S.K.M. Informatik GmbH

Ihr Systemhaus in der Landeshauptstadt Schwerin

„Gefahr erkannt, Gefahr gebannt – was interne Datenströme verraten“

Dirk Scharberth
IT-Consultant

Aus Ideen **Lösungen** machen.

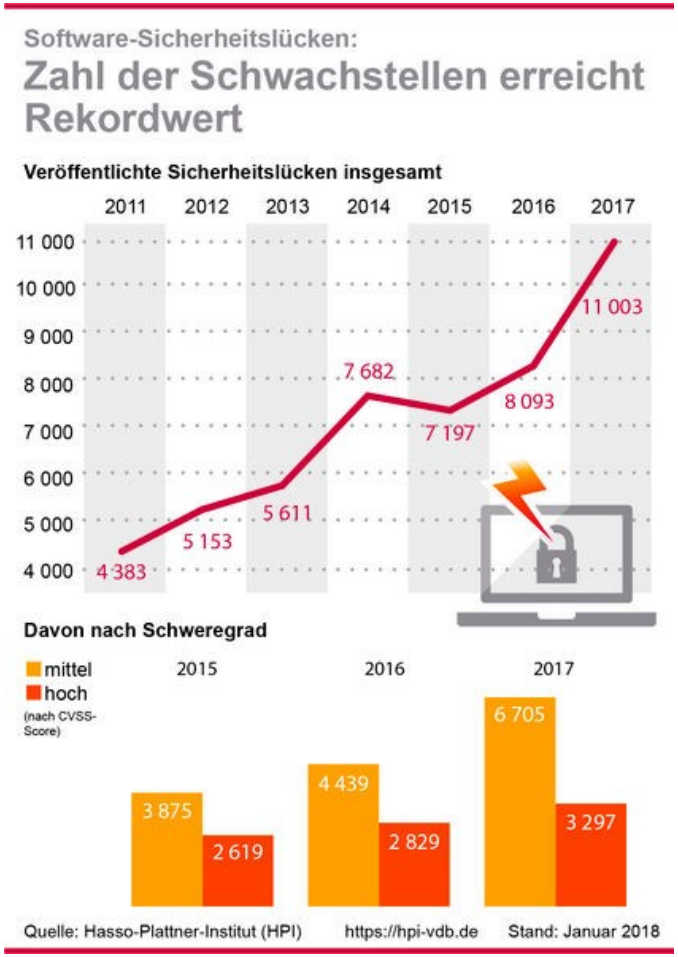
„Es gibt zwei Arten von Unternehmen: diejenigen, die gehackt wurden, und diejenigen, die noch nicht wissen, dass sie gehackt wurden.“ (John Chambers, CEO von Cisco)

