

wie finden wir die Nadel im Heuhaufen?

Karl Jaeger
pro4bizz GmbH
15.März 2017

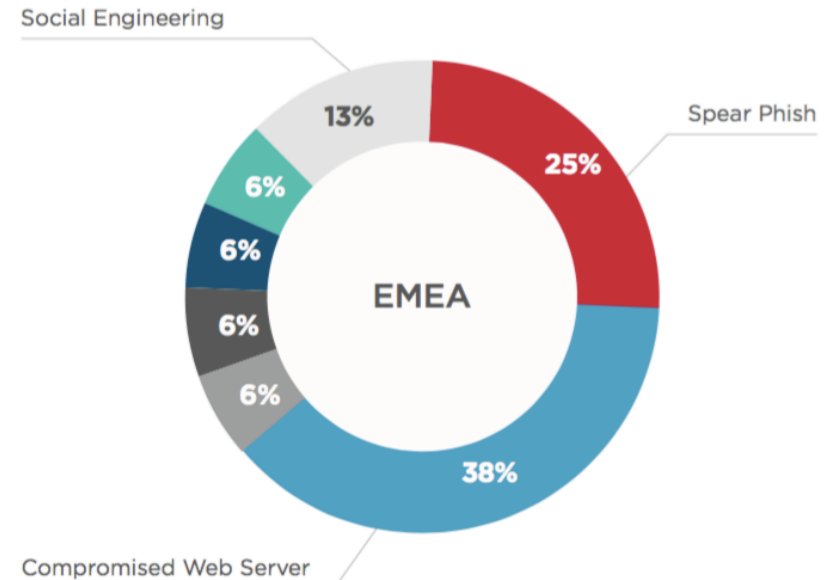
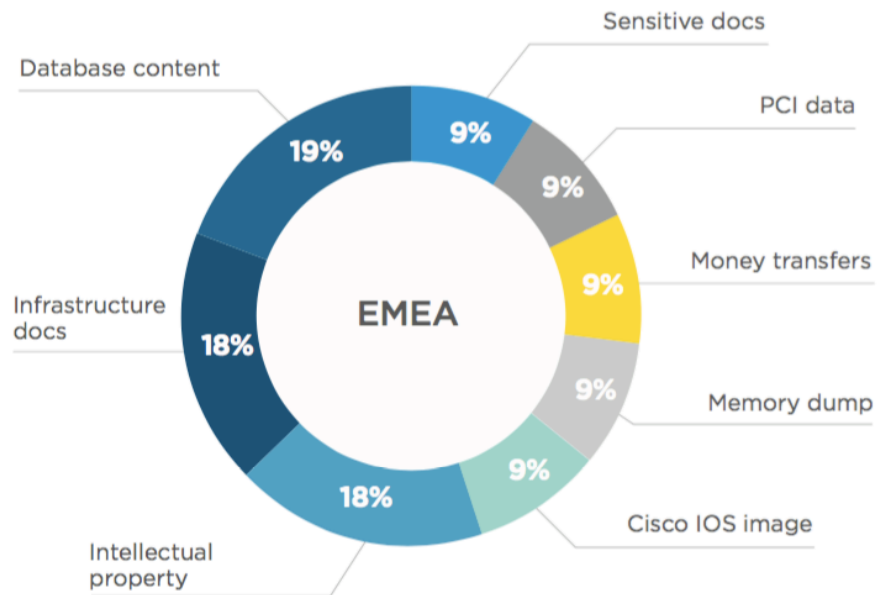


