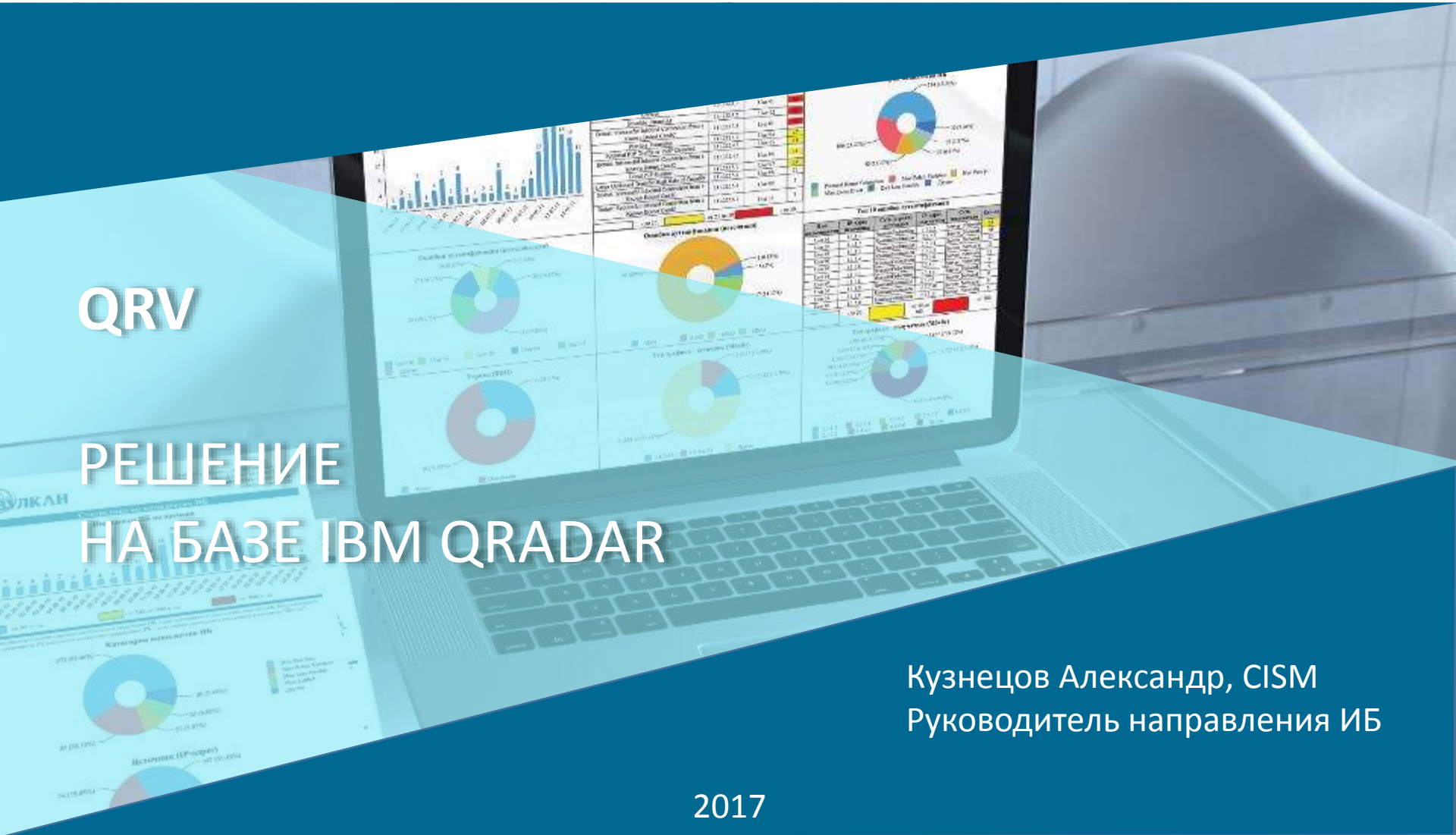
НТЦ ВУЛКАН

www.ntc-vulkan.ru



QRV

РЕШЕНИЕ НА БАЗЕ IBM QRADAR

Кузнецов Александр, CISM
Руководитель направления ИБ

2017

СОДЕРЖАНИЕ

- Что такое QRV?
- Возможности
- Для кого?
- Для чего?
- Как это работает?
- Как использовать?

ЧТО ТАКОЕ QRV?

