TeleTrusT-interner Workshop

Bochum, 27./28.06.2013

Big Data im Bereich Information Security

Axel Daum | RSA – The Security Division of EMC

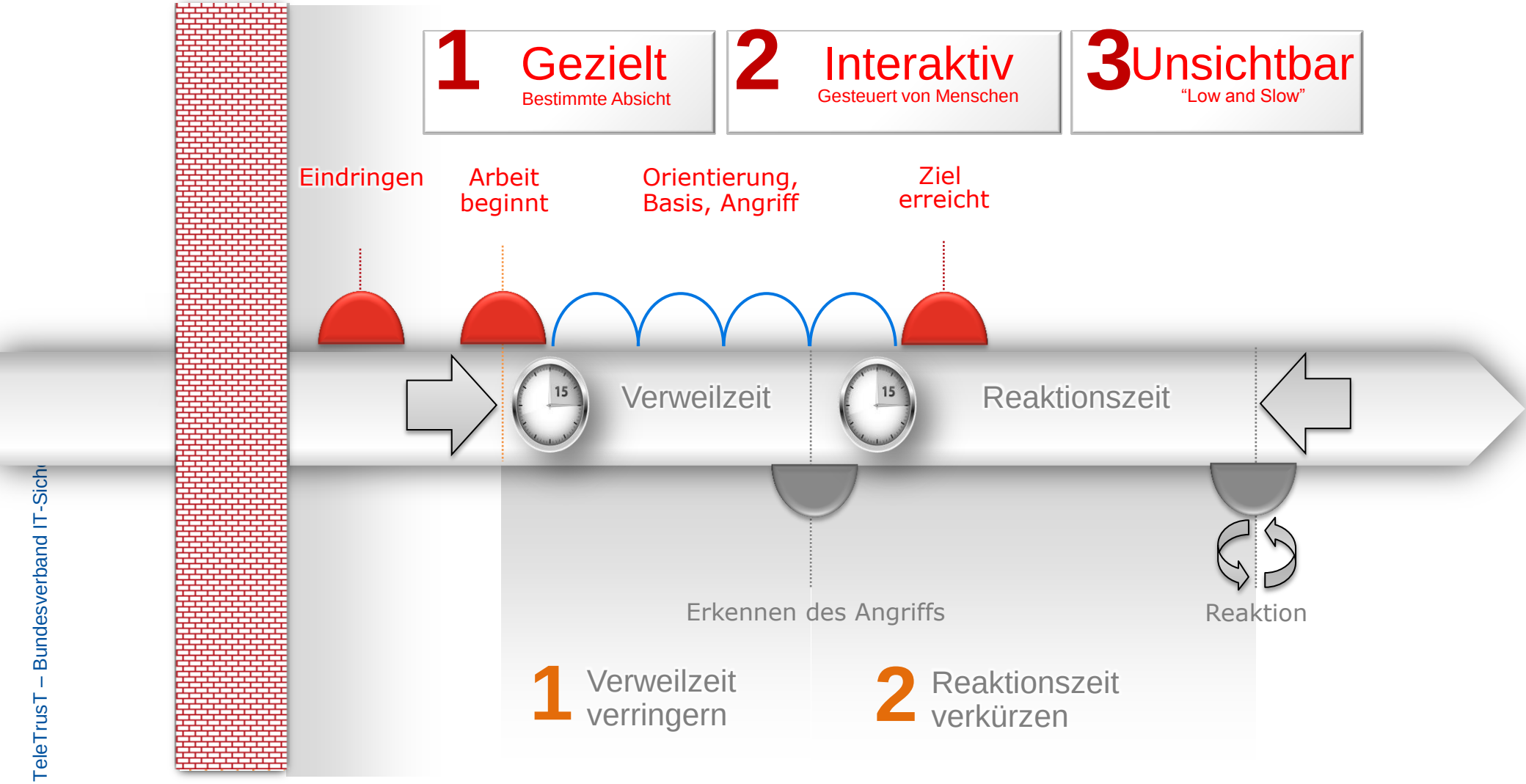
Agenda

- Ausgangslage – Die Angreifer kommen immer in das Netzwerk
- Anforderung – Risiko-Orientierung, Kontext, Agilität
- Intelligence / Big Data - Einsatzbeispiele
- Intelligence Driven Securitry - Zusammenfassung