Agenda

- 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

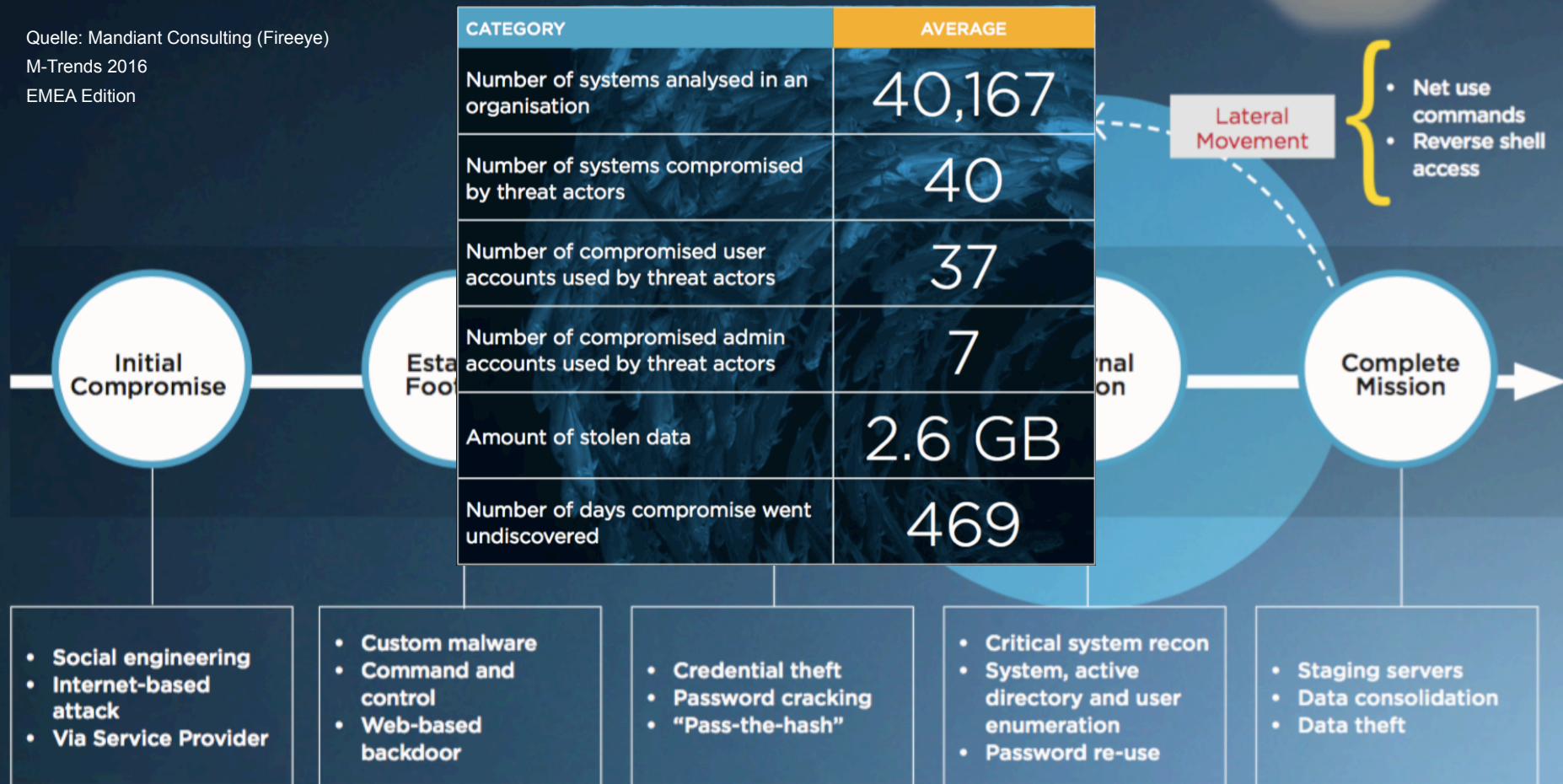
KEY

	Default Credentials
	SQL Injection
	Compromised Mail Server
	Social Engineering
	Citrix Vulnerability
	Spear Phish
	Compromised Web Server

