НТЦ ВУЛКАН

www.ntc-vulkan.ru

ОТЧЕТНОСТЬ 2.0

В SOC НА БАЗЕ IBM QRADAR

Кузнецов Александр, CISM
Руководитель направления ИБ

2016

СОДЕРЖАНИЕ

- Измерения и отчетность, точки соприкосновения
- Важна ли отчетность?
- Место инструментов для отчетности в модели SOC
- Оформление vs содержание
- Потребитель отчета, кто он?
- Формат отчета, какой он?
- От периодической отчетности к непрерывной
- Отчетность 1.0
- Отчетность 2.0 – отчет
- Отчетность 2.0 – dashboard
- Отчетность 2.0 – как это работает?
- Заключение

ИЗМЕРЕНИЕ ЭФФЕКТИВНОСТИ SECURITY OPERATIONS CENTER
ИЗМЕРЕНИЯ И ОТЧЕТНОСТЬ, ТОЧКИ СОПРИКОСНОВЕНИЯ

Зачем измерять? → **Цель**

- Что измерять?
- Где измерять?
- Когда измерять?
- Как измерять?
- Чем измерять?
- Как представить результат измерений?
- Как довести до «заказчика» результат измерений?

- *Измерить/вывести в отчет хоть что-нибудь*
- *Мы всегда это измеряли/выводили в отчет*
- *Мы измеряем/выводим в отчет именно это потому, что можем это сделать*

SECURITY OPERATIONS CENTER
ВАЖНА ЛИ ОТЧЕТНОСТЬ?

A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Finding a balance in proactive reporting to constituents and other partner SOCs will help the SOC gain recognition as a valued resource.

MITRE

2.1 Security Operations Goals

A security operations program should endeavor to achieve the following goals:

- To monitor, report, escalate and advise on security incidents.

Step 8 – Reporting

In addition to metrics and key performance indicators, a valuable tool that the security operations team can utilize is effective reporting to executive, management and technical stakeholders.

SANS

Whether an organization is building a new SOC or looking to expand existing capabilities, here are 10 considerations for success:

