Отчётность SIEM – шашечки или ехать?

Александр Кузнецов, CISM
Руководитель направления ИБ
НТЦ «Вулкан»

2016

Содержание

- Потребность в отчёте
- Отчёт как форма отдачи от SIEM
- Ожидание и реальность
- Мнение Gartner
- Главные вопросы при подготовке отчёта
- Самый главный вопрос: «ЗАЧЕМ?»
- Рекомендации по наполнению отчётов
- Примеры
- Заключение

Потребность в отчёте

Отчёт как форма отдачи от SIEM

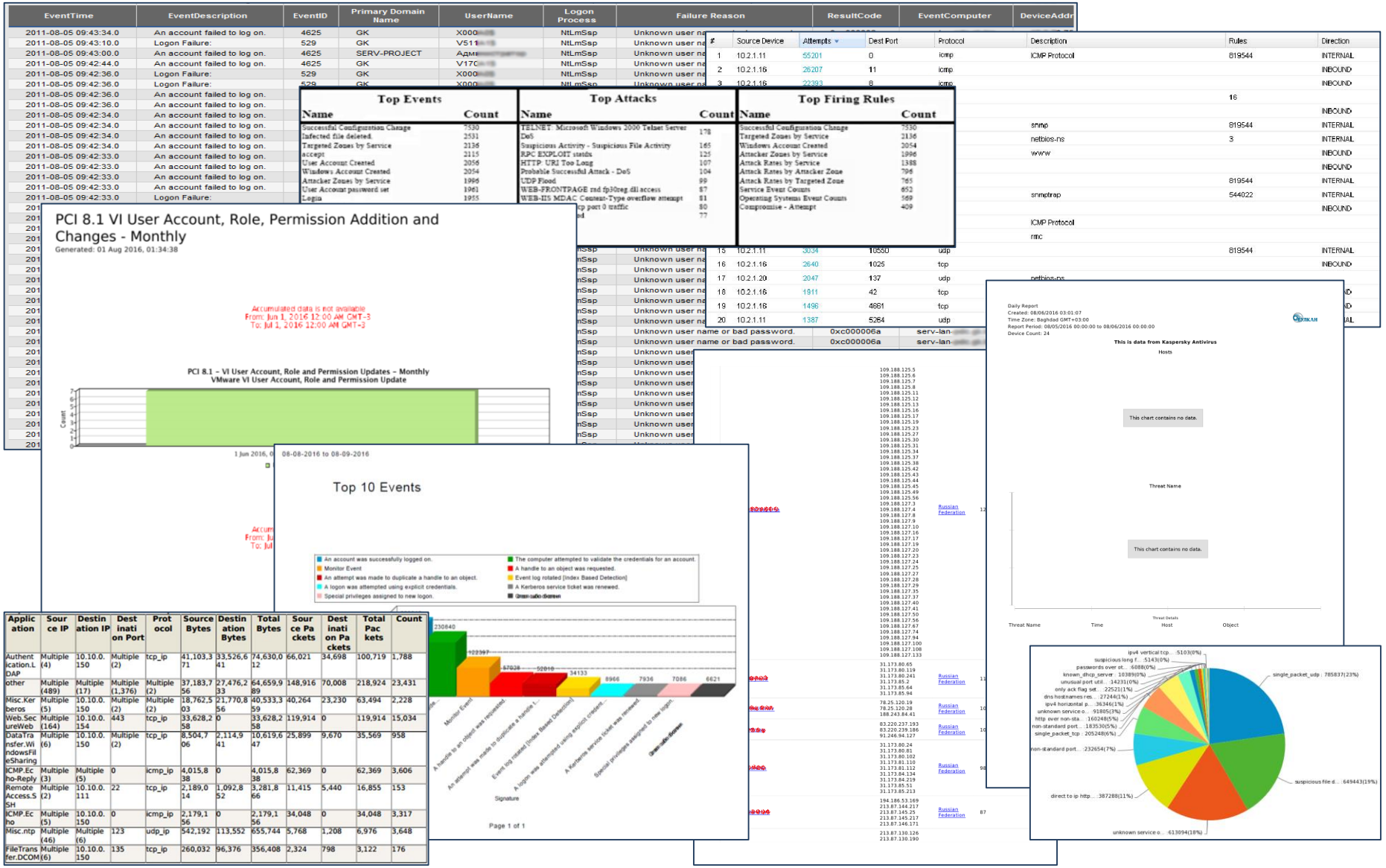
Источники событий

SIEM-система

Отчётность

ОЖИДАНИЕ и реальность

Ожидание и РЕАЛЬНОСТЬ



Мнение Gartner

- Critical Capability
- Reporting capabilities should include predefined reports, as well as the ability to define ad hoc reports or use third-party reporting tools

Critical Capabilities	Compliance	Threat Management	SIEM
Log Management and Reporting	55%	10%	26%

Weighting for Critical Capabilities in Use Cases

AccelOps	AlienVault	Black Stratus	EMC	Event Tracker	HP	IBM	Intel Security	Log Rhythm	NetIQ	Solar Winds