Inhalte

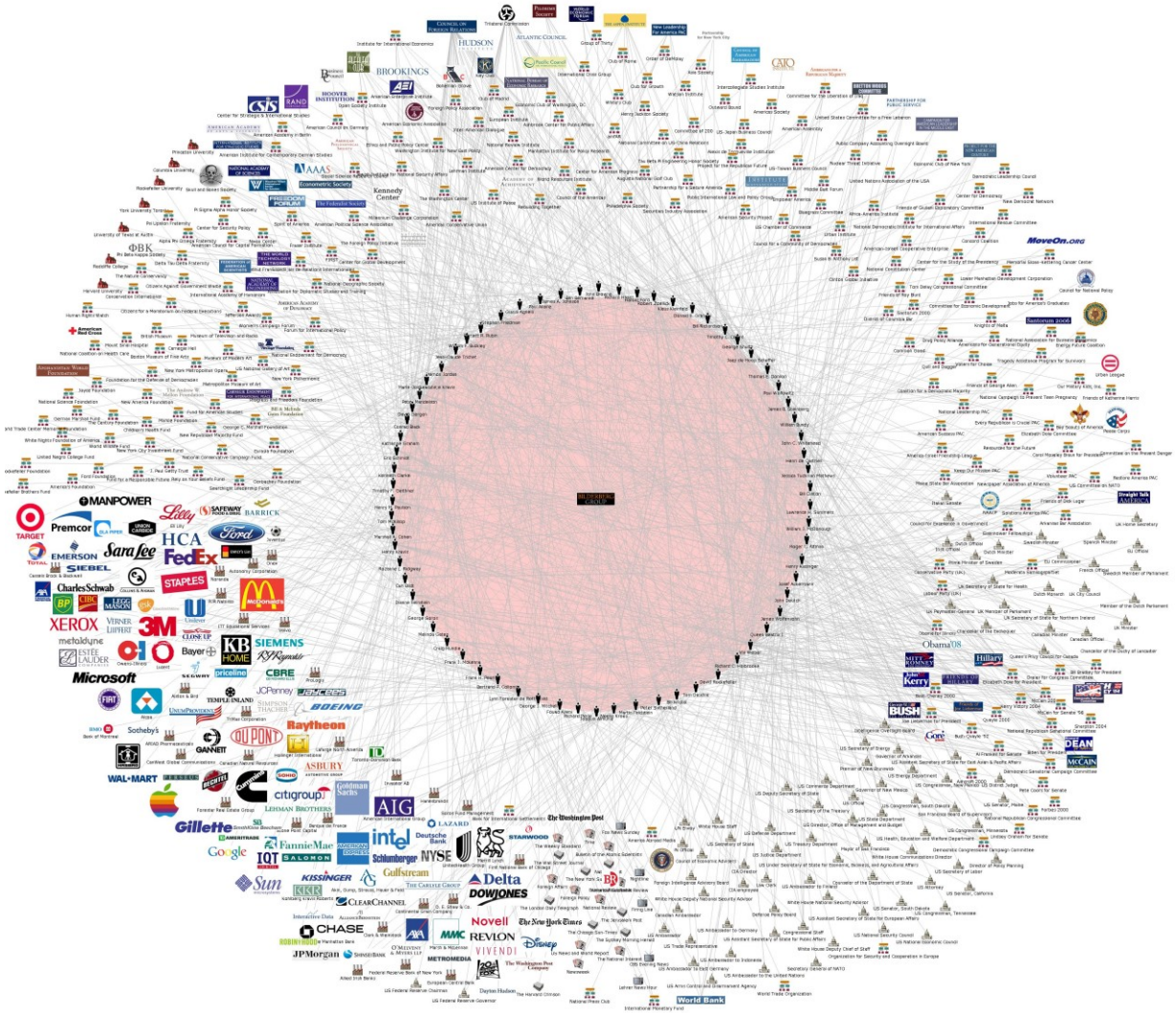
1. **IT-Sicherheit – die Herausforderungen**
   Was beeinflusst die Entwicklung der IT-Sicherheit?
2. **Aktueller Stand**
   Was kennzeichnet die IT-Sicherheit aktuell?
3. **Aktuelle Gefahren**
   Was gefährdet die IT-Sicherheit?
4. **Schlussfolgerungen**
   Wie muss unsere IT-Sicherheit in Zukunft aussehen?

