

# Как собирать все логи и выявлять инциденты на одной платформе без больших затрат?



Олег Бакшинский  
Ведущий советник по вопросам информационной безопасности

# Основные проблемы заказчиков

Нормативы  
и законы

Критические  
уязвимости

Угрозы  
инсайдеров

Защита  
данных

Сегодняшнее состояние

Много данных, но  
не хватает  
понимания

73%

ОРГАНИЗАЦИЙ ИСПОЛЬЗУЮТ  
БОЛЕЕ 25 РАЗНЫХ СРЕДСТВ  
ЗАЩИТЫ

44%

ВСЕХ ИНЦИДЕНТОВ  
НЕ РАССЛЕДУЮТСЯ

54%

РЕАЛЬНЫХ ИНЦИДЕНТОВ  
НЕ ВОССТАНАВЛИВАЮТСЯ

# Не отвлекаемся от темы

## Сбор логов

- Кол-во и тип источников  
(ограничено, без ограничений / платно, бесплатно)
- Объем собираемых логов  
(ограничено, без ограничений / платно, бесплатно)
- Сроки хранения собираемых логов  
(кроме объема хранилища есть еще архивация)

Кому нужен быстрый обзор, как сделать быстро и бесплатно,  
отсылаю к статьям на Хакере и на HABR с известными всем словами  
logstash, fluentd, syslog-ng, elastic, kibana, grafana

# Не отвлекаемся от темы

Разбираемся со словом «BCE» логи

- Сколько может собрать и обработать ваш LM/SIEM ?
- Какие ресурсы для этого нужны ? Сколько ядер/оперативки ?
- А если включить полное логирование (BCE логи) ?
- А если мы хотим перейти от одной ноды к распределенной архитектуре – от All-In-One к Консоль + Процессоры + Коллекторы ?
- А если хотим объединить железо и софт или виртуалки в единой архитектуре ?

# Не отвлекаемся от темы

Выявление инцидентов – SIEM, правила корреляции

- В режиме близком к реальному времени ? А при каком объеме собираемых логов ?
- Можете ли вы сами написать правила без сложностей ?

На одной платформе

- Сколько виртуальных машин / серверов нужно, чтобы всё это работало ?
- Администрирование распределенной архитектуры из одной консоли

Без больших затрат **НЕ** значит **бесплатно**



# Выявить и остановить угрозы

## IBM QRadar

*User and entity profiling*

*Statistical analysis*

*Pattern identification*

*Entity and user context*

*Network-based anomaly detection*

*External threat correlation*

*Real-time analytics*

*Risk-based analytics*

*Threat hunting*

*DNS analytics*

*Business context*

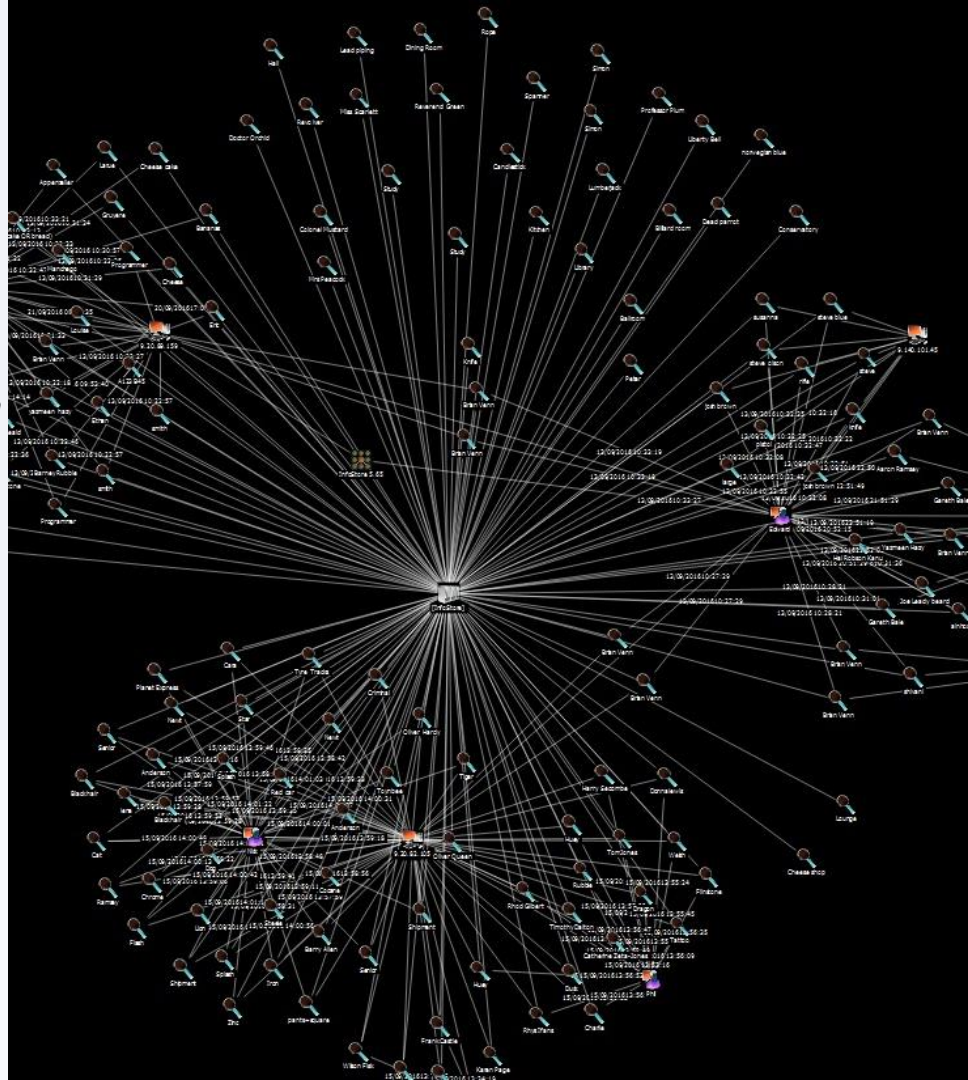
#1 SIEM в классе  
Advanced Threat Defense

- Gartner

“3 млрд событий ИБ в день с использованием аналитики преобразуются в 25 приоритетных значимых для бизнеса инцидентов для работы аналитиков.”

- Крупная энергетическая

КОМПАНИЯ



# IBM QRadar

Больше функционала с меньшими затратами

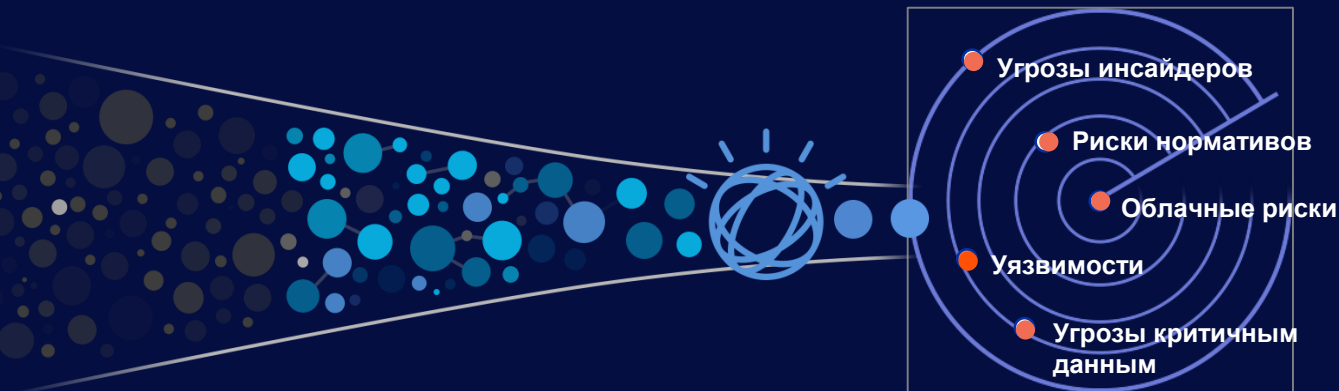
Централизованный  
сбор логов

Аналитика из  
коробки

Приоритизация  
угроз

Отчеты  
из коробки

Рабочие станции и сервера  
Сетевая активность  
Активность данных  
Пользователи и учетные записи  
Анализ угроз  
Информация о конфигурации  
Уязвимости и угрозы  
Активность приложений  
Облачные платформы





# Разработан, чтобы облегчить работу

“Данные базы X-Force и  
возможности аналитики  
QRadar из коробки —  
главное отличие...”