Bedrohungslage EMEA 2016

Figure 1: Attack lifecycle model complemented with classic attacker techniques

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



Anforderungen an SIEM

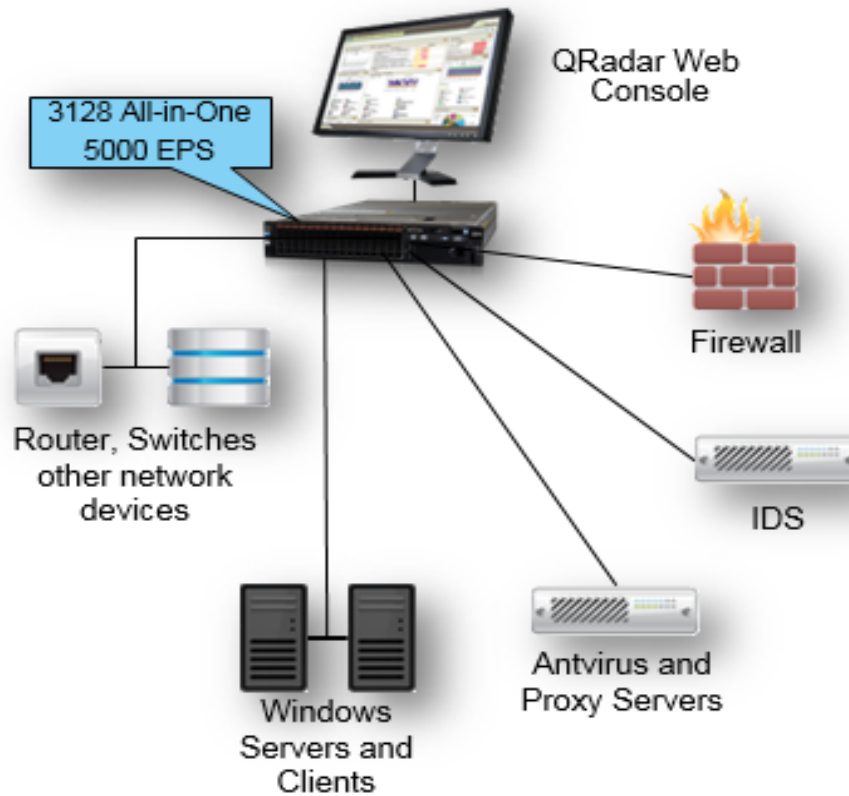
- gesetzliche und regulatorische Anforderungen
- ganzheitliches Überwachungssystem
- Einhaltung der Datenschutzanforderungen
- proaktive Alarmierung
- Integration in operationelle Services (SLAs)
- Analyse von Vorfällen in Realzeit
- Erhöhung des Sicherheitsniveaus

QRadar SIEM Architektur



QRadar SIEM Architektur

QRadar SIEM All-in-One Architektur



wieso? Audit Policy

was? Kategorisierung

was genau? Ereignis

wie gefährlich? Priorisierung

wer? User

wann?
Zeitstempel

woher? Network (IPAM)