IT-Sicherheit – die Herausforderungen

IT-Sicherheit – die Herausforderungen

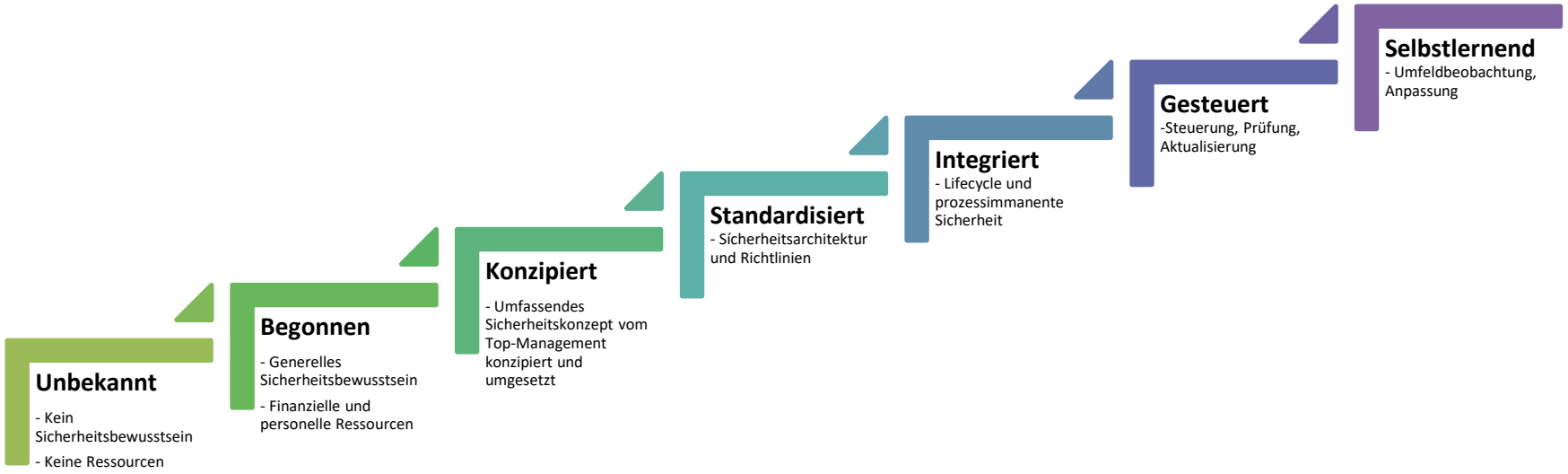


IT-Sicherheit – die Herausforderungen

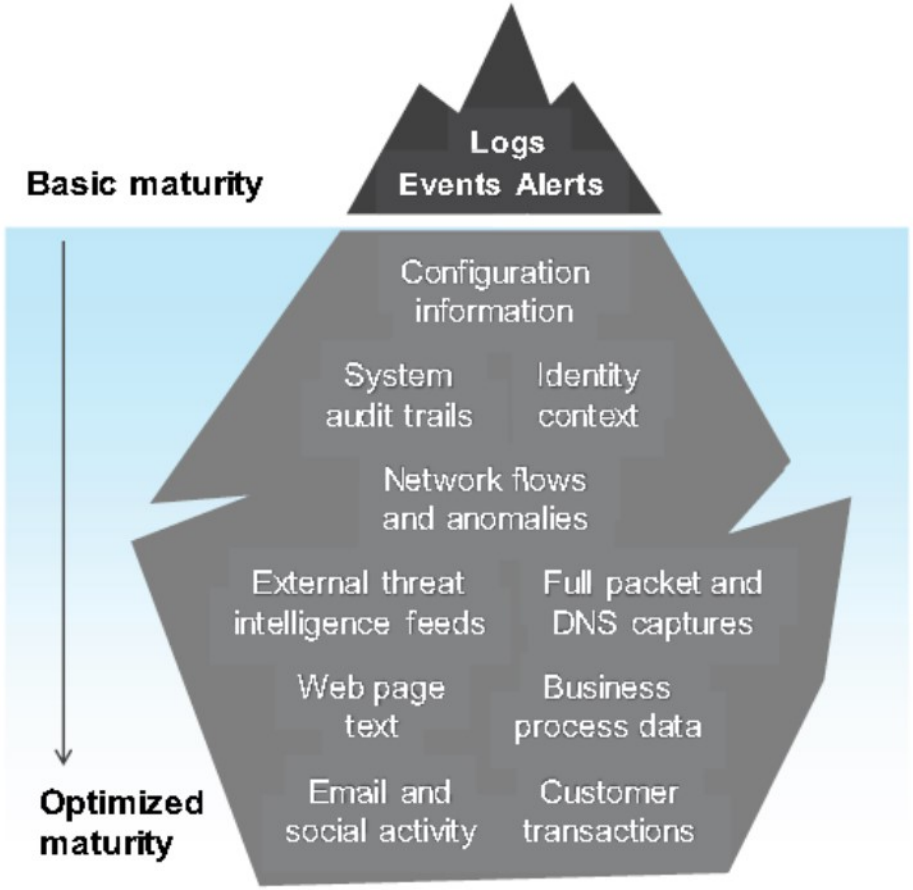


Aus Ideen **Lösungen** machen.

