wie finden wir die Nadel im Heuhaufen?

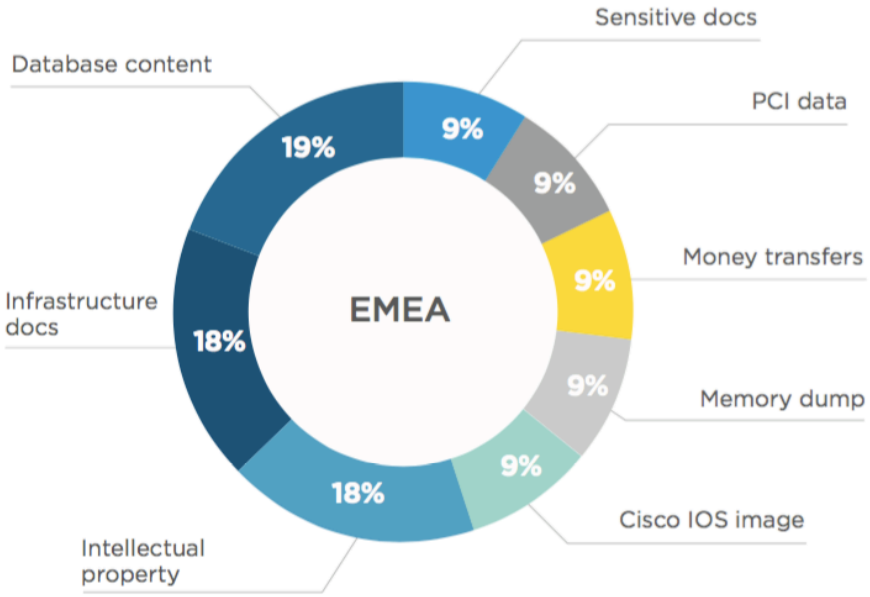
Karl Jaeger
pro4bizz GmbH
15.März 2017

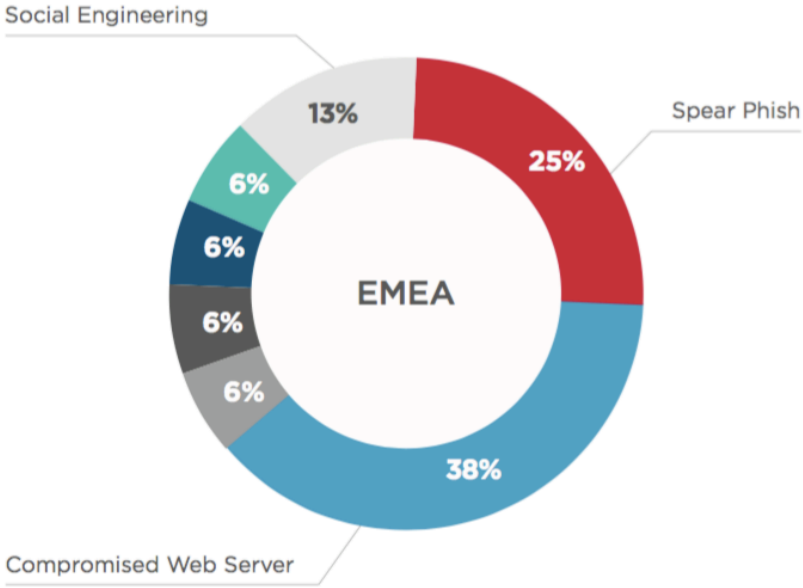
Agenda

- Bedrohungslage und „Kill Chain“
- Anforderungen an SIEM
- QRadar
  - Architektur
  - dashboard
  - customizing
  - Beispielalarm
  - Reporting
  - Kontextinformationen
  - Netzwerkanalyse
  - Erweiterungen
- Live Demo

Bedrohungslage EMEA 2016

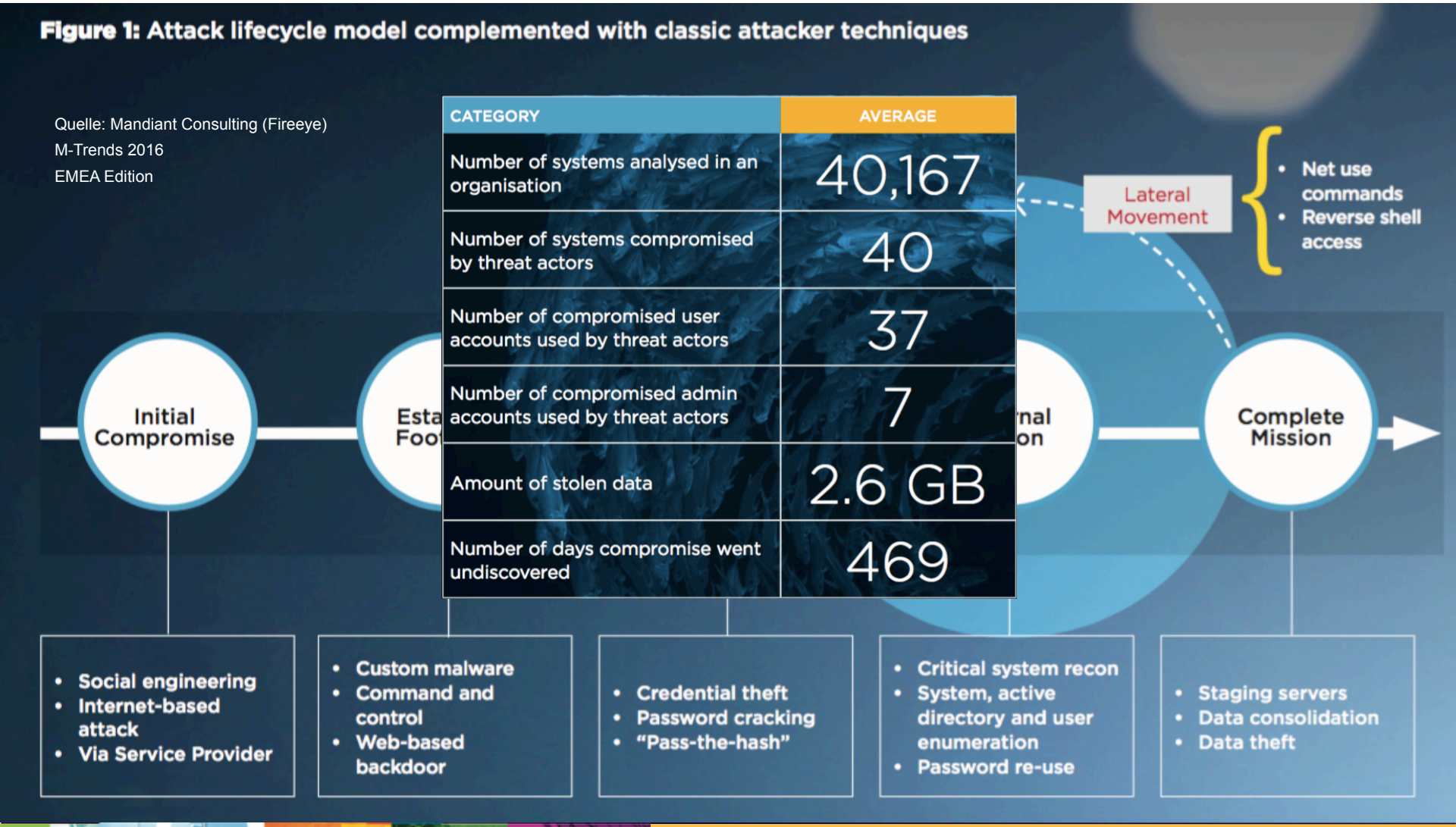
Figure 5: Information stolen classifications