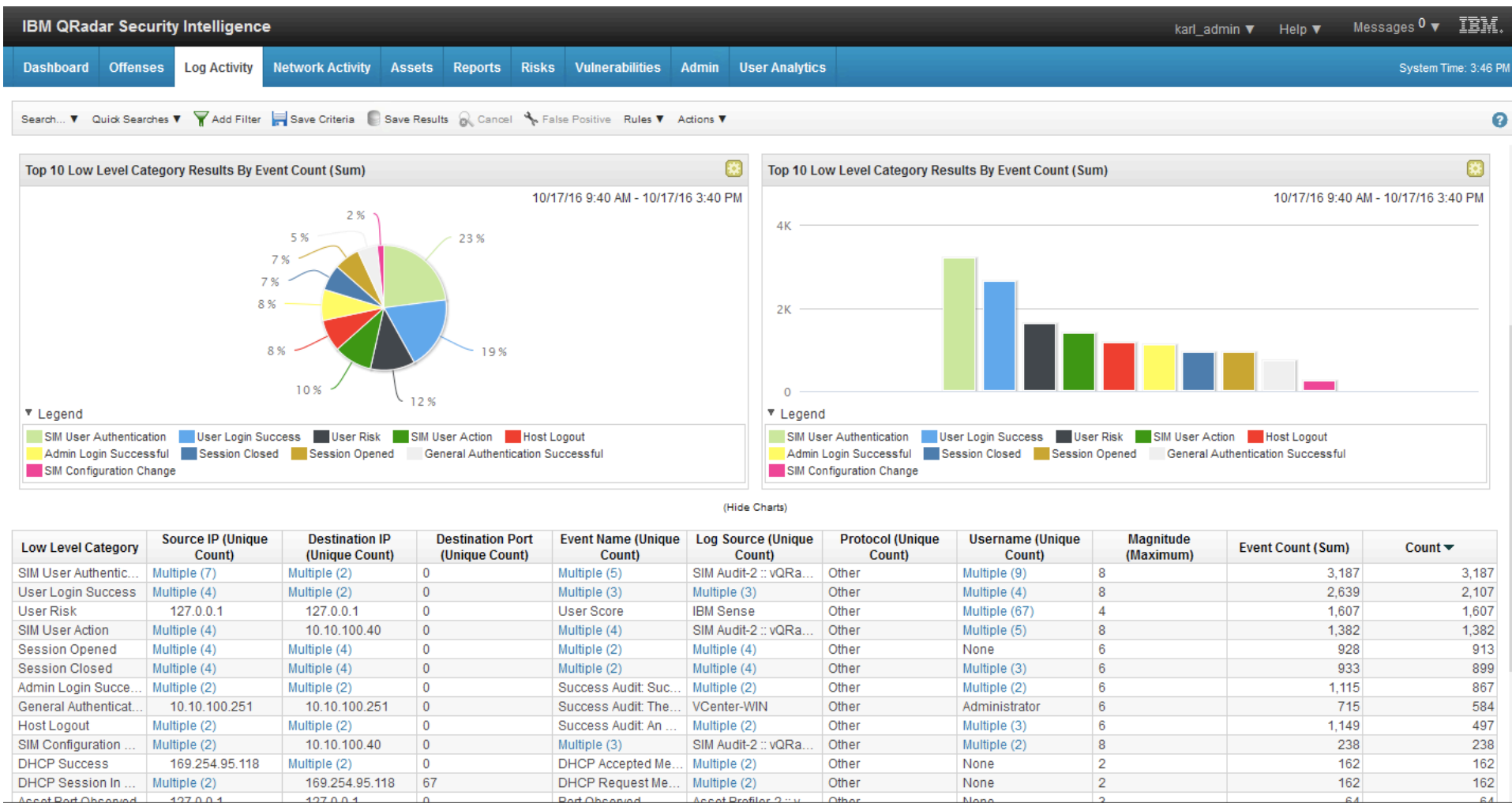
worauf? Asset DB

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
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	
<input type="checkbox"/> Wrap Text	
<132>ns5gt-adsl-wlan: NetScreen device_id=0128032005000468 [Root]system-warning-00515: Login attempt to system	



IBM Security QRadar SIEM

admin ▾ Preferences ▾ Help ▾ IBM.

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Admin

System Time: 10:39

Show Dashboard: Threat and Security Monitoring ▾

New Dashboard

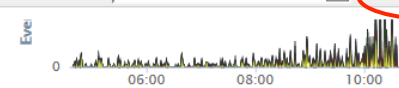
Rename Dashboard

Delete Dashboard

Add Item... ▾

Next Refresh: 00:00:15

⏸ ↺ ?

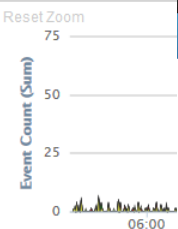


Legend

- SNMPTRAP-AUDIT:UNKNOWN-VERSION
- HTTP: Norton Internet Security Products
- Slapper Worm
- POP3:EXT:DOT-CRT
- NFS:ERR-SHORT-READ
- Remainder

[View in Log Activity](#)

Top Systems Attacked (Event Count)

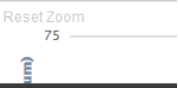


Legend

- 69.20.125.168
- 10.0.250.20
- 69.2

[View](#)

Top Systems Sourcing Attacked (Event Count)



QRadar

Most Recent Offenses

Offense Name	Magnitude
IRC Connections containing Firewall Permit	<div><div></div></div>
HTTP: WinAmp	<div><div></div></div>
Slapper Worm preceded by HTTP: Norton Internet Security Products	<div><div></div></div>
Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	<div><div></div></div>
DLP - Potential Data Loss containing Web.MSNLive.Text	<div><div></div></div>

Category	Offenses
Web Exploit	2
Firewall Permit	1
Worm Active	1
IRC/IM Policy Violation	1
Rate Limiting	0

Top Local Destinations

Destination	Offenses
-------------	----------

IBM QRadar Security Intelligence

karl_admin ▾ Help ▾ Messages 0 ▾ IBM.

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin User Analytics

System Time: 3:28 PM

Show Dashboard: p4bdemo ▾

New Dashboard

Rename Dashboard

Delete Dashboard

Add Item... ▾

Refresh Paused: 00:01:00

⏸ ↺ ?

You have not selected any item

- Event Category Distribution
- Event Processor Distribution
- Top Log Source Groups
- Exploit By Source
- Exploits By Destination
- Exploits by Type
- Firewall Deny by DST IP
- Inbound Events by Country/Region
- Login Failures by Log Source
- Offenses by Destination IP
- Offenses by Rule Name
- Offenses by Source IP
- Offenses by User
- Outbound Events by Country/Region
- Event Rate (EPS)
- Flow Rate (FPS)
- Offenses Over Time
- Remote Access Failures (VPN and Others)
- Remote Access Success (VPN and Other)
- Remote Recon and Scanning Activity by Destination IP
- Remote Recon and Scanning Activity by Destination Port
- Remote Recon and Scanning Activity by Source IP
- Top Authentication Failures by User