Aktueller Stand anhand eines Reifegradmodells



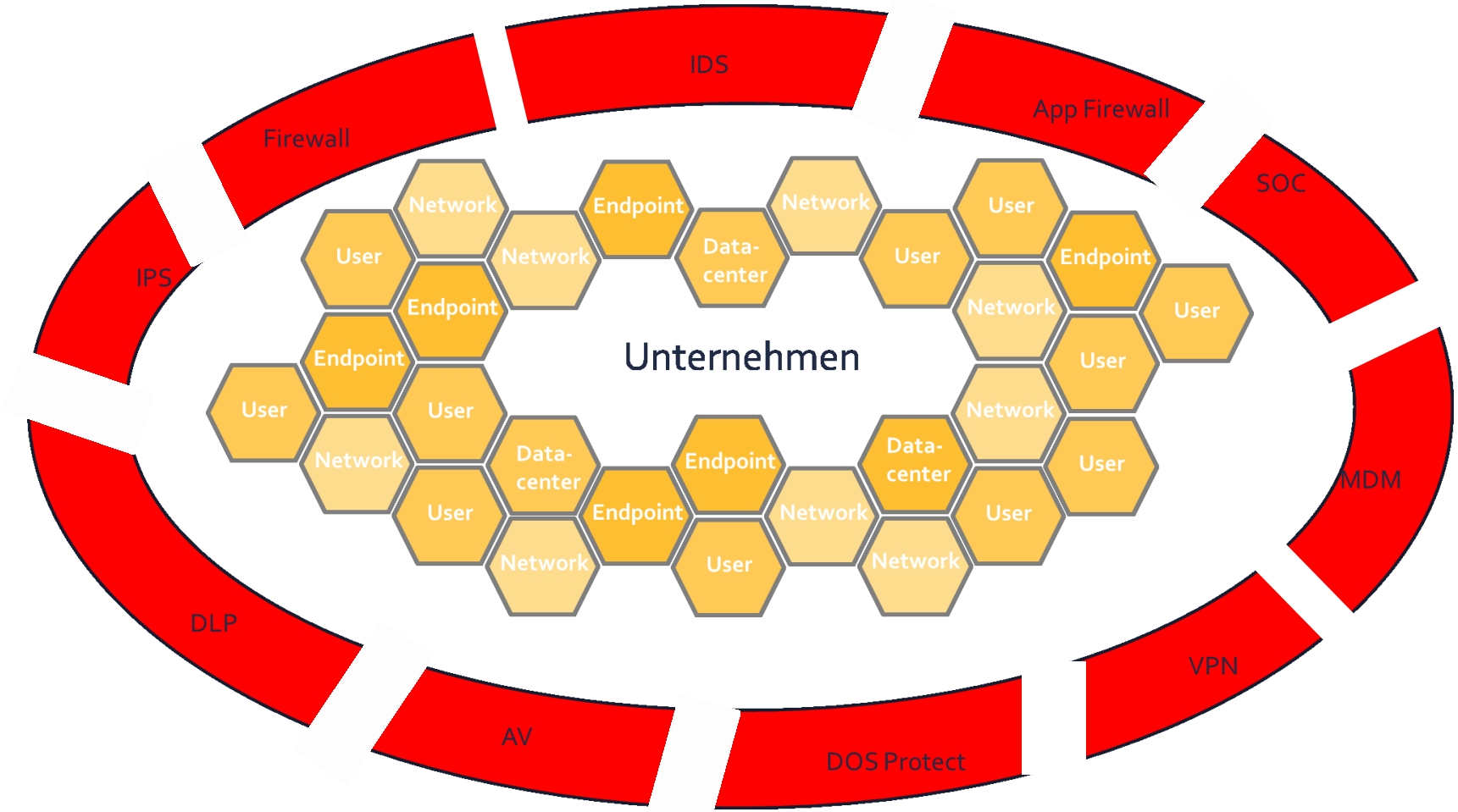
Aktueller Stand – Auswirkungen des Reifegrades