2.8	3.0	2.5	3.2	2.8	3.5	3.6	2.8	4.2	3.8	3.3

Product/Service Rating on Critical Capabilities

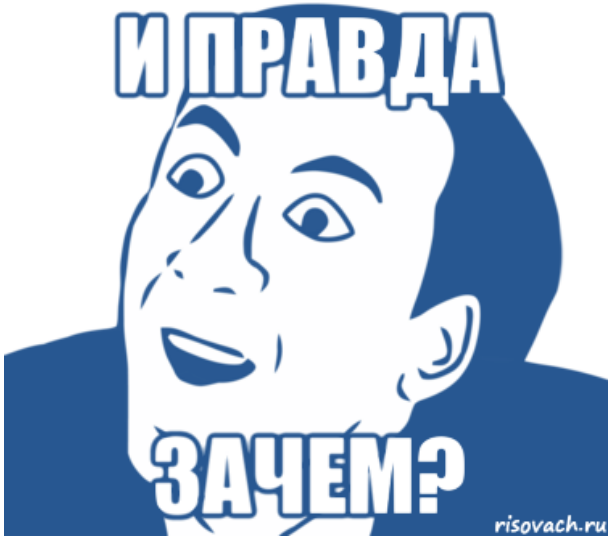
* - Источник: Gartner (September 2015)

Главные вопросы при подготовке отчёта

- **В какой форме отчёт?**
  - Табличной
  - Графической (*диаграммы, графики и т.д.*)
  - Инфографика
- **Кто потребитель отчёта?**
  - Технический специалист *(сетевик, системщик и т.д.)*
  - Владелец процесса (*Event Mgmt, Incident Mgmt, Access Mgmt и т.д.*)
  - IS-менеджер
  - IT-менеджер
  - Compliance-менеджер
  - Risk-менеджер
  - Top менеджер
- **Зачем отчёт?**

Самый главный вопрос: «ЗАЧЕМ?»

- **Раскройте вопрос:**
  - Почему эти данные важны?
  - Как дальше их использовать?
  - Что они позволят улучшить?



- **Тренд vs Количество**
  - Количество инцидентов (↑↓ *vs 88*)
- **Нормированные значения vs [0; +∞)**
  - Количество узлов с уязвимостями (*33% vs 77*)
- **Соответствие или отклонение**