Quelle: Mandiant Consulting (Fireeye)
M-Trends 2016
EMEA Edition

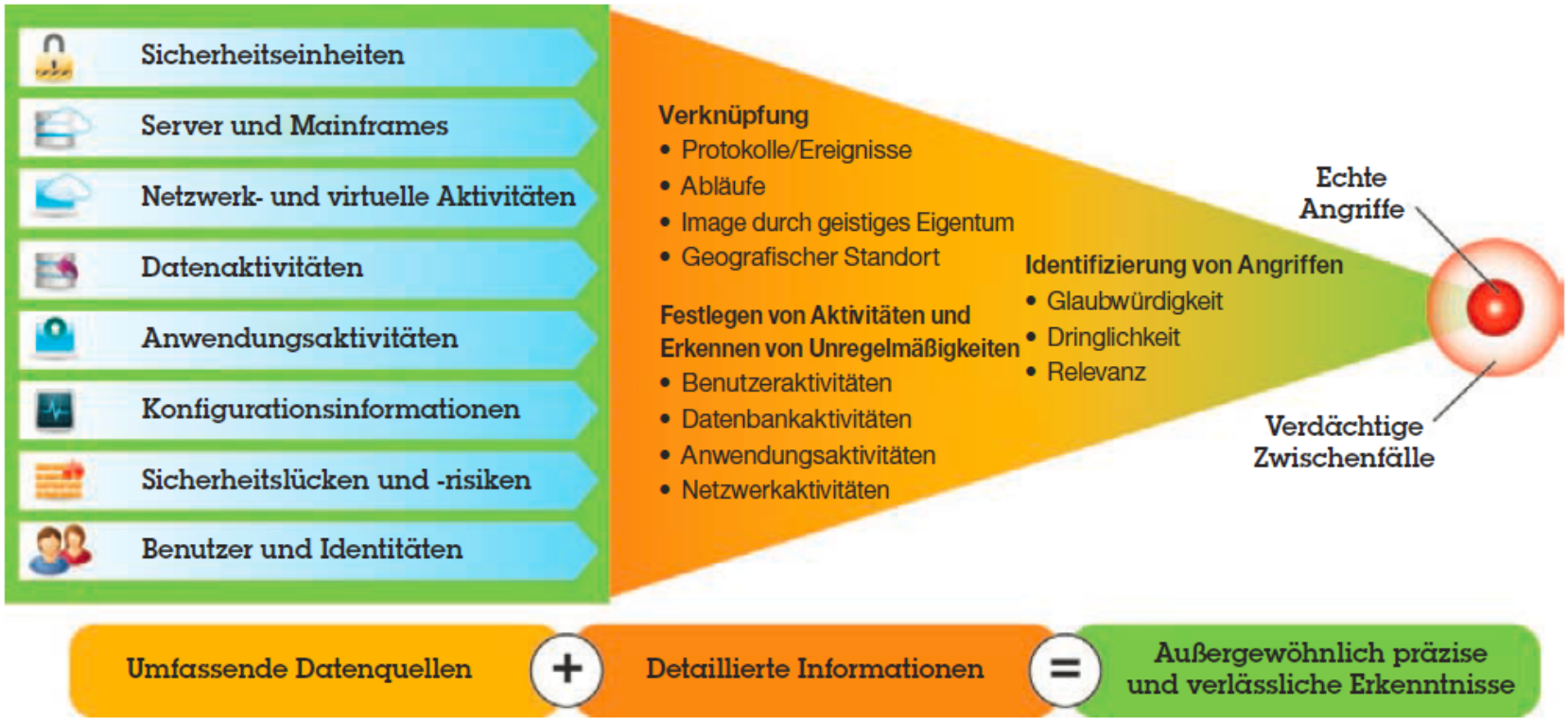
Bedrohungslage EMEA 2016



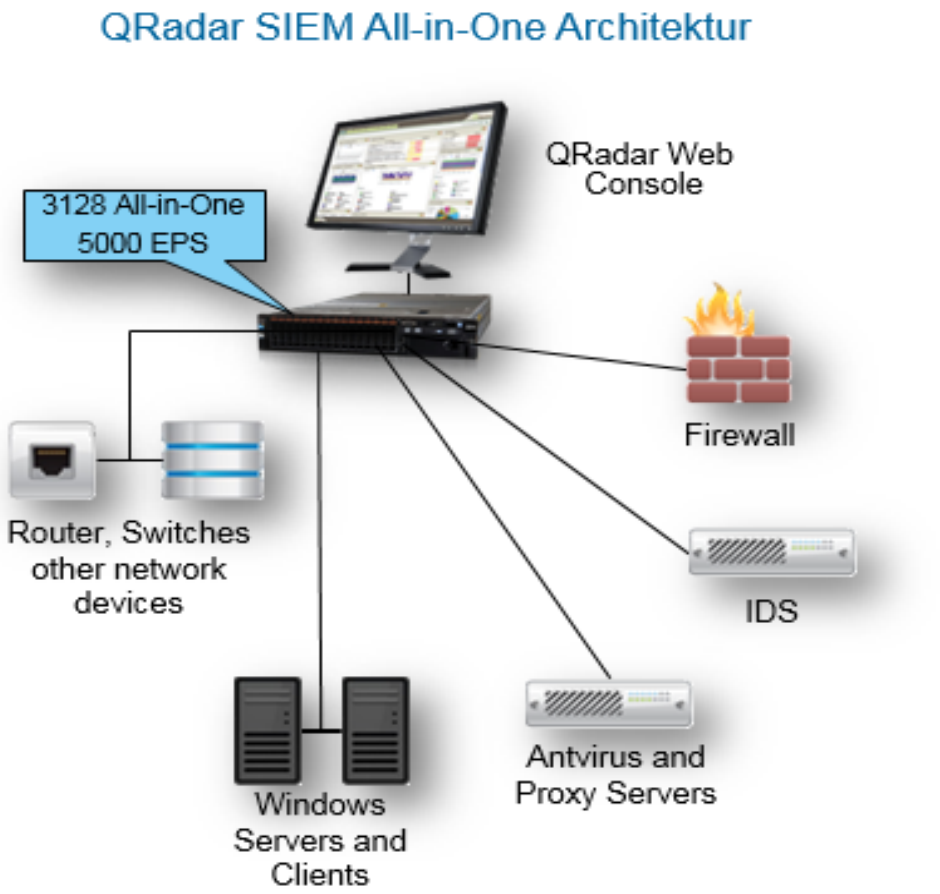
Anforderungen an SIEM

- gesetzliche und regulatorische Anforderungen
- ganzheitliches Überwachungssystem
- Einhaltung der Datenschutzanforderungen
- proaktive Alarmierung
- Integration in operationelle Services (SLAs)
- Analyse von Vorfällen in Realzeit
- Erhöhung des Sicherheitsniveaus

QRadar SIEM Architektur



QRadar SIEM Architektur



Log Normalisierung

wieso? Audit Policy

was? Kategorisierung

was genau? Ereignis

wie gefährlich? Priorisierung

wer? User

wann? Zeitstempel

woher? Network (IPAM)

worauf? Asset DB

definiere eigene Felder via regexp

Event Information

Event Name:	Login Failed						
Low Level Category:	Telnet Login Failed						
Event Description:	Telnet Login Failed						
Magnitude:	(4)	**Relevance:**	5	**Severity:**	3	**Credibility:**	5
Username:	admin						
Start Time:	2012-03-21 16:39:06	**Storage Time:**	2012-03-21 16:39:06	**Log Source Time:**	2012-03-21 16:39:06		
Date_Time (custom):	2012-03-21 18:55:53						
Duration_Seconds (custom):	N/A						
Policy (custom):	N/A						

Source and Destination Information

Source IP:	10.10.1.192	**Destination IP:**	10.10.1.210
Source Asset Name:	N/A	**Destination Asset Name:**	ns5gt
Source Port:	35259	**Destination Port:**	0
Pre NAT Source IP:		**Pre NAT Destination IP:**	
Pre NAT Source Port:	0	**Pre NAT Destination Port:**	0
Post NAT Source IP:		**Post NAT Destination IP:**	
Post NAT Source Port:	0	**Post NAT Destination Port:**	0
IPv6 Source:	0:0:0:0:0:0:0:0	**IPv6 Destination:**	0:0:0:0:0:0:0:0
Source MAC:	00:00:00:00:00:00	**Destination MAC:**	00:00:00:00:00:00

