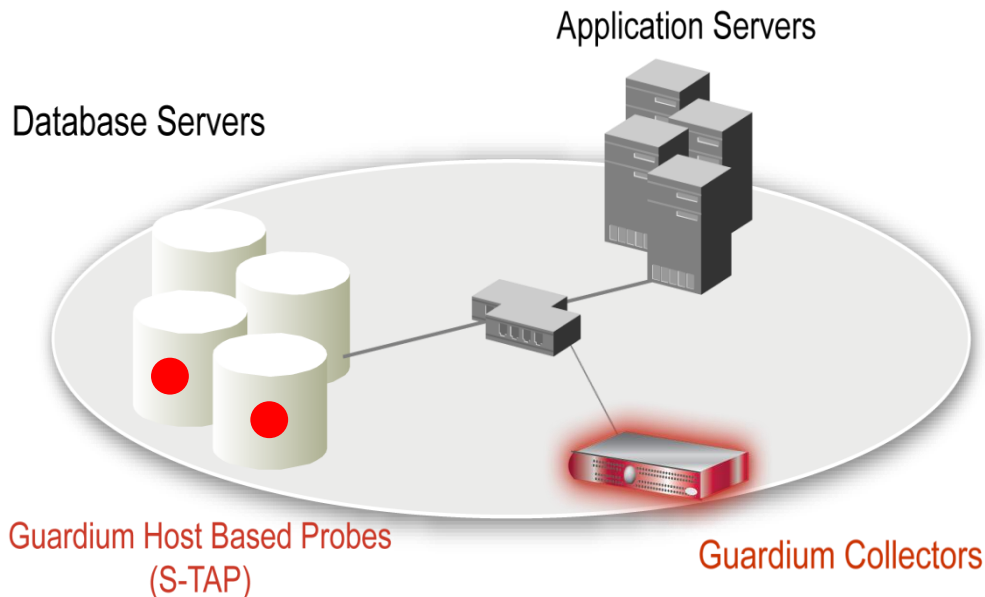


Уменьшение нагрузки на СУБД

- 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.)

СПАСИБО


FOLLOW US ON:

 ibm.com/security

 securityintelligence.com

 ibm.com/security/community

 xforce.ibmcloud.com

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

 youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. 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.