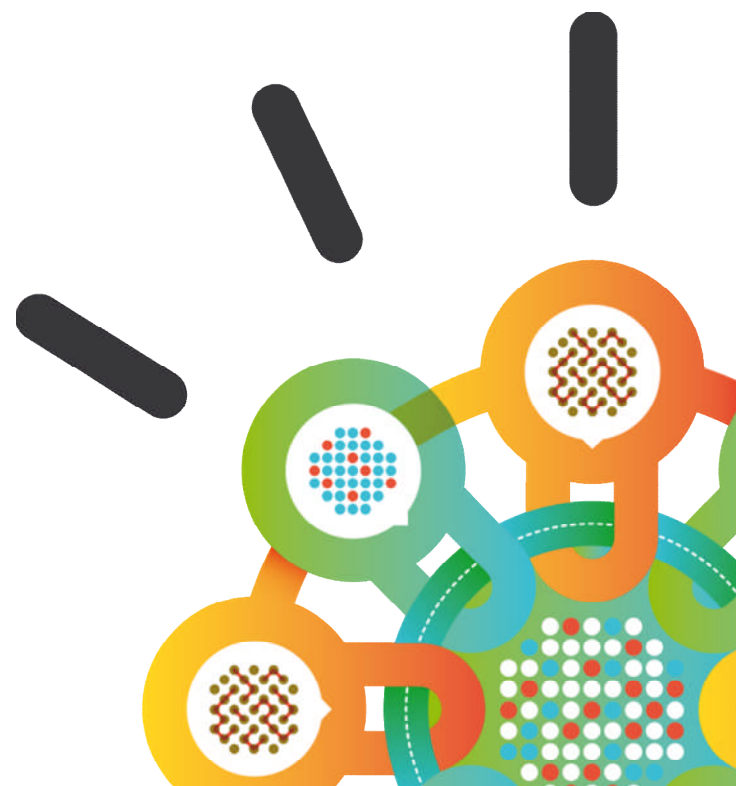


Security Intelligence.  
Think Integrated.