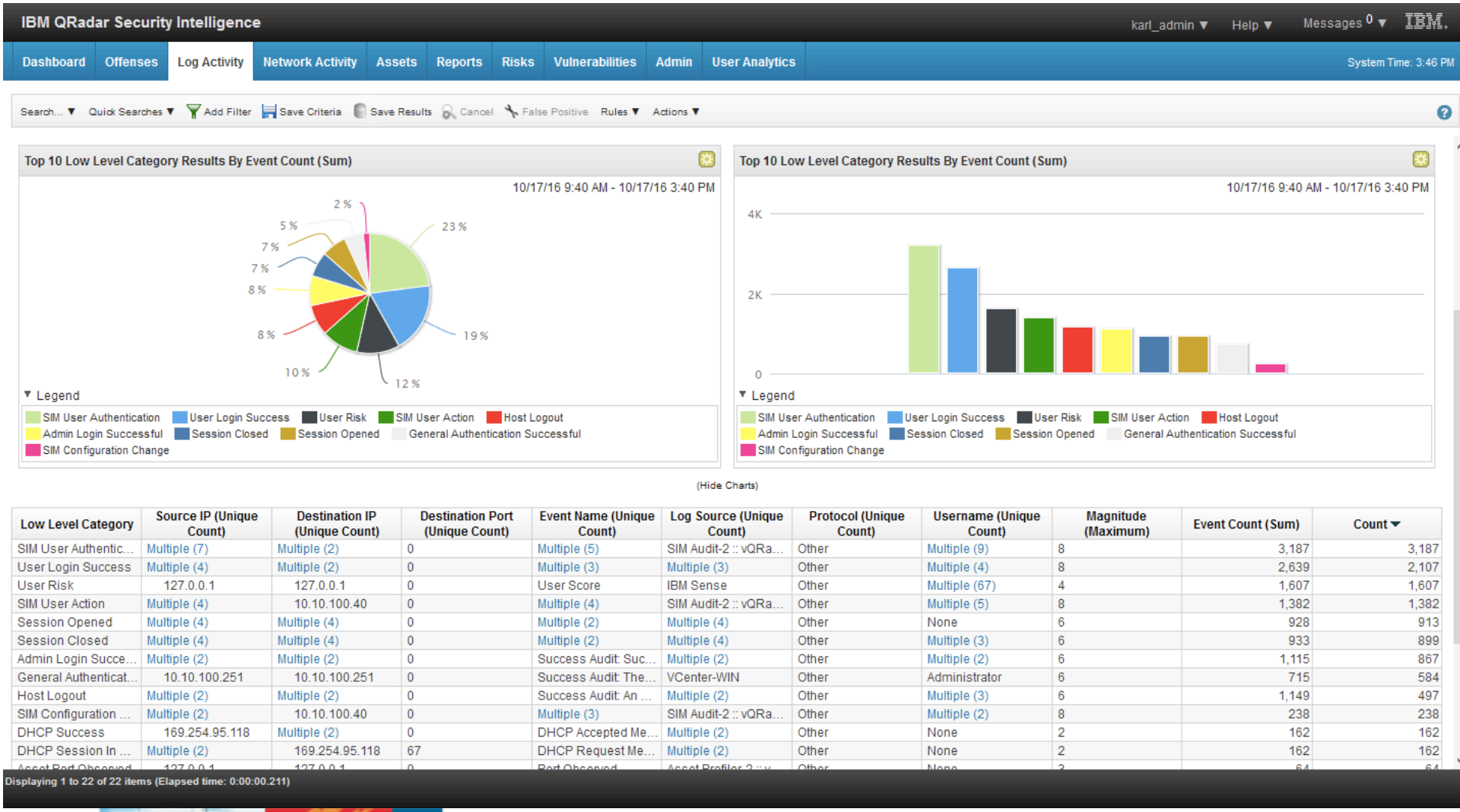
Payload Information

utf | hex | base64

Wrap Text

```
<132>ns5gt-adsl-wlan: NetScreen device_id=0128032005000468  [Root]system-warning-00515: Login attempt to system
```