— CTO, Large IT Consulting Firm in Europe

*Независимое исследование пользователей QRadar с помощью Ponemon Institute*

## 73%

КЛИЕНТОВ УВИДЕЛИ ПОЛЬЗУ  
В ТЕЧЕНИЕ ПЕРВОЙ НЕДЕЛИ

## 51%

СРЕДНЕЕ УЛУЧШЕНИЕ В  
ТОЧНОСТИ ВЫЯВЛЕНИЯ УГРОЗ

## 50%

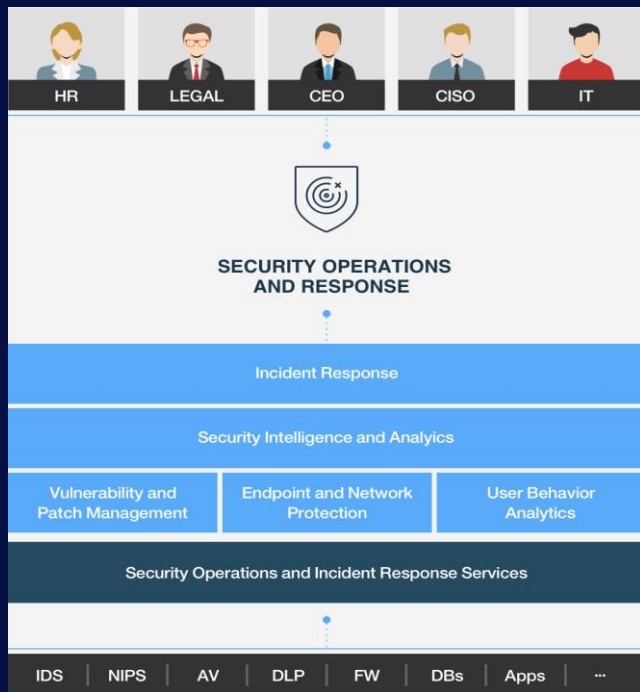
МЕНЬШЕ  
ЛОЖНЫХ СРАБАТЫВАНИЙ  
ЧЕМ У ДРУГИХ SIEM РЕШЕНИЙ

## 5+

ТОЧЕЧНЫХ РЕШЕНИЙ ЗАМЕНЕНЫ  
ОДНОЙ ИНСТАЛЛЯЦИЕЙ QRADAR

# Портфель продуктов IBM QRadar

## Многофункциональная платформа управления инцидентами ИБ



### QRadar Log Manager (Data Store)

- Сбор и обработка большого количества событий безопасности
- Возможность обновления до SIEM

### QRadar SIEM

- Сбор логов и сетевой статистики, соответствие регуляторным требованиям
- Профилирование активов, анализ сетевой активности и угроз ИБ
- Инциденты ИБ и их расследование

### Репутационная база IBM X-Force

### QFlow и QRadar Network Insights

Сетевая аналитика, обнаружение аномалий

- Анализ 7 уровня модели OSI
- Анализ сетевых пакетов в реальном времени

### QRadar Vulnerability Manager и Risk Management

- Встроенные механизмы сканирования сети
- Управление рисками и приоритезация уязвимостей
- Моделирование и симуляция атак злоумышленников
- Мониторинг и аудит конфигурации сетевых устройств
- Продвинутый анализ угроз и последствий

### QRadar Incident Forensics & Packet Capture

- Восстанавливает последовательность действий киберпреступников
- Восстанавливает исходные сетевые данные, связанные с инцидентами ИБ

# Data Store

# Проблема

Необходимо собирать больше данных

–Расследования, Аудит, Compliance

Данные не сразу ценны для обнаружения угроз и / или сценариев ИБ

–Не нужны корреляция, offenses, UEBA и т.д..

Цена корреляции всех логов в SIEM слишком дорогая

Нет желания использовать дополнительные решения для сбора, хранения и управления журналами событий (LM)

# QRadar Data Store

## Свобода данных

- Сбор, парсинг, нормализация и хранение данных
- Нет лимита по объему данных
- Доступен функционал Search, Reports, Dashboard и Apps\*\*
- Простое, фиксированное, недорогое лицензирование на appliance/node
- Лицензия не привязана к конкретному node/appliance
- Отсутствие отдельной системы хранения, данные собираются и хранятся совместно
- Создание приложений для нового функционала !

Входит в "Data Store"	Не входит в "Data Store"
Сбор	Корреляция (в реальном времени и историческая)
DSM Builder	Сетевые потоки
Нормализация	Assets*
Хранение	Offenses
Querying (AQL)	UBA*
Time Series	X-Force
SDK и Apps	Cloud Discovery*
Dashboards и Reporting	Data Discovery*