Aktueller Stand - Felder der IT-Sicherheit

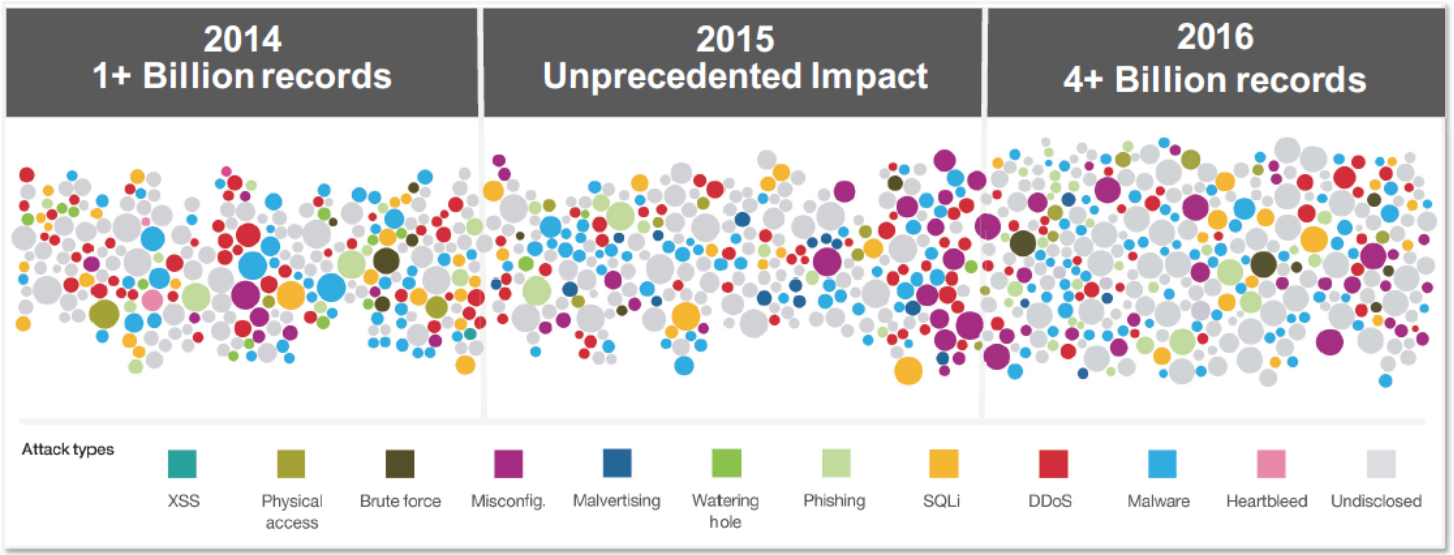
Aus Ideen **Lösungen** machen.

Aktueller Stand



Aktuelle Gefahren

Attackers break through conventional safeguards every day



average time to identify data breach

201 days

average cost of a U.S. data breach

$7M

Aktuelle Gefahren – Ablauf eines Angriffs

Analyzing a real-world large-scale attack

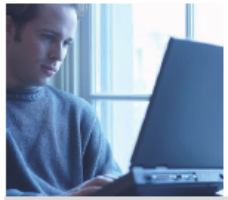
Verlauf eines Angriffs

Anatomy of an attack - Lions at the watering hole

In July 2012, several high-profile institutions in the financial and technology sectors were victimized by a "watering hole" attack

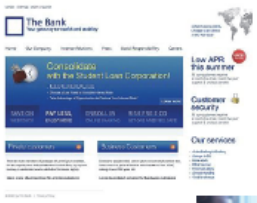
Step 1: Stake out the watering hole
Insert iFrame that redirects visitors to a zero-day malware download

Step 2: Catch the visiting "gazelles"



Employee using corporate laptop at home …

… visits compromised consumer banking site …



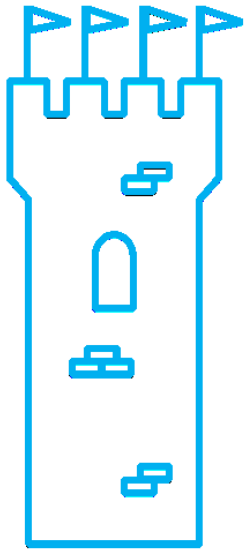
… redirected to a zero-day malware download