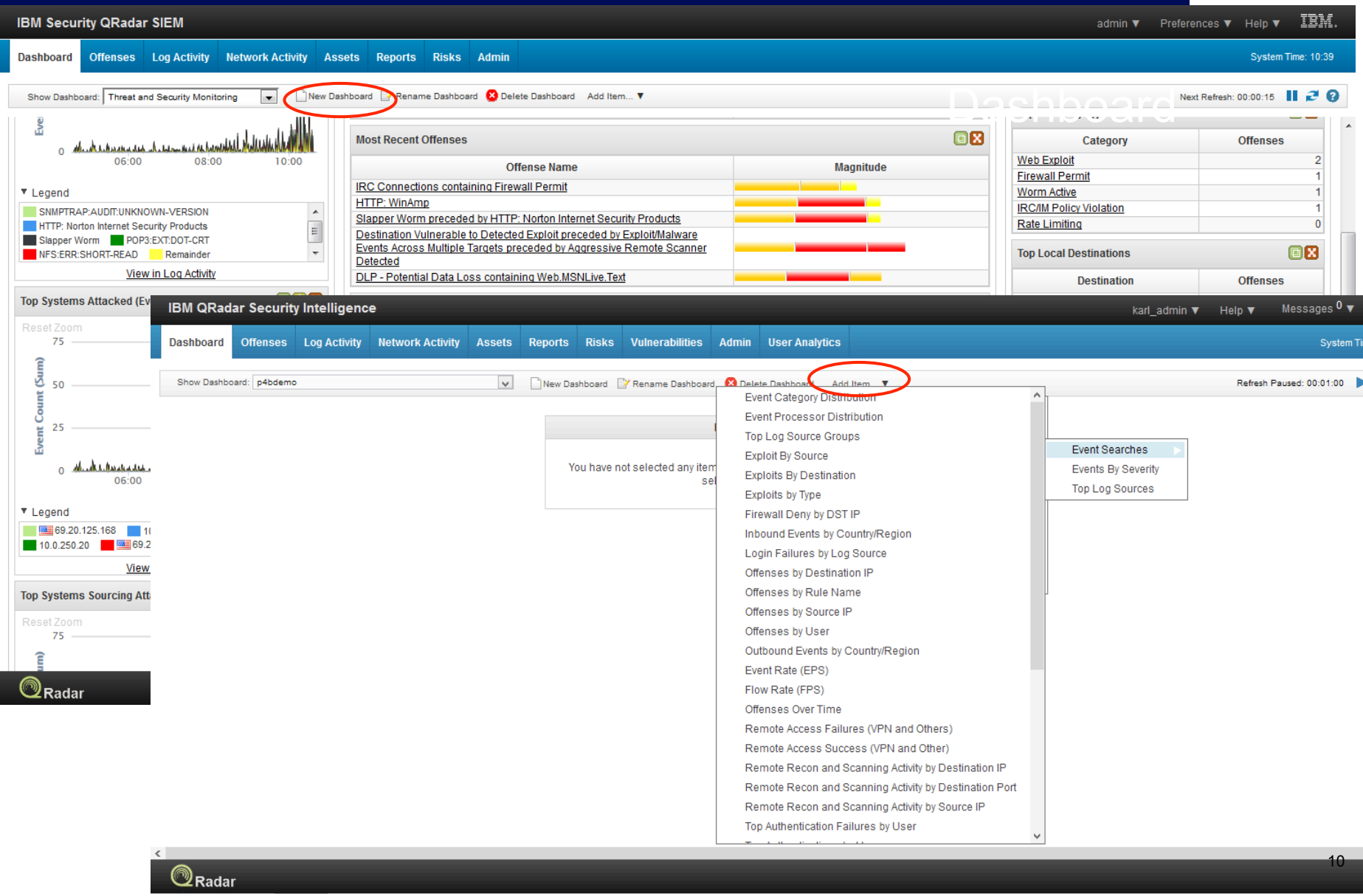
Event Taxonomie

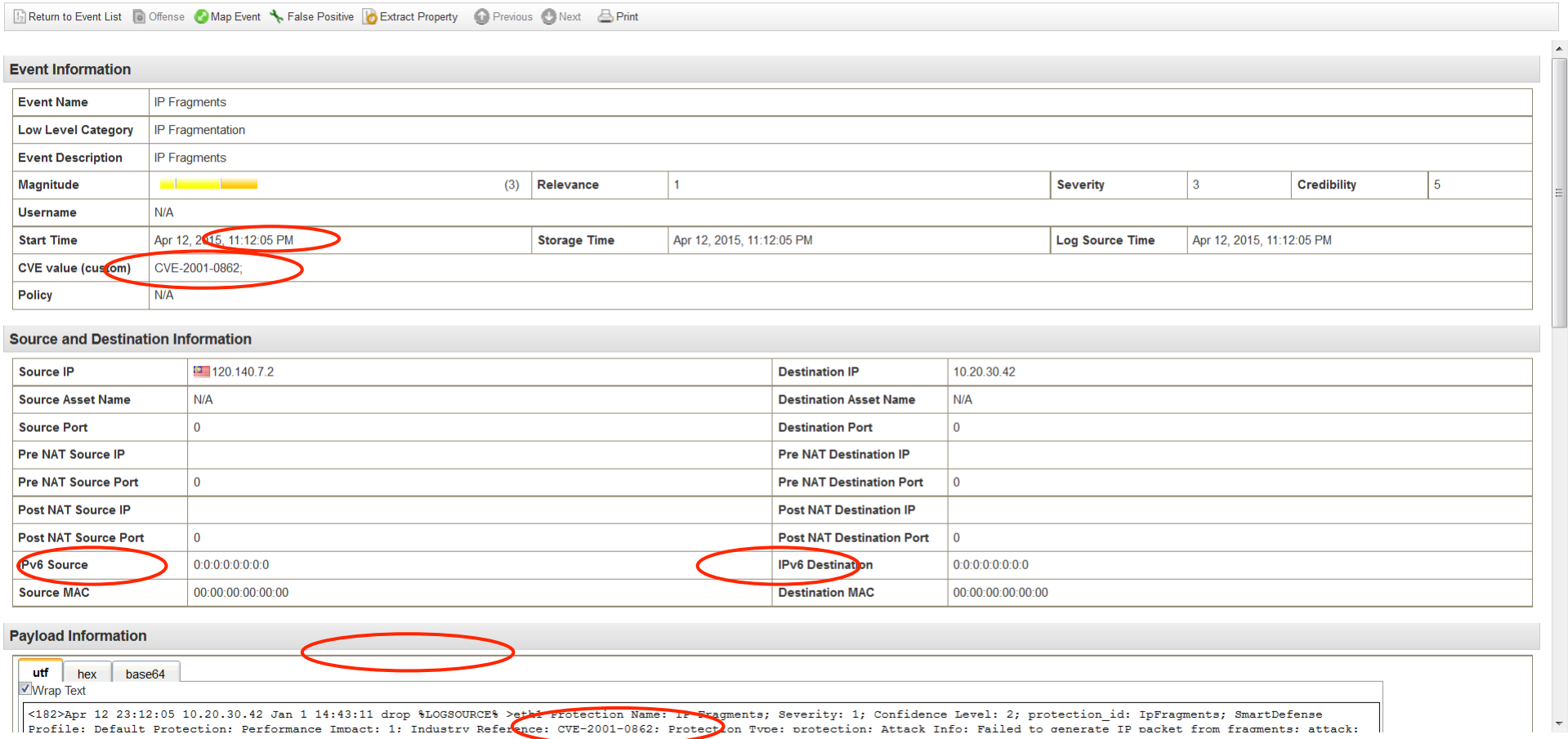


Low Level Category	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
SIM User Authentic...	Multiple (7)	Multiple (2)	0	Multiple (5)	SIM Audit-2 :: vQRa...	Other	Multiple (9)	8	3,187	3,187
User Login Success	Multiple (4)	Multiple (2)	0	Multiple (3)	Multiple (3)	Other	Multiple (4)	8	2,639	2,107
User Risk	127.0.0.1	127.0.0.1	0	User Score	IBM Sense	Other	Multiple (67)	4	1,607	1,607
SIM User Action	Multiple (4)	10.10.100.40	0	Multiple (4)	SIM Audit-2 :: vQRa...	Other	Multiple (5)	8	1,382	1,382
Session Opened	Multiple (4)	Multiple (4)	0	Multiple (2)	Multiple (4)	Other	None	6	928	913
Session Closed	Multiple (4)	Multiple (4)	0	Multiple (2)	Multiple (4)	Other	Multiple (3)	6	933	899
Admin Login Succe...	Multiple (2)	Multiple (2)	0	Success Audit: Suc...	Multiple (2)	Other	Multiple (2)	6	1,115	867
General Authenticat...	10.10.100.251	10.10.100.251	0	Success Audit: The...	VCenter-WIN	Other	Administrator	6	715	584
Host Logout	Multiple (2)	Multiple (2)	0	Success Audit: An ...	Multiple (2)	Other	Multiple (3)	6	1,149	497
SIM Configuration ...	Multiple (2)	10.10.100.40	0	Multiple (3)	SIM Audit-2 :: vQRa...	Other	Multiple (2)	8	238	238
DHCP Success	169.254.95.118	Multiple (2)	0	DHCP Accepted Me...	Multiple (2)	Other	None	2	162	162
DHCP Session In ...	Multiple (2)	169.254.95.118	67	DHCP Request Me...	Multiple (2)	Other	None	2	162	162

Displaying 1 to 22 of 22 items (Elapsed time: 0:00:00.211)

Dashboard




Return to Event List
Offense
Map Event
False Positive
Extract Property
Previous
Next
Print
Event Information
Event Name
IP Fragments
Low Level Category
IP Fragmentation
Event Description
IP Fragments
Magnitude
(3)
Relevance
1
Severity
3
Credibility
5
Username
N/A
Start Time
Apr 12, 2015, 11:12:05 PM
Storage Time
Apr 12, 2015, 11:12:05 PM
Log Source Time
Apr 12, 2015, 11:12:05 PM
CVE value (custom)
CVE-2001-0862;
Policy
N/A
Source and Destination Information
Source IP
120.140.7.2
Destination IP
10.20.30.42
Source Asset Name
N/A
Destination Asset Name
N/A
Source Port
0
Destination Port
0
Pre NAT Source IP
Pre NAT Destination IP
Pre NAT Source Port
0
Pre NAT Destination Port
0
Post NAT Source IP
Post NAT Destination IP
Post NAT Source Port
0
Post NAT Destination Port
0
IPv6 Source
0:0:0:0:0:0:0:0
IPv6 Destination
0:0:0:0:0:0:0:0
Source MAC
00:00:00:00:00:00
Destination MAC
00:00:00:00:00:00
Payload Information
utf
hex
base64
Wrap Text
<182>Apr 12 23:12:05 10.20.30.42 Jan 1 14:43:11 drop %LOGSOURCE% >eth1 protection Name: IP Fragments; Severity: 1; Confidence Level: 2; protection_id: IpFragments; SmartDefense
Profile: Default Protection; Performance Impact: 1; Industry Reference: CVE-2001-0862; Protection Type: protection; Attack Info: Failed to generate IP packet from fragments; attack:

Beispielalarm

Offense 41761 — Summary | Display ▼ | Events | Connections | Flows | View Attack Path | Actions ▼ | Print

Magnitude		**Status**		**Relevance**	1	**Severity** 5	**Credibility** 3
Description	Multiple Login Failures to the Same Destination preceded by Multiple Login Failures from the Same Source	**Offense Type**	Source IP				
		Event/Flow count	69 events and 0 flows in 5 categories				
Source IP(s)	61.172.206.75	**Start**	Aug 2016, 12:24:03 PM				
Destination IP(s)	10.1 127.0.0.1	**Duration**	2m 55s				
Network(s)	Multiple (2)	**Assigned to**	Unassigned				

China VPN Pool

Offense Source Summary

IP	61.172.206.75	**Location**	China
Magnitude		**Vulnerabilities**	0
Username	Unknown	**MAC Address**	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	**Weight**	0
Offenses	4	**Events/Flows**	166

Original Filters:

Offense is Multiple Login Failures to the Same Destination preceded b... (Clear Filter)

Current Statistics

Total Results	55 (443B Total)	Compressed Data Files Searched		Subsearch (No Compressed Data Files)	Duration 263ms
Data Files Searched	Subsearch (No Data Files)	Index File Count		Subsearch (No Index Files)	More Details

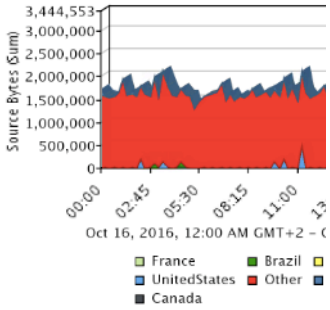
(Show Charts)

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destinatic Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)
Primary Authentication Failure	61.172.206.75	127.0.0.1	0	secure	Host Login Failed
User failed to login to SSH, incorrect password	61.172.206.75	10.1	0	firewall@	SSH Login Failed
Root Login Failed	61.172.206.75	10.1	0	firewall@	Admin Login Failure
Multiple Login Failures to the Same Destination	61.172.206.75	Multiple (2)	0	Custom Rule Engine-138 :	Remote Access Login Failed
Multiple Login Failures from the Same Source	61.172.206.75	127.0.0.1	0	Custom Rule Engine-138 :	Misc Login Failed

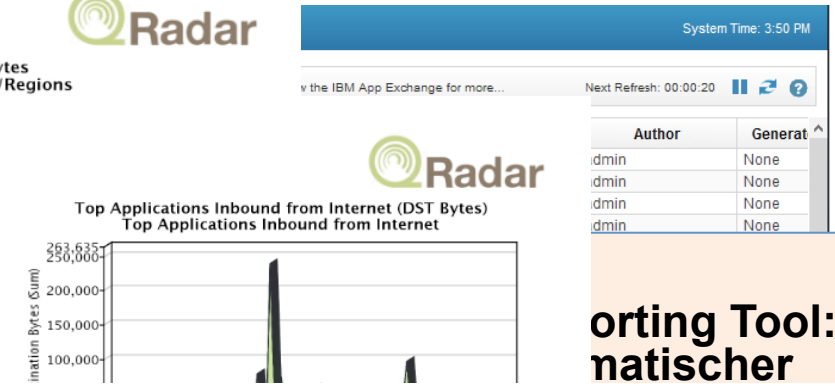
Geographic Traffic Distribution

Generated: Oct 17, 2016, 1:06:10 AM

By SRC Bytes
Top Countries/Regions



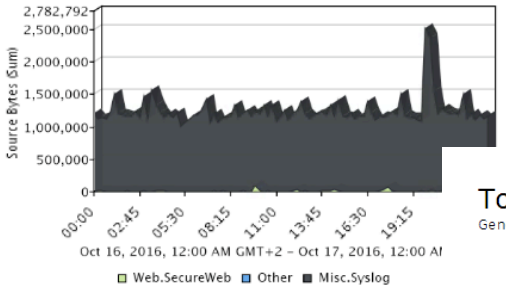
By DST Bytes
Top Countries/Regions



Top Applications (Internet)

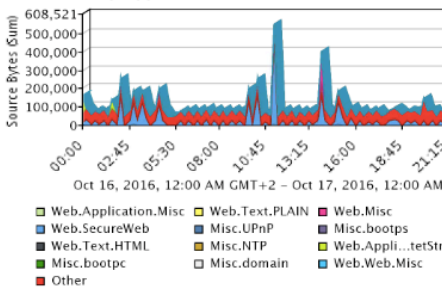
Generated: Oct 17, 2016, 1:09:17 AM

Top Applications Inbound from Internet (SRC Bytes)
Top Applications Inbound from Internet



Top Applications Inbound from Internet (DST Bytes)
Top Applications Inbound from Internet

Top Applications Outbound to Internet (SRC Byt
Top Applications Outbound to the Internet



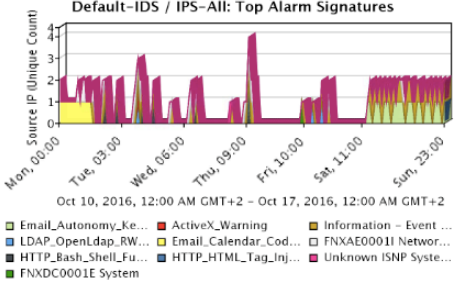
Details
Top Countries/Regions
Oct 16, 2016, 12:00:00 AM - Oc

Geographic Country/Region	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)
UnitedStates	Multiple (33)	Multiple (75)	Multiple (1)
Other	Multiple (41)	Multiple (11)	Multiple (3)
Netherlands	Multiple (7)	Multiple (10)	Multiple (5)
Ireland	Multiple (5)	Multiple (3)	443
Germany	Multiple (22)	Multiple (15)	Multiple (4
France	195.154.41.130	10.20.100.237	443

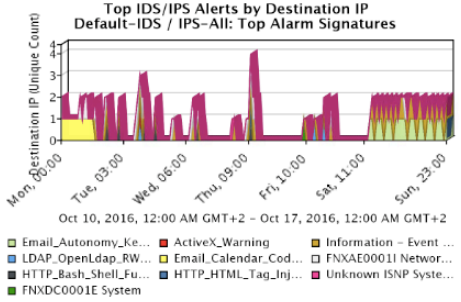
Top IDS/IPS Alerts (Weekly)