8 Analytics and reporting

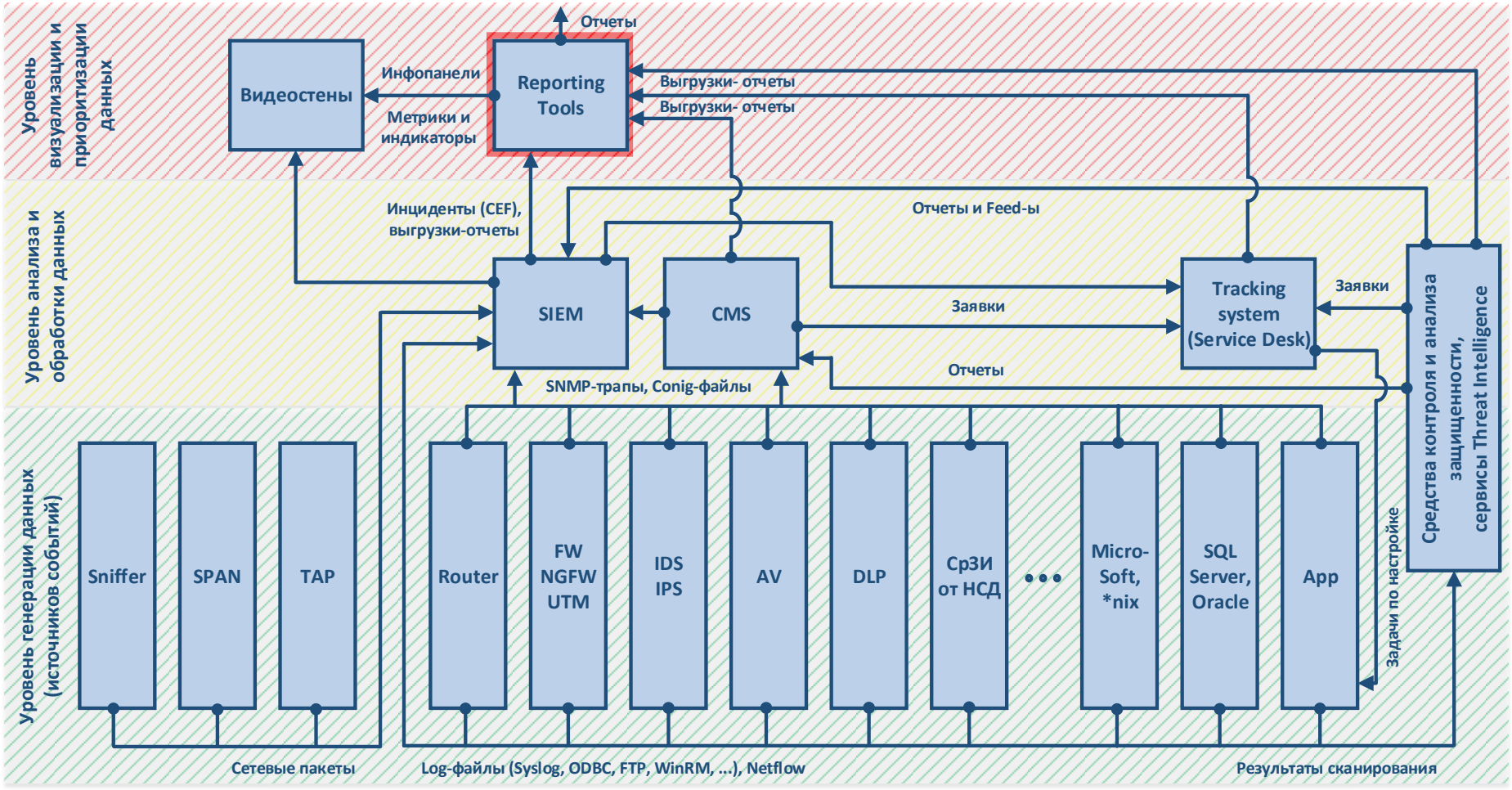
EY
Building a better working world

What is an enterprise SOC?

… the enterprise SOC specifically focuses on cyber threat, monitoring, forensic investigation, incident management and reporting.

IBM

SECURITY OPERATIONS CENTER
МЕСТО ИНСТРУМЕНТОВ ДЛЯ ОТЧЕТНОСТИ В МОДЕЛИ SOC



ПОДГОТОВКА ОТЧЕТА
ОФОРМЛЕНИЕ VS СОДЕРЖАНИЕ

Оформление

Корпоративное оформление (логотипы, цвета, шрифты и т.п.)

Форматирование таблиц и графиков/рисунков

Компоновка данных

Русификация

Интерактивность/ гиперссылки

Содержание

Значимая информация*

Ориентация на зафиксированные метрики и целевые показатели

Приоритизация данных

Отражение тенденций (в идеале прогнозирование)

Отсутствие записей типа «Unknown»

* - Использование аналога метода Goal-Question-Metric (GQM), а именно Goal-Question-Report (GQR)

ПОДГОТОВКА ОТЧЕТА
ПОТРЕБИТЕЛЬ ОТЧЕТА, КТО ОН?

- ✓ Top-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

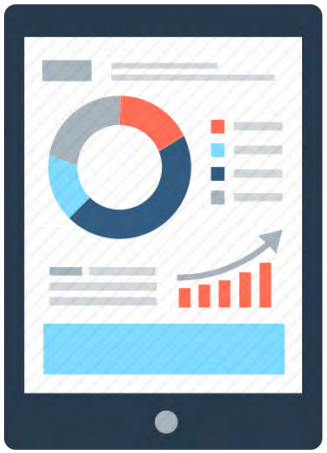
ПОДГОТОВКА ОТЧЕТА
ФОРМАТ ОТЧЕТА, КАКОЙ ОН?

