QRadar braindump

15. März. 2017

Karl Jaeger

Pro4bizz GmbH
https://www.pro4bizz.de
karl.jaeger@pro4bizz.de
0721-909 81 720

Agenda

- SIEM Markt und Einführung QRadar
- IBM Training und Zertifizierung
- QRadar Dokumentation
- IBM Fix Central und Installationsschritte
- Demo VM
- Betrieb QRadar
- Einbindung in IT Infrastruktur
- Einbindung in Workflow
- QRadar Architektur und Plattformen
- SIEM Sizing
- QRadar Finetuning
- Logs & Flow (Datenquellen, Netzwerkinfrastruktur)
- Alarme & Regeln
- System Monitoring (Beispielalarme)
- Trouble Shooting
- IBM Service Request
- High Availability

SIEM Markt

- Gartner MQ August 2016
  - Leaders: IBM, HPE, EMC, Splunk, Intel Security, LogRhythm
  - Challengers: EMC
  - Visionaries: AlienVault

- Hype/Top
  - APT / Cyberdefense
  - RM / VM
  - Forensik
  - HP TAP
  - Know How
  - NG SIEM
  - Fireeye HX/NX

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (August 2016)

Einführung QRadar & Marktüberblick

2017-p4b-IT-Sicherheit

ITSiG: Ziel, Inhalt und Herausforderung

P4B SIEM und Q1Labs 2017

Q1 Training

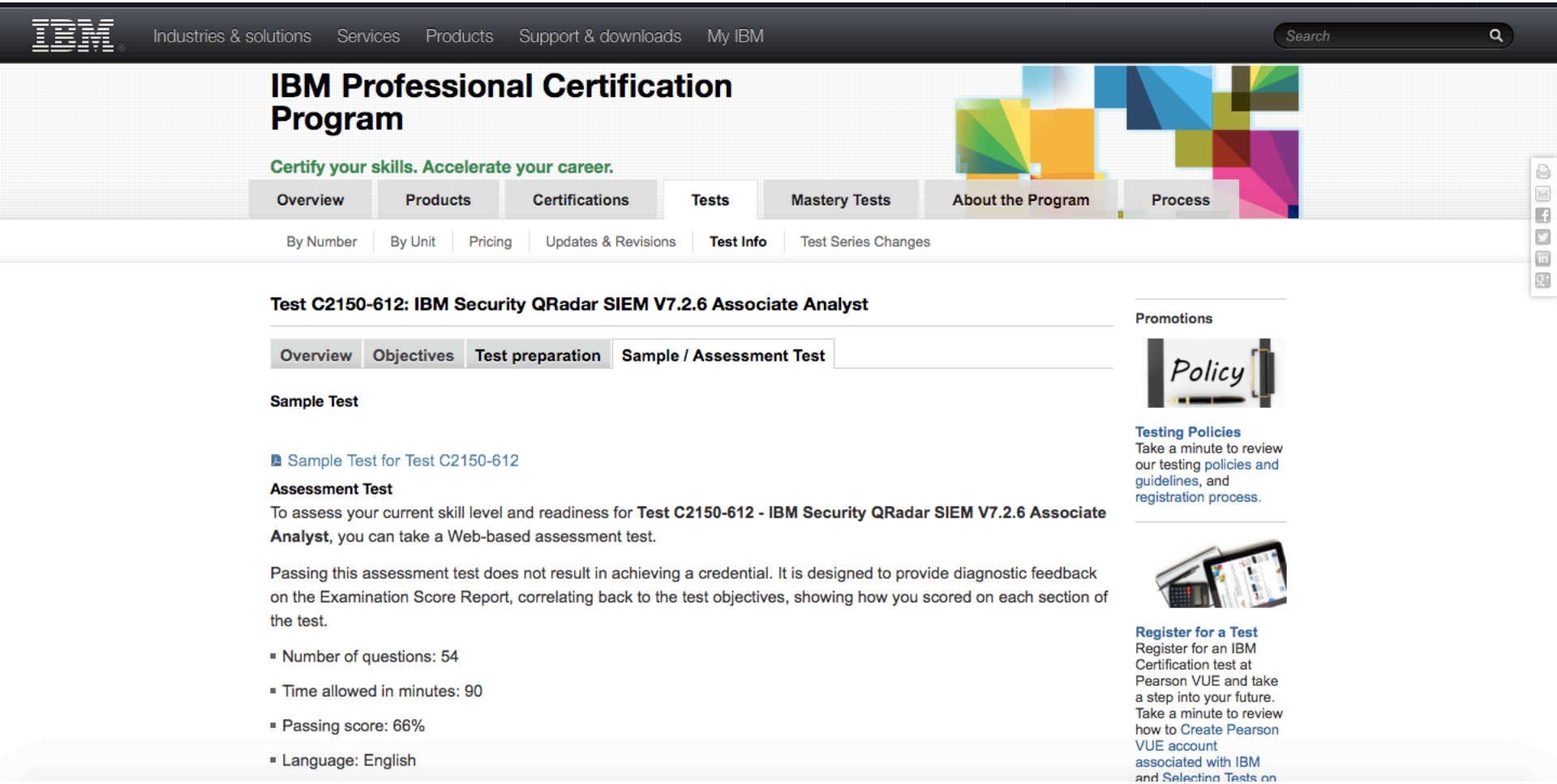
- **IBM Security QRadar SIEM 7.2 Foundations**

https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=course_description&cc=&courseCode=BQ102G

- **IBM Security QRadar SIEM 7.2 Administration and Configuration (Advanced)**

https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=course_description&cc=&courseCode=BQ150G

Q1 Zertifizierung



Q1 Dokumentation

IBM QRadar Security Intelligence Platform

Version 7.2.6

Quick Start Guide

This guide gets you started with a typical installation.

National Language Version: To obtain the Quick Start Guide in other languages, print the language-specific PDF from the installation media.

Product overview

IBM® QRadar® Security Intelligence Platform products provide a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics, and configuration and vulnerability management. This Quick Start Guide provides information about installing IBM Security QRadar appliances.

1 Step 1: Access the software and documentation

Review the release notes for the QRadar component you want to install.

Download the ISO for your QRadar component from the IBM FIX Central website.

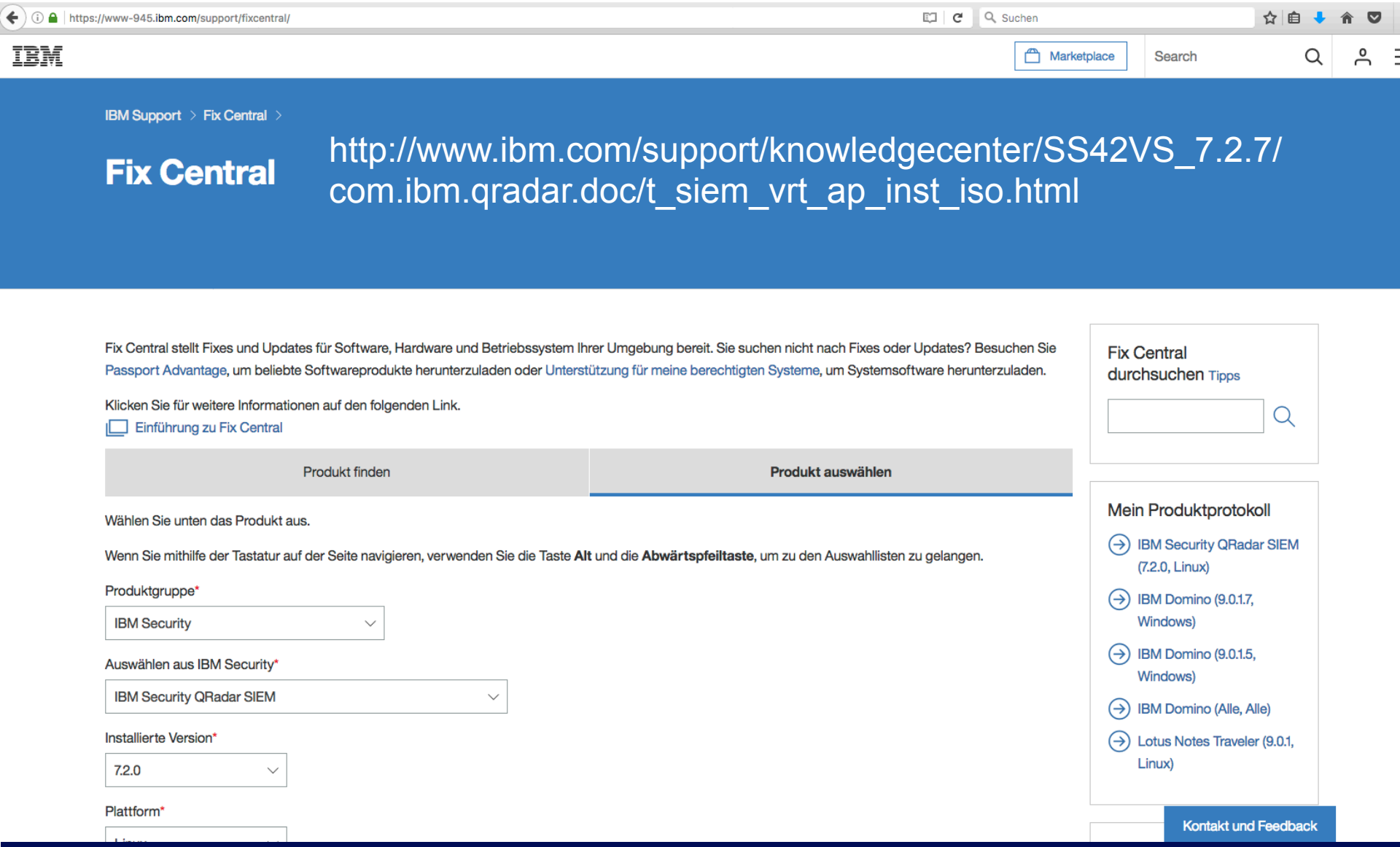
Q1 Dokumentation

References:

- *IBM Security QRadar SIEM Users Guide* http://ibm.co/1wvpSEE
- *IBM Security QRadar SIEM Administration Guide* http://ibm.co/1wvpSEE
- *IBM Security QRadar Log Sources User Guide* http://ibm.co/1wvpSEE
- *IBM Security QRadar WinCollect User Guide* http://ibm.co/1wvpSEE
- *IBM Security QRadar Adaptive Log Exporter Users Guide* http://ibm.co/1wvpSEE
- Microsoft Windows Management Instrumentation http://technet.microsoft.com/en-us/library/ee692942.aspx
- *IBM Security QRadar Vulnerability Assessment Configuration Guide* http://ibm.co/1wvpSEE

DSM Configuration Guide (b_dsm_guide.pdf)

IBM Fix Central



Q1 installation steps

- download des iso image von
- https://www-945.ibm.com/support/fixcentral/
- dort QRadar als Produkt auswählen
- dann wählen Sie das entsprechende ISO Image, zB QR 7.2.8 als Basis aus und installieren darauf den entsprechenden fixpack, also 7.2.8 patch1
- zum installieren wird der activation key der VM benötigt
- Lizenz wird automatisch für 30 Tage generiert

Demo VM

- Prerequisites Demo VM
- Recommended hardware and software requirements for each demo VM
- VMware Workstation 9 or above, or equivalent ESXi/ vSphere
- min. 2 core CPU
- min. 24 GB available RAM (32GB empfohlen)
- Solid state drive (SSD) with 100GB available space

here we go...

IBM

IBM Knowledge Center

IBM QRadar Security Intelligence Platform > IBM QRadar Security Intelligence Platform 7.2.7 > Installing > QRadar installations > Installing the QRadar software on a virtual machine

Installing the QRadar software on a virtual machine

Version 7.2.7

After you create your virtual machine, you must install the IBM® Security QRadar® software on the virtual machine.

Before you begin

Ensure that the activation key is readily available.

Procedure

1. In the left navigation pane of your VMware vSphere Client, select your virtual machine.
2. In the right pane, click the **Summary** tab.
3. In the **Commands** pane, click **Edit Settings**.
4. In the left pane of the **Virtual Machine Properties** window, click **CD/DVD Drive 1**.
5. In the **Device Type** pane, select **DataStore ISO File**.
6. In the **Device Status** pane, select the **Connect at power on** check box.
7. In the **Device Type** pane, click **Browse**.
8. In the Browse Datastores window, locate and select the QRadar product ISO file, click **Open** and then click **OK**.
9. After the QRadar product ISO image is installed, right-click your virtual machine and click **Power** > **Power On.**
10. Log in to the virtual machine by typing `root` for the user name.