Generated: Oct 17, 2016, 1:07:11 AM

Top IDS/IPS Alerts by Source IP
Default-IDS / IPS-All: Top Alarm Signatures



Top IDS/IPS Alerts by Destination IP
Default-IDS / IPS-All: Top Alarm Signatures

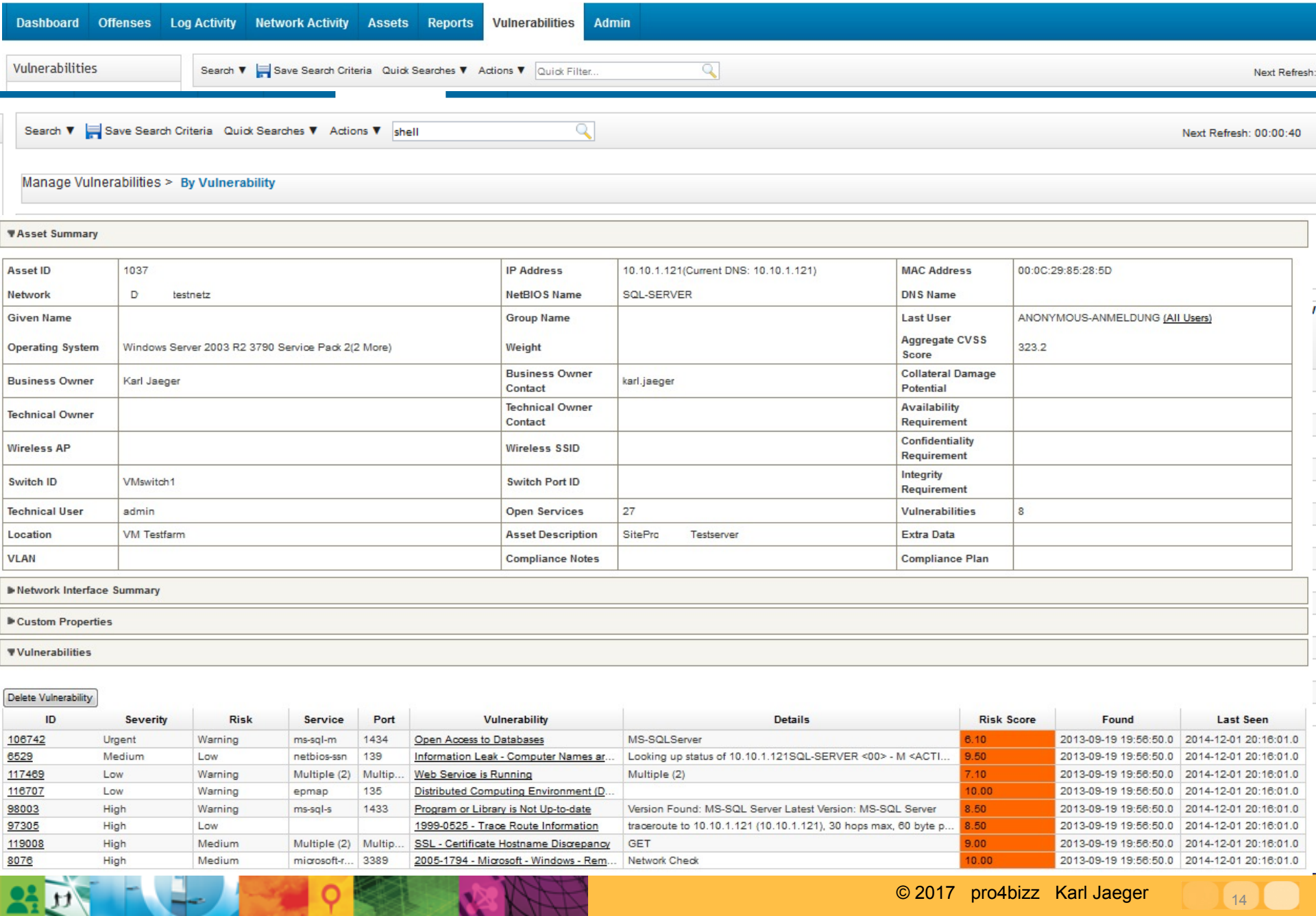


Top IDS/IPS Alerts by Name
Default-IDS / IPS-All: Top Alarm Signatures
Oct 10, 2016, 12:00:00 AM - Oct 17, 2016, 12:00:00 AM

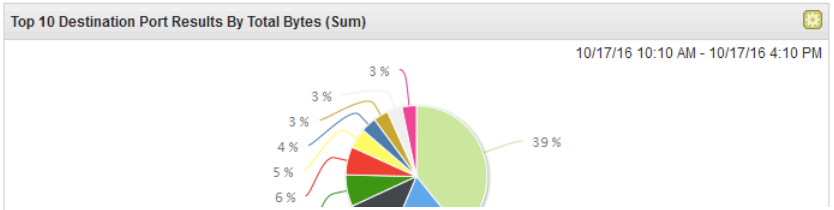
Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Magnitude (Maximum)	Event Count (Sum)	Count
Unknown ISNP System event	10.10.100.45	10.10.100.45	0	IBMSecurity NetworkProtectionXGS @ 10.10.100.45	System Status	other	None	8	2	2
FNXDC0001E System	10.10.100.45	10.10.100.45	0	IBMSecurity NetworkProtectionXGS @ 10.10.100.45	System Status	other	None	10	1	1
FNXAE0001I Network_Access	Multiple (3)	Multiple (2)	Multiple (2)	IBMSecurity NetworkProtectionXGS @ 10.10.100.45	Misc Network Communication Event	Multiple (3)	Unauthenticated Users	8	32	5
Information - Event CRE	Multiple (2)	Multiple (2)	Multiple (2)	IBMSecurity NetworkProt	Multiple (2)	Multiple (2)	Multiple (2)	8	30	6

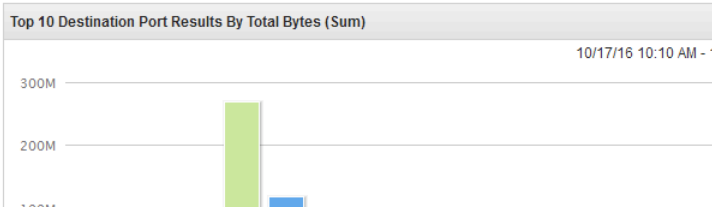
orting Tool:
natischer

1

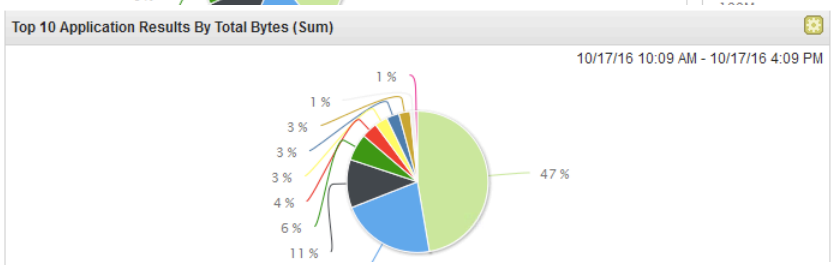


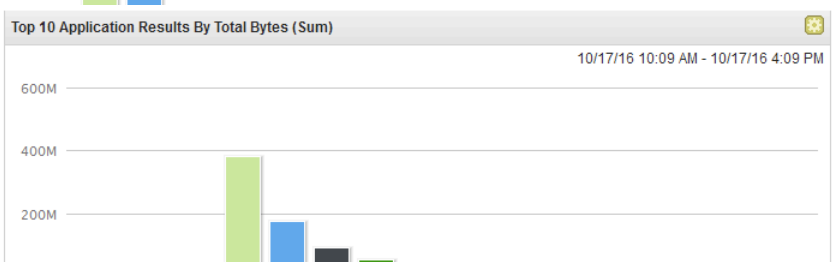
Netzwerk Analyse



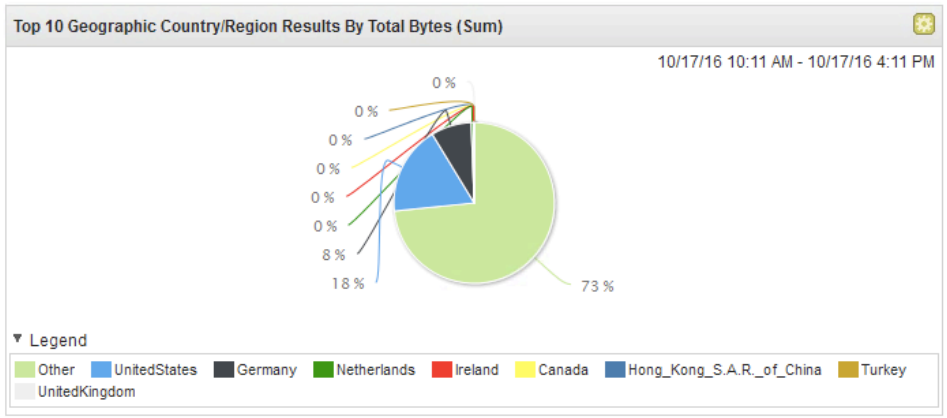


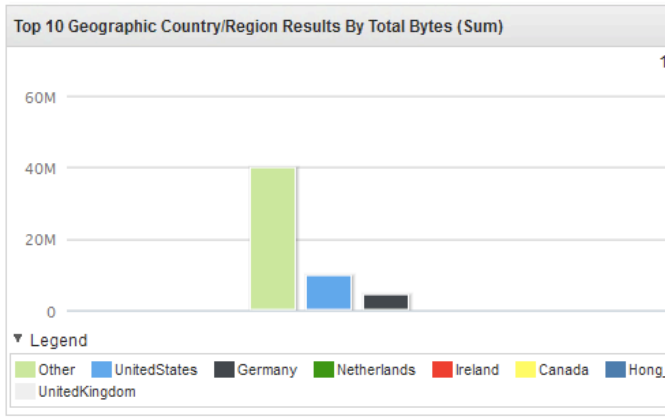
Destination Port
443
1352
5989
514
4172
53477
50000
32010
445
50001
25
8182
8879
80