- Event Searches
- Events By Severity
- Top Log Sources

QRadar


10

[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	<div><div></div><div></div><div></div></div>	(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	IPv6 Destination	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:

Offense 41761

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	

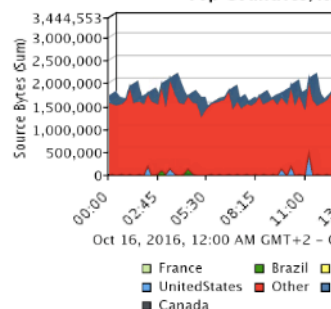
(Show Charts)

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination 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



Details

Top Countries/Regions

Oct 16, 2016, 12:00:00 AM - Oct 17, 2016, 12:00:00 AM

Geographic Country/Region	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)
UnitedStates	Multiple (3)	Multiple (7)	Multiple (1)
Other	Multiple (4)	Multiple (1)	Multiple (1)
Netherlands	Multiple (7)	Multiple (1)	Multiple (1)
Ireland	Multiple (5)	Multiple (3)	443
Germany	Multiple (2)	Multiple (1)	Multiple (1)
France	195.154.41.130	10.20.100.237	443

100,000,000

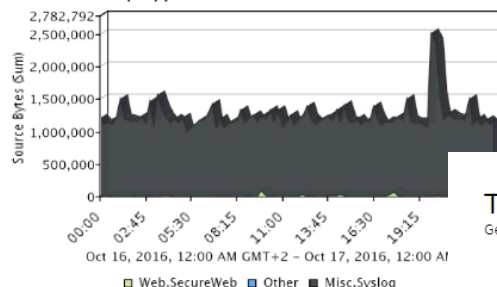


By DST Bytes
Top Countries/Regions

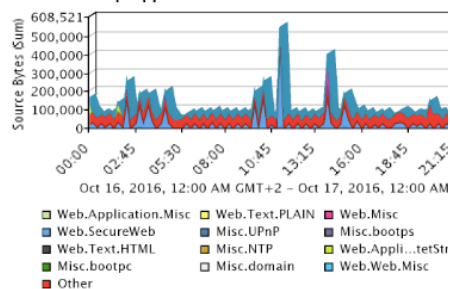
Top Applications (Internet)

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

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



Top Applications Outbound to Internet (SRC Bytes)
Top Applications Outbound to the Internet



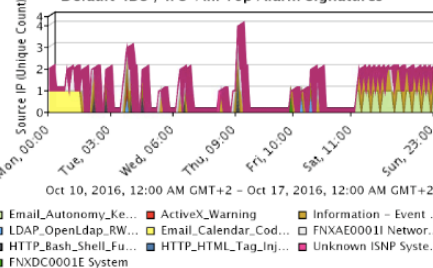
Top Applications Inbound from Internet (DST Bytes)
Top Applications Inbound from Internet



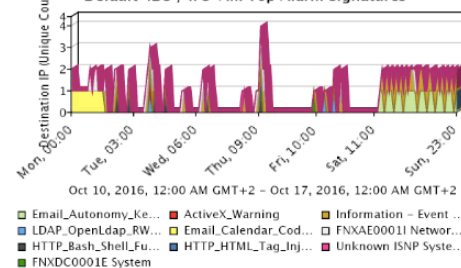
Top IDS/IPS Alerts (Weekly)

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 NetworkProt...	System Status	other	None	8	2	2
FNXDC0001E System	10.10.100.45	10.10.100.45	0	IBMSecurity NetworkProt...	System Status	other	None	10	1	1
FNXA00011 Network_Access	Multiple (3)	Multiple (2)	Multiple (2)	IBMSecurity NetworkProt...	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

Manage Vulnerabilities > [By Vulnerability](#)

▼ Asset Summary

Asset ID	1037	IP Address	10.10.1.121(Current DNS: 10.10.1.121)	MAC Address	00:0C:29:85:28:5D
Network	D testnetz	NetBIOS Name	SQL-SERVER	DNS Name	
Given Name		Group Name		Last User	ANONYMOUS-ANMELDUNG (All Users)
Operating System	Windows Server 2003 R2 3790 Service Pack 2(2 More)	Weight		Aggregate CVSS Score	323.2
Business Owner	Karl Jaeger	Business Owner Contact	karl.jaeger	Collateral Damage Potential	
Technical Owner		Technical Owner Contact		Availability Requirement	
Wireless AP		Wireless SSID		Confidentiality Requirement	
Switch ID	VMswitch1	Switch Port ID		Integrity Requirement	
Technical User	admin	Open Services	27	Vulnerabilities	8
Location	VM Testfarm	Asset Description	SitePro Testserver	Extra Data	
VLAN		Compliance Notes		Compliance Plan	