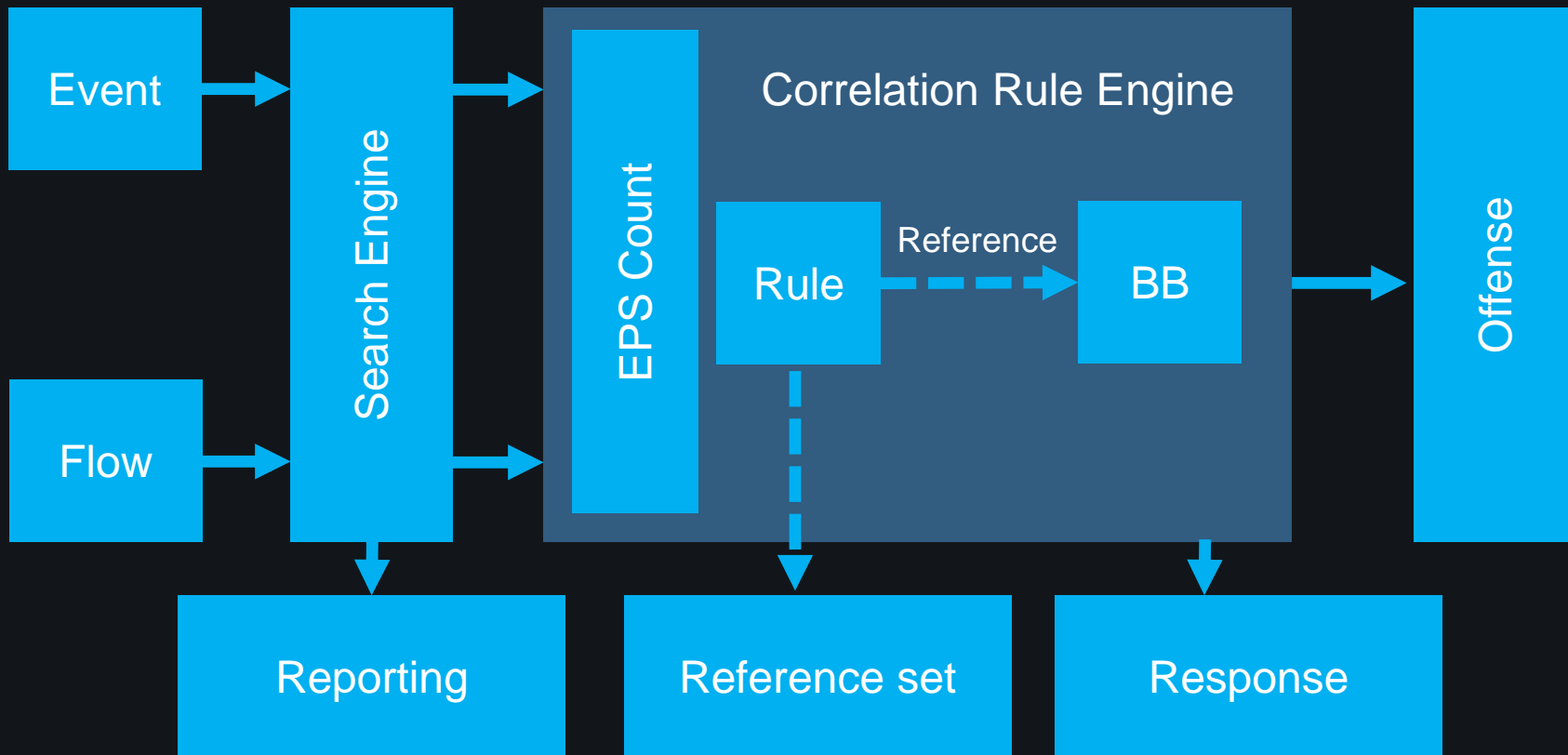
\*\* Кроме UBA, Cloud Discovery

# Примеры сценариев использования

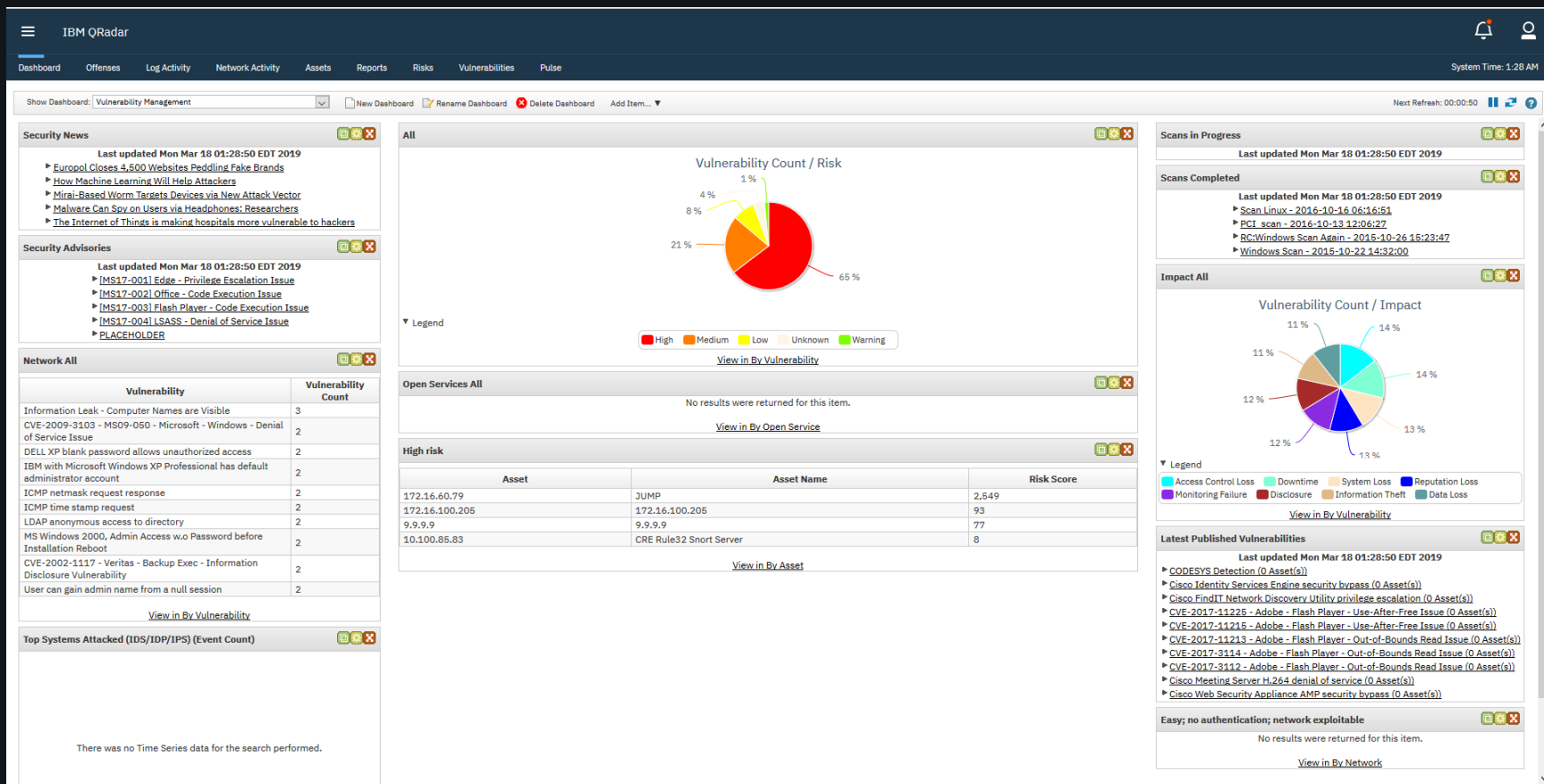
- Планируется внедрение решений класса Data Lake / Big Data
- Логи аудита рабочих станций и debug нужны для соответствия требованиям регуляторов и расследований
- Сбор логов аудита Unix/Windows для соответствия требованиям регуляторов и расследований
- Внедрены новые сервисы приложений и необходимо отчитываться о их работе, и пока сценарии ИБ не до конца разработаны / внедрены, данные нужно хранить для расследований / отчетности / соответствия требованиям регуляторов
- Снизить количество инструментов для соответствия. Требуется единая платформа данных, которая может поддерживать хранилище, аудит, отчетность и аналитику
- IT Ops / Internet of Things (IOT)



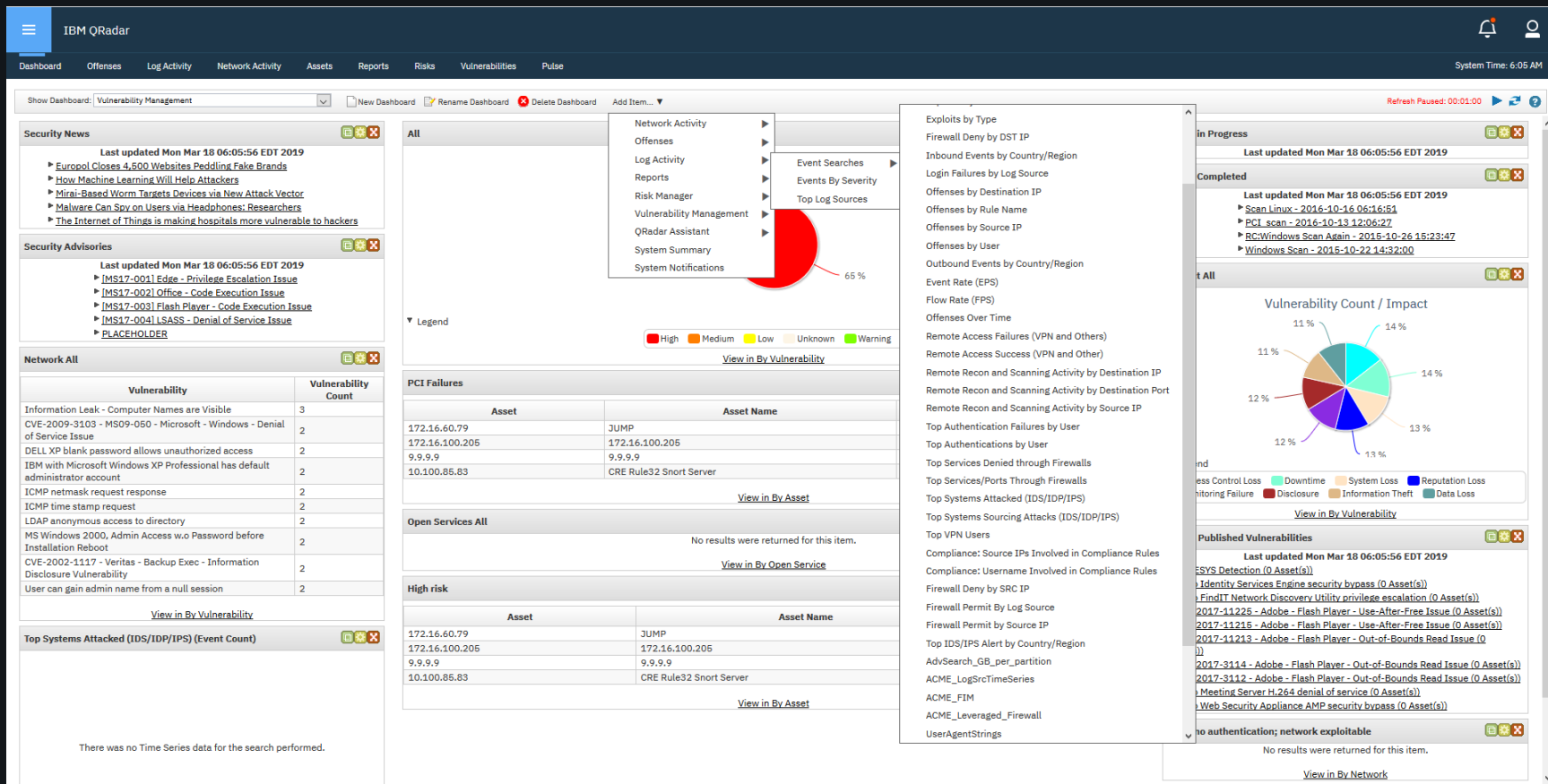
# QRadar – Правила корреляции



# QRadar – Консоль администраторов – Отчетность



# QRadar – Консоль администраторов – Отчетность – Поиск



# QRadar – Консоль администраторов – Отчетность – Поиск

IBM QRadar

DashboardOffensesLog ActivityNetwork ActivityAssets

Show Dashboard: Vulnerability Management

Security News

Last updated Mon Mar 18 06:05:56 EDT 2019

- [Europool Closes 4,800 Websites Peddling Fake Brands](#)
- [How Machine Learning Will Help Attackers](#)
- [Mirai-Based Worm Targets Devices via New Attack Vector](#)
- [Malware Can Spy on Users via Headphones: Researchers](#)
- [The Internet of Things is making hospitals more vulnerable to hackers](#)

Security Advisories

Last updated Mon Mar 18 06:05:56 EDT 2019

- [\[MS17-001\] Edge - Privilege Escalation Issue](#)
- [\[MS17-002\] Office - Code Execution Issue](#)
- [\[MS17-003\] Flash Player - Code Execution Issue](#)
- [\[MS17-004\] LSASS - Denial of Service Issue](#)
- [PLACEHOLDER](#)

Network All

Vulnerability	Vulnerability Count
Information Leak - Computer Names are Visible	3
CVE-2009-3103 - MS09-050 - Microsoft - Windows - Denial of Service Issue	2
DELL XP blank password allows unauthorized access	2
IBM with Microsoft Windows XP Professional has default administrator account	2
ICMP netmask request response	2
ICMP time stamp request	2
LDAP anonymous access to directory	2
MS Windows 2000, Admin Access w/o Password before Installation Reboot	2
CVE-2002-1117 - Veritas - Backup Exec - Information Disclosure Vulnerability	2
User can gain admin name from a null session	2

View in By Vulnerability

Top Systems Attacked (IDS/IDP/IPS) (Event Count)

There was no Time Series data for the search performed.