Представления:

- Табличное
- Графическое (диаграммы, графики и т.д.)
- Инфографика

Формат*:

- HTML
- PDF/DOCX
- CSV/XLSX



Рекомендации:

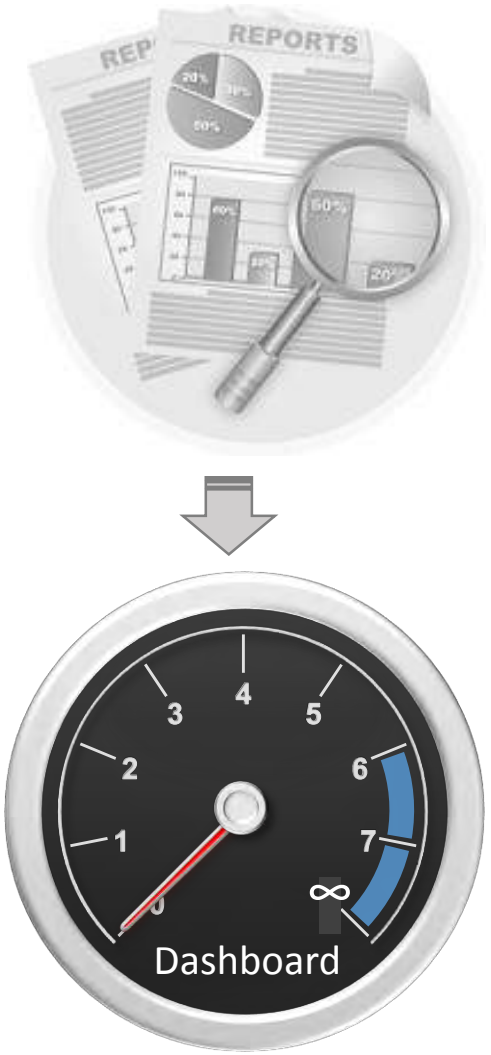
- Объём ≠ Качество
- Top vs All data
- Принцип «7±2»
- Графики ≥ таблиц
- Русификация (адаптированный перевод)
- Кастомизация оформления
- Приоритизация результатов («светофоры»)

* - Доступность на ряде устройств

ОТЧЕТНОСТЬ
ОТ ПЕРИОДИЧЕСКОЙ ОТЧЕТНОСТИ К НЕПРЕРЫВНОЙ

Недостатки периодической отчетности:

- $T_{выхода\ отчета}$: неделя – месяц
- Отсутствие понимания ситуации в режиме он-лайн – «здесь и сейчас»
- Дополнительные ~~мозговые~~ усилия по отслеживанию трендов на базе нескольких отчетов
- Накапливание множества файлов-отчетов
- Необходимость ротации файлов-отчетов
- Распространение файлов-отчетов



IBM QRADAR SIP
ОТЧЕТНОСТЬ 1.0

Оценка «Critical Capability: Log Management and Reporting»: 3.6

Gartner

Чего не хватает в части работы с отчетами:

- Изменить ширину столбцов в таблице
- Изменить заголовки столбцов в таблице
- Настроить ширину таблицы/графика в отчете
- Выделить цветом строки/части строк в таблице или части графика по заданным значениям
- Группировать таблицы/графики в отчете по горизонтали
- Изменить шрифты
- Использовать оглавление в отчете (гиперссылки)
- Создать многостраничные отчеты с рядом разделов
- Вывести более 130/300 global views на dashboard
- Вывести таблицу (результат Custom Search) как элемент dashboard-а