## IBM Security – Lab Services für QRadar

Serviceangebote für ein QRadar SIEM  
Deployment in 10 bzw. 15 Tagen

28.01.2015



# Agenda

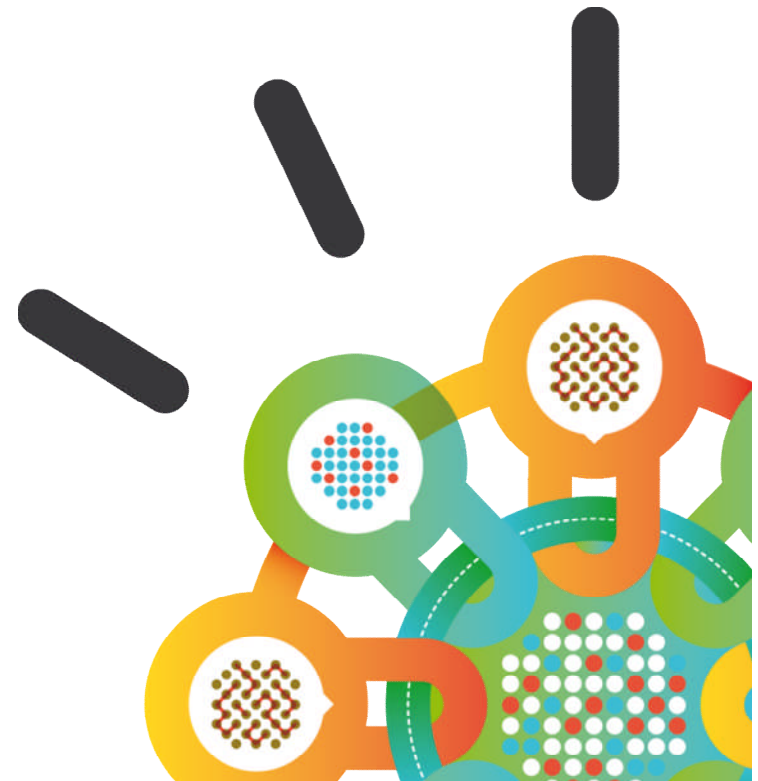
## 1 Inhalt der angebotenen Leistungen

- Allgemeines
- Erbrachte Leistungen

## 2 Zusatzleistungen

- Einrichtung von Hochverfügbarkeit
- Custom universal Device Support Module

## 3 IBM Preise

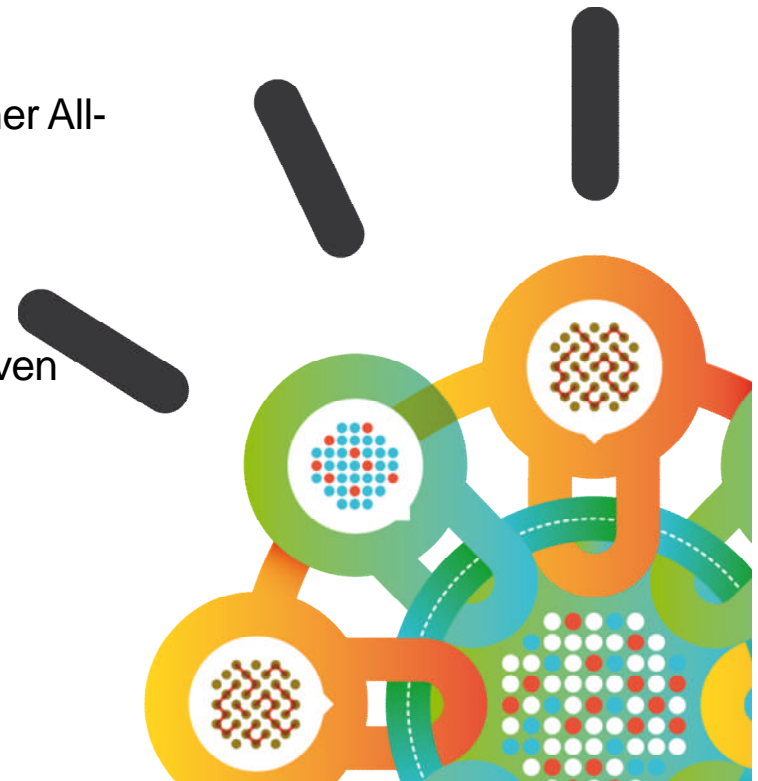


# Inhalt der angebotenen Leistungen



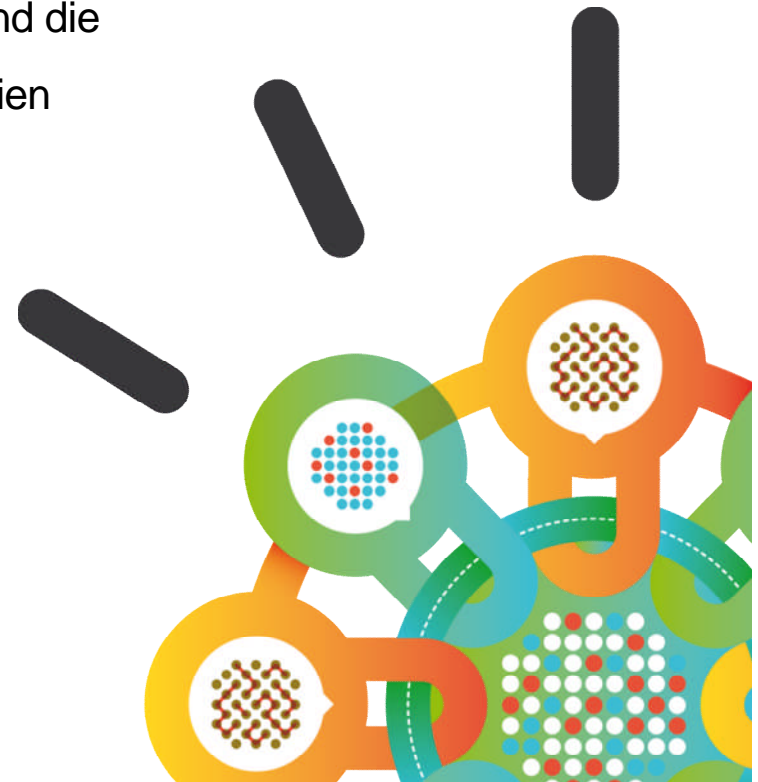
## Allgemeines

- Verfügbar für die aktuellen Appliances
- Empfohlen für alle neuen QRadar Installationen
- Unterstützung bei der Installation und dem Deployment einer All-In-One Appliance
- Erstellung einer Basiskonfiguration, welche für den operativen Betrieb erforderlich ist