► Network Interface Summary

► Custom Properties

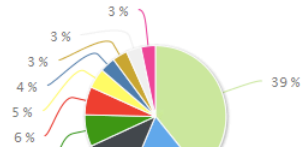
▼ Vulnerabilities

Delete Vulnerability

ID	Severity	Risk	Service	Port	Vulnerability	Details	Risk Score	Found	Last Seen
106742	Urgent	Warning	ms-sql-m	1434	Open Access to Databases	MS-SQLServer	6.10	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0
6529	Medium	Low	netbios-ssn	139	Information Leak - Computer Names ar...	Looking up status of 10.10.1.121SQL-SERVER <00> - M <ACTI...	9.50	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0
117469	Low	Warning	Multiple (2)	Multip...	Web Service is Running	Multiple (2)	7.10	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0
116707	Low	Warning	epmap	135	Distributed Computing Environment (D...		10.00	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0
98003	High	Warning	ms-sql-s	1433	Program or Library is Not Up-to-date	Version Found: MS-SQL Server Latest Version: MS-SQL Server	8.50	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0
97305	High	Low			1999-0525 - Trace Route Information	traceroute to 10.10.1.121 (10.10.1.121), 30 hops max, 60 byte p...	8.50	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0
119008	High	Medium	Multiple (2)	Multip...	SSL - Certificate Hostname Discrepancy	GET	9.00	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0
8076	High	Medium	microsoft-r...	3389	2005-1794 - Microsoft - Windows - Rem...	Network Check	10.00	2013-09-19 19:56:50.0	2014-12-01 20:16:01.0

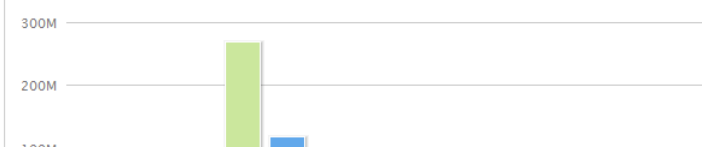
Top 10 Destination Port Results By Total Bytes (Sum)

10/17/16 10:10 AM - 10/17/16 4:10 PM



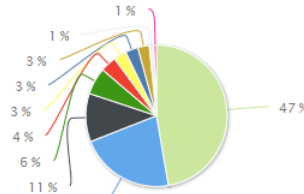
Top 10 Destination Port Results By Total Bytes (Sum)

10/17/16 10:10 AM -



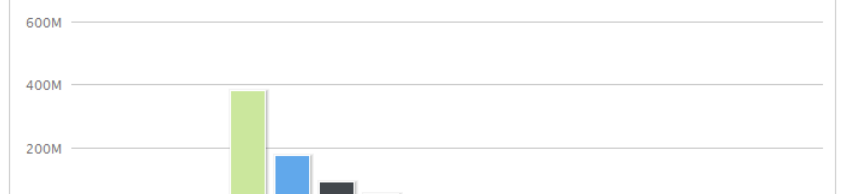
Top 10 Application Results By Total Bytes (Sum)

10/17/16 10:09 AM - 10/17/16 4:09 PM



Top 10 Application Results By Total Bytes (Sum)

10/17/16 10:09 AM - 10/17/16 4:09 PM



Legend

4

Destination Port

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

Legend

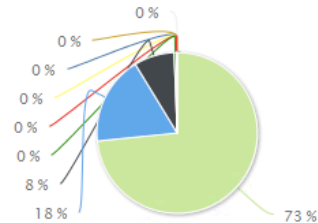
Web.SecureWeb
DataTransfer.Winc

Applica

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

Top 10 Geographic Country/Region Results By Total Bytes (Sum)

10/17/16 10:11 AM - 10/17/16 4:11 PM

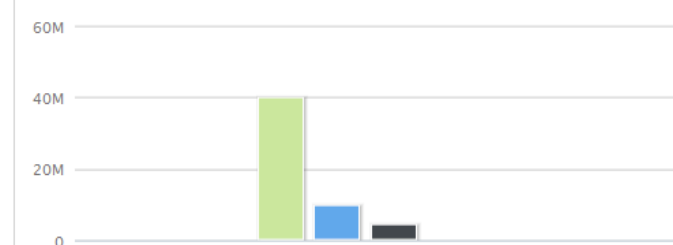


Legend

Other UnitedStates Germany Netherlands Ireland Canada Hong_Kong_S.A.R._of_China Turkey
UnitedKingdom