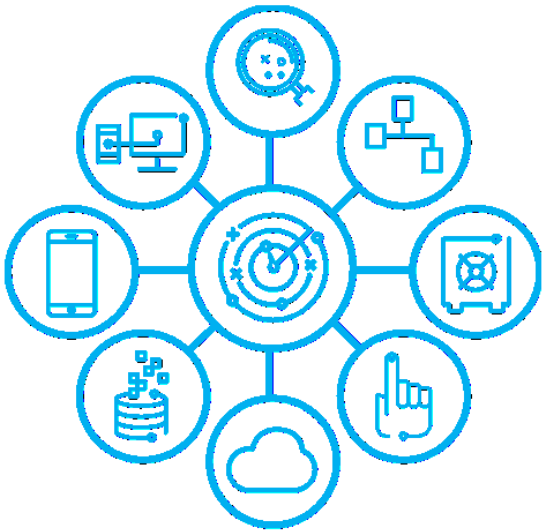
Step 3: The prey returns to the herd

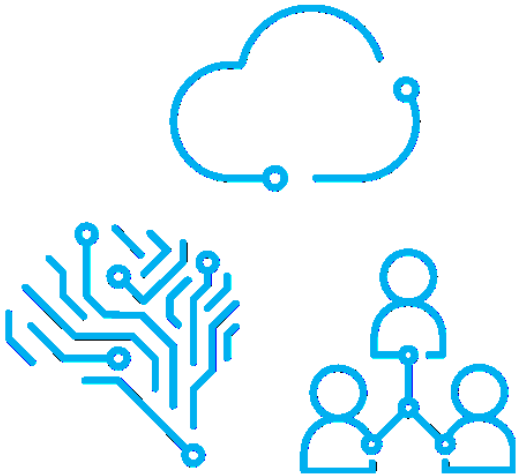
Employees bring their infected laptops to work the next day …

… and infected laptops siphon off sensitive data to a command and control server in China