Betrieb Qradar

- Infrastrukturmgmt

•DNS intern
•CMDB
•Namenskonzept
•Netzwerkkonzept

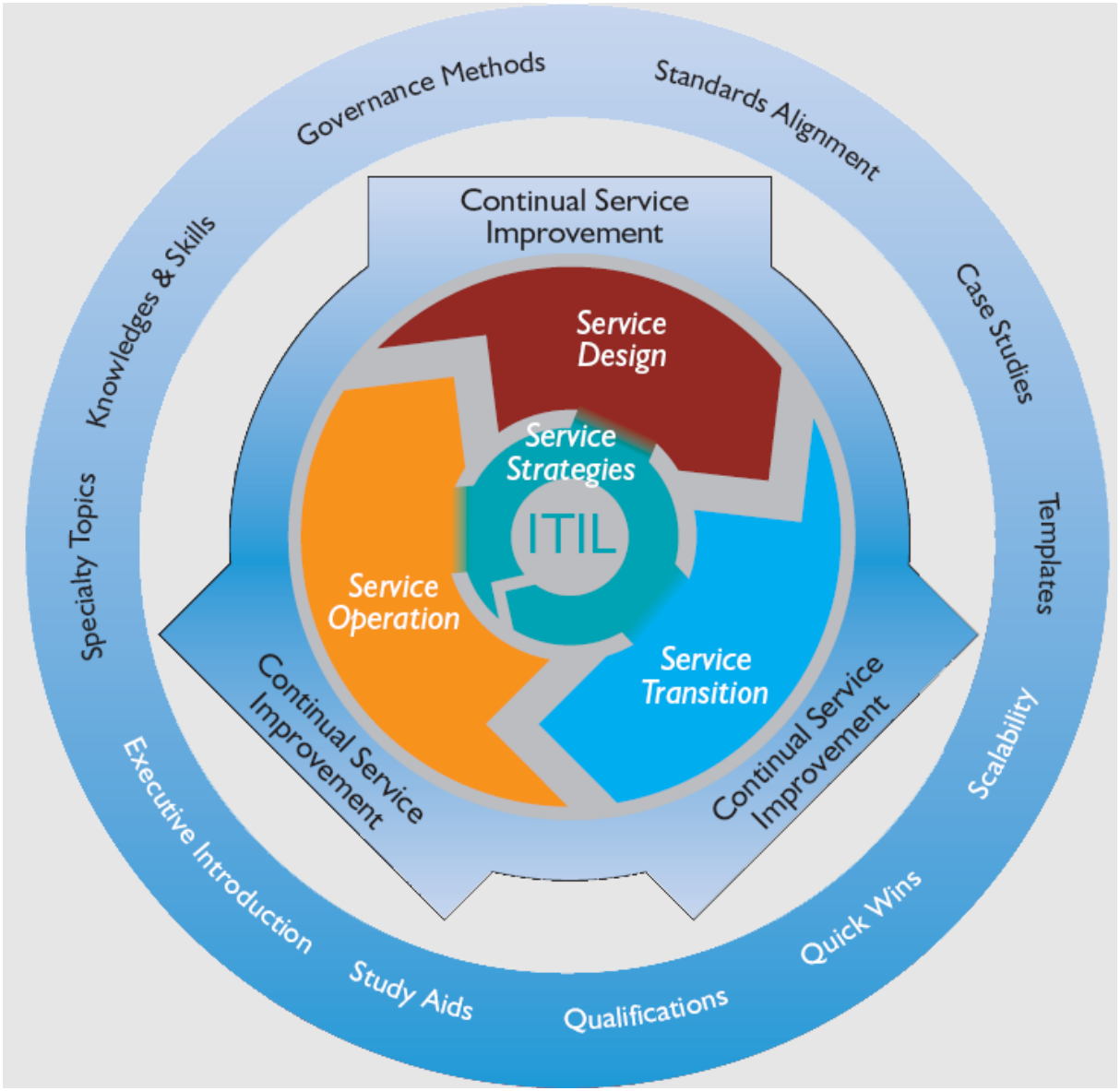
- Best Practice

•Change Mgmt
•Patch Mgmt
•Security Mgmt (Incident Handling, CERT, NOC)
•Risk Mgmt

- ITIL Prozesse

•Service Operation
•Continuous Service Improvement

ITIL v3



Einbindung in IT Infrastruktur

- Rekursives DNS
- CMDB import oder autodiscovery via Flow
- Netzwerkhierarchie (notfalls aus Regelwerk)
- Syslog forwarder (may need IP spoofing)
- DMZ
- BBs

Einbindung in SI Workflow

Offense Workflow

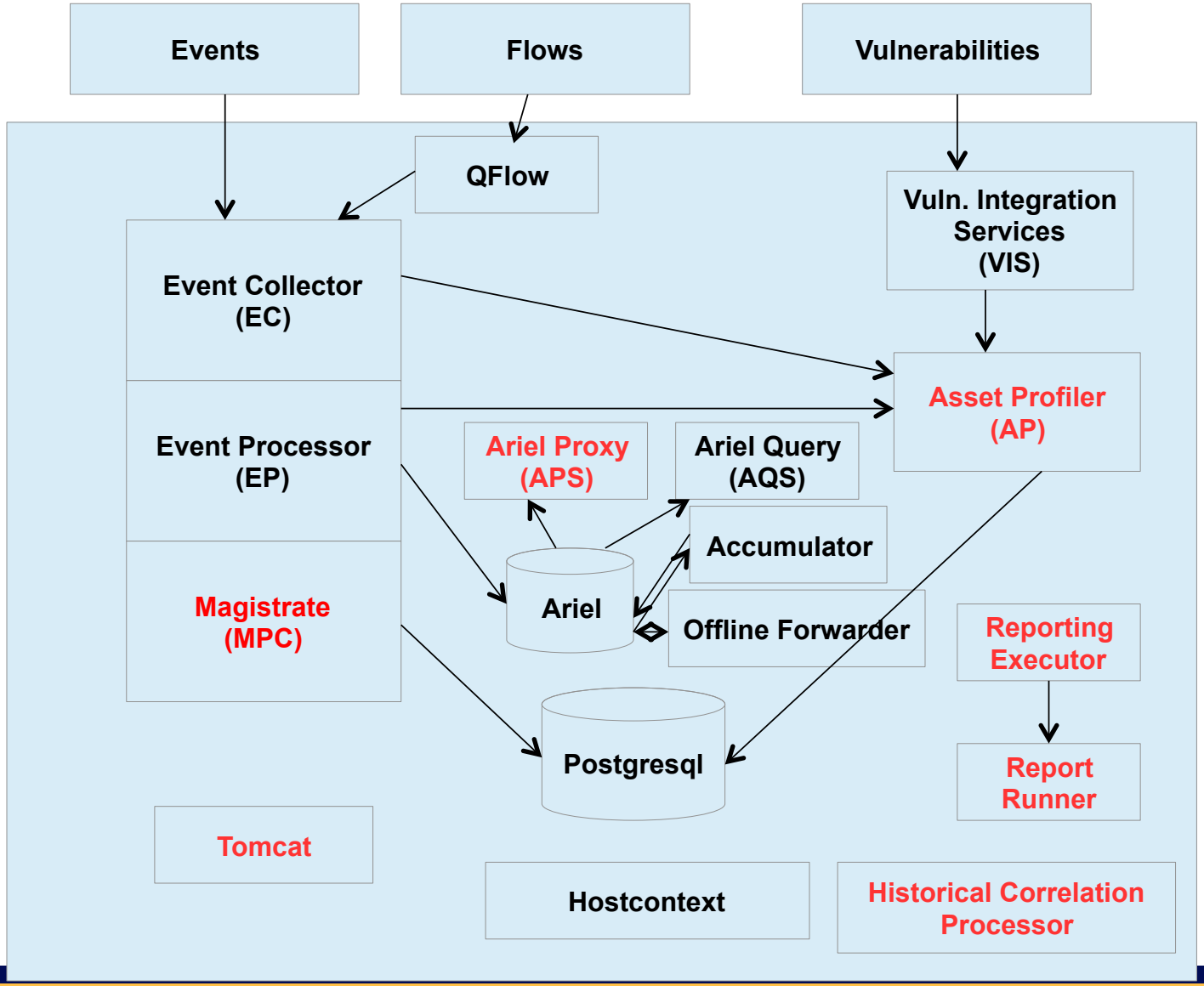
Protokolle

- SMTP
- SNMP
- syslog
- API (REST)

Products

- OTRS
- Service Now
- Remedy
- ...

Qradar Architektur



Plattformen

1. Appliance incl. HA-Option
2. Software (Server Platform)
3. VM (ESX)

- QRadar_Hardware_Guide.pdf

QRadar_hardware_guide.pdf - Verkn,pfung.lnk

Sizing

- Design

AiO vs. Distributed

- Tools

EPS and Flow Calculator V2

- Lab

Boot Camp
SAO
VM

Finetuning

1. Network Hierarchy
2. Asset Discovery / BBs / VA
3. False Pos
4. Offense disable
5. User defined rules
6. LSX

Logs & Flow (Datenquellen, Netzwerkinfrastruktur)

- Logsources
- 80% autodiscovered
- Rest nach DSM Guide und Log Source Guide
- Unknown Logsource
- Advanced: BQ121_Unit06_CollLogs

b_dsm_guide.pdf - Verkn,pfung.lnk

b_logsource.pdf - Verkn,pfung.lnk

Flow Sources

- Flow Typen
- IPFIX
- Foundations: **Unit 7 Investigating an offense triggered by flowsQRadar**
- Admin Guide.pdf: **Chapter 12. Flow sources management**
- ESX Switch
- Offene Fragen

Netzwerkhierarchie

- Advanced: IBM Security QRadar SIEM 7.2 Administration and Configuration - **Unit 02**

- QRadar Admin Guide: **Chapter 6. Set up Qradar: Network hierarchy**

- CLI
- Demo

Alarme = Offenses

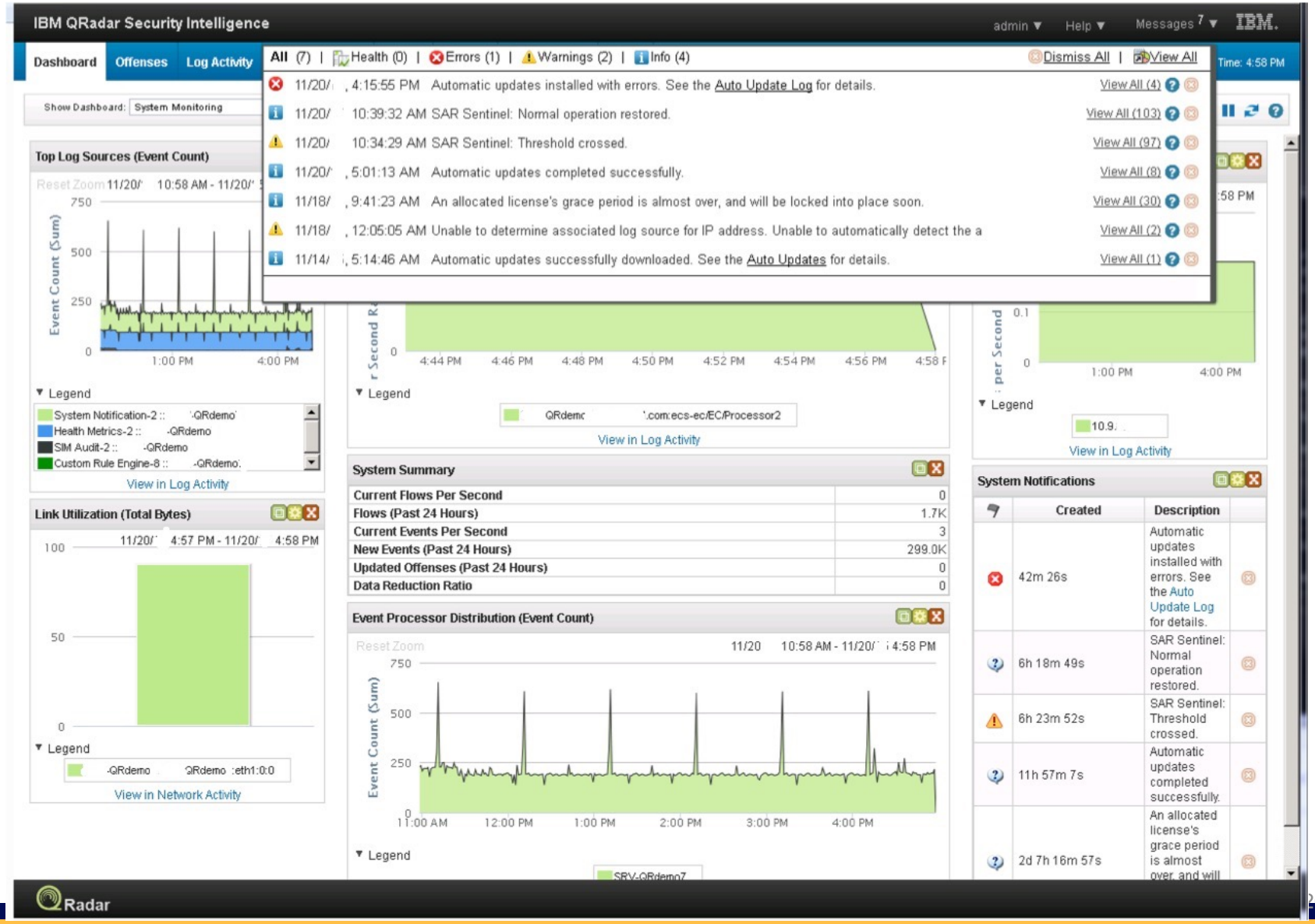
- Unit 4 Foundations (BQ101): BQ101_04_OffenseEvents_slides - Investigating an offense triggered by events
- Unit 9/10 Advanced (BQ121):
  BQ121_Unit09_RulesOverview
  BQ121_Unit10_RulesDesign
- Admin Guide: Chapter 6 Setup QRadar - Configuring custom email notifications
- Unit 12 Advanced (BQ121): Creating Reference Maps (BQ121_Unit12_RefMaps)
- User Guide: Chapter 4 Offense Management
- Rules.pdf
- Health Monitoring Rules

Offenses – alle Links

- **P4B QRadar hacks: false alarm (pro4bizz)**
- Unit 4/5 Foundations (BQ101)
- Unit 9/10 Advanced (BQ121):
- Admin Guide: Chapter 6 - Configuring custom email notifications
- Unit 12 Advanced (BQ121)
- User Guide: Chapter 4 Offense Management
- Rules.pdf

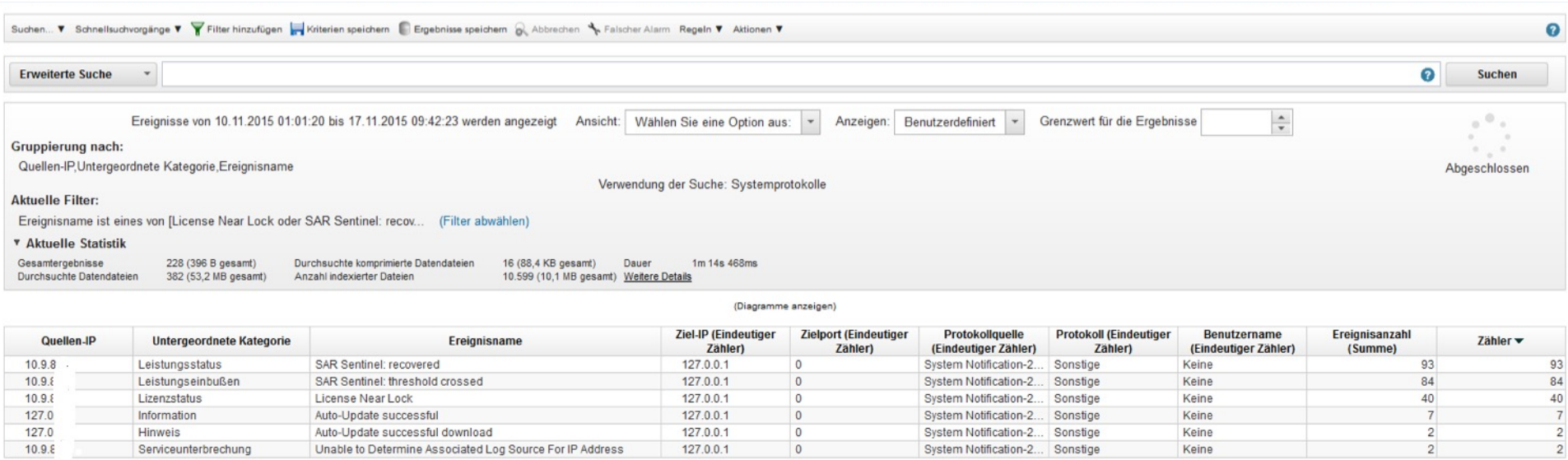
- Security Monitoring Rules (health check)

