

# Отчётность SIEM – шашечки или ехать?

Александр Кузнецов, CISM  
Руководитель направления ИБ  
NTSC «Вулкан»

# 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



# ОЖИДАНИЕ и реальность



# Ожидание и РЕАЛЬНОСТЬ

EventTime	EventDescription	EventID	Primary Domain Name	UserName	Logon Process	Failure Reason	ResultCode	EventComputer	DeviceAddr
2011-08-05 09:43:34.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:43:10.0	Logon Failure:	529	GK	V511	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:43:00.0	An account failed to log on.	4625	SERV-PROJECT	Azire	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:44.0	An account failed to log on.	4625	GK	V17C	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:36.0	Logon Failure:	529	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:36.0	Logon Failure:	529	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:36.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:36.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:34.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:34.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:34.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:33.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:33.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:33.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:33.0	An account failed to log on.	4625	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:33.0	Logon Failure:	529	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 09:42:33.0	Logon Failure:	529	GK	X000	NtLmSsp	Unknown user name or bad password.	0xc000006a	serv-lan	

Top Events		Top Attacks		Top Firing Rules	
Name	Count	Name	Count	Name	Count
Successful Configuration Change	7530	HELNBT: Microsoft Windows 2000 Telnet Server	178	Successful Configuration Change	7530
Infected file detected.	2551	DoS	165	Targeted Zones by Service	2136
Targeted Zones by Service	2136	Suspicious Activity - Suspicious File Activity	165	Windows Account Created	2054
accept	2115	RPC EXPLOIT issues	125	Attacker Zones by Service	1996
User Account Created	2056	HTTP URI Top Log	107	Attack Rates by Service	1388
Windows Account Created	2054	Probable Successful Attack - DoS	104	Attack Rates by Attacker Zone	796
Attacker Zones by Service	1996	UDP Flood	89	Attack Rates by Targeted Zone	765
User Account password set	1961	WEB-FRONTPAGE read file/obj.dll access	87	Service Event Counts	652
Legia	1955	WEB-MS MDAC Control-Type overflow attempt	81	Operating System Event Counts	569
		Try port 0 traffic	77	Compromise - Alterng	429

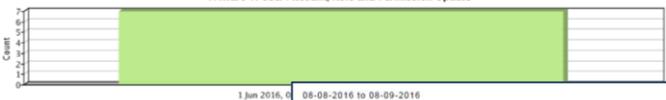
## PCI 8.1 VI User Account, Role, Permission Addition and Changes - Monthly

Generated: 01 Aug 2016, 01:34:38

Accumulated data is not available  
From: Jun 1, 2016 12:00 AM GMT-3  
To: Jul 3, 2016 12:00 AM GMT-3

### PCI 8.1 - VI User Account, Role and Permission Updates - Monthly

#### VMware VI User Account, Role and Permission Update

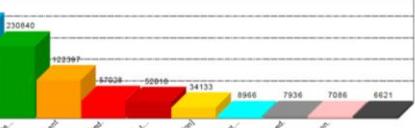


### Top 10 Events

Account From: Jul To: Jul

- An account was successfully logged on.
- Monitor Event
- An attempt was made to duplicate a handle to an object.
- A logon was attempted using explicit credentials.
- Special privileges assigned to new logon.
- The computer attempted to validate the credentials for an account.
- An event log rotated (Index Based Detection).
- A Kerberos service ticket was renewed.
- Special privileges assigned to new logon.