Edit Dashboard Item

Name \*

Active offenses over time

Query

Data source \*AQL

Refresh TimeEvery Minute

AQL Statement

```
1 select ("SUM_Active Offense Count" / 2), "Time" * 1000
2 from GLOBALVIEW('Offenses Over Time','NORMAL')
3 order by "Time" desc
4 last 2 days
```

Results Limit

10000

Run Query

# QRadar – Отчетность

☰

IBM QRadar

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Risks

Vulnerabilities

Pulse

System Time: 1:19 AM

Reports

▼ Reports

- Manual
- Hourly
- Daily
- Weekly
- Monthly

Branding

Group: Reporting Groups

Manage Groups

Actions ▼

Hide Inactive Reports

Search Reports...

View the IBM App Exchange for more...

Next Refresh: 00:00:50

Report Name	Group ▼	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
Default-Security Access Devices-WindowsAuthServer: Top Host Successful Auth...	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Administrative Changes	WindowsAuthServer	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Application / OS-WindowsAuthServer: Errors	WindowsAuthServer	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Errors	WindowsAuthServer	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Application / OS-WindowsAuthServer: Warnings	WindowsAuthServer	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Top Host Successful Auth...	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Top Host Failed Authentic...	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Application / OS-WindowsAuthServer: Failed Logins by IP	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Application / OS-WindowsAuthServer: Successful Logins by IP	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Top Host Failed Authentic...	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Sessions Opened	WindowsAuthServer	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Top Host Successful Auth...	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Application / OS-WindowsAuthServer: Failed Logins by User	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Failed Authentications	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Top Hosts Failed Authent...	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Warnings	WindowsAuthServer	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Sessions Closed	WindowsAuthServer	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Application / OS-WindowsAuthServer: Successful Logins by User	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Security Access Devices-WindowsAuthServer: Successful Authentications	WindowsAuthServer	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Application / OS-WebProxy: Successful Logins by IP	WebProxy	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Application / OS-WebProxy: Failed Logins by IP	WebProxy	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Application / OS-WebProxy: Warnings	WebProxy	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Application / OS-WebProxy: Failed Logins by User	WebProxy	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-Application / OS-WebProxy: Errors	WebProxy	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	
Default-Application / OS-WebProxy: Successful Logins by User	WebProxy	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Weekly PCI Compliance Failures	Vulnerability Management	Manual	Manual	Apr 28, 2013, 5:03 ...	admin	admin	None	
Vulnerability Exceptions	Vulnerability Management	Manual	Manual	Apr 30, 2013, 6:28 ...	admin	admin	None	
PCI Compliance Failures	Vulnerability Management	Manual	Manual	Apr 28, 2013, 4:57 ...	admin	admin	None	
Monthly Vulnerability Overview	Vulnerability Management	Manual	Manual	Apr 30, 2013, 6:36 ...	admin	admin	None	
Default logon vulnerabilities	Vulnerability Management	Manual	Manual	Apr 30, 2013, 6:54 ...	admin	admin	None	
Last 7 Days Vulnerability Overview	Vulnerability Management	Manual	Manual	Apr 28, 2013, 5:20 ...	admin	admin	None	
Network Vulnerability Overview	Vulnerability Management	Manual	Manual	Apr 28, 2013, 5:21 ...	admin	admin	None	
Accessible files vulnerability	Vulnerability Management	Manual	Manual	Apr 30, 2013, 6:56 ...	admin	admin	None	
Annual Vulnerability Overview	Vulnerability Management	Manual	Manual	Apr 30, 2013, 6:37 ...	admin	admin	None	
Vulnerability Overview	Vulnerability Management	Manual	Manual	Apr 28, 2013, 5:27 ...	admin	admin	None	
Obsolete Environments	Vulnerability Management	Manual	Manual	Apr 28, 2013, 5:32 ...	admin	admin	None	
Default-VPN-VPNGateway: Top Time Connected by User	VPNGateway	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-VPN-VPNGateway: Top Permitted Connections by User	VPNGateway	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-VPN-VPNGateway: Top Denied Connections by IP	VPNGateway	Daily	Inactive	Sep 11, 2008, 8:56...	admin	admin	None	
Default-VPN-VPNGateway: Warnings	VPNGateway	Daily	Inactive	Sep 9, 2008, 2:28 ...	admin	admin	None	

Displaying 1 to 40 of 1645 items (Elapsed time: 0:00:00.627)

Page: 1 → < 1 2 3 ... 42 >

# QRadar – Отчетность

New Group

Edit

Copy

Remove

Share

Reporting Groups

Compliance

COBIT

FISMA

GLBA

GPG13

GSX-Memo22

HIPAA

ISO 27001

NERC

PCI

SOX

Configuration and Change Management

Executive

Log Sources

AntiVirus

Applications / OS

Databases

Firewalls / Routers / Switches

IDS / IPS

Security Access Log Sources

VPNs

Network Management

QRadar Network Insights (QNI)

Security

Usage Monitoring

Virtual Infrastructure

VI PCI

VI User Authentication Reports

VoIP

Vulnerability Management

CIS Benchmark Reports

Scan Reports


Other

Name	User	Description	Date Modified	Shared With
PCI 7.1 - Access to Cardholder and Trusted Systems (Monthly)	admin		Sep 16, 2010, 12:44:07...	
PCI 5.2 - Malware	admin		Sep 16, 2010, 11:49:02...	
PCI 7.1 - Access to Cardholder and Trusted Systems (Weekly)	admin		Sep 16, 2010, 12:44:19...	
PCI 2.1 - Vendor Defaults (Monthly)	admin		Sep 16, 2010, 12:42:58...	
PCI 2.3 - Traffic to Trusted Segments (Weekly)	admin		Sep 16, 2010, 12:43:18...	
Network Traffic Volume	admin	This report provides a summary of network traffic volume.	Sep 16, 2010, 7:29:41 ...	
PCI 5.2 - Top Malware Activity	admin		Sep 16, 2010, 11:50:46...	
PCI 8.1 - User Account Additions and Changes	admin		Sep 16, 2010, 12:13:23...	
PCI 1.3 - Traffic Summaries (Weekly)	admin		Sep 16, 2010, 12:42:01...	
PCI 1.3 - Traffic Summaries (Monthly)	admin		Sep 16, 2010, 12:41:55...	
PCI 4.1 - Traffic to Trusted Segments from Untrusted Segments (Weekly)	admin		Sep 16, 2010, 12:43:31...	
PCI 4.1 - Traffic to Trusted Segments from Untrusted Segments (Monthly)	admin		Sep 16, 2010, 12:43:25...	
PCI 10.2 - User Accounts Additions by Admin (Weekly)	admin		Sep 16, 2010, 12:42:46...	
PCI 1.2.1a - Internal Network (not DMZ) to Internet	admin		Sep 16, 2010, 11:17:15...	
PCI 6.6 - Attacks against Public Facing Applications or Services	admin		Sep 16, 2010, 12:08:43...	
PCI 5.2 - Malware or Virus Clean Failed	admin		Sep 16, 2010, 11:51:09...	
PCI 1.2.1b - Inbound and Outbound Traffic (Weekly)	admin		Sep 16, 2010, 12:41:49...	
PCI 6.1 - Vulnerabilities	admin		Sep 16, 2010, 12:38:40...	
Network Traffic Volume	admin	This report provides a summary of network traffic volume.	Sep 17, 2010, 7:56:33 ...	
PCI 2.3 - Traffic to Trusted Segments	admin		Sep 16, 2010, 11:43:46...	
PCI 6.6 - Attacks against Public Facing Applications or Services (Monthly)	admin		Sep 16, 2010, 12:43:53...	
PCI 10.2 - User Accounts Additions by Admin (Monthly)	admin		Sep 16, 2010, 12:42:40...	
Top Users by Remote Access Activity	admin	This report displays top users by number of successful remote logins o...	Sep 16, 2010, 7:34:43 ...	
PCI 8.1 - User Account Additions and Changes (Weekly)	admin		Sep 16, 2010, 12:44:43...	
PCI 10 - Audit of Data (Weekly)	admin		Sep 16, 2010, 12:42:14...	
PCI 2.2 - Server Function	admin		Sep 16, 2010, 11:40:00...	
PCI 1.2.1b - Inbound and Outbound Traffic	admin		Sep 16, 2010, 11:16:43...	
PCI 2.1 - Vendor Defaults	admin		Sep 16, 2010, 11:32:11...	
PCI 7.1 - Access to Cardholder and Trusted Systems	admin		Sep 16, 2010, 12:23:15...	
PCI 11.3/11.2 Vulnerability Report	admin	This report provides a detailed vulnerability reference report for the To...	Sep 16, 2010, 12:23:26...	
PCI 2.3 - Traffic to Trusted Segments (Monthly)	admin		Sep 16, 2010, 12:43:12...	
PCI 4.1 - Traffic to Trusted Segments from Untrusted Segments	admin		Sep 16, 2010, 11:44:57...	
PCI 1.2.1a - Internal Network (not DMZ) to Internet (Monthly)	admin		Sep 16, 2010, 12:41:10...	
PCI 8.1 - User Account Additions and Changes (Monthly)	admin		Sep 16, 2010, 12:44:36...	
PCI 10 - Audit of Data (Monthly)	admin		Sep 16, 2010, 12:42:08...	
PCI 5.2 - Malware (Monthly)	admin		Sep 16, 2010, 12:43:38...	
PCI 1.3 - Traffic Summaries (Details)	admin		Sep 16, 2010, 11:25:26...	
PCI 6.6 - Attacks against Public Facing Applications or Services (Weekly)	admin		Sep 16, 2010, 12:44:01...	
PCI 1.2.1b - Inbound and Outbound Traffic (Monthly)	admin		Sep 16, 2010, 12:41:41...	
PCI 5.2 - Malware (Weekly)	admin		Sep 16, 2010, 12:43:44...	
PCI 10.2 - User Accounts Additions by Admin	admin		Sep 16, 2010, 12:15:56...	
PCI 1.2.1a - Internal Network (not DMZ) to Internet (Weekly)	admin		Sep 16, 2010, 12:41:17...	