Рекомендации по оформлению отчётов

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

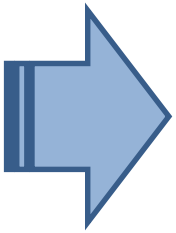
Примеры оформления

ASA - VPN Session Closed

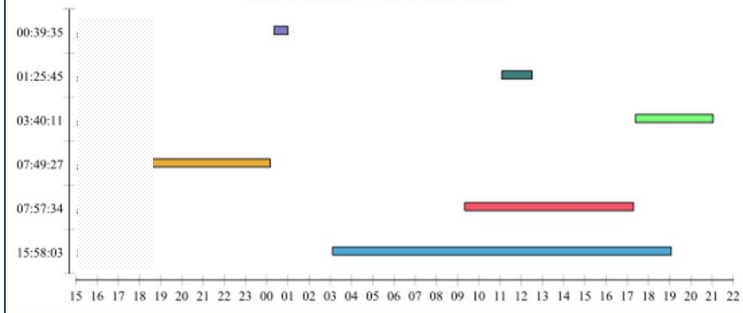
Generated: 11 May 2016, 00:41:58

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	35
10 May 2016, 00:10:07		90.154.71.48	RussianFederation	125.650.351	14.949.010	7	49	27



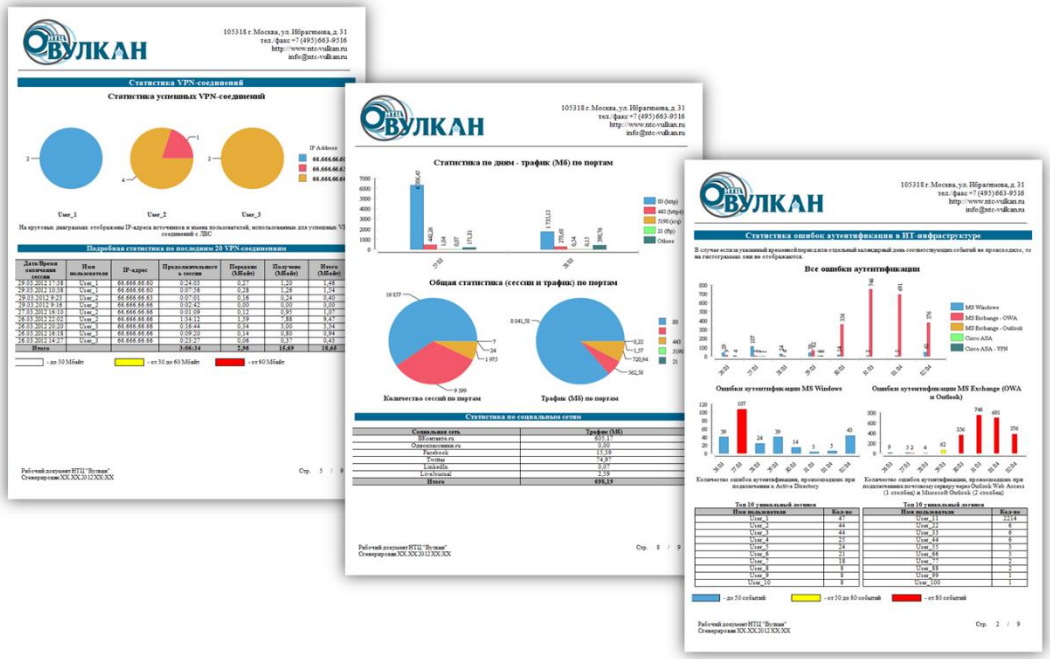
Статистика VPN-соединений



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	238,00	14,00	252
10.05.2016 09:20:30	10.05.2016 17:18:04		5.18.82.66	RussianFederation	238,00	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



Заключение

- Не бояться вопроса «ЗАЧЕМ?»
- Ориентироваться на потребителя
- Соблюсти баланс «внешности» и «содержания»
- «Не гнаться» за объёмом отчёта
- Приоритизировать результаты
- Работать с отчётами

Спасибо за внимание!

Александр Кузнецов, CISM
Руководитель направления ИБ
НТЦ «Вулкан»

105318, г. Москва, ул. Ибрагимова, д. 31
тел./факс +7 (495) 663-9516
http://www.ntc-vulkan.ru
info@ntc-vulkan.ru