QR System Monitoring Labsystem 1



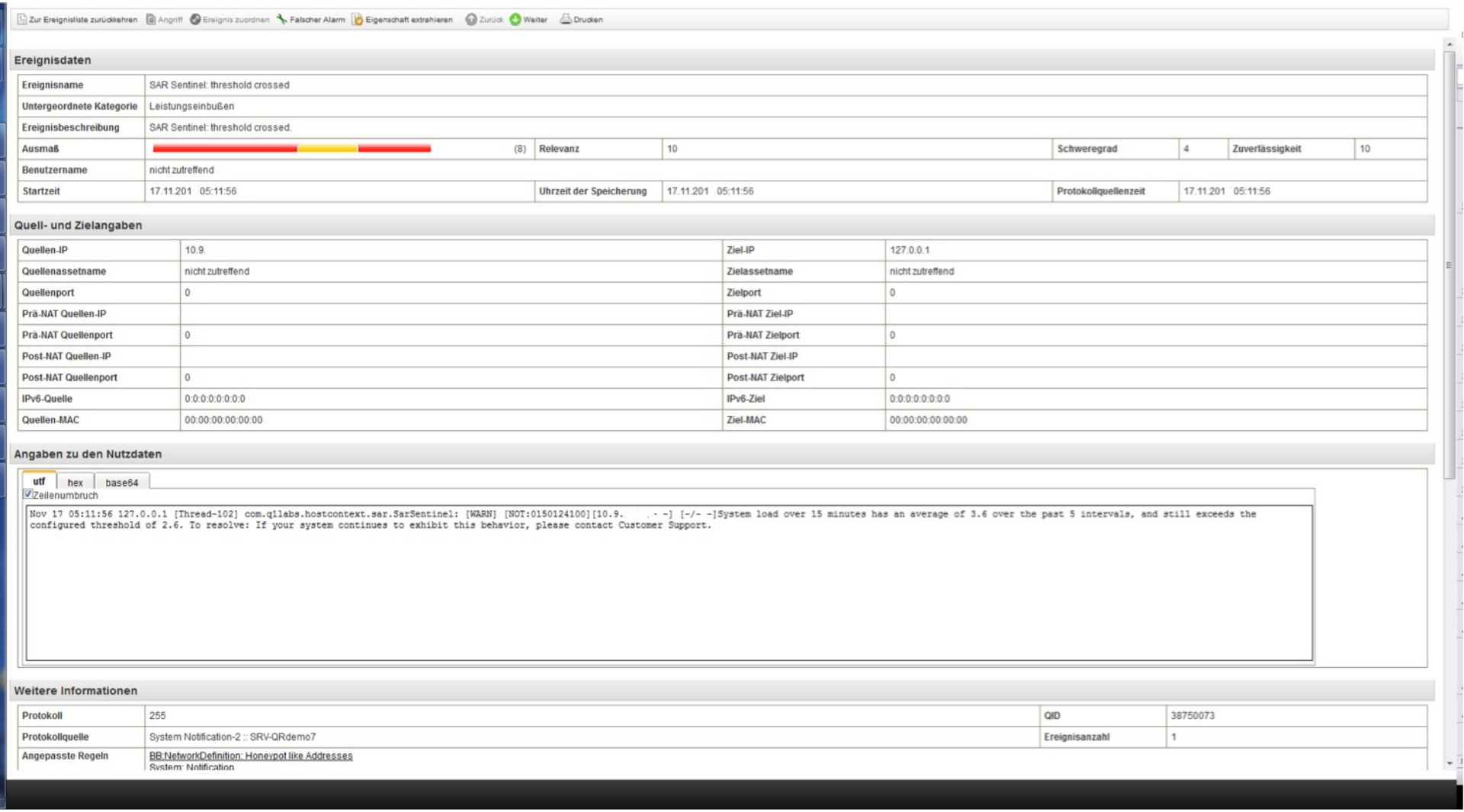
QR System Monitoring Labsystem 2

- View All
- Select Leistungseinbußen

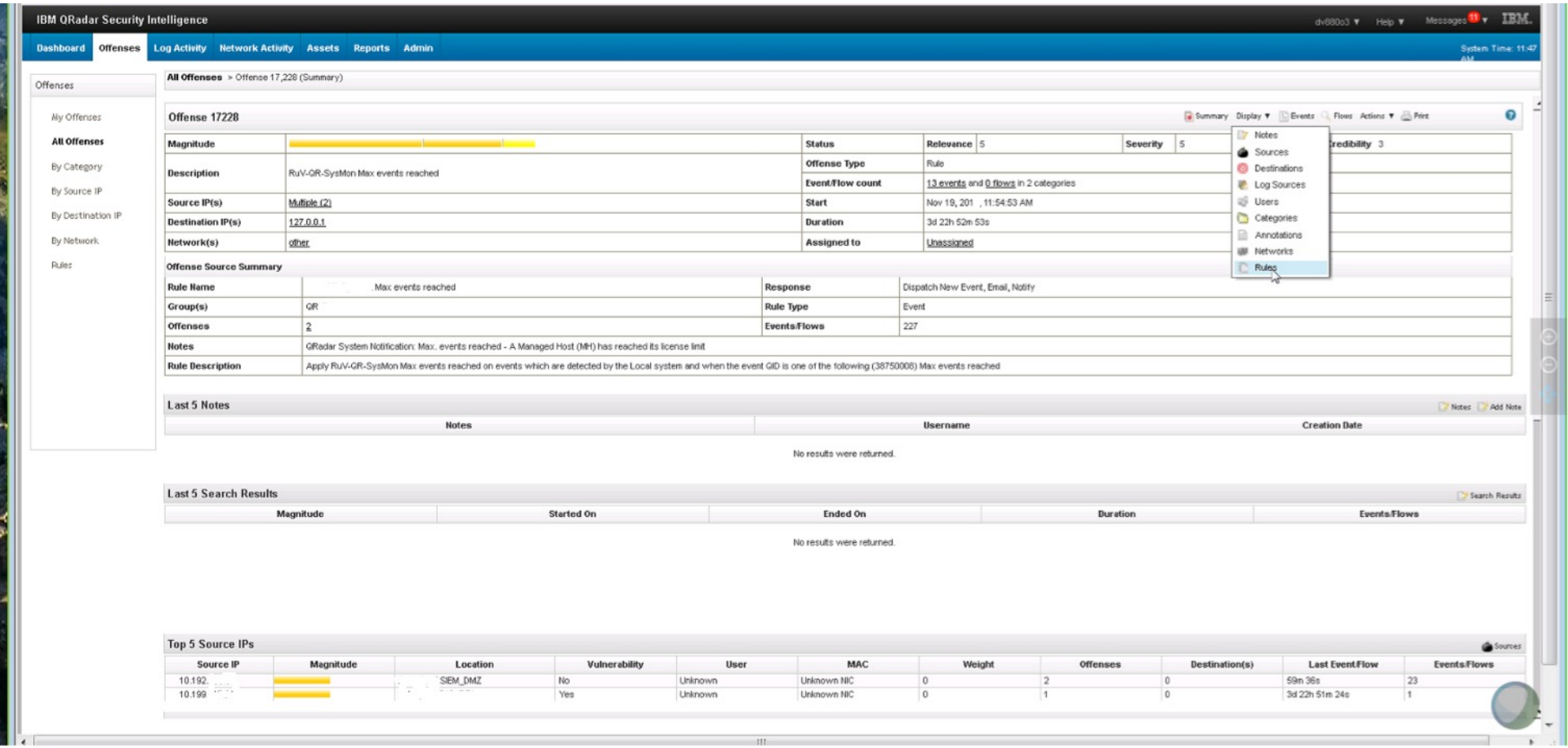


Quellen-IP	Untergeordnete Kategorie	Ereignisname	Ziel-IP (Eindeutiger Zähler)	Zielport (Eindeutiger Zähler)	Protokollquelle (Eindeutiger Zähler)	Protokoll (Eindeutiger Zähler)	Benutzername (Eindeutiger Zähler)	Ereignisanzahl (Summe)	Zähler ▼
10.9.8	Leistungsstatus	SAR Sentinel: recovered	127.0.0.1	0	System Notification-2...	Sonstige	Keine	93	93
10.9.8	Leistungseinbußen	SAR Sentinel: threshold crossed	127.0.0.1	0	System Notification-2...	Sonstige	Keine	84	84
10.9.8	Lizenzstatus	License Near Lock	127.0.0.1	0	System Notification-2...	Sonstige	Keine	40	40
127.0	Information	Auto-Update successful	127.0.0.1	0	System Notification-2...	Sonstige	Keine	7	7
127.0	Hinweis	Auto-Update successful download	127.0.0.1	0	System Notification-2...	Sonstige	Keine	2	2
10.9.8	Serviceunterbrechung	Unable to Determine Associated Log Source For IP Address	127.0.0.1	0	System Notification-2...	Sonstige	Keine	2	2