Всё что есть в IBM QRadar SIEM

+

Автоматизатизированная корпоративная отчетность

АВТОМАТИЗАТИЗИРОВАННАЯ КОРПОРАТИВНАЯ ОТЧЕТНОСТЬ
ВОЗМОЖНОСТИ

Оформление отчетов по ИБ согласно корпоративному стилю

Dashboard'ы с функцией drilldown

Русифицированные отчеты и dashboard'ы

Приоритизация данных

Автоматическая рассылка отчетов по e-mail

50+ предустановленных наборов отчетов

ДЛЯ КОГО?
ЦЕЛЕВАЯ АУДИТОРИЯ

- ✓ Финансовые институты
- ✓ Телеком
- ✓ ТЭК и Нефтегазовый сектор
- ✓ Промышленность и транспорт
- ✓ Ритейл и оптовая торговля

ПОТРЕБИТЕЛИ ОТЧЕТА

- ✓ ТОП-менеджер
- ✓ Compliance-менеджер
- ✓ Risk-менеджер
- ✓ IT-менеджер
- ✓ IS-менеджер
- ✓ Владелец процесса (*Event Mgmt, Incident Mgmt, Access Mgmt и т.д.*)
- ✓ Технический специалист (*сетевик, системщик и т.д.*)
- ✓ Член SOC-команды

ПОЧЕМУ ?
ДЛЯ ЧЕГО?

- Необходима актуальная картина инцидентов ИБ
- Есть потребность в оценке эффективности работы ИБ-подразделений в ежедневном режиме
- Необходимо доносить важную информацию по ИБ до руководства
- Регулярная подготовка отчетов для смежных подразделений
- Требуется доступное обоснование (аргументация) для дальнейшего выделения бюджета на развитие ИБ

КАК ЭТО РАБОТАЕТ?
ПРИМЕРЫ ОТЧЕТОВ

ASA - VPN Session Closed

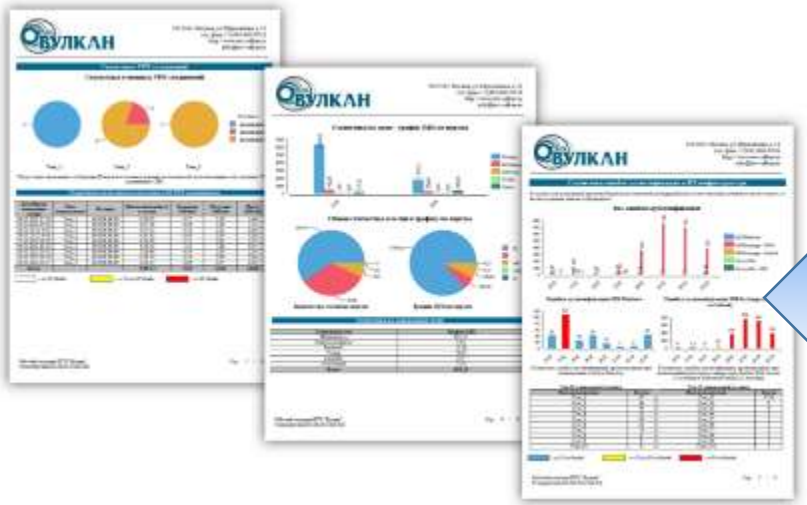
Generated: 11 May 2016, 00:41:58

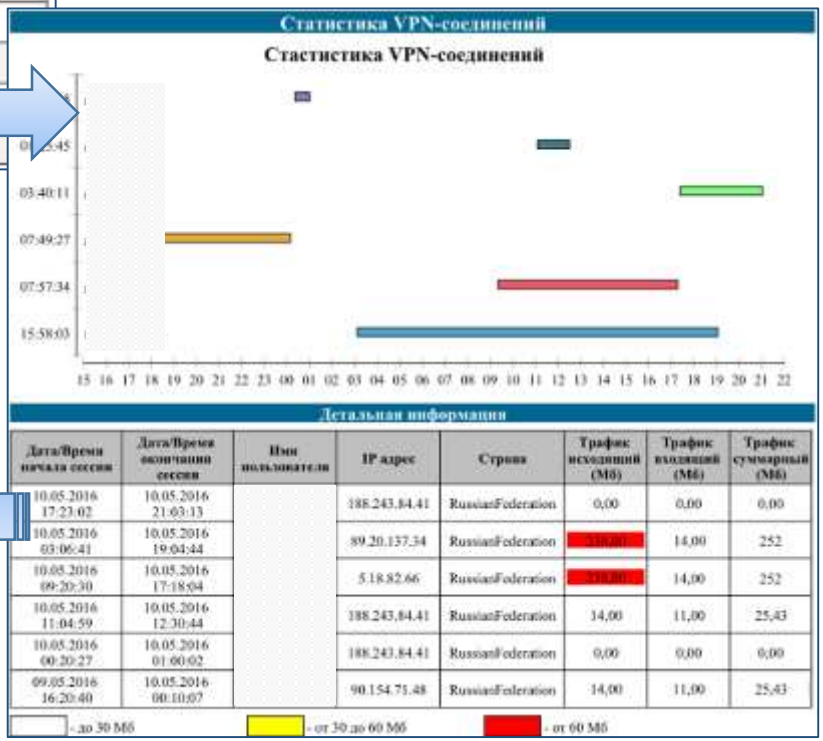
ASA - VPN Session Closed
ASA - VPN Session Closed
10 May 2016, 00:00:00 - 11 May 2016, 00:00:00