# QRadar – Отчетность

Report Wizard

 **Report Wizard**

This report should be scheduled to generate:

☒ Manually

☐ Hourly

☐ Daily

☐ Weekly


☐ Monthly


[<< Back](#) [Next >>](#) [Finish](#) [Cancel](#)

# QRadar – Отчетность

Report Wizard

Report Wizard

 Report Wi

 Report Wizard

This report should be s

Choose a Layout

Each divided section holds one chart. Click the layout that represents the size and number of charts required.

Orientation: Landscape

☒ Manually

☐ Hourly

☐ Daily

☐ Weekly

☐ Monthly

<< Back

Next >>

Finish


Cancel


# QRadar – Отчетность


Report Wizard

Report Wizard

Report Wizard

 **Report Wi**

 **Report Wizard**

 **Report Wizard**

This report should be:

☒ Manually

☐ Hourly

☐ Daily

☐ Weekly

☐ Monthly

Choose a Layout

Each divided section holds one chart

Orientation: Landscape

Specify Report Contents

Enter a report title and choose a logo. Select a chart type and click 'Define' for each chart you wish to configure. Configured charts become highlighted. Click Next.

Report Title:

Logo: coolblue.png

Chart Type:  
Top Offenses

Define

Chart Type:  
Asset Vulnerabilities

Define

Chart Type:  
Log Sources

Define

Pagination Options: Bottom Center

Report Classification:

<< Back

Next >>

Finish

Cancel


# QRadar – Отчетность

Report Wizard

Report Wizard


Report Wizard

Report Wizard

 Report Wi

This report should be s


☒ Manually  
☐ Hourly  
☐ Daily  
☐ Weekly  
☐ Monthly

 Report Wizard

Choose a Layout

Each divided section holds one ch

Orientation: Landscape

 Report Wizar

Specify Report Contents

Enter a report title and c

charts become highlight

asdasd


Generated: Mar 18, 2019

dasdaa

asd

asd


1

 Report Wizard

Layout Preview

This report preview displays the report layout and chart types you have chosen. It does not reflect live data.

<< Back

Next >>

Finish

Cancel

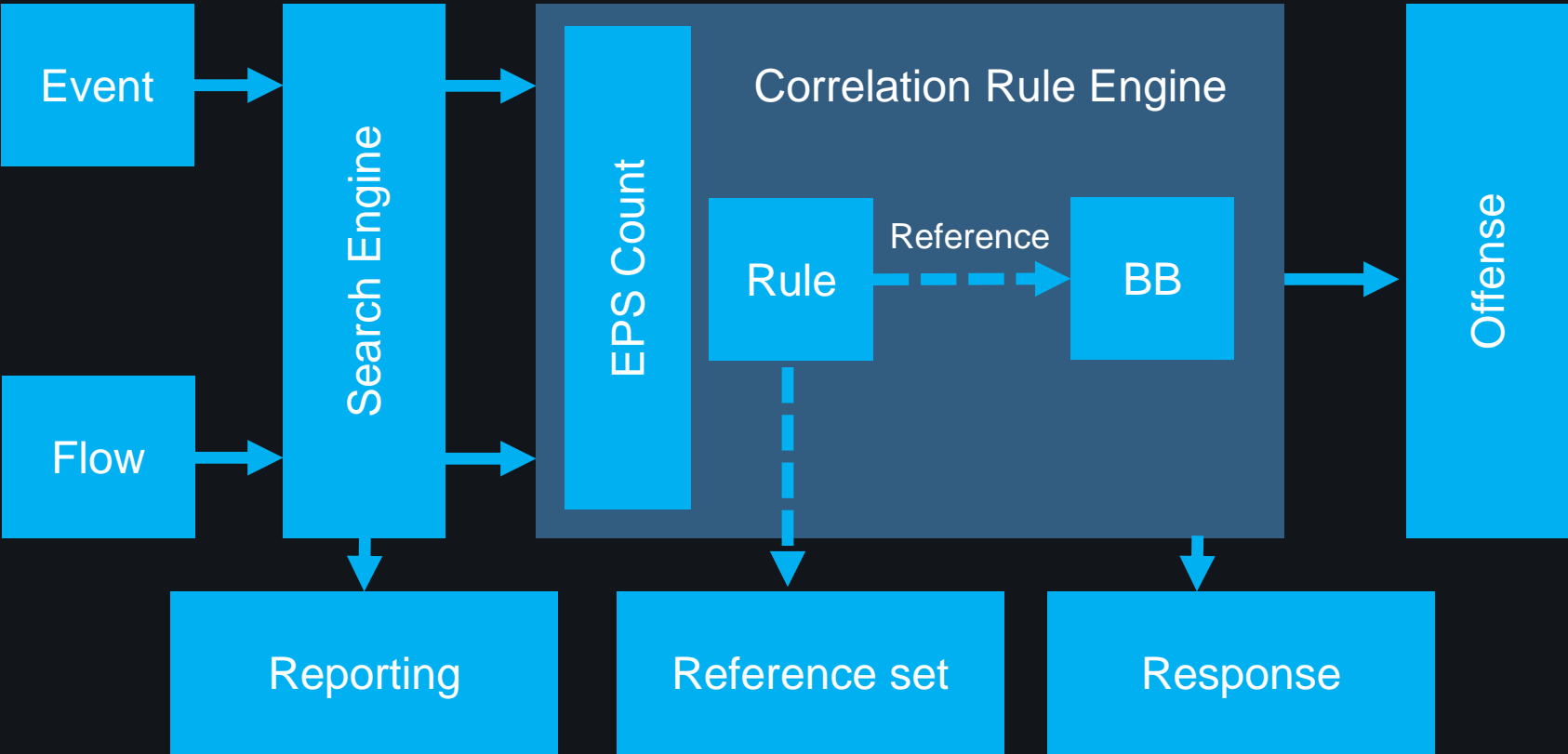
# QRadar – Отчетность

The image displays a sequence of five screenshots from the SAP 'Report Wizard' interface, illustrating the steps to create a report.

- Step 1: This report should be scheduled**
  - Choose a Layout: Each divided section holds one chart. Orientation: Landscape.
  - Frequency: ☒ Manually, ☐ Hourly, ☐ Daily, ☐ Weekly, ☐ Monthly.
- Step 2: Specify Report Contents**
  - Enter a report title and content. Charts become highlighted.
  - Orientation: Landscape.
- Step 3: Layout Preview**
  - This report preview displays the layout.
  - Preview shows a table with columns 'asdasd' and 'Generated: Mar 2010'.
- Step 4: Choose the report format**
  - Choose the report format: ☒ PDF (An easily printable and transferable document), ☐ HTML (Useful displaying reports on the web in your browser), ☐ RTF (Report data in Rich Text Format).
  - The following formats are available for single table templates only: ☐ XML (Extensible Markup Language), ☐ XLS (Excel), ☐ CSV (Comma-Separated Values).

The bottom of the screenshots shows navigation buttons: << Back, Next >>, Finish, Cancel.


# QRadar – Правила корреляции





# QRadar – Правила корреляции

Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming flows and events?