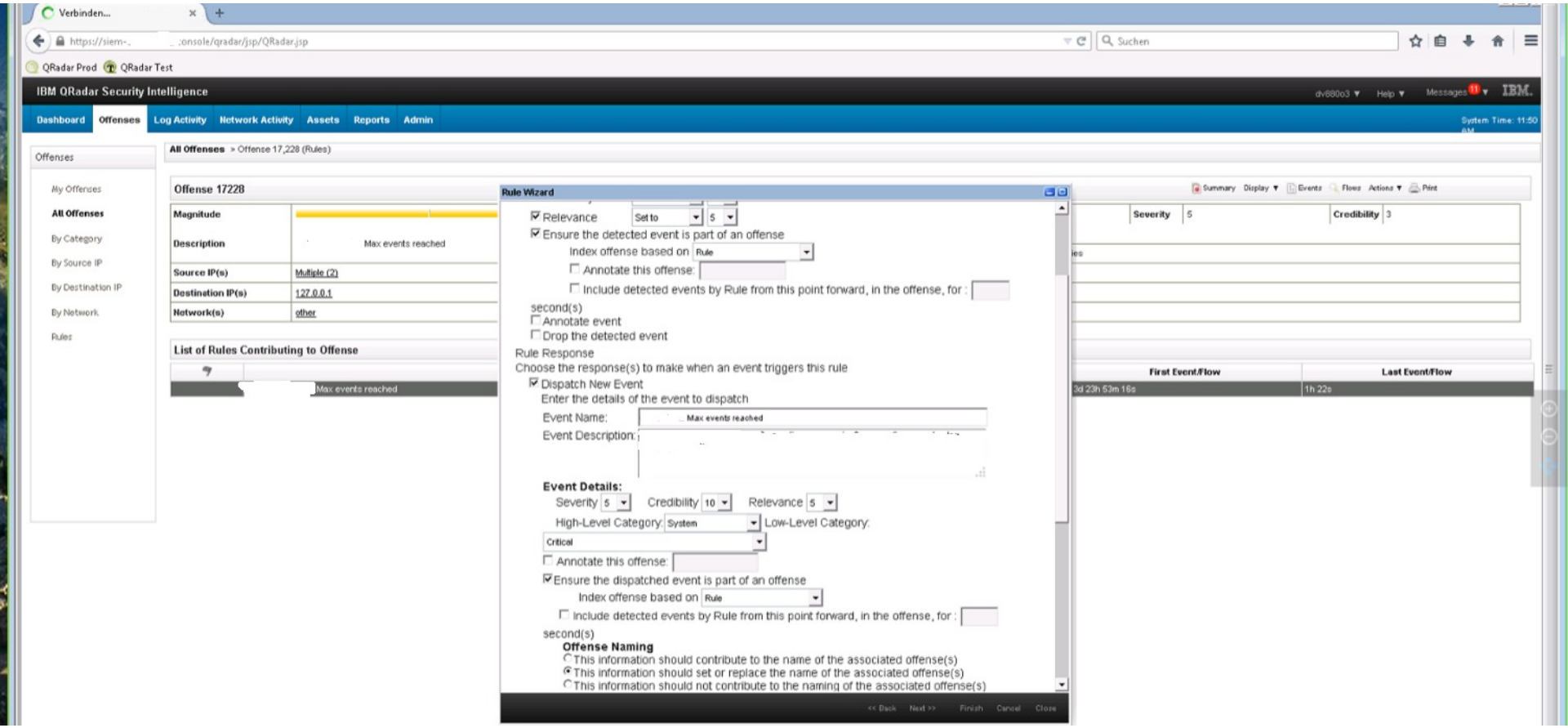
QR System Monitoring Labsystem 3



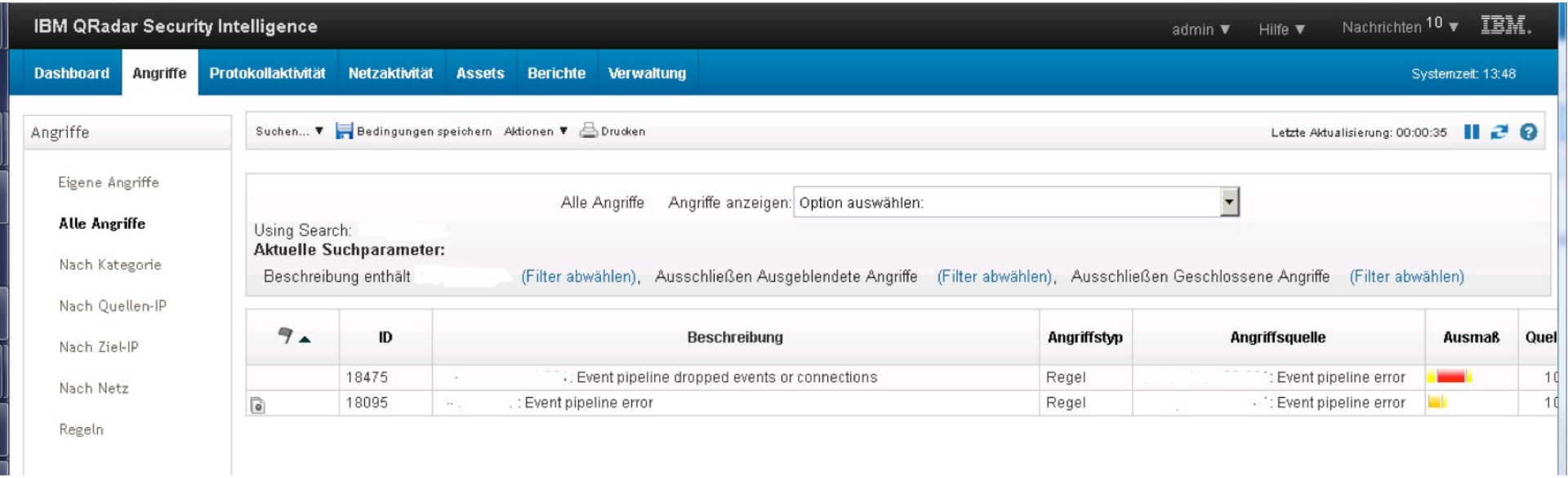
QR Beispielalarm - Summary



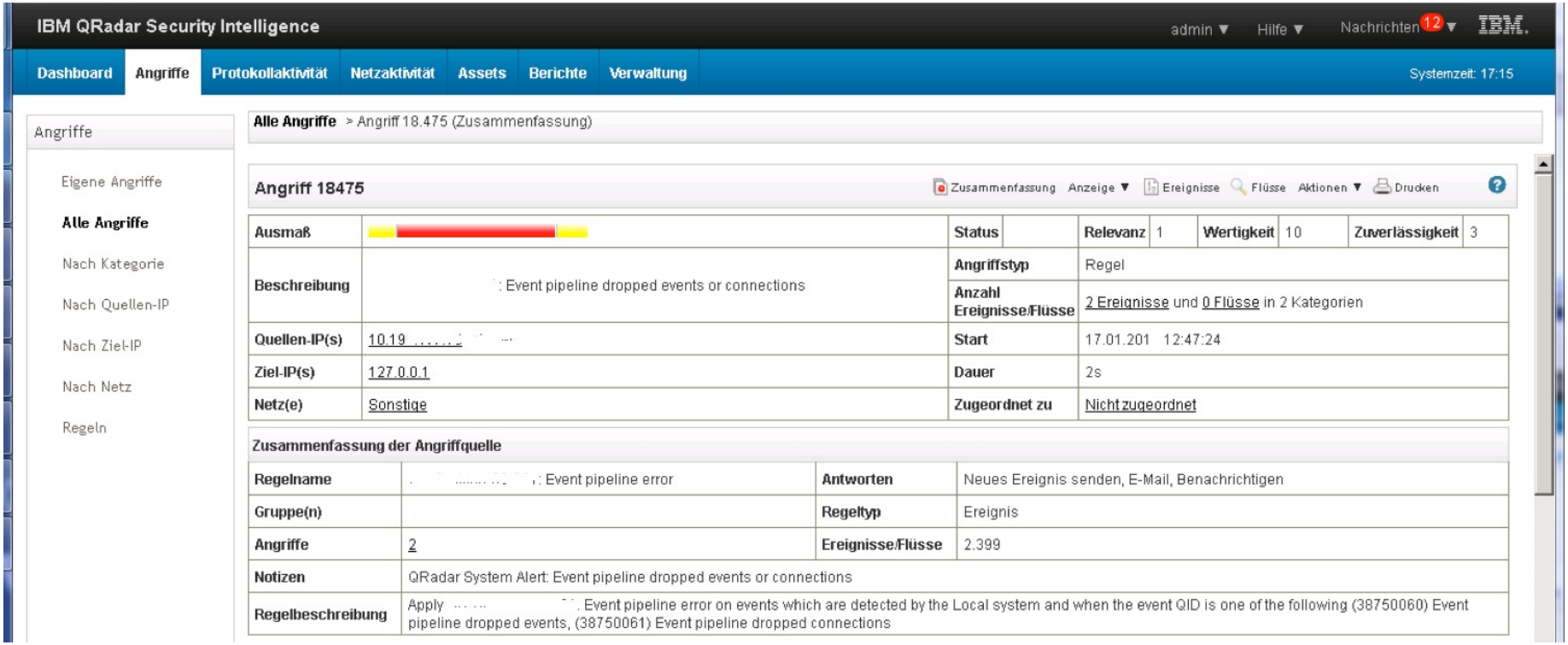
QR Beispielalarm - Regel



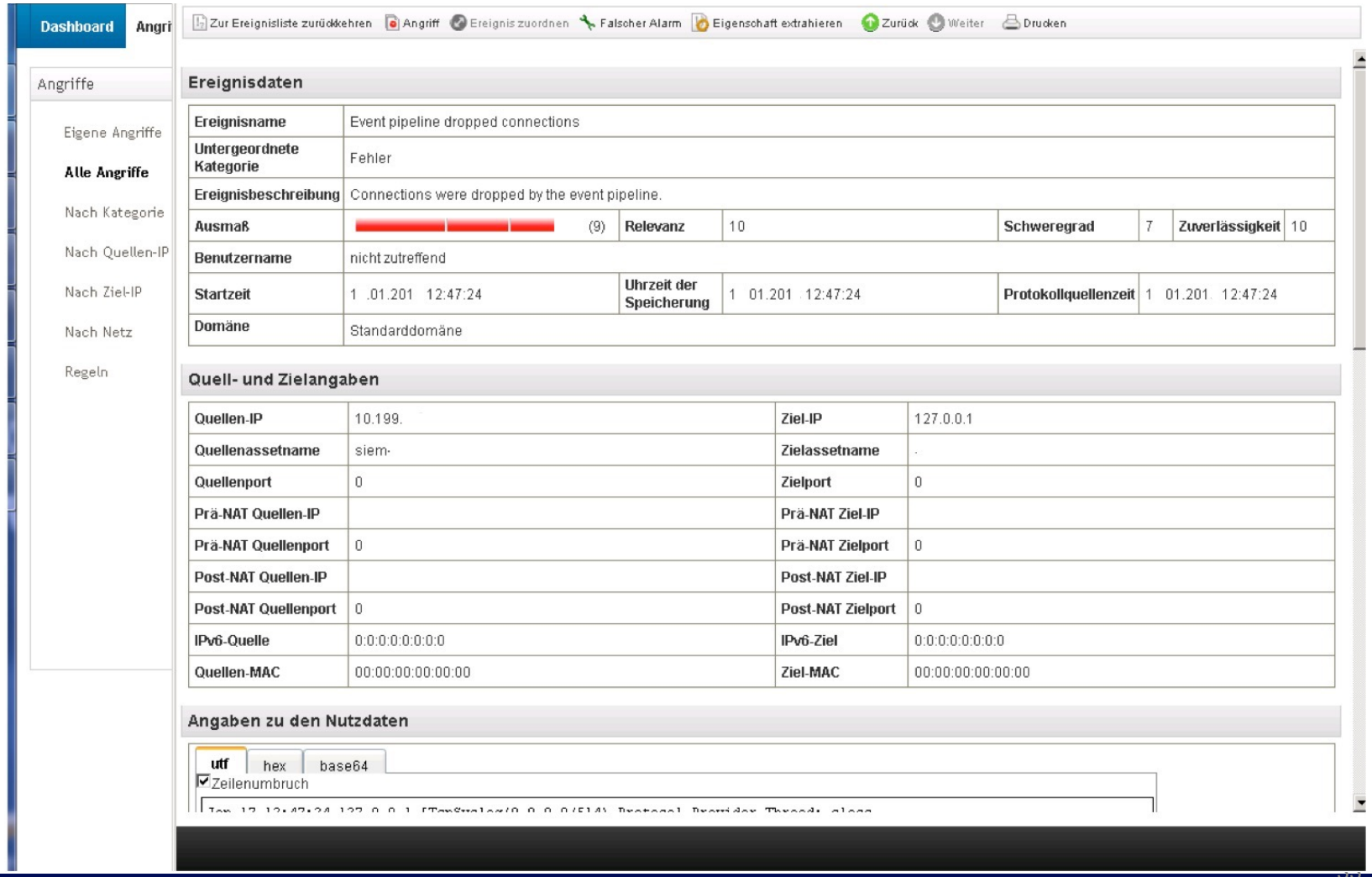
QR Beispielalarm - Alarmsearch



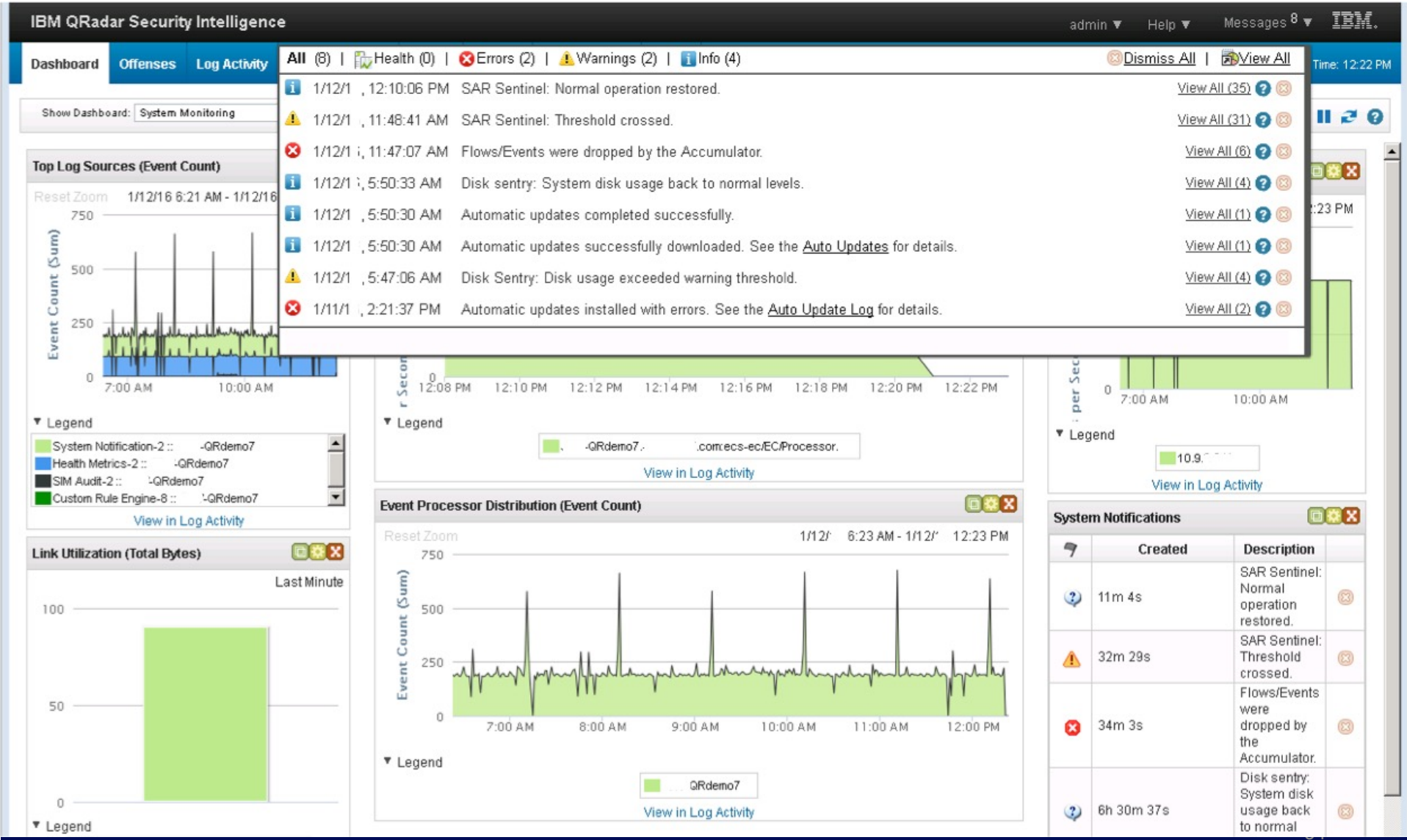
offense details



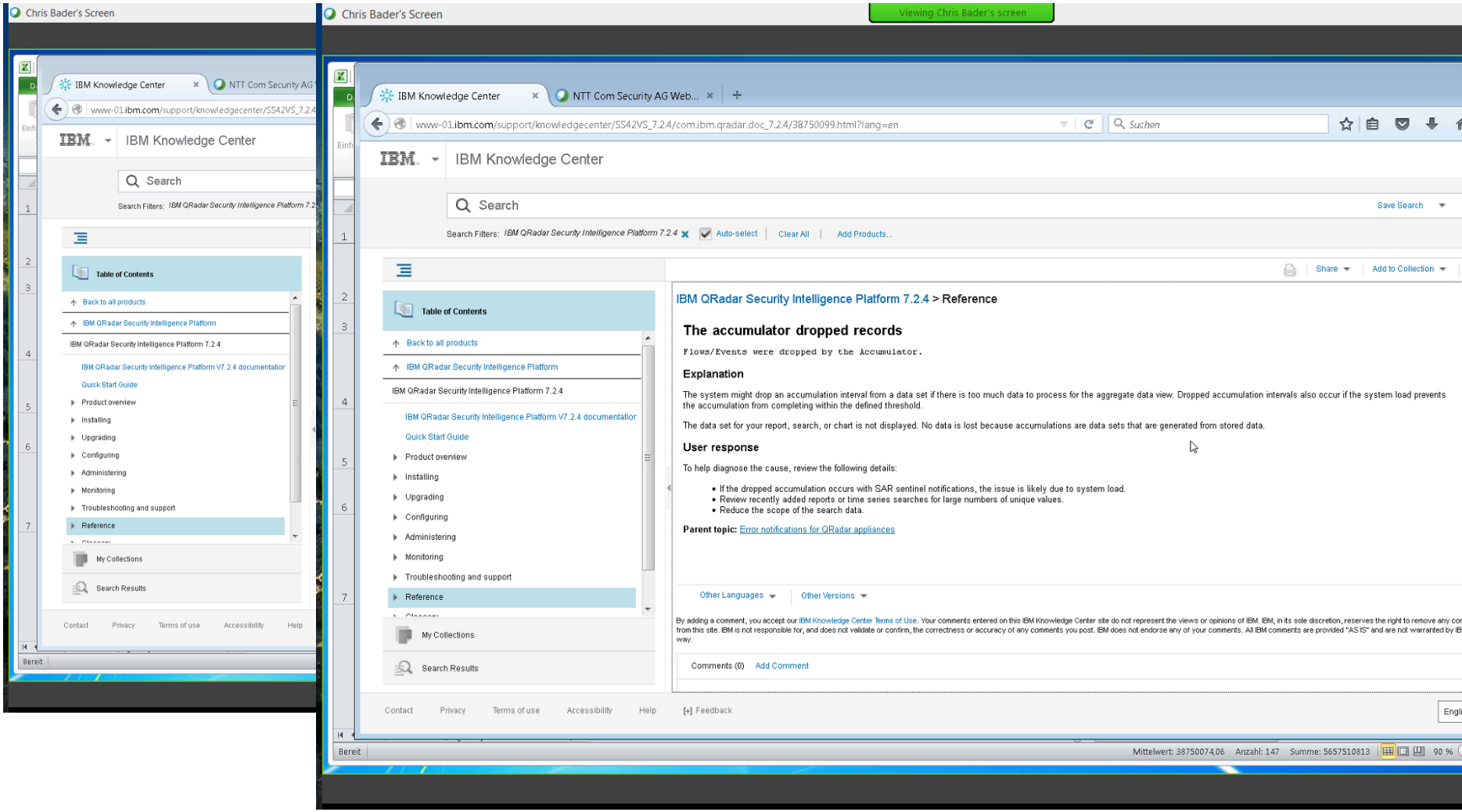
event details



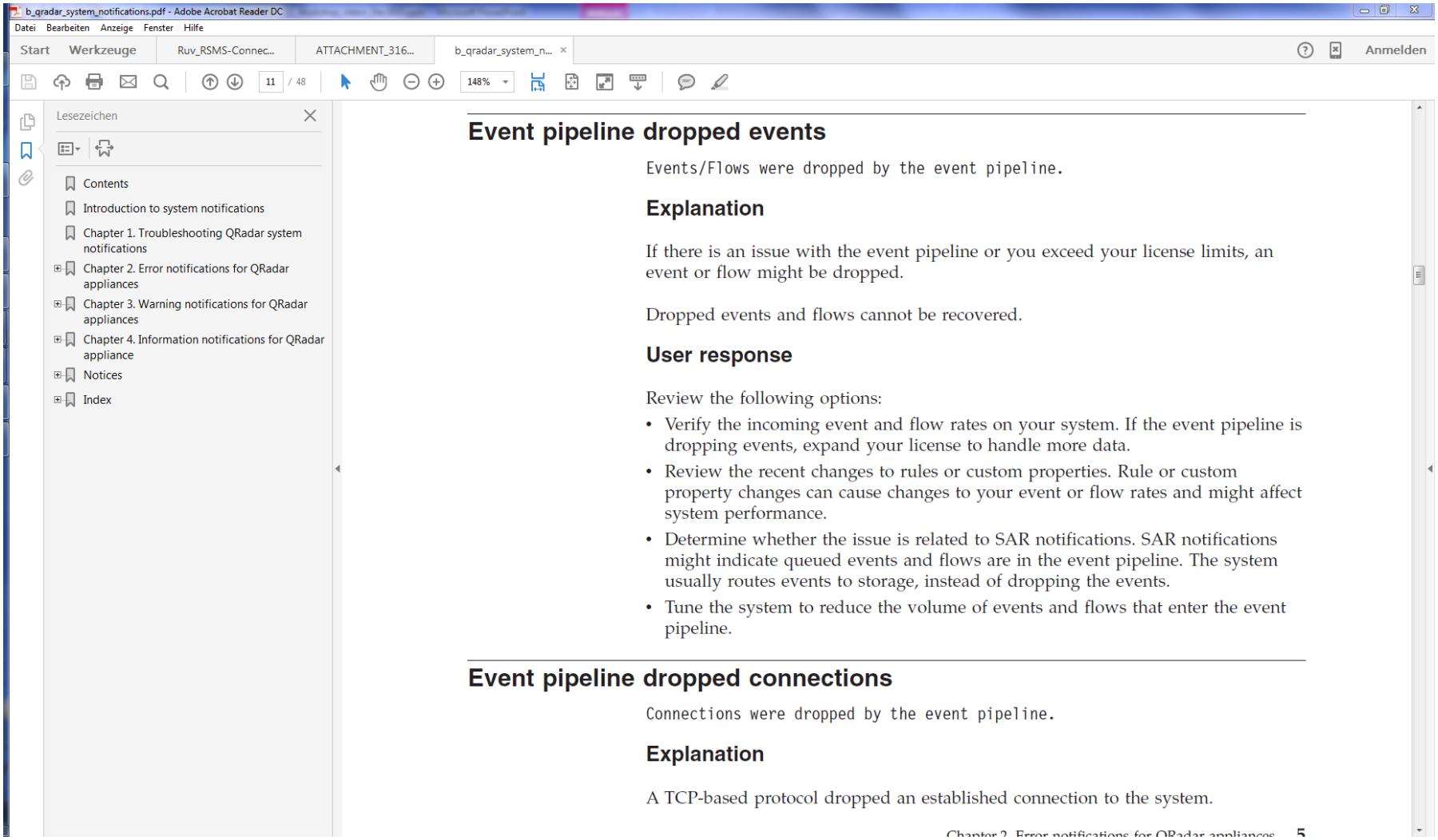
QR Beispiel Systemerror Labsystem



IBM Knowledgebase via Help



IBM System notifications



Event pipeline dropped events

`Events/Flows were dropped by the event pipeline.`

Explanation

If there is an issue with the event pipeline or you exceed your license limits, an event or flow might be dropped.

Dropped events and flows cannot be recovered.

User response

Review the following options:

- Verify the incoming event and flow rates on your system. If the event pipeline is dropping events, expand your license to handle more data.
- Review the recent changes to rules or custom properties. Rule or custom property changes can cause changes to your event or flow rates and might affect system performance.
- Determine whether the issue is related to SAR notifications. SAR notifications might indicate queued events and flows are in the event pipeline. The system usually routes events to storage, instead of dropping the events.