Start Time	Username	Source IP	Geographic Country/Region	BytesSent (custom)	BytesReceived (custom)	Duration_Hours (custom)	Duration_Minutes (custom)	Duration_Seconds (custom)
10 May 2016, 21:03:13		188.243.84.41	RussianFederation	179.488	191.461	3	40	11
10 May 2016, 19:04:44		89.20.137.34	RussianFederation	250.302.663	3,630.605.331	15	58	3
10 May 2016, 17:18:04		5.18.82.66	RussianFederation	302.173.578	2.546.320.604	7	57	34
10 May 2016, 12:30:44		188.243.84.41	RussianFederation	15.015.851	11.645.754	1	25	45
10 May 2016, 01:00:02		188.243.84.41	RussianFederation	171.064	86.238	0	39	3
10 May 2016, 00:10:07		90.154.71.48	RussianFederation	125.650.351	14.949.010	7	49	2

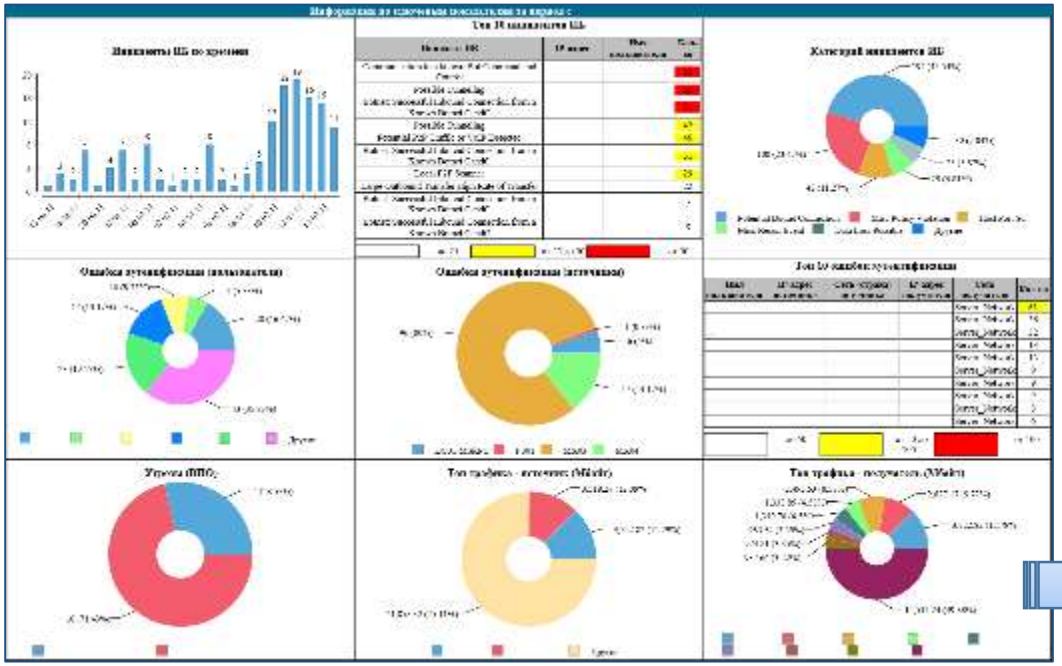
IBM QRadar

НТЦ «Вулкан»





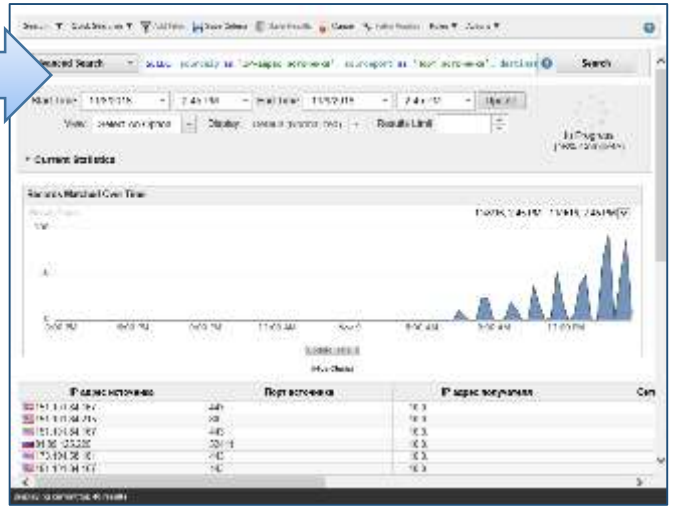
КАК ЭТО РАБОТАЕТ?
ПРИМЕРЫ ОТЧЕТОВ



НТЦ «Вулкан»

Drilldown

IBM QRadar



https://

КАК ИСПОЛЬЗОВАТЬ?

Как IBM QRadar SIEM

+

Как информационную панель для ситуационной осведомленности

Как инструмент для приоритизации ресурсов на возникающие инциденты ИБ

Как средство для выстраивания коммуникации внутри и за пределами ИБ-подразделения

СПАСИБО ЗА ВНИМАНИЕ!

105318 г. Москва, ул. Ибрагимова, д. 31
тел. +7 (495) 663-95-16
info@ntc-vulkan.ru
www.ntc-vulkan.ru

Кузнецов Александр
Руководитель направления ИБ