Applica
Web.SecureWeb
Other
Authentication.LDAP
Misc.Syslog
Misc.LotusNotes
DataTransfer.Windov
InnerSystem.Flowge
Mail.SMTP
Web.Misc
Misc.Kerberos
Misc.domain
DHCP.IPv6





(Hide Charts)

Geographic Country/Region	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Application (Unique Count)	Protocol (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)
Other	Multiple (24)	Multiple (11)	Multiple (14)	Multiple (8)	Multiple (5)	39,888,965	524	39,889,489	173,446	6
UnitedStates	Multiple (23)	Multiple (62)	Multiple (24)	Multiple (7)	Multiple (2)	977,759	8,746,352	9,724,111	4,792	7,604
Germany	Multiple (11)	Multiple (11)	Multiple (5)	Multiple (10)	Multiple (3)	942,935	3,475,583	4,418,518	6,874	5,249
Netherlands	Multiple (5)	Multiple (10)	Multiple (5)	Multiple (8)	Multiple (2)	103,008	141,002	244,010	1,052	637
Ireland	10.10.100.66	52.164.240.59	80	Multiple (2)	tcp_ip	21,720	29,936	51,656	40	75
Canada	10.10.100.59	198.199.14....	80	Web.Misc	tcp_ip	4,026	11,806	15,832	36	36
Hong_Kong_S....	10.10.100.66	207.46.129....	80	Multiple (2)	tcp_ip	3,387	5,252	8,639	32	19
Turkey	212.58.31.37	Multiple (2)	443	Web.SecureWeb	tcp_ip	1,449	650	2,099	16	9
UnitedKingdom	10.10.100.247	195.122.141.2	53	Misc.domain	udp_ip	89	297	386	1	1

Flow Normalisierung

Event Information

Event Name:	Information - Event CRE						
Low Level Category:	HTTP In Progress						
Event Description:							
Magnitude:	(6)	**Relevance:**	10	**Severity:**	0	**Credibility:**	10
Username:	N/A						
Start Time:	2012-03-21 08:25:30	**Storage Time:**	2012-03-21 08:25:30	**Log Source Time:**	2012-03-21 08:25:30		
CRE Description (custom):	N/A						
CRE Name (custom):	N/A						

Source and Destination Information

Source IP:	218.201.187.130	**Destination IP:**	194.62.236.193
Source Asset Name:	N/A	**Destination Asset Name:**	N/A
Source Port:	6000	**Destination Port:**	1080
Pre NAT Source IP:		**Pre NAT Destination IP:**	
Pre NAT Source Port:	0	**Pre NAT Destination Port:**	0
Post NAT Source IP:		**Post NAT Destination IP:**	
Post NAT Source Port:	0	**Post NAT Destination Port:**	0
IPv6 Source:	0:0:0:0:0:0:0:0	**IPv6 Destination:**	0:0:0:0:0:0:0:0
Source MAC:	00:00:00:00:00:00	**Destination MAC:**	00:00:00:00:00:00