Test GroupAll

Export as Building Block

Type to filter

+

when the local network is **one of the following networks**

+

when the **destination** network is **one of the following networks**

+

when the IP protocol is one of the following **protocols**

+

when the Flow Source or Destination Payload contains **this string**

+

when the source port is one of the following **ports**

+

when the destination port is one of the following **ports**

+

when the local port is one of the following **ports**

+

when the remote port is one of the following **ports**

+

when the source IP is one of the following **IP addresses**

+

when the destination IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  on events or flows which are detected by the 

Local

 system

and

when the Flow Source or Destination Payload contains this string

and

when a subset of at least this number of these rules, in order, from the same source IP to the same destination IP, over this many seconds

and

when any of these properties is the key and any of these properties is the value in any of these reference maps

Please select any groups you would like this rule to be a member of:

Anomaly

Asset Reconciliation Exclusion

Authentication

Botnet

Category Definitions

Notes (Enter your notes about this rule)

<< Back


Next >>

Finish

Cancel

# QRadar – Правила корреляции

Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming flows and events?

Test Group All Export

Type to filter

- when the local network is **one of the following networks**
- when the **destination** network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Flow Source or Destination Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)

Invalid tests are highlighted and must be fixed before rule can be saved.

Apply enter rule name here on events or flows which are detected by the Local

and when the Flow Source or Destination Payload contains this string

and when a subset of at least this number of these rules, in order, from the same source IP to the same destination this many seconds

and when any of these properties is the key and any of these properties is the value in any of these reference monitors


Please select any groups you would like this rule to be a member of:

- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☐ Category Definitions

Notes (Enter your notes about this rule)

<< Back Next >>

Rule Wizard

Rule Wizard: Rule Response

### Rule Action

Choose the action(s) to take when an event or flow occurs that triggers this rule

<input type="checkbox"/> Severity	Set to	<span>0</span>
<input type="checkbox"/> Credibility	Set to	<span>0</span>
<input type="checkbox"/> Relevance	Set to	<span>0</span>
<input type="checkbox"/> Ensure the detected event or flow is part of an offense		
<input type="checkbox"/> Annotate event or flow		
<input type="checkbox"/> Drop the detected event or flow		

### Rule Response

Choose the response(s) to make when an event or flow triggers this rule

- ☐ Dispatch New Event
- ☐ Email
- ☐ Send to Local SysLog
- ☐ Send to Forwarding Destinations
- ☐ Notify
- ☐ Add to a Reference Set
- ☐ Add to Reference Data
- ☐ Remove from a Reference Set
- ☐ Remove from Reference Data
- ☐ Trigger Scan
- ☐ Execute Custom Action

### Response Limiter

Use this section to configure the frequency with which you want this rule to respond


☐ Respond no more than 1 time(s) per 30 minute(s) per Rule

### Enable Rule

☒ Enable this rule if you want it to begin watching events or flows right away.

# QRadar – Правила корреляции – Event chain, Reference set

Rule Wizard

 Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group Functions - Sequence 

Export as Building Block

Type to filter

+

when all of these rules, in|in any order, from the same|any source IP to the same|any destination IP, over this many seconds

+

when a subset of at least this number of these rules, in|in any order, from the same|any source IP to the same|any destination IP, over this many seconds

+

when this sequence of rules, involving the same source and destination hosts in this many seconds

+

when a subset of at least this many of these rules, in|in any order, with the same username followed by a subset of at least this many of these rules in|in any order to|from the same destination IP from the previous sequence, within this many minutes

+

when these rules match at least this many times in this many minutes after any of these rules match

+

when these rules match at least this many times with the same event properties in this many minutes after these rules match

+

when these rules match at least this many times with the same event properties and different event properties in this many minutes

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  on events which are detected by the 

Local

 system

Please select any groups you would like this rule to be a member of:

Anomaly

Asset Reconciliation Exclusion

Authentication

Botnet

Category Definitions

Notes (Enter your notes about this rule)

<< Back

Next >>

Finish

Cancel

# QRadar – Правила корреляции – Event chain, Reference set

Rule Wizard

**Rule Wizard: Rule Test Stack Editor**

Which tests do you wish to perform on incoming events?

Test Group Functions - Sequence

Type to filter

- when all of these rules, in any order, from the same any source IP to the same any destination seconds
- when a subset of at least this number of these rules, in any order, from the same any source destination IP, over this many seconds
- when this sequence of rules, involving the same source and destination hosts in this many seconds
- when a subset of at least this many of these rules, in any order, with the same username follow this many of these rules in any order to from the same destination IP from the previous seconds
- when these rules match at least this many times in this many minutes after any of these rules
- when these rules match at least this many times with the same event properties in this many minutes
- when these rules match at least this many times with the same event properties and different

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  on events which are detected by

Please select any groups you would like this rule to be a member of:

- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☐ Category Definitions

Notes (Enter your notes about this rule)

Rule Wizard

**Rule Wizard: Rule Test Stack Editor**

Which tests do you wish to perform on incoming events?

Test Group All Export as Building Block

Type to filter

- when the source IP is vulnerable to one of the following CVEs
- when the source IP is a part of any of the following remote network locations
- when the source IP is a part of any of the following remote services network locations
- when the source IP is a part of any of the following geographic network locations
- when any of these event properties are contained in any of these reference set(s)
- when any of these event properties is the key and any of these event properties is the value in any of these reference maps
- when any of these event properties is the key and any of these event properties is the value in any of these reference map of sets
- when any of these event properties is the key of the first map and any of these event properties is the key of the second map and any of these event properties is the value in any of these reference map of maps
- when Reference Table Key data matches any/all selected event properties and selected reference table column Select

Rule (Click on an underlined value to edit it)  
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply  on events which are detected by the Local system

☐ and when any of Identity Username is the key and any of Username is the value in any of MGRS: Domain Admin Groups Attributes - AlphaNumeric

Please select any groups you would like this rule to be a member of:

- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☐ Category Definitions

Notes (Enter your notes about this rule)

<< Back Next >> Finish Cancel

# Портфель продуктов IBM QRadar

## Многофункциональная платформа управления инцидентами ИБ



### QRadar Log Manager (Data Store)

- Сбор и обработка большого количества событий безопасности
- Возможность обновления до SIEM

### QRadar SIEM

- Сбор логов и сетевой статистики, соответствие регуляторным требованиям
- Профилирование активов, анализ сетевой активности и угроз ИБ
- Инциденты ИБ и их расследование

### Репутационная база IBM X-Force

### QFlow и QRadar Network Insights

Сетевая аналитика, обнаружение аномалий

- Анализ 7 уровня модели OSI
- Анализ сетевых пакетов в реальном времени

### QRadar Vulnerability Manager и Risk Management

- Встроенные механизмы сканирования сети
- Управление рисками и приоритезация уязвимостей
- Моделирование и симуляция атак злоумышленников
- Мониторинг и аудит конфигурации сетевых устройств
- Продвинутый анализ угроз и последствий

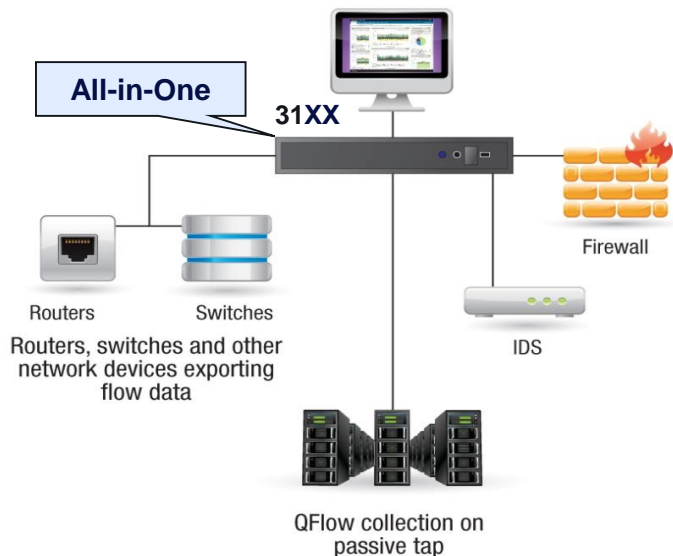
### QRadar Incident Forensics & Packet Capture

- Восстанавливает последовательность действий киберпреступников
- Восстанавливает исходные сетевые данные, связанные с инцидентами ИБ