- Tune the system to reduce the volume of events and flows that enter the event pipeline.

Event pipeline dropped connections

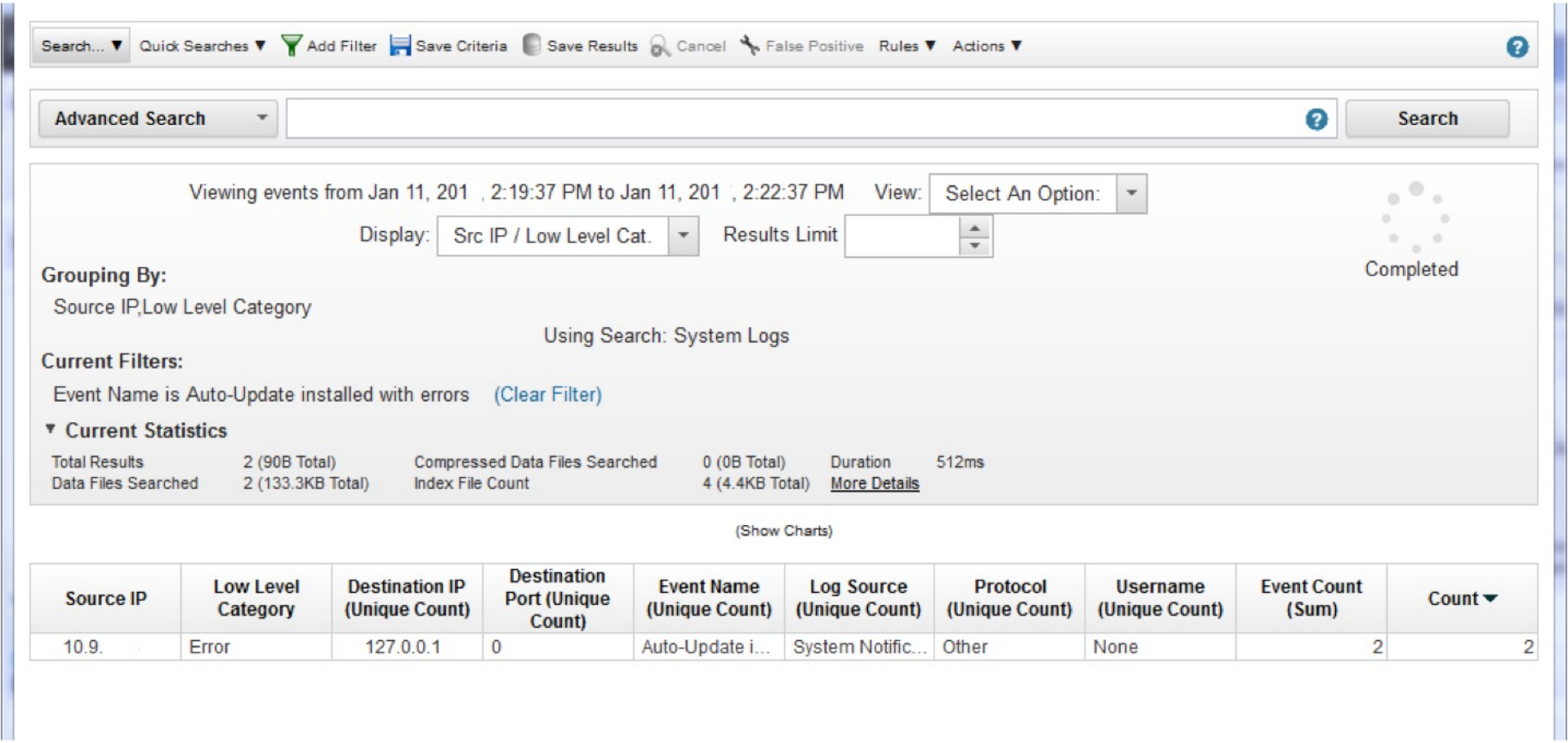
`Connections were dropped by the event pipeline.`

Explanation

A TCP-based protocol dropped an established connection to the system.

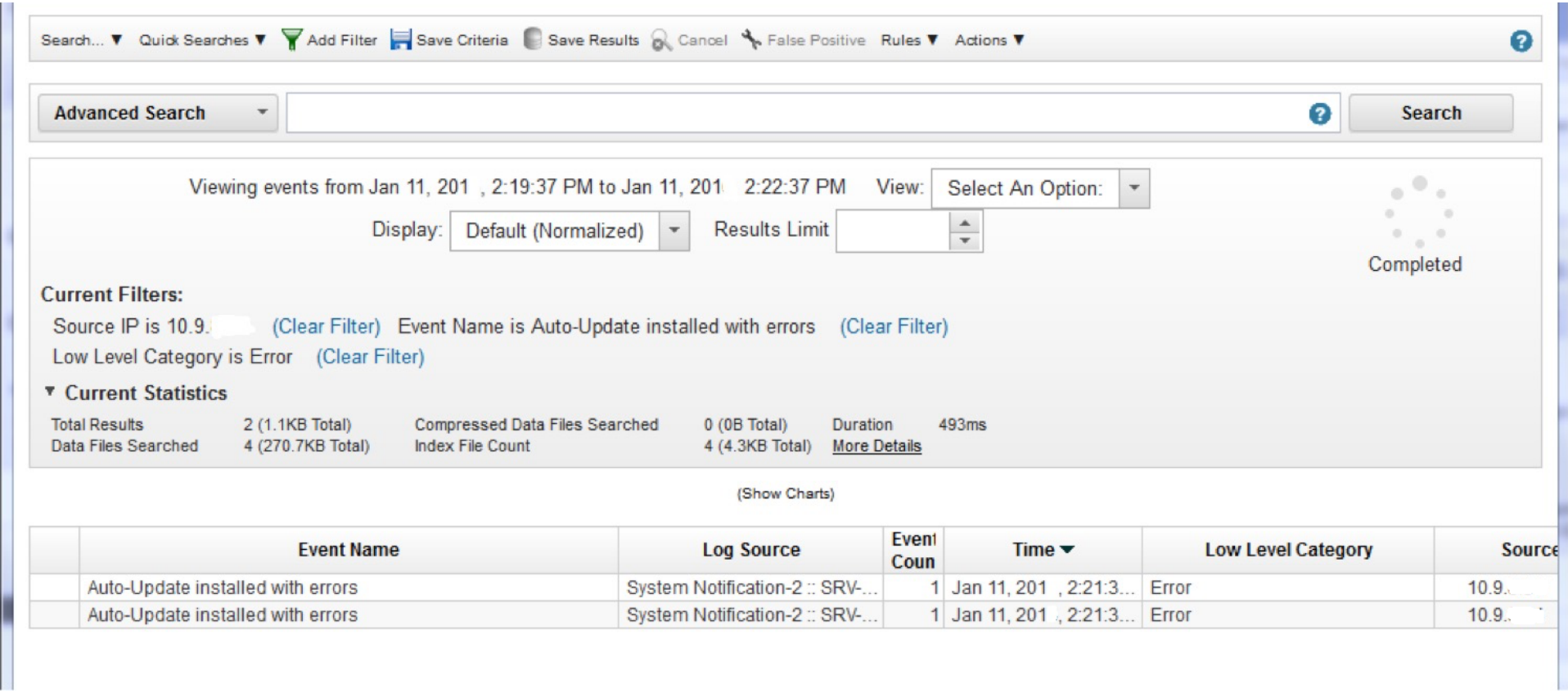
Chapter 2. Error notifications for QRadar appliances 5

Drilldown auto update error from dashboard 1



Source IP	Low Level Category	Destination IP (Unique Count)	Destination Port (Unique Count)	Event Name (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Event Count (Sum)	Count
10.9.	Error	127.0.0.1	0	Auto-Update i...	System Notific...	Other	None	2	2

Drilldown auto update error from dashboard 2



Drilldown auto update error from dashboard 3

Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print

Event Information

Event Name	Auto-Update installed with errors						
Low Level Category	Error						
Event Description	Automatic updates installed with errors. See the Auto Update Log for details.						
Magnitude	(9)	Relevance	10	Severity	7	Credibility	10
Username	N/A						
Start Time	Jan 11, 201 , 2:21:36 PM	Storage Time	Jan 11, 201 , 2:21:36 PM	Log Source Time	Jan 11, 201 , 2:21:36 PM		

Source and Destination Information

Source IP	10.9	Destination IP	127.0.0.1
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