Ausgangslage:
Die Angreifer kommen immer in das Netzwerk

Sicherheits-Herausforderungen heute

Die Angreifer kommen immer in das Netzwerk



Analyse von Bedrohungen und Angriffen

Bei der Analyse von 900 erfolgreichen Angriffen fand man in 90% der Fälle Hinweise in den Log Dateien, wobei nur 5% der Unternehmen den Angriff erkannt haben.
Quelle: Verizon Data Breach Report 2011

83% der befragten Unternehmen glauben, dass ein gezielter Angriff (APT)bei Ihnen stattgefunden hat.
Quelle: Ponemon Studie 2011

Aber man beachte !!!

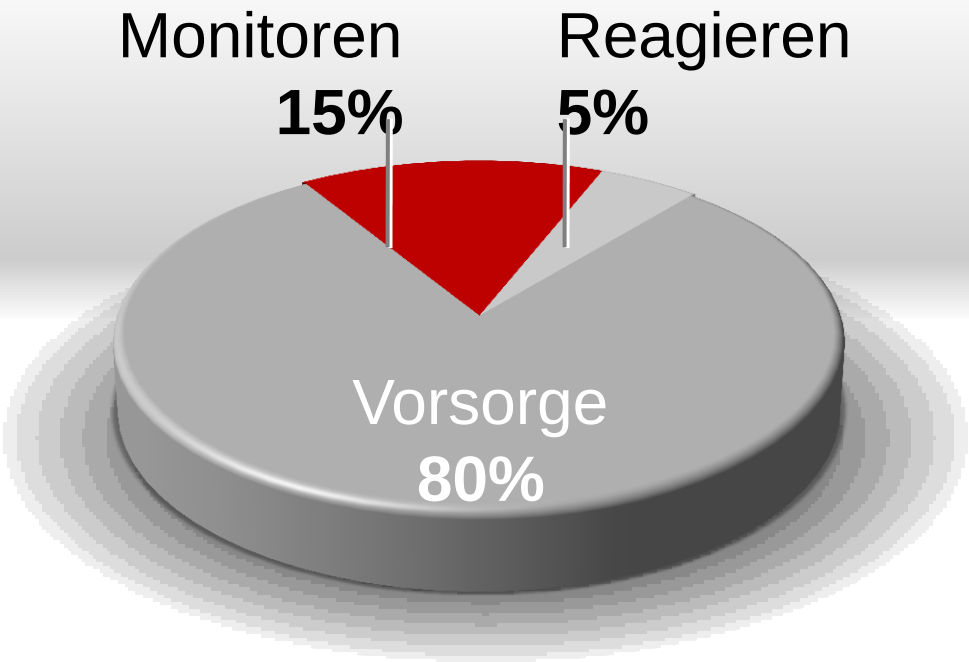
Bis 2015 werden 80% aller erfolgreichen Angriffe durch Ausnutzen von wohlbekannten Schwachstellen erfolgen.
Quelle: Gartner „Top Security Trends 2012 & 2013“, Juni 2012