Top 10 Geographic Country/Region Results By Total Bytes (Sum)

1



Legend

Other UnitedStates Germany Netherlands Ireland Canada Hong_Kong_S.A.R._of_China Turkey
UnitedKingdom

(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

Event Information

Event Name:	Information - Event CRE						
Low Level Category:	HTTP In Progress						
Event Description:							
Magnitude:	<div><div></div></div> (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

☐ Wrap Text

System: Flow Source Stopped Sending Flows, flow sources: stim:SRX210_10_10_1_109

definiere eigene
Felder via regexp

Kontextinformationen: Beispiel

Positive Rules Actions 10.10.1.121

Search terms can include any plain text which you expect to find in the payload...

An Option: Display: Low Level Category

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
User Right Assigned	10.10.1.121	10.10.1.121	0	Special privileges assigned to new logon success			Administrator	6	5	5
User Login Success	10.10.1.121	10.10.1.121					Administrator	6	5	5
Misc Login Succeeded	10.10.1.198	10.10.1.198					Administrator	3	5	5
System Status	10.10.1.121	10.10.1.121							2	2
Information	10.10.1.198	10.10.1.198							2	2

Filter on Destination IP is 10.10.1.121	Filter on Username is Administrator	View Assets
Filter on Destination IP is not 10.10.1.121	Filter on Username is not Administrator	View User History
Filter on Source or Destination IP is 10.10.1.121	More options...	View Events
More options...		

WHOIS Lookup
Port Scan
Asset Profile
Search Events
Search Flows

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Risks

Vulnerabilities

Admin

User Analytics

System Time: 5:57 PM

Risk Manager

Connections

Configuration Monitor

Topology

Policy Monitor

Policy Management

Simulation

Group: Select a group...

Question Groups

Compliance

CIS

PCI

PCI 1

PCI 10

PCI 6

Templates

DMZ

Configuration Policies

Groups

Monitor

Events

Offenses

Compliance

Actions

Name	Group	Return Type	Impo...	Monit...	Created By	Modified By	Policy Execution Time
that allow banned protocols (i.e Kazza - port 1214 traffic)...	Configuratio...	Devices/Rules	5	No	admin	admin	N/A
that allow risky protocols (i.e telnet and FTP traffic - port ...	Configuratio...	Devices/Rules	5	No	admin	admin	N/A
from the internet to anywhere on the internal network	Internet, PCI,...	Assets	5	No	admin	admin	N/A
from the internet to the DMZ	DMZ, PCI, P...	Assets	5	No	admin	admin	N/A
protocols from a list of known unsecure protocols (i.e. ftp (...	Intranet, PCI,...	Assets	5	No	admin	admin	N/A
vulnerabilities which have communicated with suspicious ...	Vulnerabilities	Assets	5	No	admin	admin	N/A

IBM QRadar Security Intelligence

Dashboard

Offenses

Log Activity

Network Activity

Assets

Reports

Risks

Vulnerabilities

Ad

Risk Manager

Connections

Configuration Monitor

Topology

Policy Monitor

Policy Management

Simulation

Group: High Vulnerabilities

Questions

Status

Name

Assess assets with high risk vulnerabilities

Description

Find Assets that
are susceptible to vulnerabilities with one of the following classifications (High, Hig
and include only the following asset saved searches (Asset seen in last 14 days b

What do you want to name this question?

Assess assets with high risk vulnerabilities

Evaluate On:

Actual Communication

What type of data do you want to return?

Assets

Importance Factor:

5

Time Range:

Interval

Last Hour

Fixed

10/18/2016

00:00

to

10/18/2016

00:00

Which tests do you want to include in your question?

have accepted communication to any destination

have accepted communication to destination networks

have accepted communication to destination IP addresses

have accepted communication to destination asset building blocks

have accepted communication to destination asset saved searches

have accepted communication to destination reference sets

Find Assets that...

are susceptible to vulnerabilities with one of the following classifications (High, High, High, High)

and include only the following asset saved searches (Asset seen in last 14 days but not scanned)

Please select the groups you would like this question to be a member of:

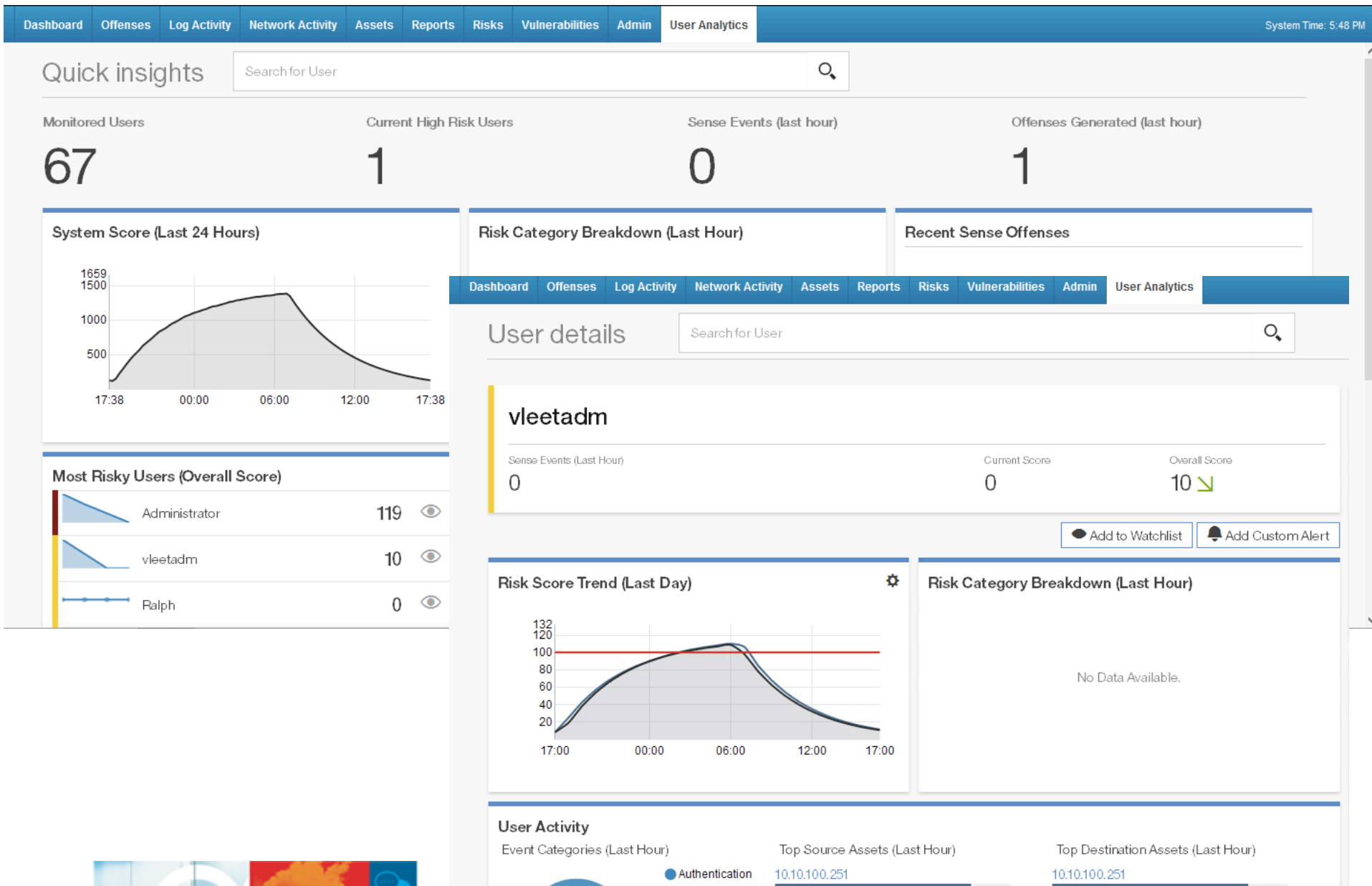
Compliance

CIS

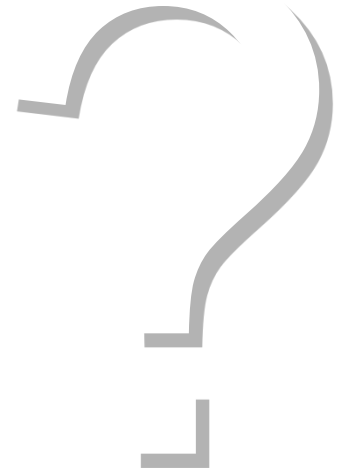
PCI

PCI 1

PCI 10



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>