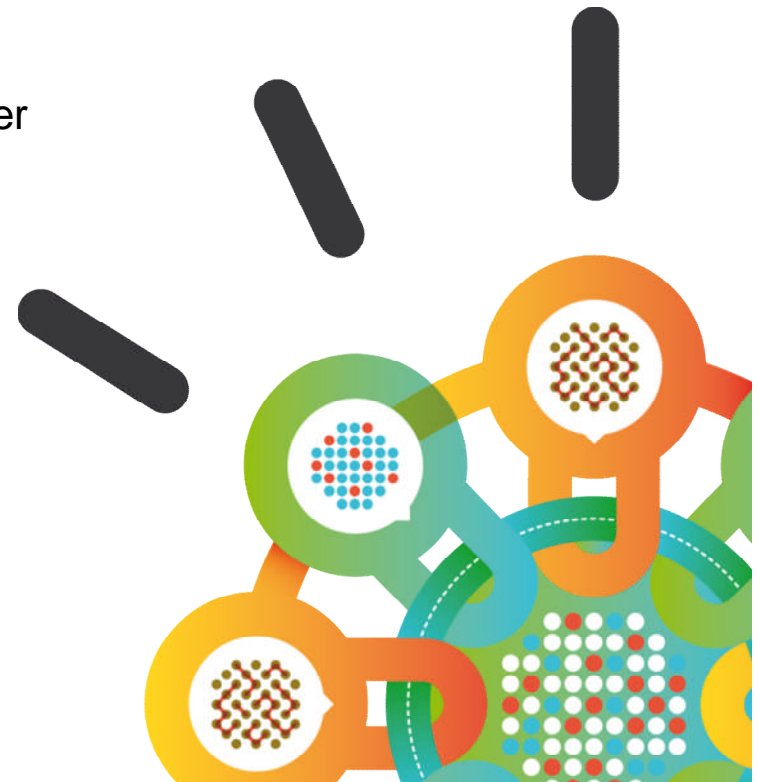
## Allgemeines

- QRadar SIEM ermöglicht einen tiefen Einblick in Netzwerk-, Anwender- und Anwendungsaktivitäten
- Ermöglicht das Sammeln, Normalisieren, die Korrelation und die sichere Aufbewahrung von Events, Flows, Assets, Topologien und Schwachstellen
- Verdächtige Vorgänge und Regelverletzungen werden als Angriffe (Offenses) hervorgehoben



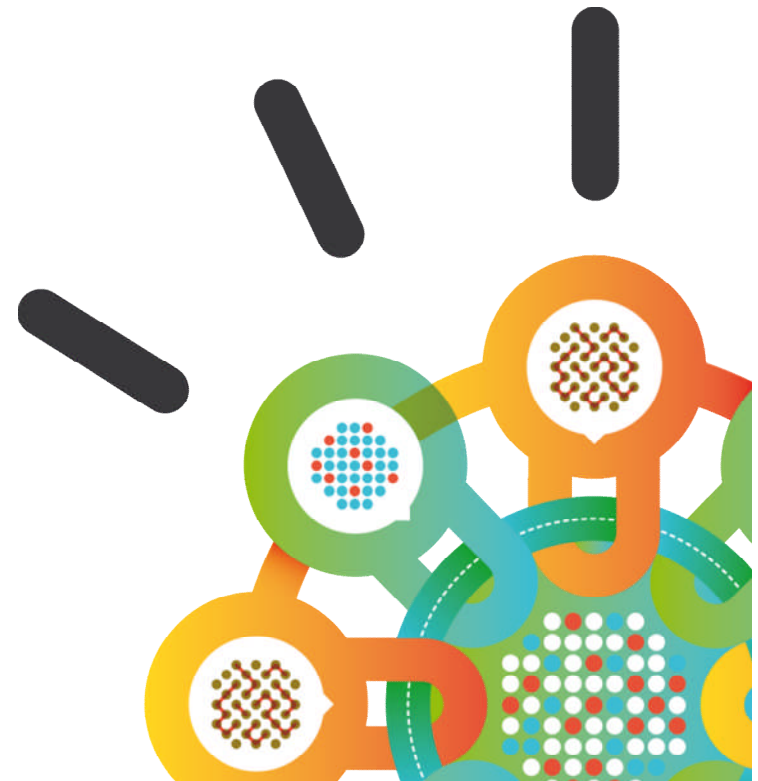
## Erbrachte Leistungen

- Inbetriebnahme der Server Appliance
- Initialisierung und Systemkonfiguration
- Erläuterung der grundlegenden Prinzipien zum Betrieb einer QRadar Appliance
- Initiale Konfiguration der Offense-Management Assets und der Custom Rules