# Две модели внедрения: All-in-One и Distributed

## Sample IBM Security QRadar SIEM all-in-one deployment

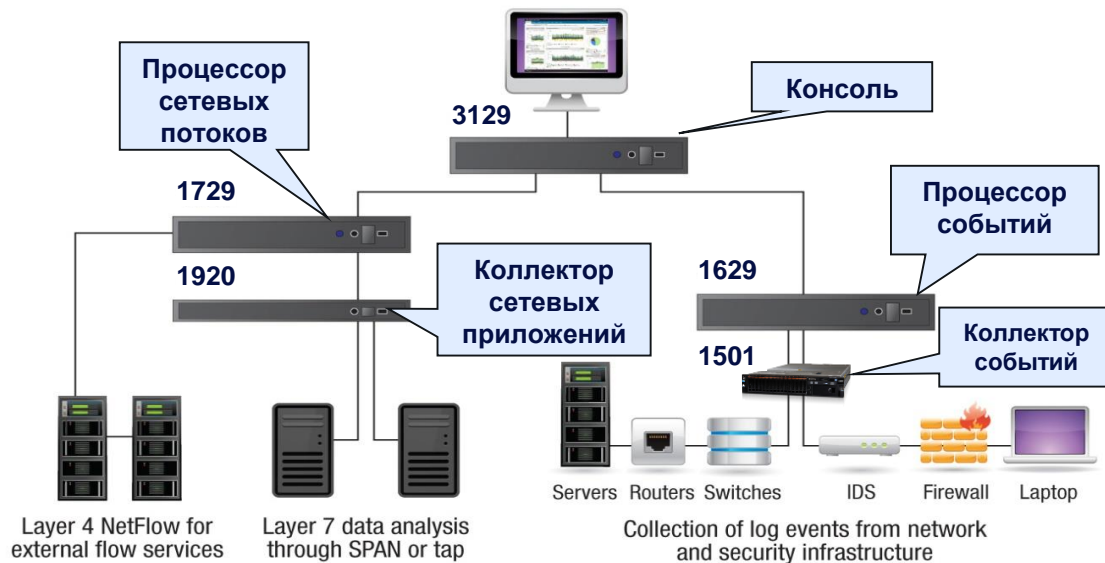
QRadar web console



**Всё-в-одном** – это единый сервер, который используется для сбора как событий так и потоков с различных источников (устройств ИБ, сетевых и пр.), осуществляя корреляцию данных и проверку правил, предоставляя уведомления и отчеты по угрозам и нарушениям, а также все функции администрирования системы через Web-консоль в браузере

## Sample IBM Security QRadar SIEM distributed deployment

QRadar web console



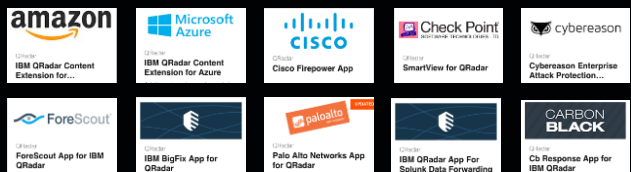
Распределенная модель состоит из множества устройств разного функционала:

- **Процессор событий** для сбора, обработки и хранения событий журналов
- **Процессор потоков** для сбора, обработки и хранения нескольких типов данных сетевых потоков генерируемых сетевыми устройствами. Опционально **Коллектор приложений** для сбора данных приложений 7-го уровня.
- **Консоль** для корреляции данных с управляемых процессоров, предоставления уведомлений и отчетов по угрозам и нарушениям, а также всех функций администрирования системы через Web-консоль в браузере

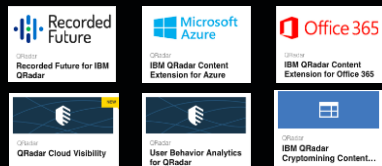
# Экосистема защиты через сотрудничество

Сотни бесплатных приложений и дополнений в IBM Security App Exchange

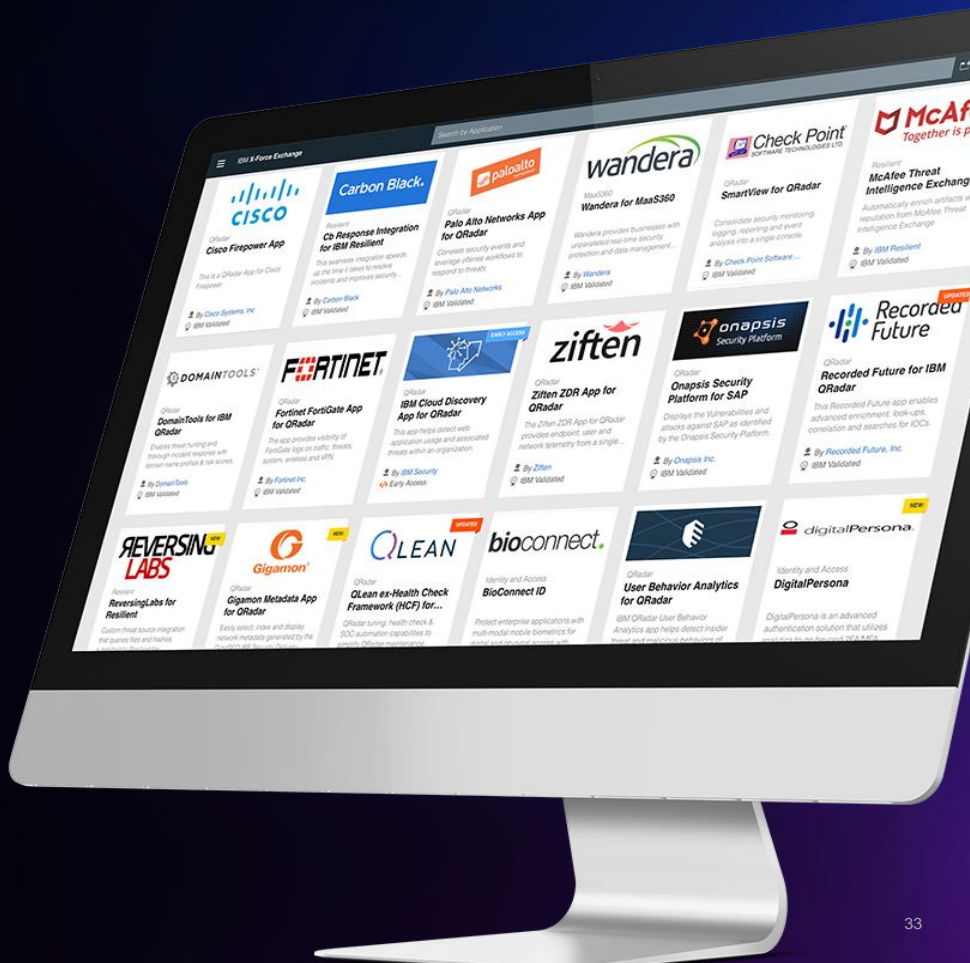
## Расширение мониторинга



## Автоматизация расследований

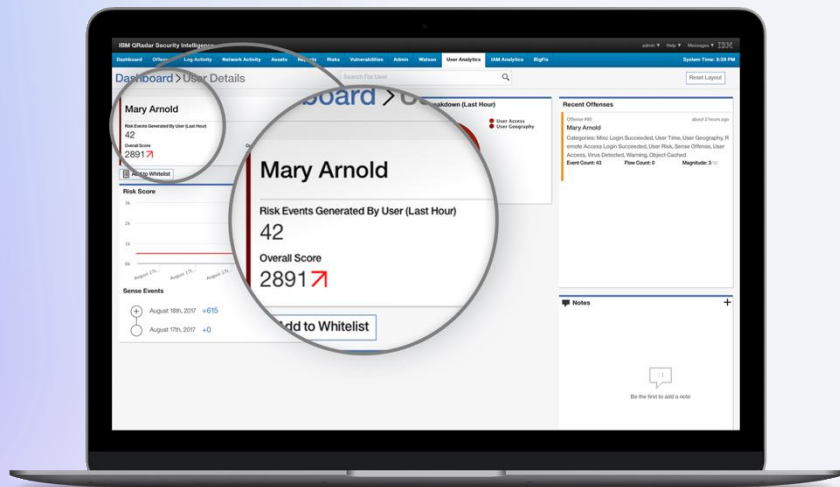


## Be Proactive



# ИИ для вашего SOC

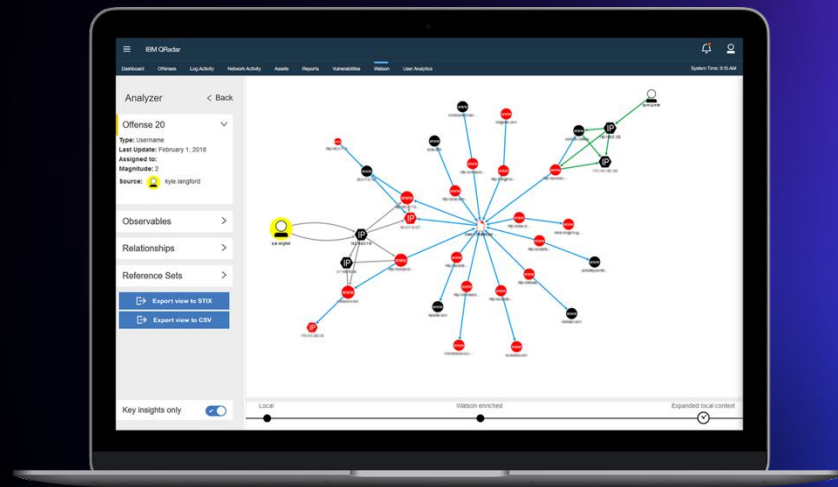
## IBM QRadar User Behavior Analytics



Выявлять угрозы инсайдеров с помощью машинного обучения

- Постоянное обучение поведению для выявления инсайдеров
- Детальная оценка рисков по каждому пользователю
- 16тыс+ скачиваний с X-Force App Exchange – **бесплатно для пользователей IBM QRadar**