Schlussfolgerungen – Entwicklungsstand IT-Sicherheit



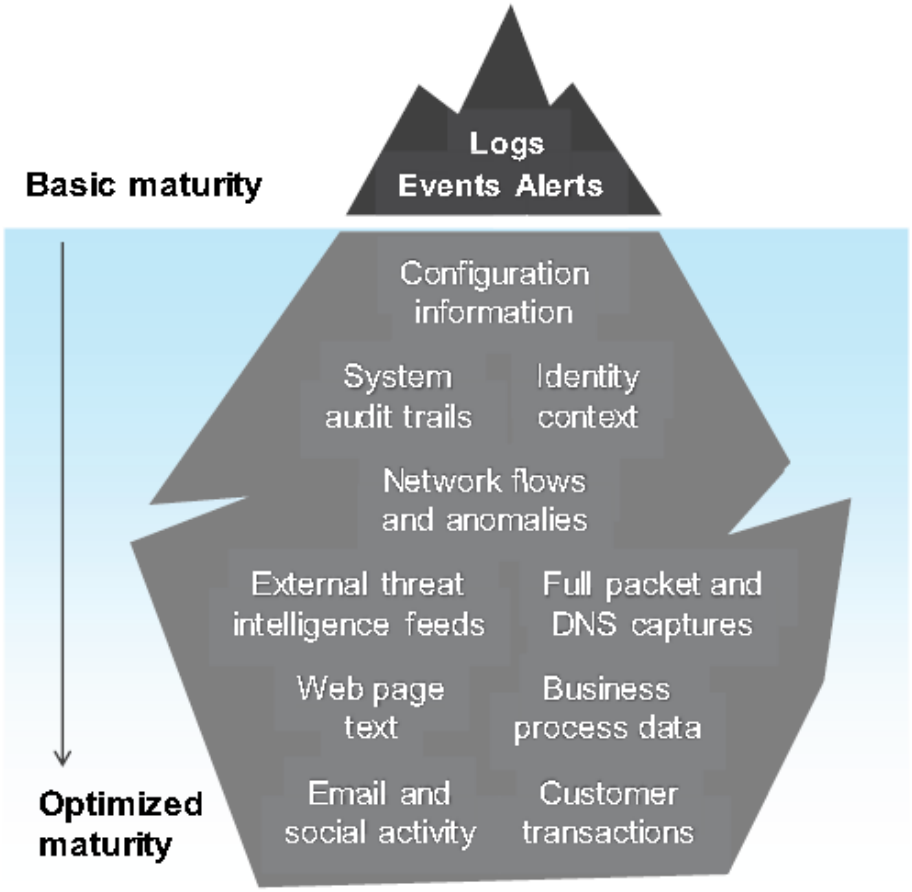




LAYERED DEFENSES → **INTELLIGENCE and INTEGRATION** → **COGNITIVE, CLOUD, and COLLABORATION**

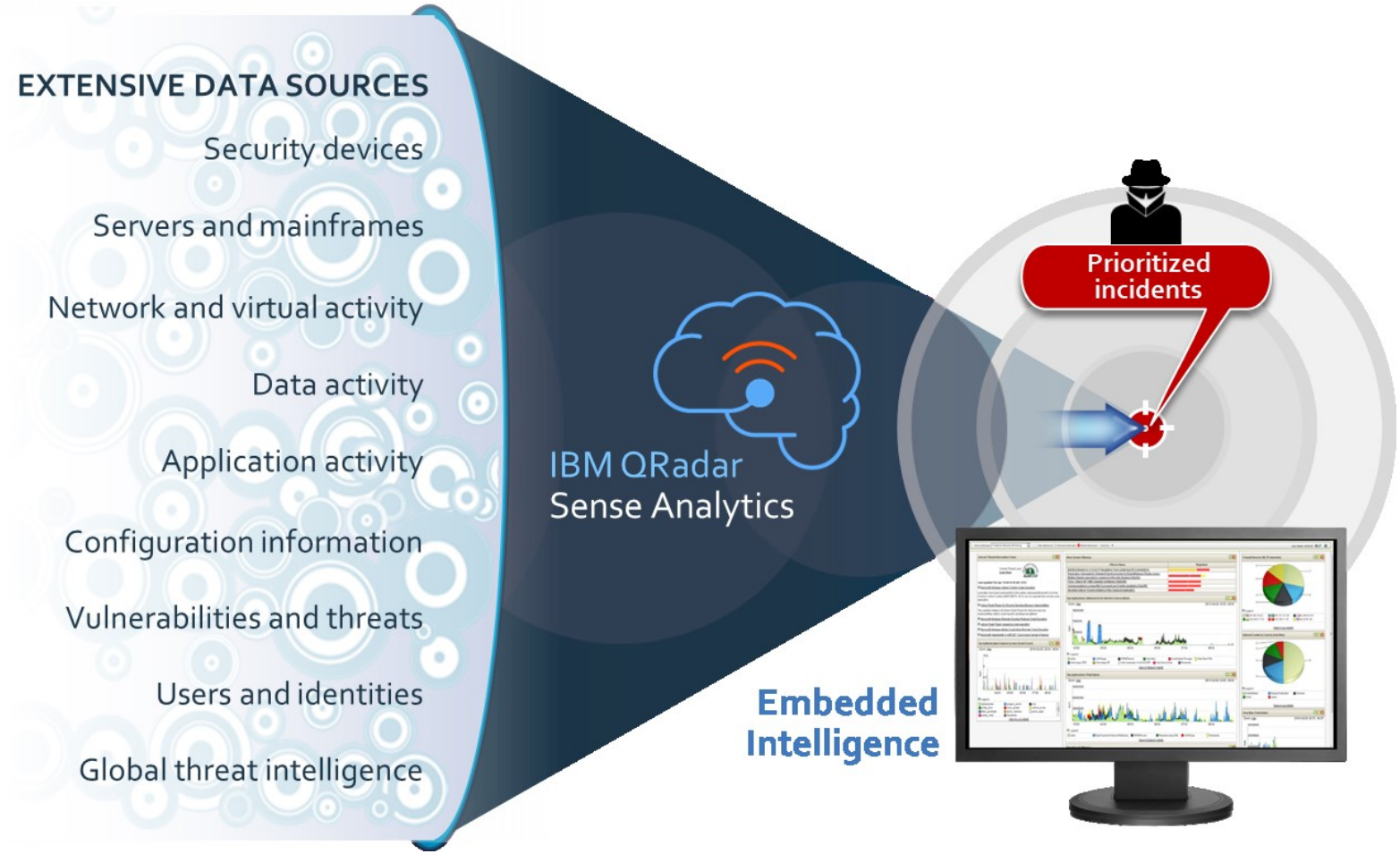
Aus Ideen **Lösungen** machen.