Anforderung: Risiko-Orientierung, Kontext, Agilität

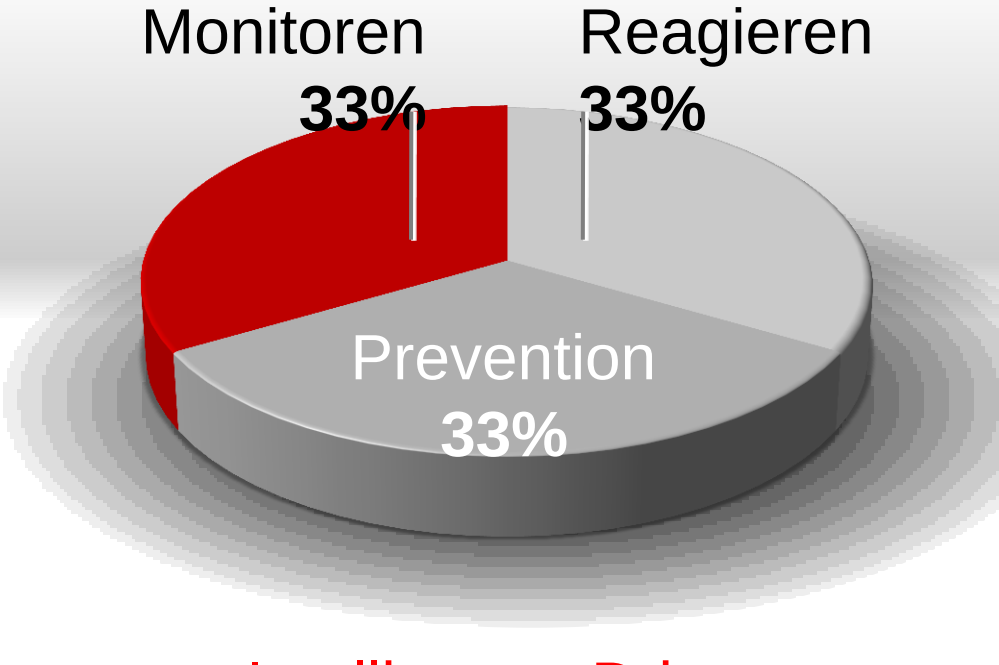
Intelligence-Driven Security

Risiko-Orientierung, Kontext und Agilität

Verschiebung der Resourcen: Budgets und Mitarbeiter



Prioritäten
Heute



Intelligence-Driven
Security

Intelligence / Big Data: Einsatzbeispiele

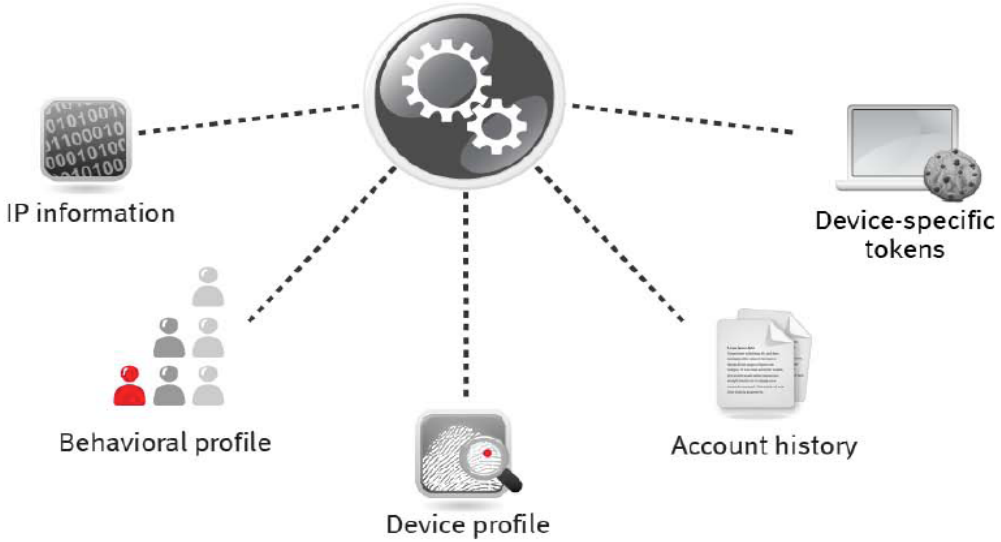
Beispiel 1 - Risikobasierte Authentifizierung