## IBM QRadar Advisor with Watson



Повышение эффективности команды ИБ с помощью искусственного интеллекта

- Автоматическое объединение данных индикаторов угроз
- Быстрая визуализация карты инцидента для реагирования
- Связь с базой угроз Watson-а содержащей **10Мпрд+** записей данных ИБ



# Как сделать демо?



## YouTube Channels

- Jose Bravo

<https://www.youtube.com/user/jbravovideos/>

- IBM Security

<https://www.youtube.com/user/IBMSecuritySolutions>

- IBM Security Support

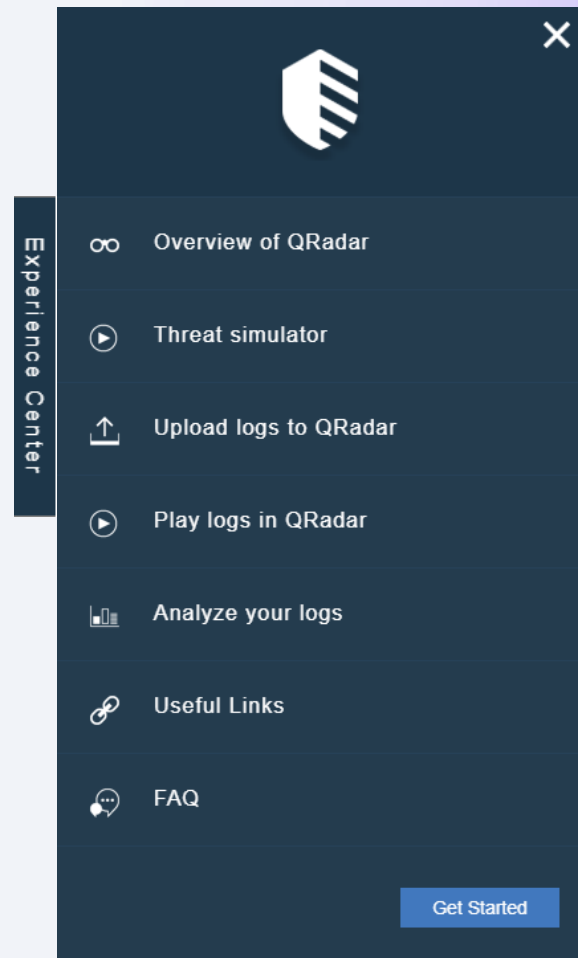
<https://www.youtube.com/user/IBMSecuritySupport>



## IBM Security Learning Academy

<https://www.securitylearningacademy.com/>

## IBM QRadar Experience Center



# Профиль идеального клиента

Зависимость бизнеса от информационных технологий

250+ сотрудников в организации

Наличие отдела ИТ  
не менее 10 человек

## Развитая инфраструктура ИБ

- Proxy
- Firewall
- User Logon (LDAP, RADIUS)
- Endpoint
- DNS
- DHCP
- AV
- IDS
- Windows

# QRadar в цифрах

Заказчики — **8,000+**

Приложения — **270+**

Базы угроз (Источники Threat Intelligence) — **10+**

- STIX/TAXII, x-Force, Threatstream, iSight, Brightpoint, RiskIQ, Custom

Уникальные Отчеты — **1664**

- Compliance, Configuration and Change Management, Executive, Log Source, Network Management, Security, Usage Monitoring, Virtual Infrastructure, Vulnerability Management

Правила корреляции / Building Blocks — **632**

Поддерживаемые Устройства, Системы, Приложения и Облачные сервисы — **550+**

Сторонние Сканеры Уязвимостей — **20**

- Qualys, Rapid7, Tenable, Tripwire, AppScan,....

Источники Потокaв — **5**

- NetFlow, J-Flow, sFlow, vFlow, QFlow

Масштабируемость и производительность — **> 4 млн EPS внедрения**

Время для полного внедрения — в среднем **< 5 месяцев**

Лидер Gartner и Forrester — **1**

# Gartner 2017-2018

## Magic Quadrant

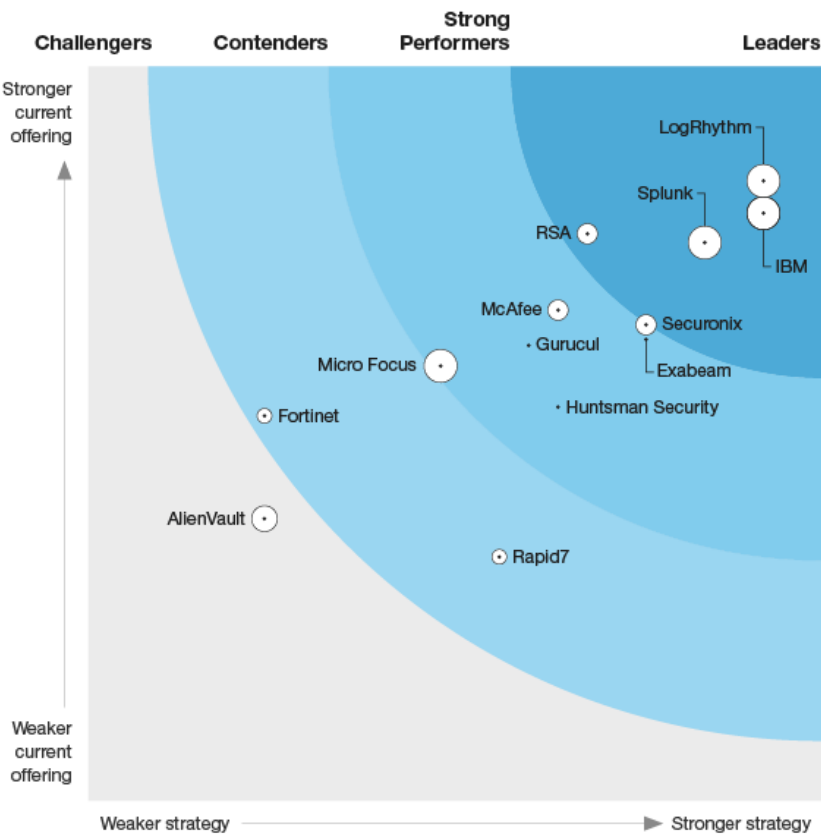
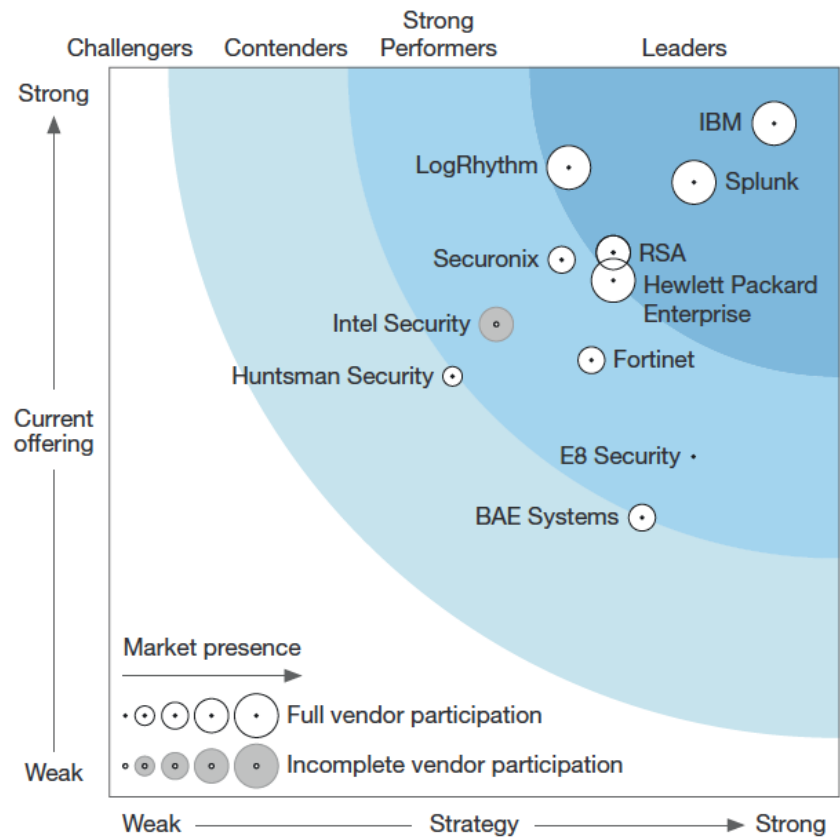
Figure 1. Magic Quadrant for Security Information and Event Management



Figure 1. Magic Quadrant for Security Information and Event Management



# Forrester 2017-2018



# СПАСИБО

FOLLOW US ON:

 [ibm.com/security](https://ibm.com/security)

 [securityintelligence.com](https://securityintelligence.com)

 [ibm.com/security/community](https://ibm.com/security/community)

 [xforce.ibmcloud.com](https://xforce.ibmcloud.com)

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

 [youtube.com/user/ibmsecuritysolutions](https://youtube.com/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.

IBM Security / © 2019 IBM Corporation