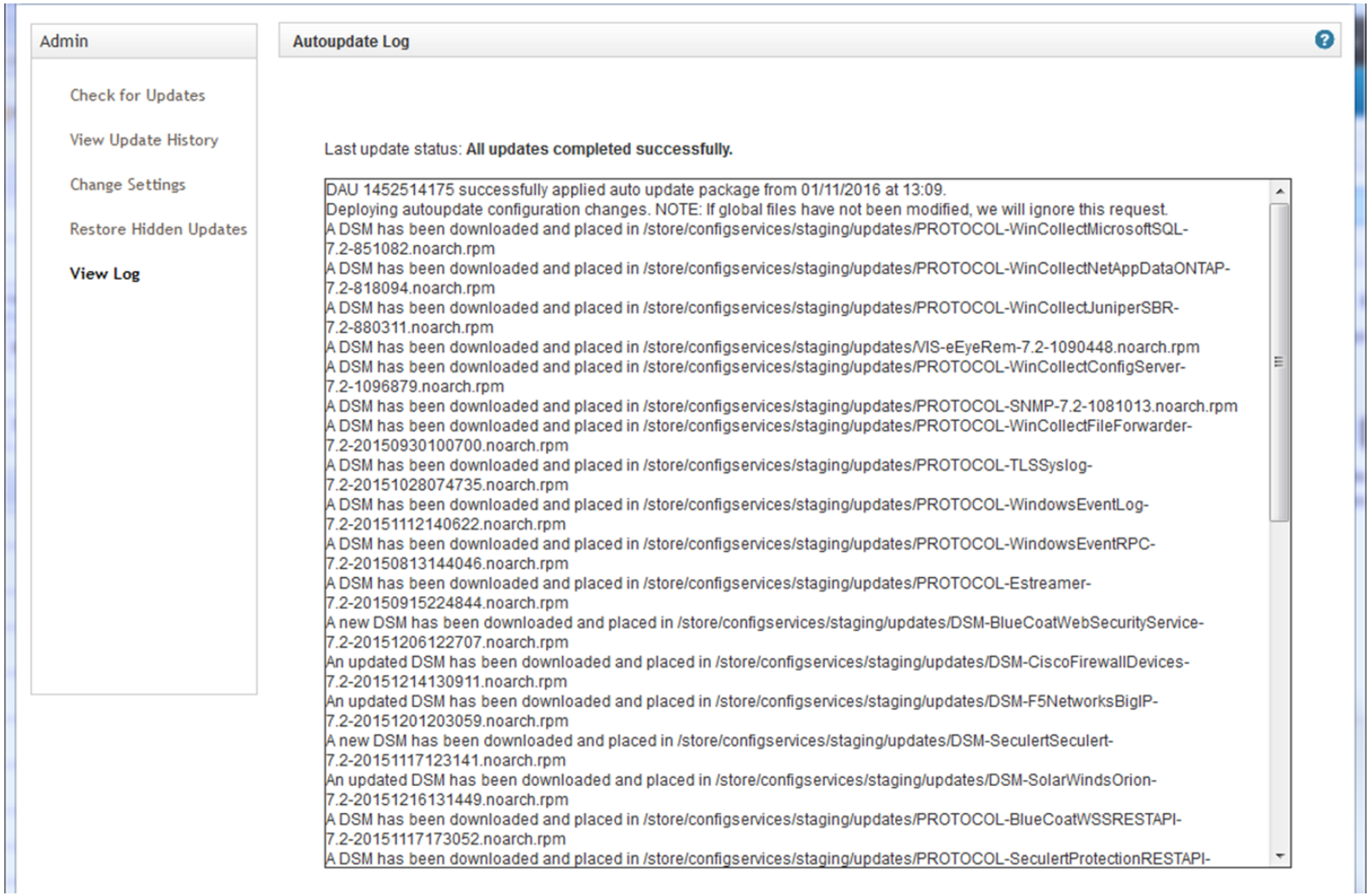
Payload Information

utf | hex | base64

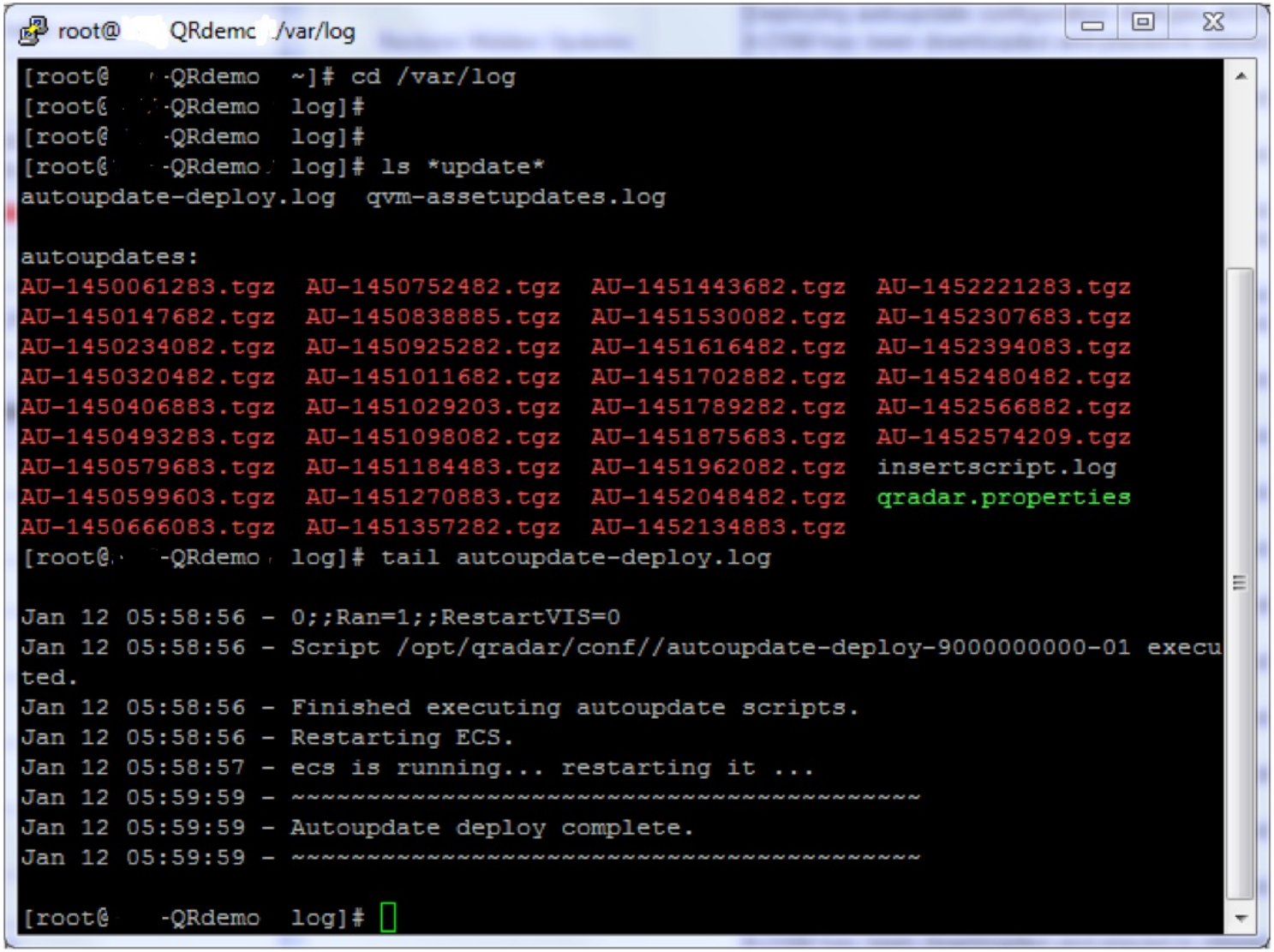
Wrap Text

```
Jan 11 14:21:36 127.0.0.1 [Thread-2610] com.q1labs.hostcontext.action.AutoUpdateQVMRPMAction: [WARN]
[NOT:0260004100][10.9.       -] [-/- -]A request was made to install autoupdate rpm /opt/qradar/conf/QVM-
Autoupdate-SQL-724-2015.12.31.x86_64.rpm but the rpm file is missing - check error logs
```