IBM QRADAR SIP
ОТЧЕТНОСТЬ 2.0 – ОТЧЕТ

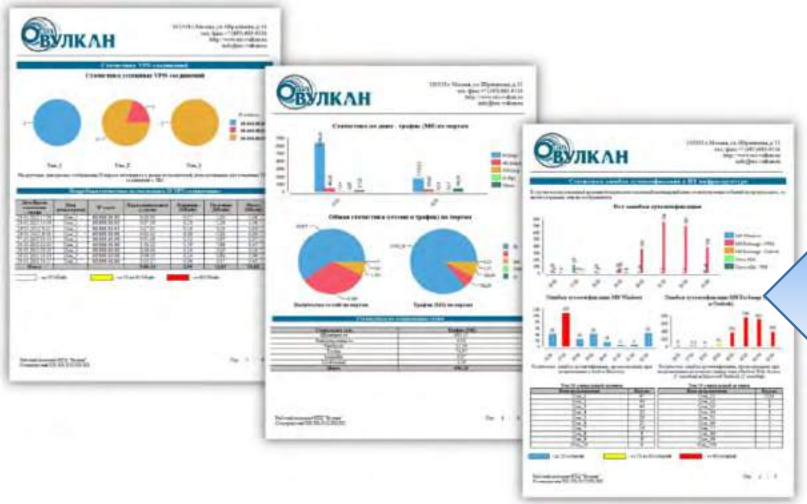
ASA - VPN Session Closed
Generated: 11 May 2016, 00:41:58

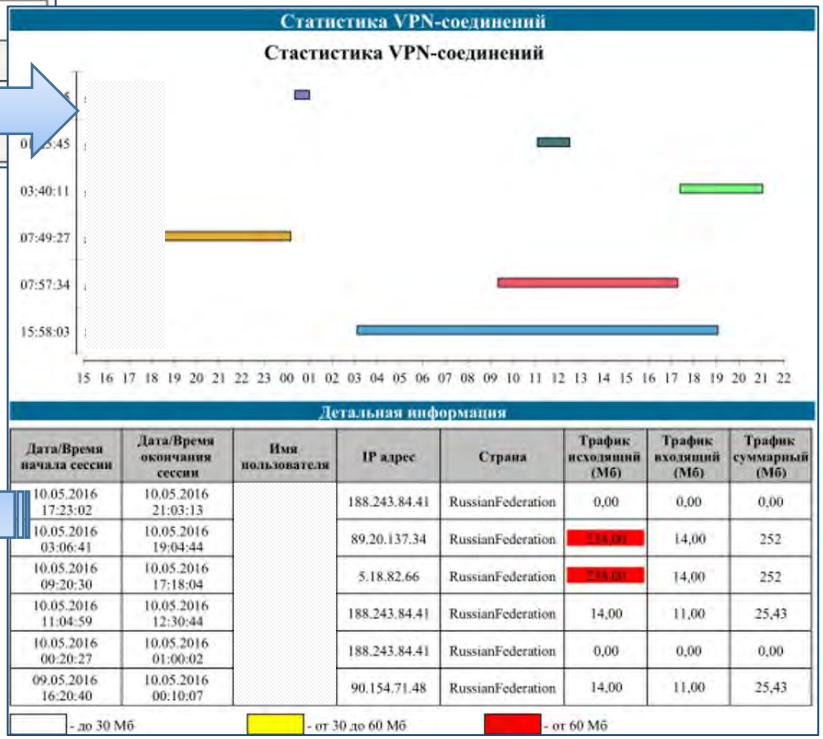
ASA - VPN Session Closed
ASA - VPN Session Closed
10 May 2016, 00:00:00 - 11 May 2016, 00:00:00

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[illegible]
10 May 2016, 00:10:07		90.154.71.48	RussianFederation	125.650.351	14.949.010	7	49	2[illegible]

IBM QRadar

НТЦ «Вулкан»