Application	Source IP	Destination IP	Destination Port	Protocol	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Total Packets	Count
Authentication.L	Multiple (4)	10.10.0.150	Multiple (2)	tcp_ip	41,103.3	33,526.6	74,630.0	66,021	34,698	100,719	1,788
Other	Multiple (489)	Multiple (17)	Multiple (1,376)	Multiple (2)	37,183.7	27,476.2	64,659.9	148,916	70,008	218,924	23,431
Misc.Kerberos	Multiple (5)	10.10.0.150	Multiple (2)	Multiple (2)	18,762.5	21,770.8	40,533.3	40,264	23,230	63,494	2,228
Web.SecureWeb	Multiple (164)	10.10.0.154	443	tcp_ip	33,628.2	0	33,628.2	119,914	0	119,914	15,034
DataTransfer.WindowsFileSharing	Multiple (6)	10.10.0.150	Multiple (2)	tcp_ip	8,504.7	2,114.9	10,619.6	25,899	9,670	35,569	958
ICMP.Echo-Reply	Multiple (5)	Multiple (0)	Multiple (0)	icmp_ip	4,015.8	0	4,015.8	62,369	0	62,369	3,606
RemoteAccess.SH	Multiple (2)	10.10.0.111	22	Multiple (2)	2,189.0	1,092.8	3,281.8	11,415	5,440	16,855	153
ICMP.Echo	Multiple (5)	10.10.0.150	Multiple (0)	icmp_ip	2,179.1	0	2,179.1	34,048	0	34,048	3,317
Misc.ntp	Multiple (4)	Multiple (123)	Multiple (6)	udp_ip	542,192	113,552	655,744	5,768	1,208	6,976	3,648
FileTransfer.DCOM	Multiple (6)	10.10.0.135	Multiple (6)	Multiple (6)	260,032	96,376	356,408	2,324	798	3,122	176



- An account was successfully logged on.
- Monitor Event
- An attempt was made to duplicate a handle to an object.
- A logon was attempted using explicit credentials.
- Special privileges assigned to new logon.
- The computer attempted to validate the credentials for an account.
- An event log rotated (Index Based Detection).
- A Kerberos service ticket was renewed.
- Special privileges assigned to new logon.

EventTime	EventDescription	EventID	Primary Domain Name	UserName	Logon Process	Failure Reason	ResultCode	EventComputer	DeviceAddr
2011-08-05 10:21:11	Unknown user name or bad password.	3034		Unknown user name	Unknown user name	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 10:21:16	Unknown user name or bad password.	2640		Unknown user name	Unknown user name	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 10:21:20	Unknown user name or bad password.	2047		Unknown user name	Unknown user name	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 10:21:16	Unknown user name or bad password.	1911		Unknown user name	Unknown user name	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 10:21:18	Unknown user name or bad password.	1496		Unknown user name	Unknown user name	Unknown user name or bad password.	0xc000006a	serv-lan	
2011-08-05 10:21:11	Unknown user name or bad password.	1387		Unknown user name	Unknown user name	Unknown user name or bad password.	0xc000006a	serv-lan	

Daily Report  
Created: 08/05/2016 01:01:07  
Time Zone: Baghdad GMT+03:00  
Report Period: 08/05/2016 00:00:00 to 08/05/2016 00:00:00  
Device Count: 24

This is data from Kaspersky Antivirus Host

This chart contains no data.

Threat Name

This chart contains no data.

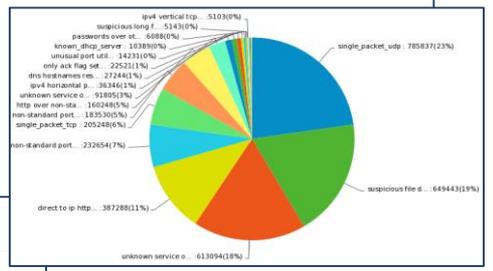
Threat Name

Time

Threat Details

Host

Object



# 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)

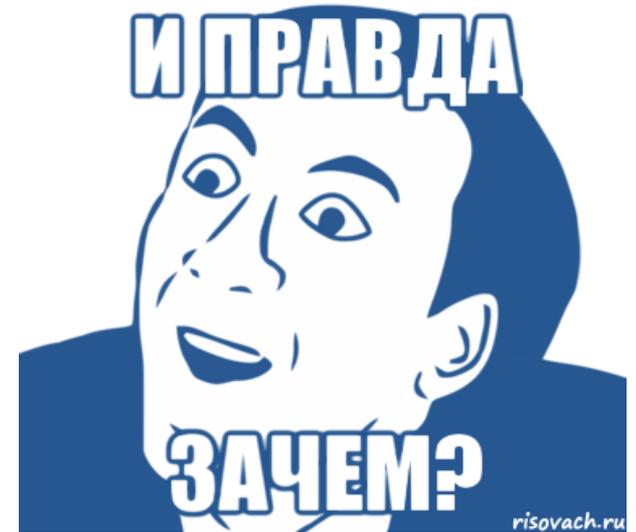
# Главные вопросы при подготовке отчёта

- **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 (  $\uparrow\downarrow$  vs 88)
- **Нормированные значения vs  $[0; +\infty)$** 
  - Количество узлов с уязвимостями (33% vs 77)
- **Соответствие или отклонение**