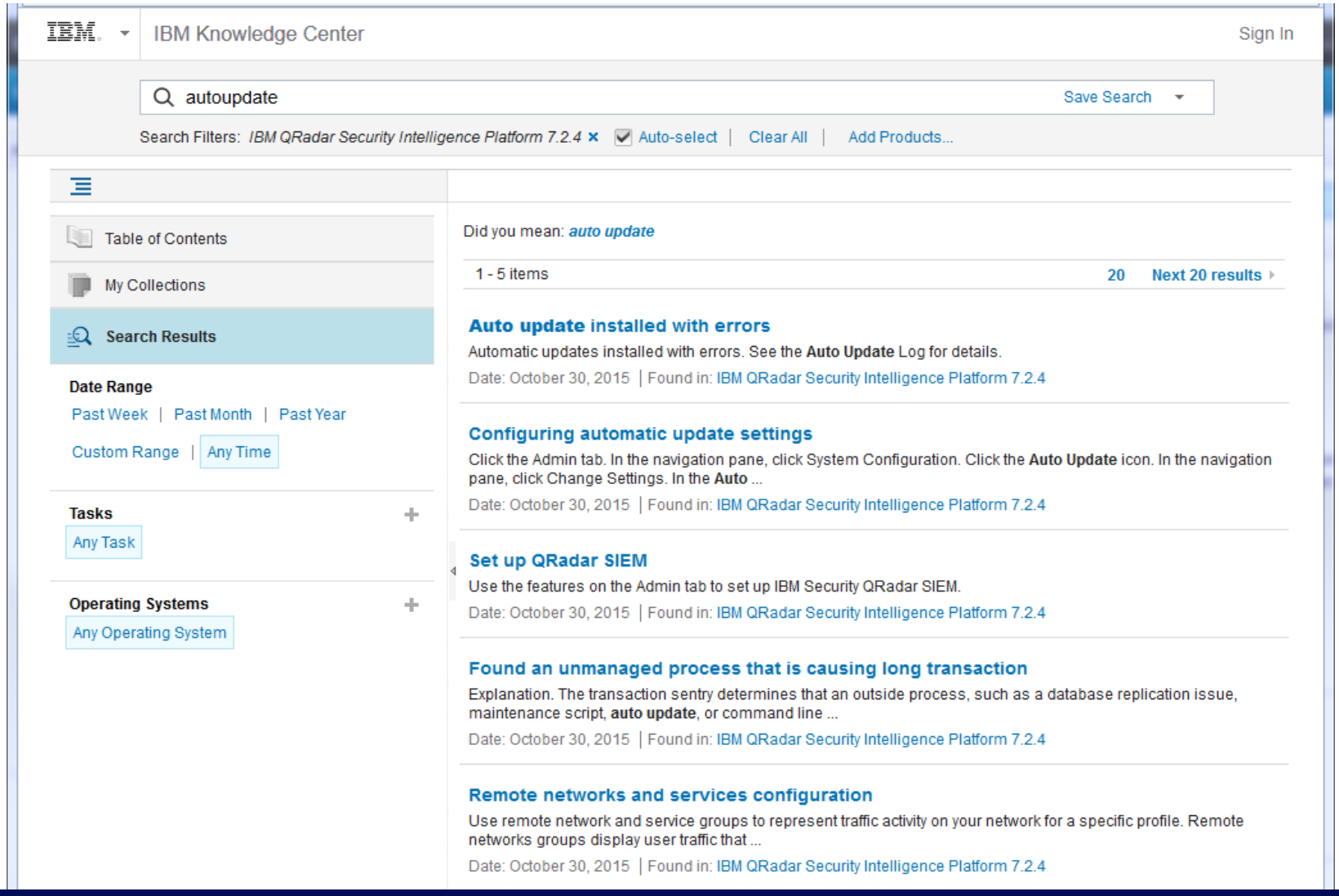
Autoupdate log



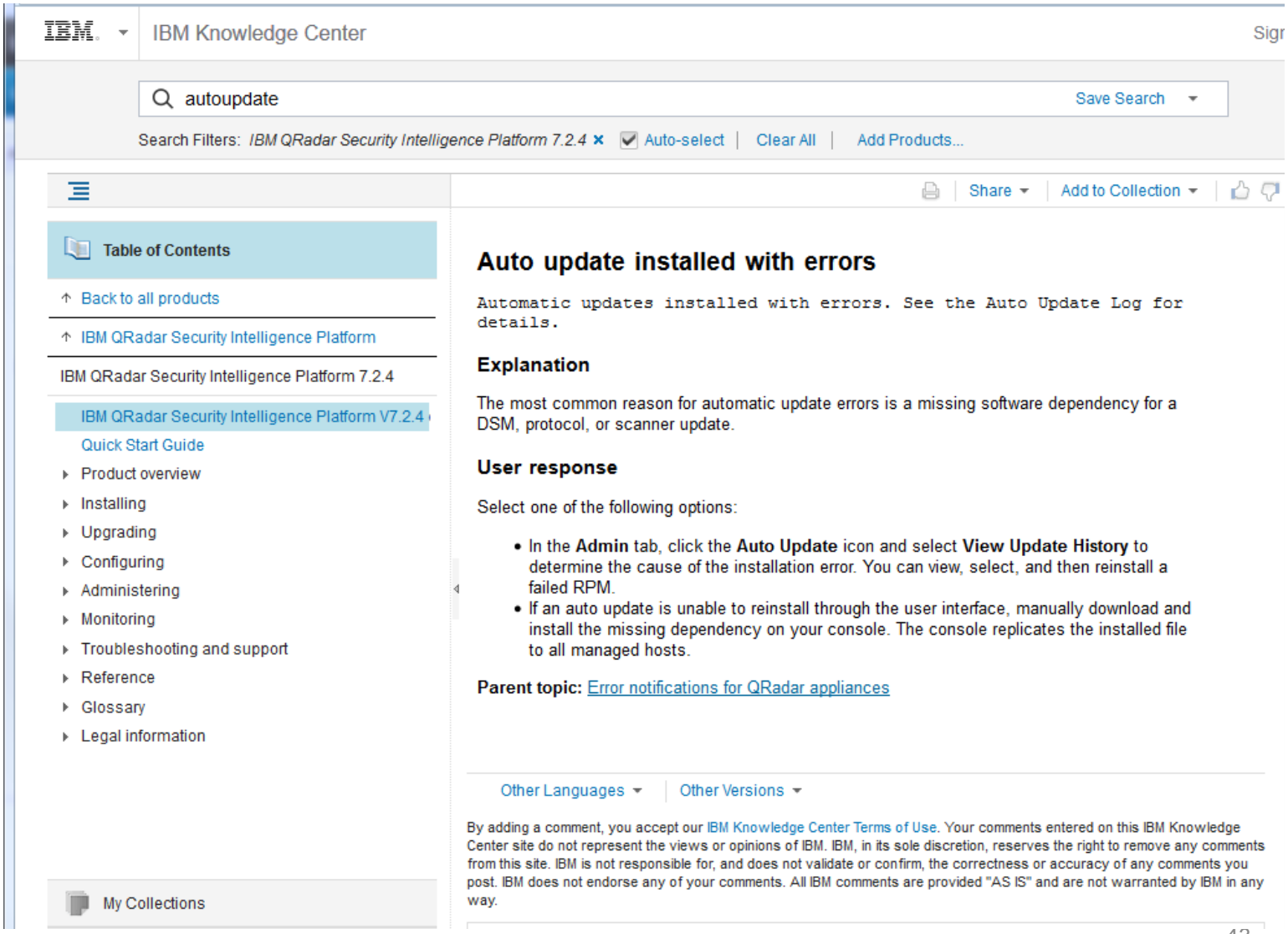
Trouble shooting auto update



auto update 2



auto update 3



Trouble Shooting

- IBM QRadar Dokumentation
- QRadar Help
- Log Activity

System (lokale IP)
SIM Audit

- QRadar_Troubleshooting_System_Notifications_Guide.pdf

b_qradar_system_notifications.pdf - Verkn,pfung.lnk

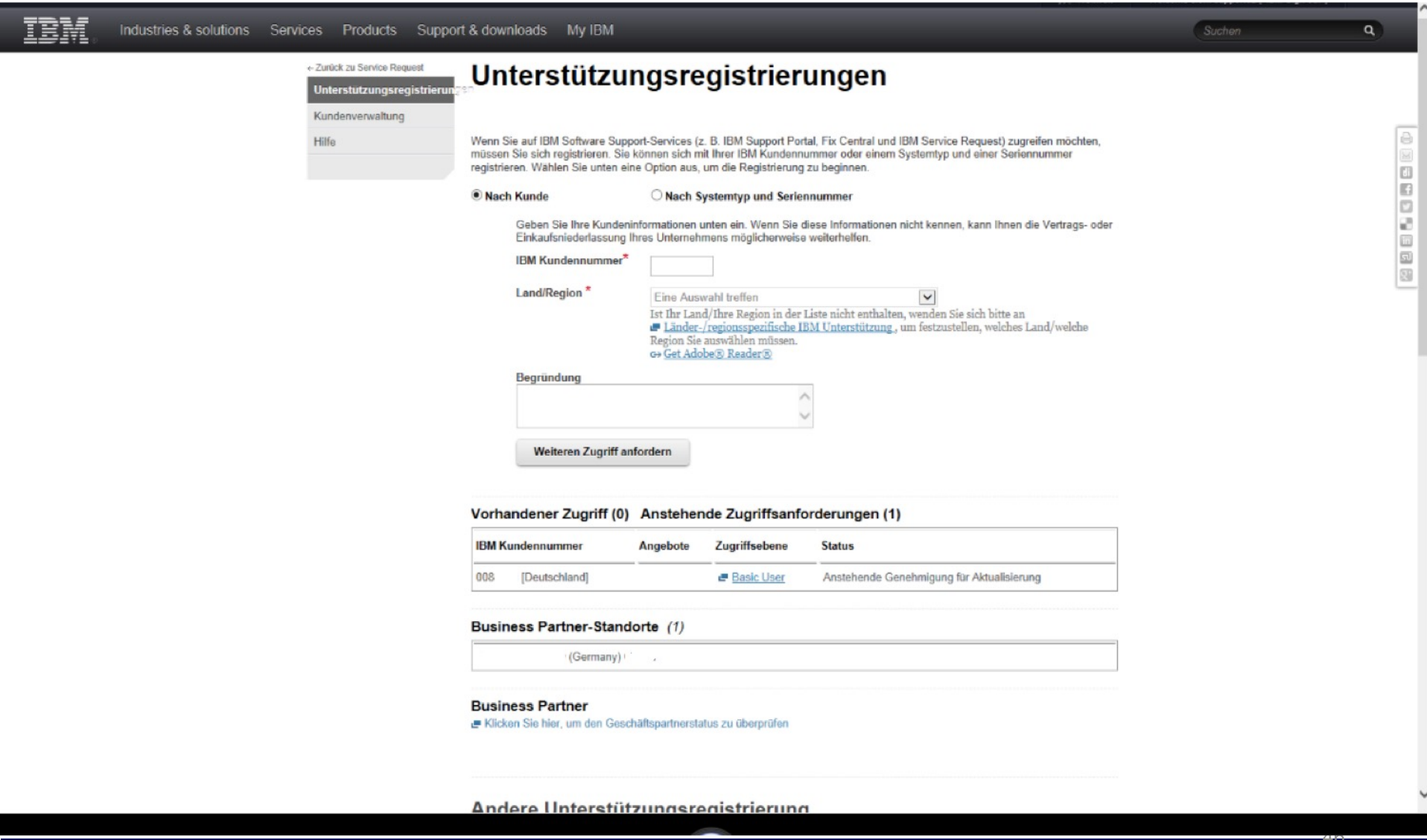
- CLI

/var/log/qradar.log
/var/log/qradar.error
/opt/qradar/support/get_logs.sh -s

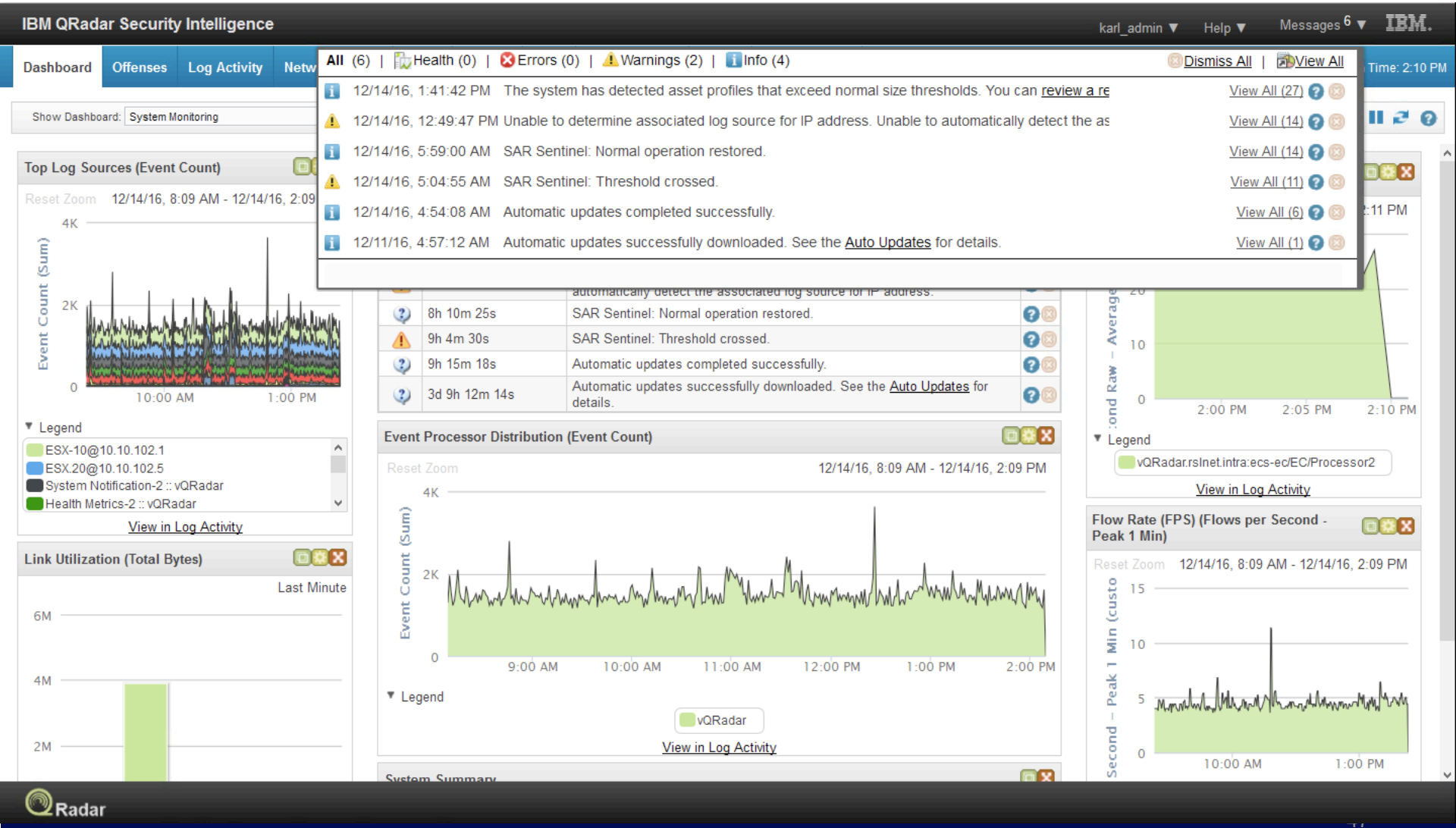
IBM SR (PMR)

- Support ICN
- Customer Contract
- SR Access right

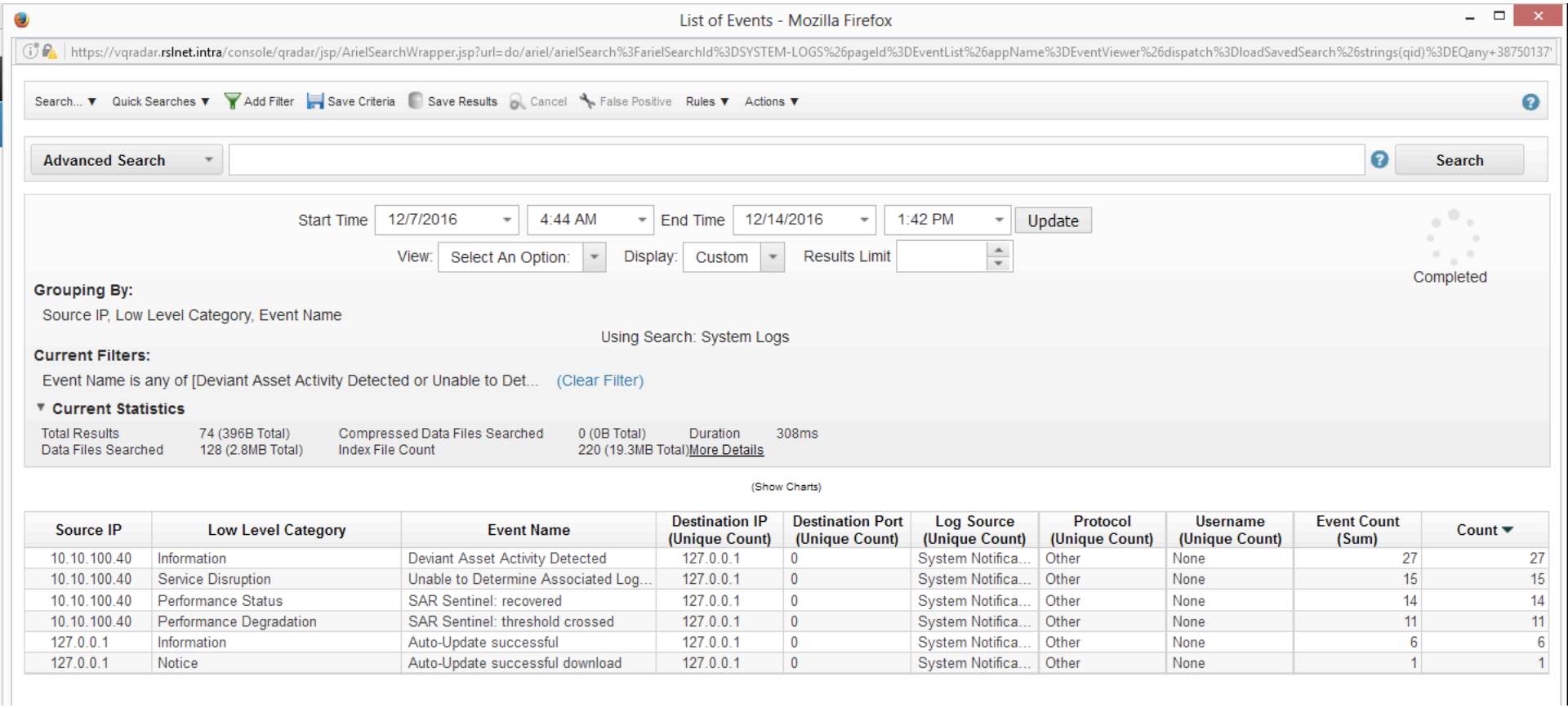
IBM SR (PMR)