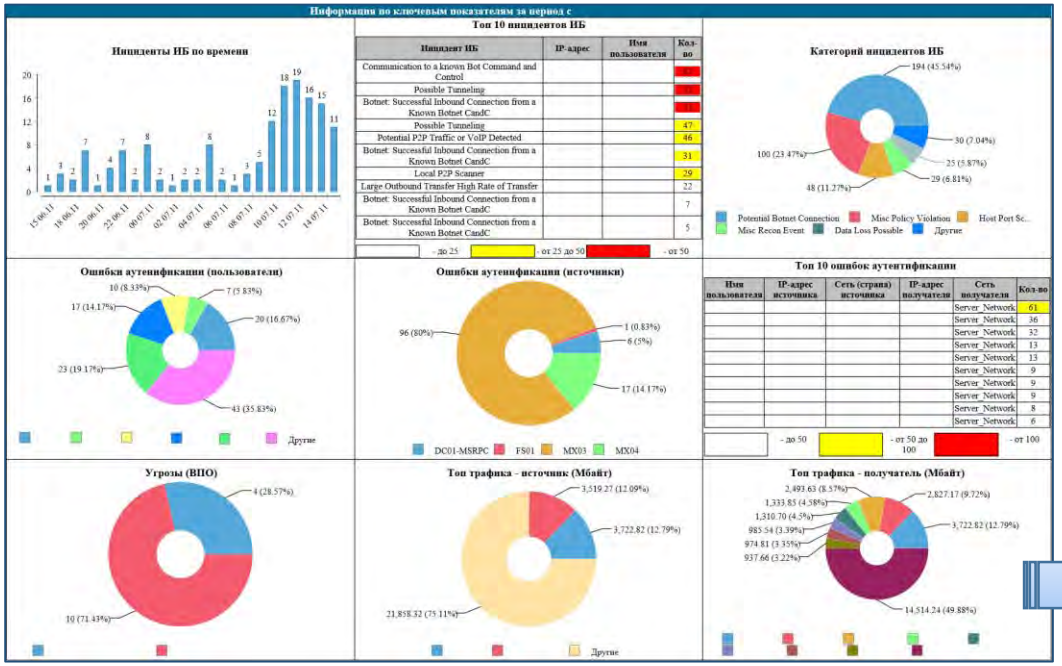


Детальная информация

Дата/Время начала сессии	Дата/Время окончания сессии	Имя пользователя	IP адрес	Страна	Трафик исходящий (Мб)	Трафик входящий (Мб)	Трафик суммарный (Мб)
10.05.2016 17:23:02	10.05.2016 21:03:13		188.243.84.41	RussianFederation	0,00	0,00	0,00
10.05.2016 03:06:41	10.05.2016 19:04:44		89.20.137.34	RussianFederation	[illegible]	14,00	252
10.05.2016 09:20:30	10.05.2016 17:18:04		5.18.82.66	RussianFederation	[illegible]	14,00	252
10.05.2016 11:04:59	10.05.2016 12:30:44		188.243.84.41	RussianFederation	14,00	11,00	25,43
10.05.2016 00:20:27	10.05.2016 01:00:02		188.243.84.41	RussianFederation	0,00	0,00	0,00
09.05.2016 16:20:40	10.05.2016 00:10:07		90.154.71.48	RussianFederation	14,00	11,00	25,43

- до 30 Мб - от 30 до 60 Мб - от 60 Мб

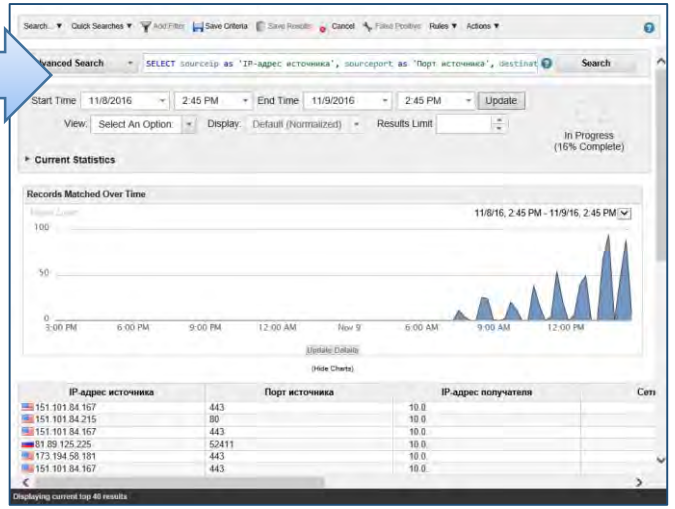
IBM QRADAR SIP
ОТЧЕТНОСТЬ 2.0 – DASHBOARD