Schlussfolgerungen - Zielstellungen



Aus Ideen **Lösungen** machen.

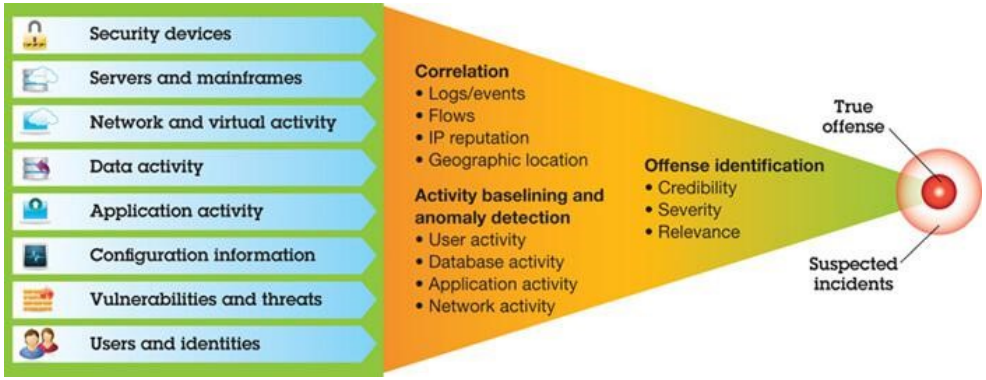
Schlussfolgerungen – Konsolidierung und Auswertung der Daten durch S.I.E.M. System



Aus Ideen **Lösungen** machen.

Schlussfolgerungen – Beispiel IBM QRadar SIEM

- Das Kürzel **SIEM** steht für Security Information and Event-Management und ist eine Kombination aus SIM (Security Information Management) und SEM (Security Event Management).
  - Erfassung und Auswertung von Systemmeldungen (Logs)
  - Erfassung und Auswertung von Datenflüssen
  - Konsolidieren und Auswerten der gesamten gesammelten Daten
  - Zentrale Anbindung an IBM X-Force (Zugriff auf die neuesten Erkennungsverfahren)
  - Optionale Anbindung an IBM Watson – Auswertung der Offenses mit Hilfe von KI-Verfahren



IBM QRadar

Fazit

1. Separate Informationen aus den einzelnen Sicherheitssystemen geben kein zuverlässiges Gesamtbild über eine Gefahrensituation ab!
2. Datenströme werden in weiten Teilen überhaupt nicht erfasst!
3. Erst eine konsolidierte Erfassung, Verarbeitung und Auswertung ermöglicht die Erkennung komplexer Angriffsmuster!
4. Eine Anbindung an übergeordnete Strukturen und KI ernöglicht eine wesentlich bessere Erkennung und einfachere Auswertung sowie einen besseren Kenntnisstand der Analysten
5. IBM QRadar SIEM sowie die angeschlossenen Komponenten ermöglichen eine tiefe Analyse sowie auch eine Anpassung an Besonderheiten des Kunden bezüglich der Datenkommunikation, da das System skalierbar und auch hinsichtlich der Funktion modular erweiterbart ist!

Quellen und Bilder

- http://www.ibm.com
- http://www.techdata.de
- https://www.fundresearch.de/PartnerCenter/Credit-Suisse-Deutschland-AG/Nachrichten/Credit-Suisse-IT-Sicherheit-durch-Hacker-Angriffe-gefaehrdet.html
- https://www.it-business.de/zahl-der-software-schwachstellen-erreicht-rekordwert-a-680644/?cmp=nl-43&uuid=E7C1A382-D4DC-4A99-8E512940BA8C2032

Für Fragen stehen wir Ihnen gern zur Verfügung!

S.K.M. Informatik GmbH
Eckdrift 95
19061 Schwerin
Telefon +49 385 48836-10
E-Mail info@skm-informatik.com
Internet www.skm-informatik.com

Dirk Scharberth
IT-Consultant

dscharberth@skm-informatik.com

Vielen Dank für Ihr Interesse

Aus Ideen **Lösungen** machen.