Payload Information

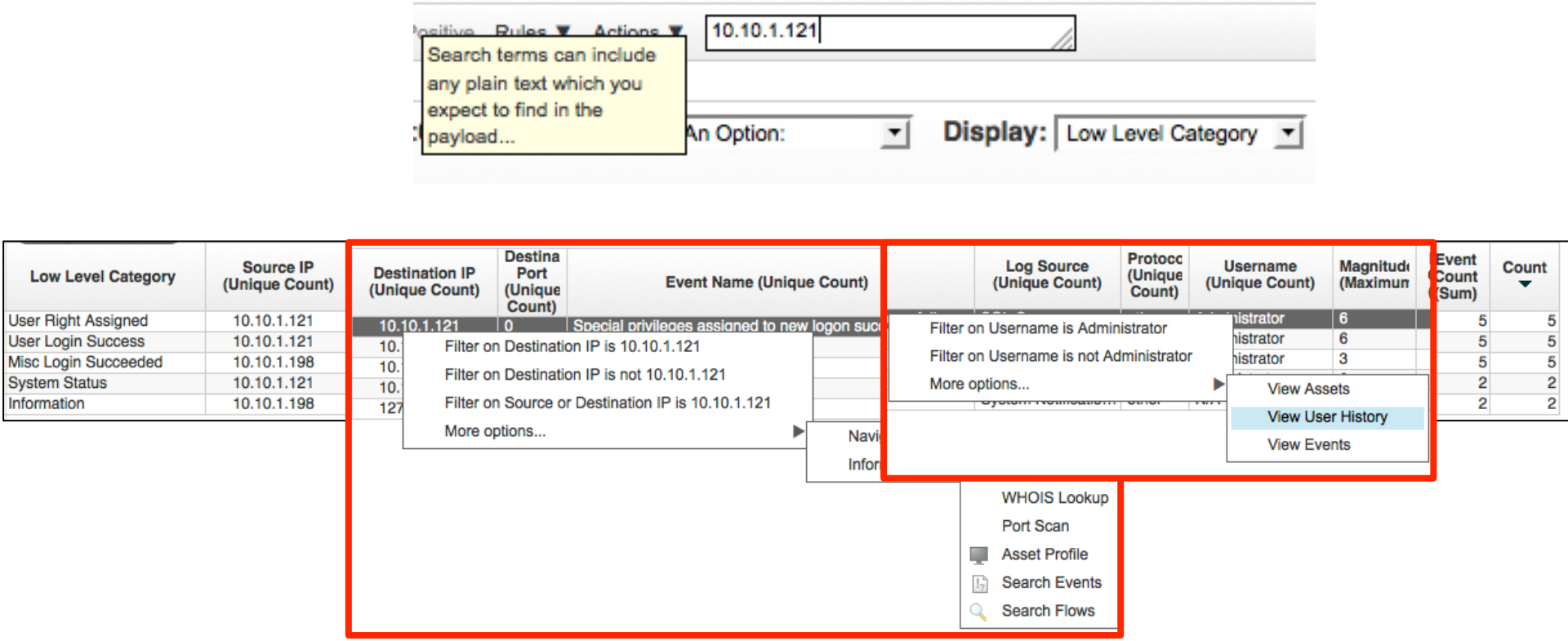
utf | hex | base64

Wrap Text

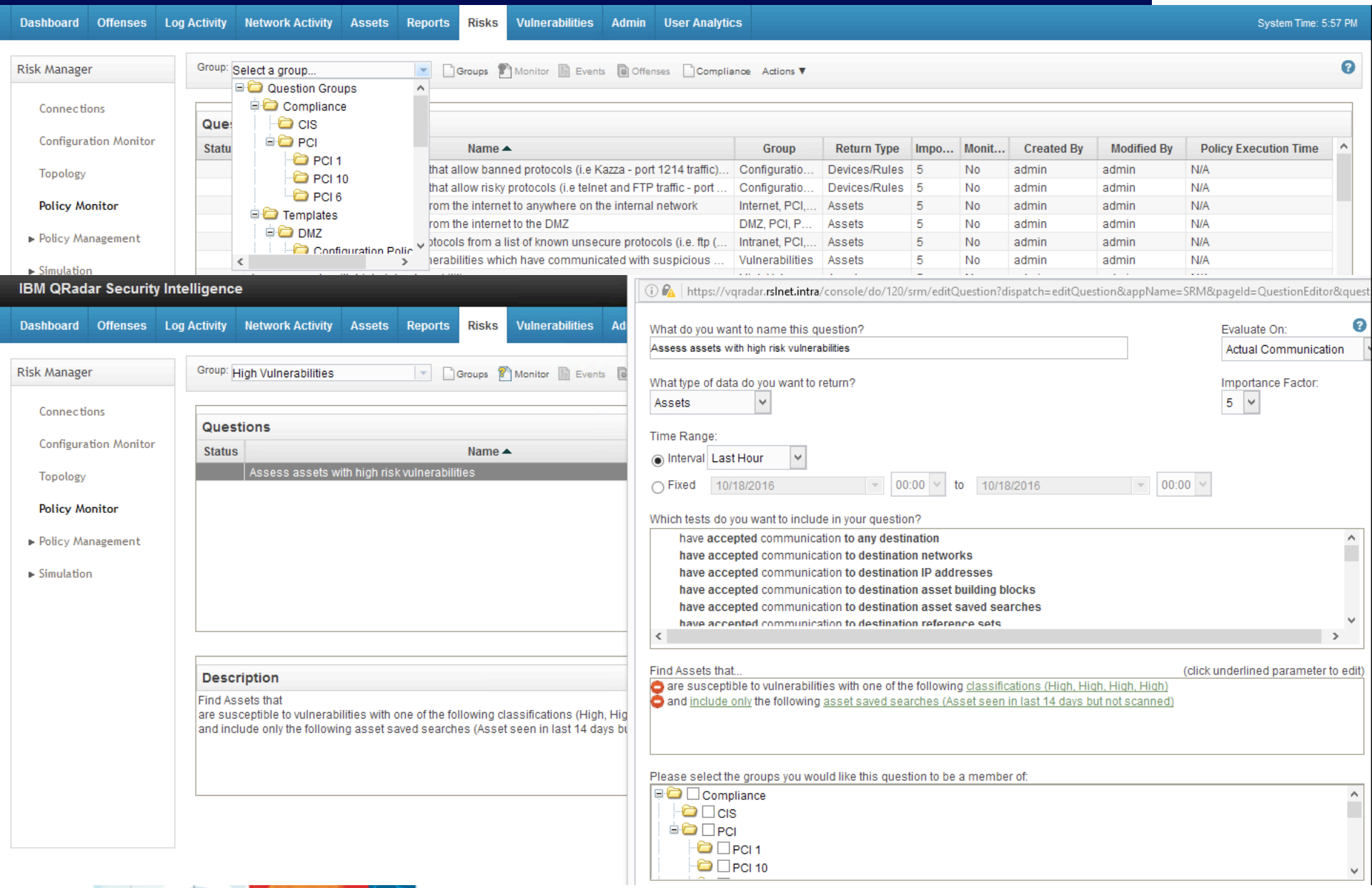
```
System: Flow Source Stopped Sending Flows, flow sources: strm:SRX210_10_10_1_109
```

definiere eigene Felder via regexp

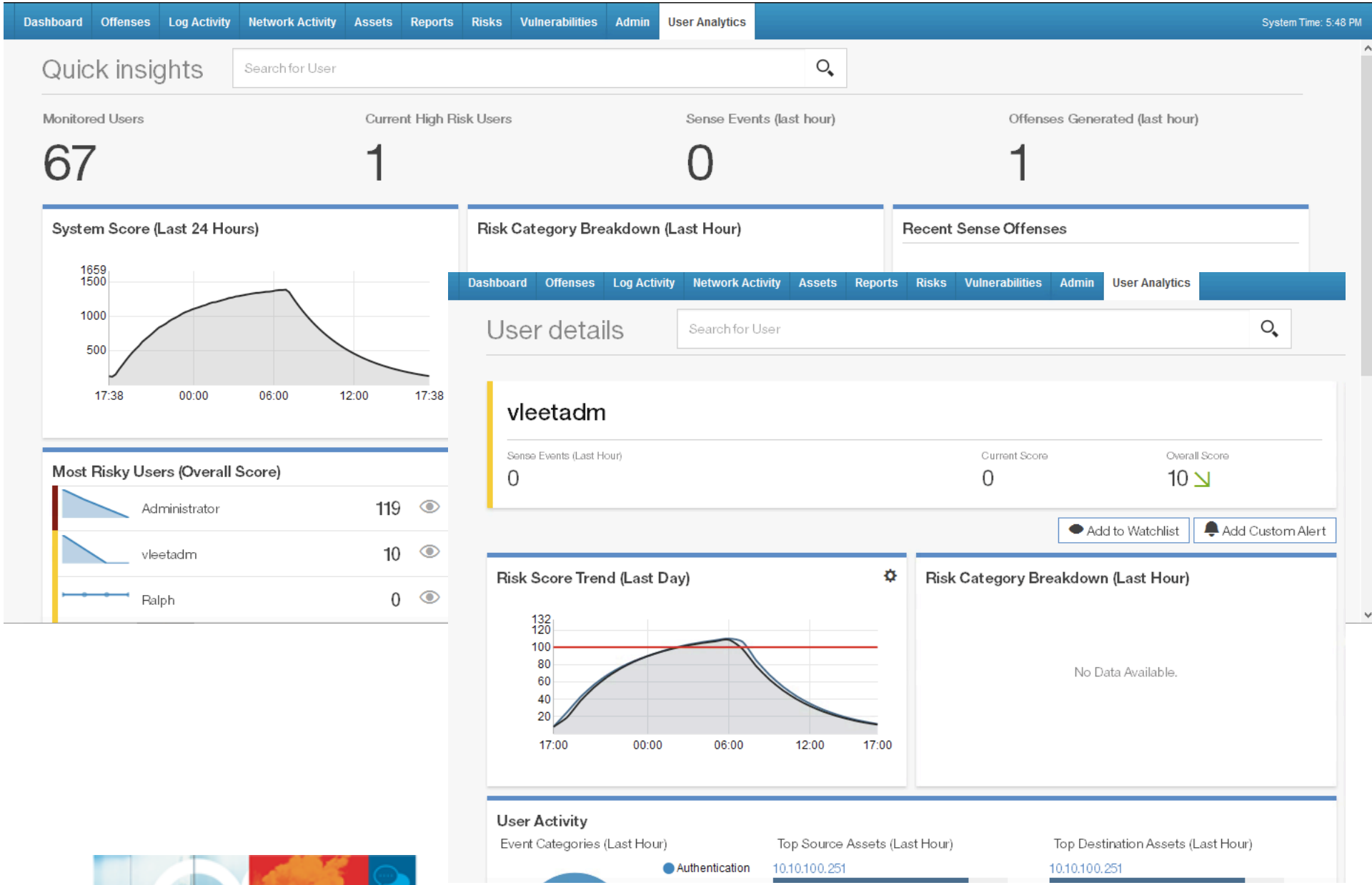
Kontextinformationen: Beispiel



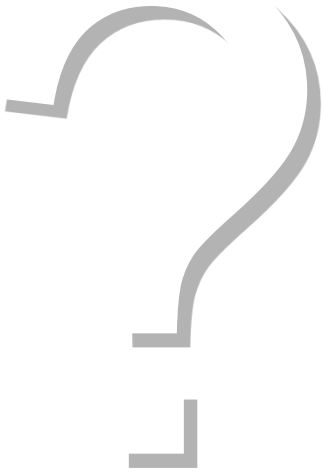
Erweiterung: Risikoanalyse



App Erweiterung: UBA



Fragen?



Kontakt

Dipl-Ing Karl Jaeger
pro4bizz GmbH
Karlsruhe

T +49 (0) 721 909 81722
M +49 (0) 163 542 3156
mailto:karl.jaeger@pro4bizz.de