НТЦ «Вулкан»

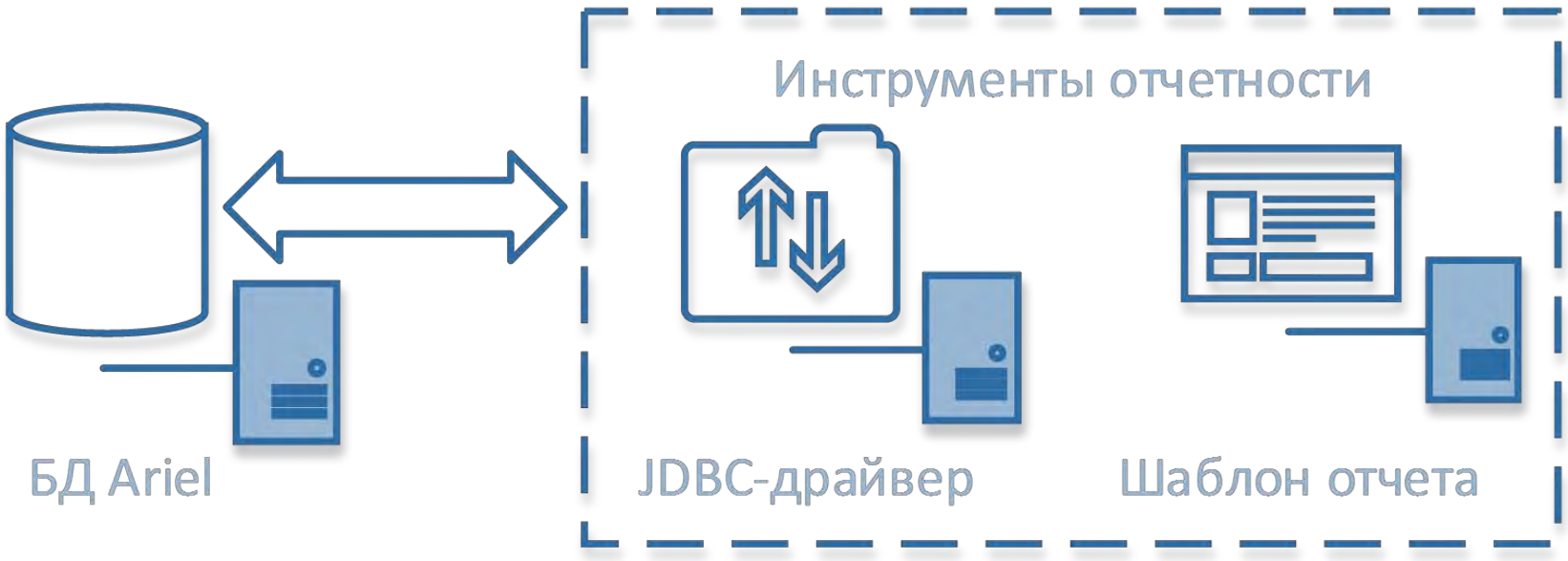
Drilldown

IBM QRadar



https://

IBM QRADAR SIP
ОТЧЕТНОСТЬ 2.0 – КАК ЭТО РАБОТАЕТ?



ОТЧЕТНОСТЬ 2.0 В SOC НА БАЗЕ IBM QRADAR
ЗАКЛЮЧЕНИЕ

Ориентироваться на потребителя

Соблюсти баланс «внешности» и «содержания»

Приоритизировать результаты

Работать с отчётами

«Прокачать» ваш IBM QRadar SIP
по линии функционала отчетности

Спасибо за внимание!

НТЦ ВУЛКАН

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

АЛЕКСАНДР КУЗНЕЦОВ, CISM
Руководитель направления ИБ
+7 (495) 663-95-16 # 401
a.kuznetsov@ntc-vulkan.ru