health check messages

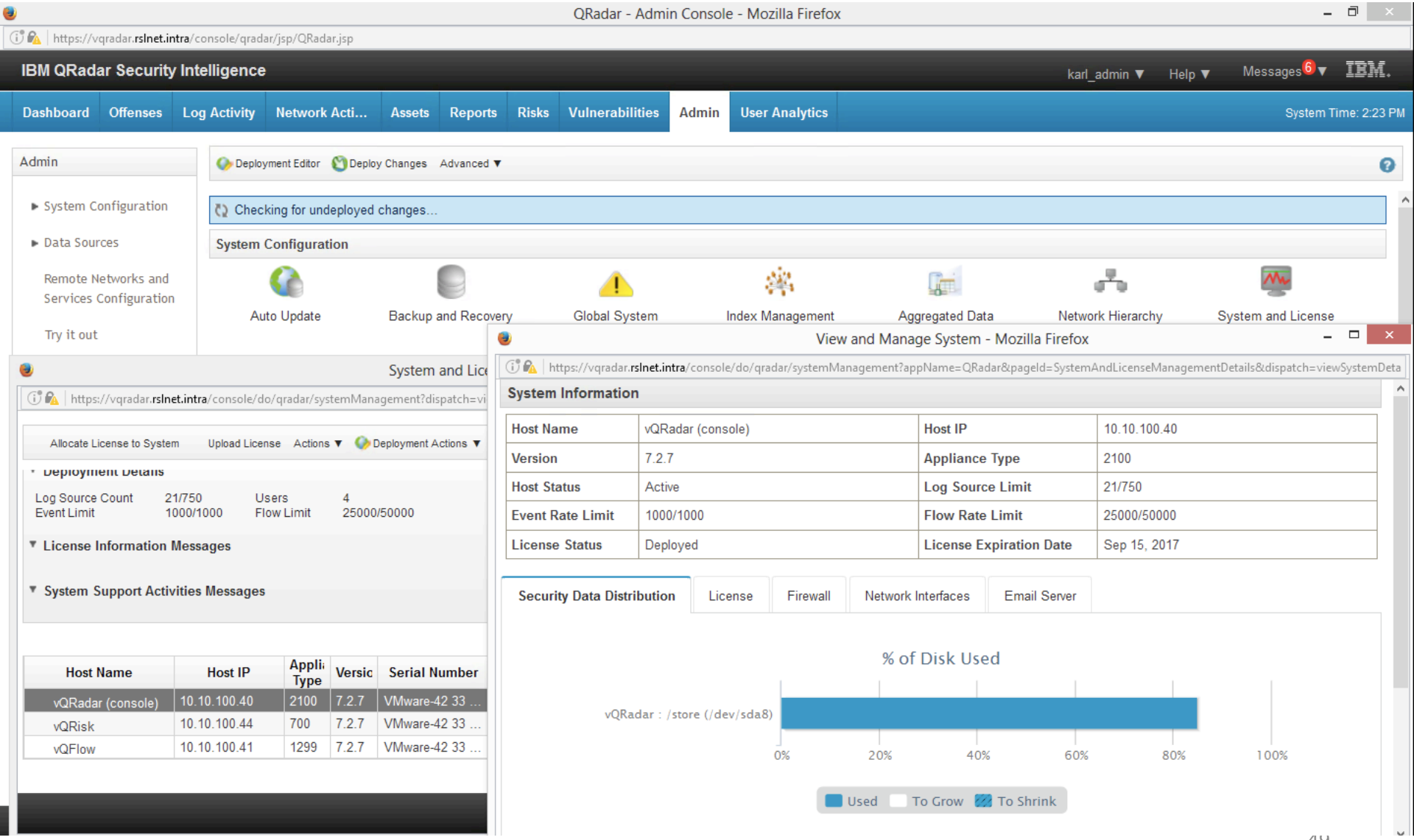


Prüfe Logaktivität

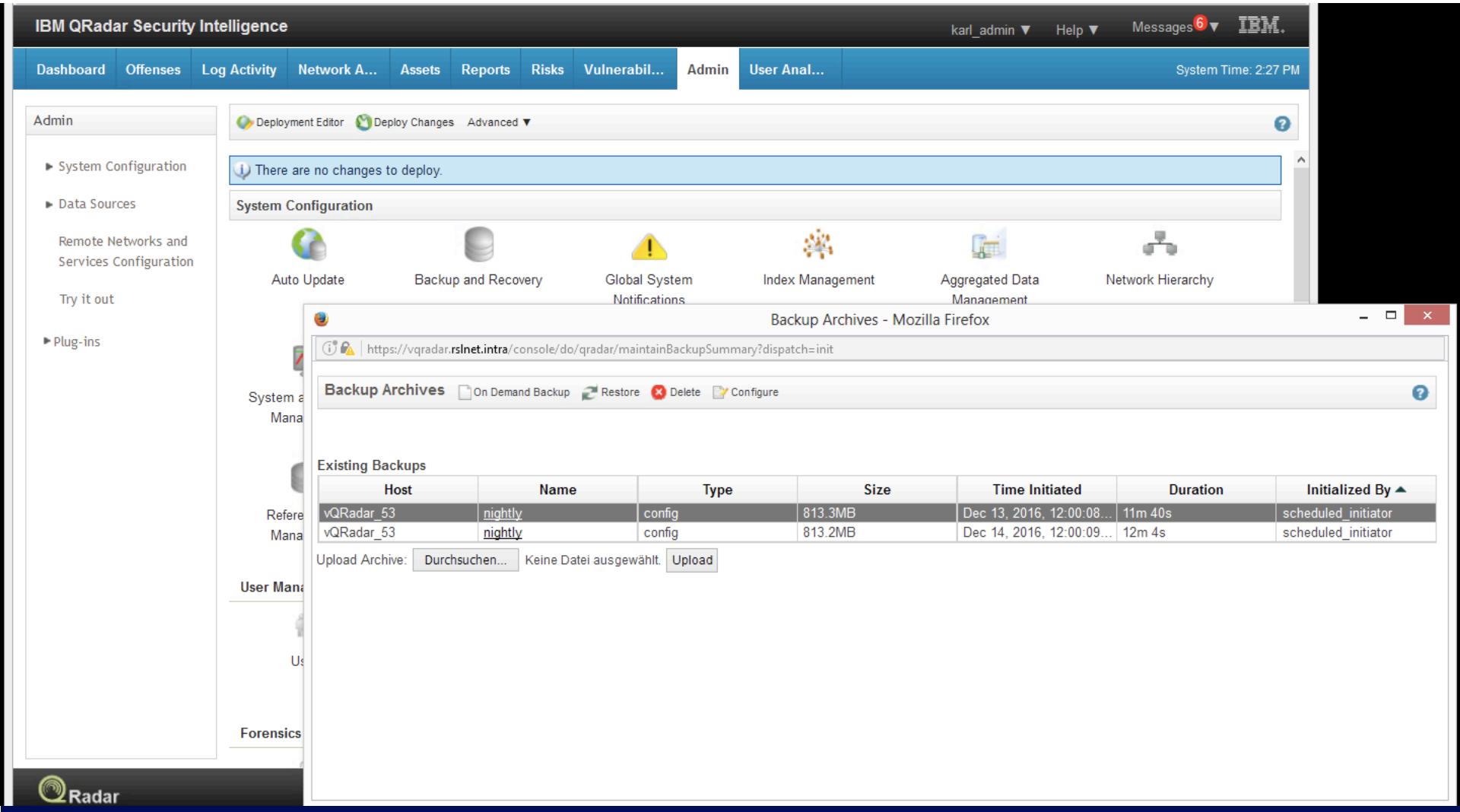


Source IP	Low Level Category	Event Name	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Protocol (Unique Count)	Username (Unique Count)	Event Count (Sum)	Count
10.10.100.40	Information	Deviant Asset Activity Detected	127.0.0.1	0	System Notifica...	Other	None	27	27
10.10.100.40	Service Disruption	Unable to Determine Associated Log...	127.0.0.1	0	System Notifica...	Other	None	15	15
10.10.100.40	Performance Status	SAR Sentinel: recovered	127.0.0.1	0	System Notifica...	Other	None	14	14
10.10.100.40	Performance Degradation	SAR Sentinel: threshold crossed	127.0.0.1	0	System Notifica...	Other	None	11	11
127.0.0.1	Information	Auto-Update successful	127.0.0.1	0	System Notifica...	Other	None	6	6
127.0.0.1	Notice	Auto-Update successful download	127.0.0.1	0	System Notifica...	Other	None	1	1

System Management

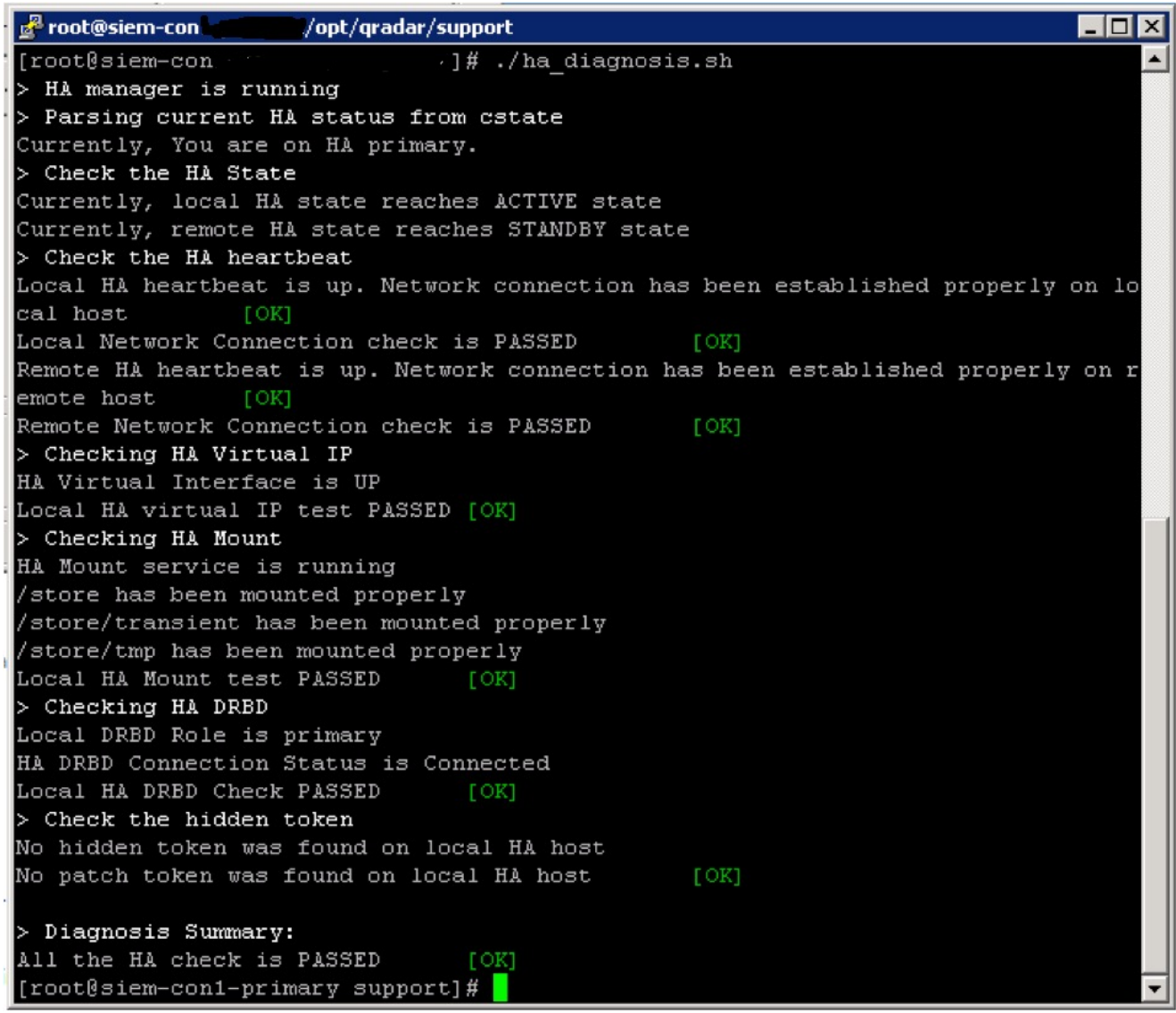


Backup

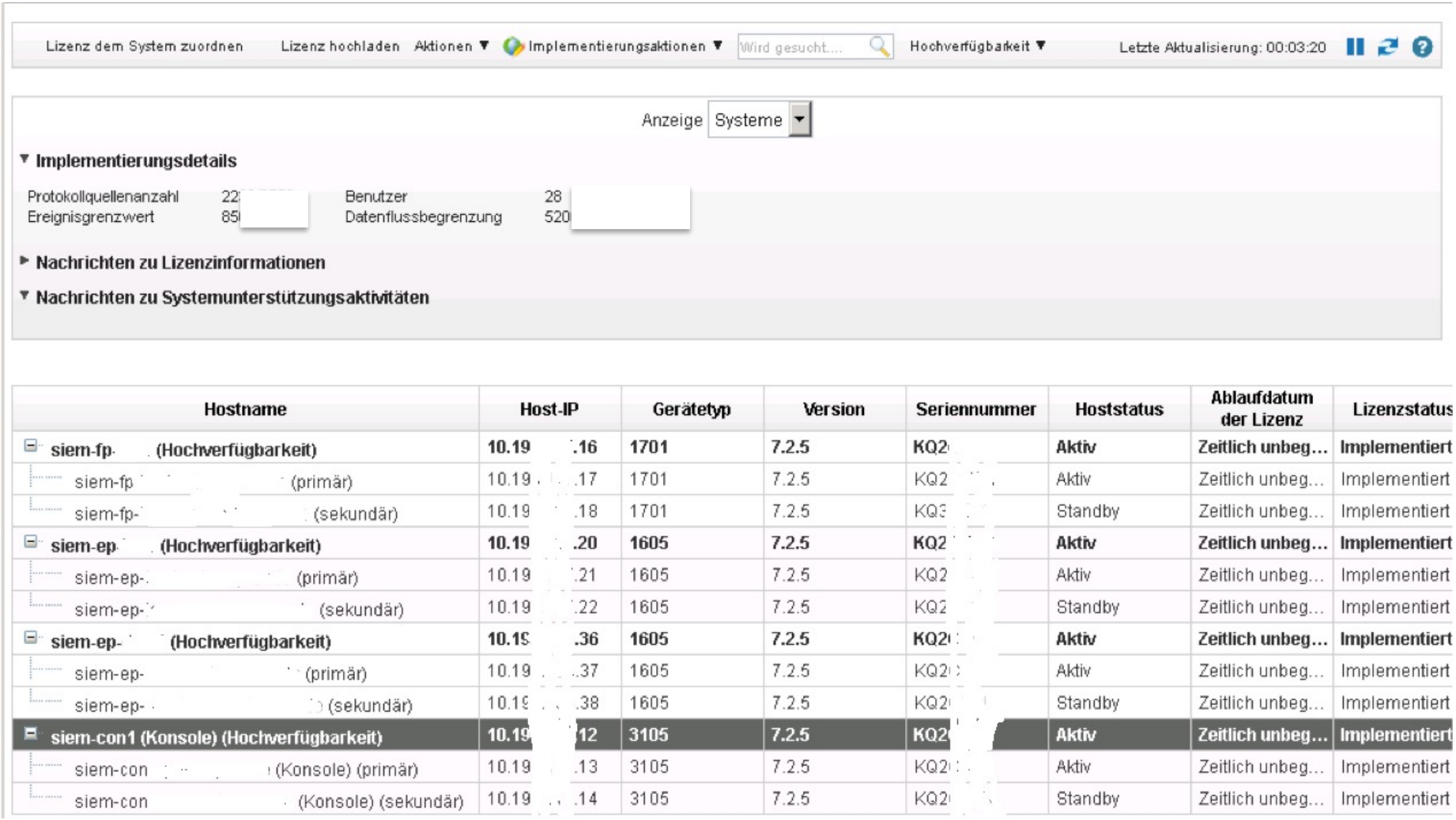


HA Status

cd /opt/qradar/support
./ha_diagnosis.sh



HA Status



Hostname	Host-IP	Gerätetyp	Version	Seriennummer	Hoststatus	Ablaufdatum der Lizenz	Lizenzstatus
siem-fp- (Hochverfügbarkeit)	**10.19 .16**	**1701**	**7.2.5**	**KQ2**	**Aktiv**	**Zeitlich unbeg...**	**Implementiert**
siem-fp (primär)	10.19 .17	1701	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-fp- (sekundär)	10.19 .18	1701	7.2.5	KQ3	Standby	Zeitlich unbeg...	Implementiert
siem-ep (Hochverfügbarkeit)	**10.19 .20**	**1605**	**7.2.5**	**KQ2**	**Aktiv**	**Zeitlich unbeg...**	**Implementiert**
siem-ep- (primär)	10.19 .21	1605	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-ep- (sekundär)	10.19 .22	1605	7.2.5	KQ2	Standby	Zeitlich unbeg...	Implementiert
siem-ep- (Hochverfügbarkeit)	**10.19 .36**	**1605**	**7.2.5**	**KQ2**	**Aktiv**	**Zeitlich unbeg...**	**Implementiert**
siem-ep- (primär)	10.19 .37	1605	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-ep- (sekundär)	10.19 .38	1605	7.2.5	KQ2	Standby	Zeitlich unbeg...	Implementiert
siem-con1 (Konsole) (Hochverfügbarkeit)	**10.19 12**	**3105**	**7.2.5**	**KQ2**	**Aktiv**	**Zeitlich unbeg...**	**Implementiert**
siem-con (Konsole) (primär)	10.19 .13	3105	7.2.5	KQ2	Aktiv	Zeitlich unbeg...	Implementiert
siem-con (Konsole) (sekundär)	10.19 .14	3105	7.2.5	KQ2	Standby	Zeitlich unbeg...	Implementiert