## Erbrachte Leistungen

- Zwei Variationen können erworben werden
  - 10 Personentage: Small Deployment, bis zu 3 Managed Hosts
  - 15 Personentage: Medium Deployment, bis zu 7 Managed Hosts
  
- Das Angebot beinhaltet u.a.:
  - Für das Small Deployment bis zu 3 Managed Hosts und 2 Event Prozessoren
  - Für das Medium Deployment bis zu 7 Managed Hosts
  - Implementierung von zusätzlichem Tuning (z.B. Custom Rules, Searches, Reports oder externem Storage)



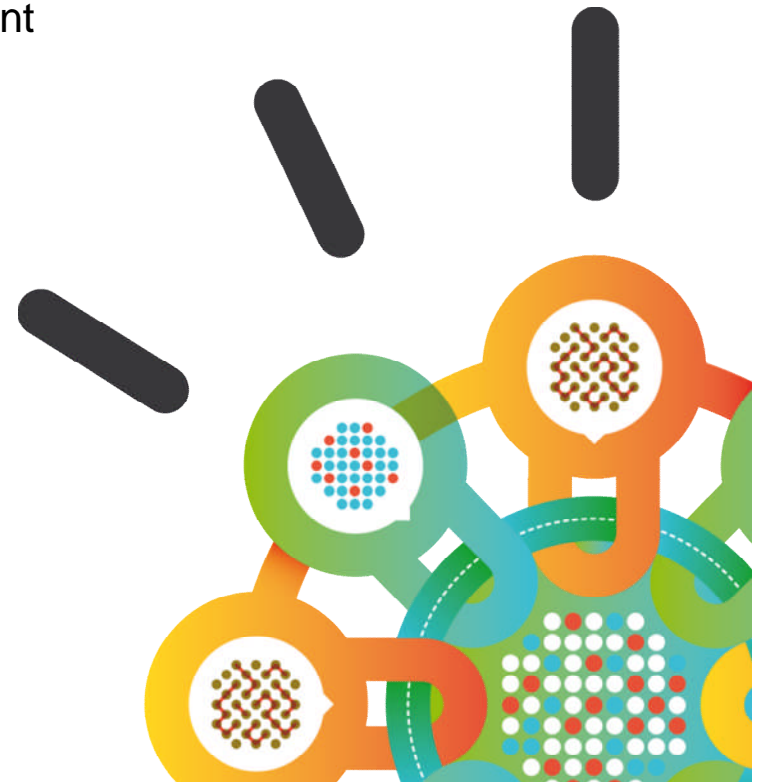
# Zusatzleistungen





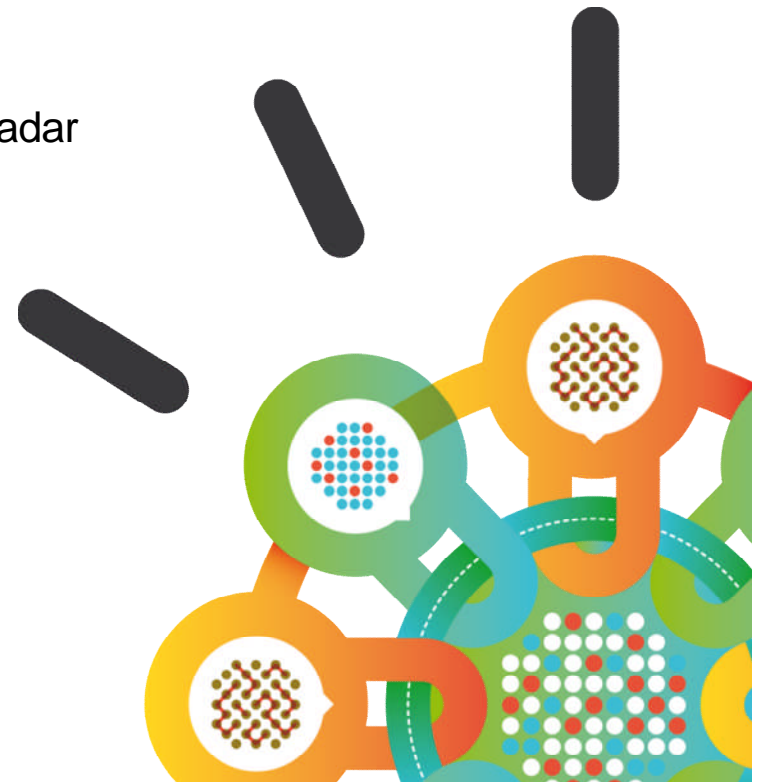
## Einrichtung von Hochverfügbarkeit

- Option der Hochverfügbarkeit kann mit anderen Deployment Angeboten kombiniert werden
- Service fokussiert auf die Konfiguration und das Deployment einer hochverfügbaren, sekundären Appliance
- 2 Dienstleistungen werden erbracht:
  - Installation der hochverfügbaren sekundären Server Appliance
  - Initialisierung und Konfiguration des HA Systems
- Umfang: 2 Personentagen