# Рекомендации по оформлению отчётов

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



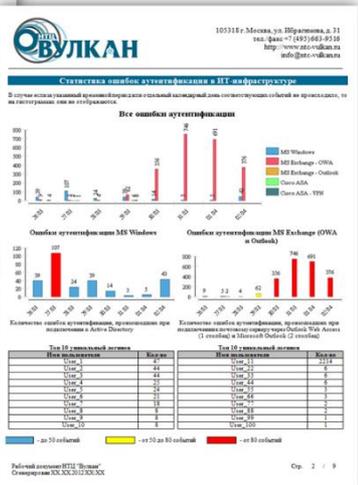
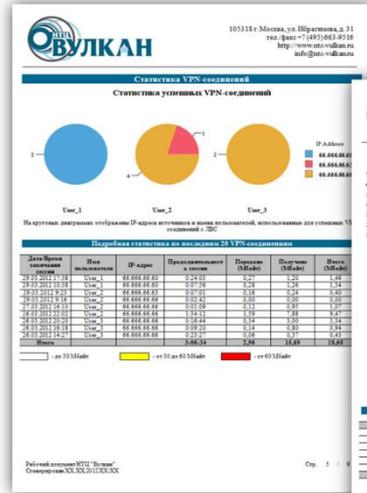
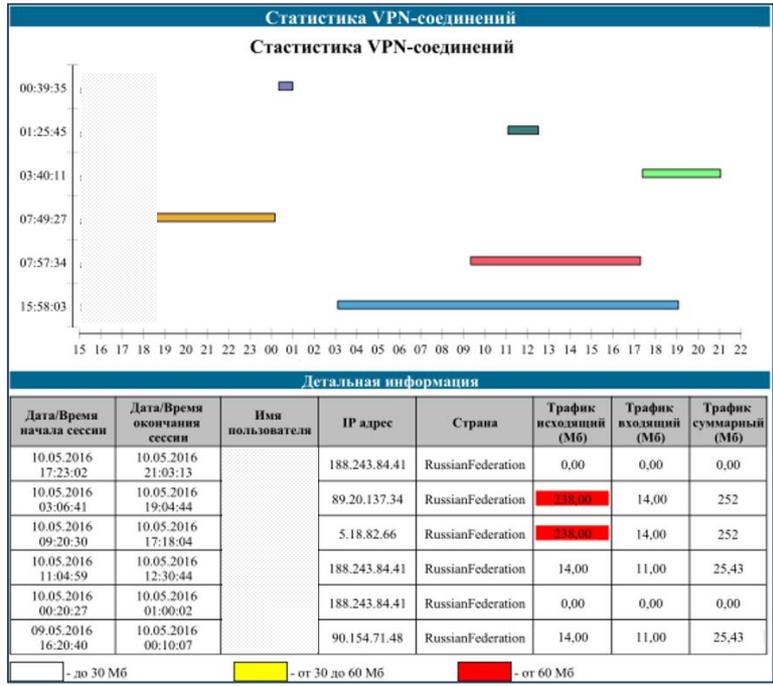
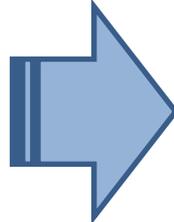
# Примеры оформления

## 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	Russian Federation	179.488	191.461	3	40	11
10 May 2016, 19:04:44		89.20.137.34	Russian Federation	250.302.663	3.630.605.331	15	58	3
10 May 2016, 17:18:04		5.18.82.66	Russian Federation	302.173.578	2.546.320.604	7	57	34
10 May 2016, 12:30:44		188.243.84.41	Russian Federation	15.015.851	11.645.754	1	25	45
10 May 2016, 01:00:02		188.243.84.41	Russian Federation	171.064	86.238	0	39	35
10 May 2016, 00:10:07		90.154.71.48	Russian Federation	125.650.351	14.949.010	7	49	27



# 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](mailto:info@ntc-vulkan.ru)