## Custom universal Device Support Module (uDSM)

- Unterstützung bei der Anlage eines uDSM
- Leistung umfasst:
  - Aufbau, Konfiguration und Mapping eines uDSM
- Kundenspezifisches uDSM ermöglicht das Parsen nicht standardisierter Logsources-Typen zur Verarbeitung in QRadar (remote erbracht)
- Festpreisangebot, welches sich auf eine uDSM bezieht
- Dienstleistung beinhaltet das Parsen von bis zu 25 verschiedenen Message Typen der betreffenden Logsource

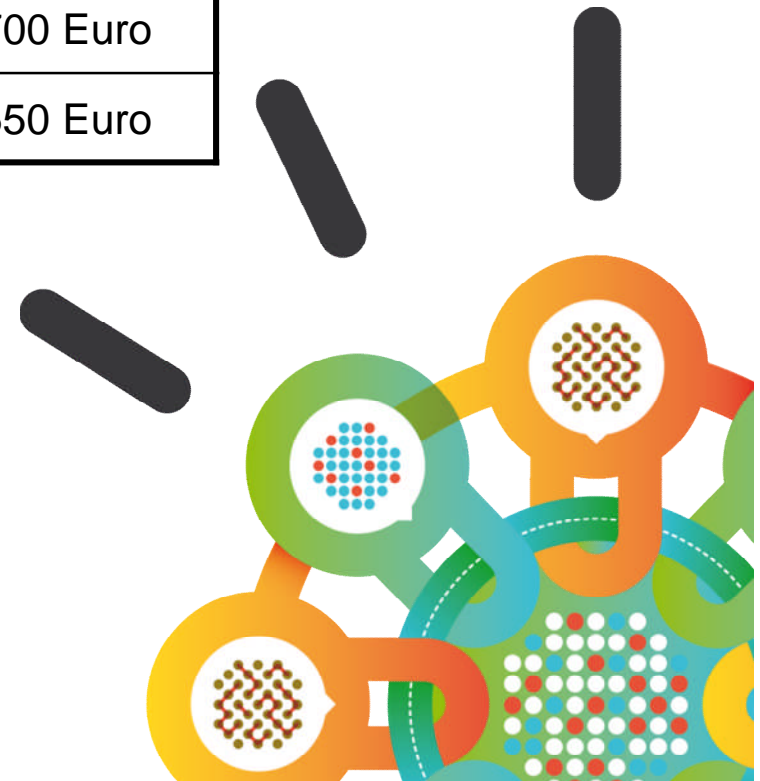


# IBM Preise



## IBM Preise (alle Preise sind zzgl. MwSt.)

Angebot	Preis
SIEM Small Distributed Deployment – 10 Tage	18.500 Euro
SIEM Medium Distributed Deployment – 15 Tage	27.750 Euro
Einrichtung von Hochverfügbarkeit – 2 Tage	3.700 Euro
uDSM (Eine Log-Source) – 3 Tage	5.550 Euro



**Statement of Good Security Practices:** IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY

# Thank You

[www.ibm.com/de/security](http://www.ibm.com/de/security)



© Copyright IBM Corporation 2015 All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.