Web

Mobile App, Browser

Web Access Management

SSL/VPN



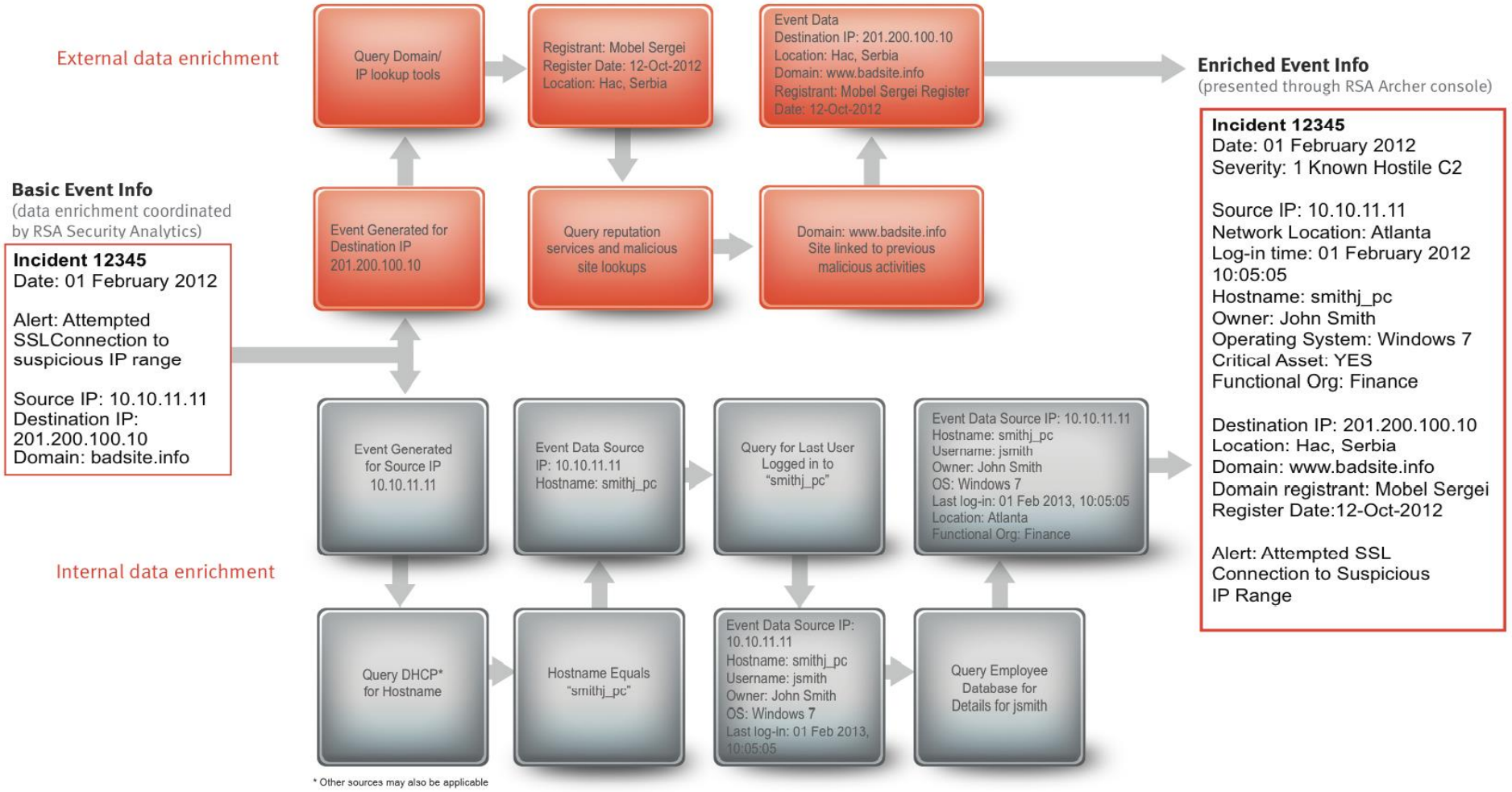
Beispiel 2: WebSession Intelligence

Kriminelle unterscheiden sich von regulären Kunden

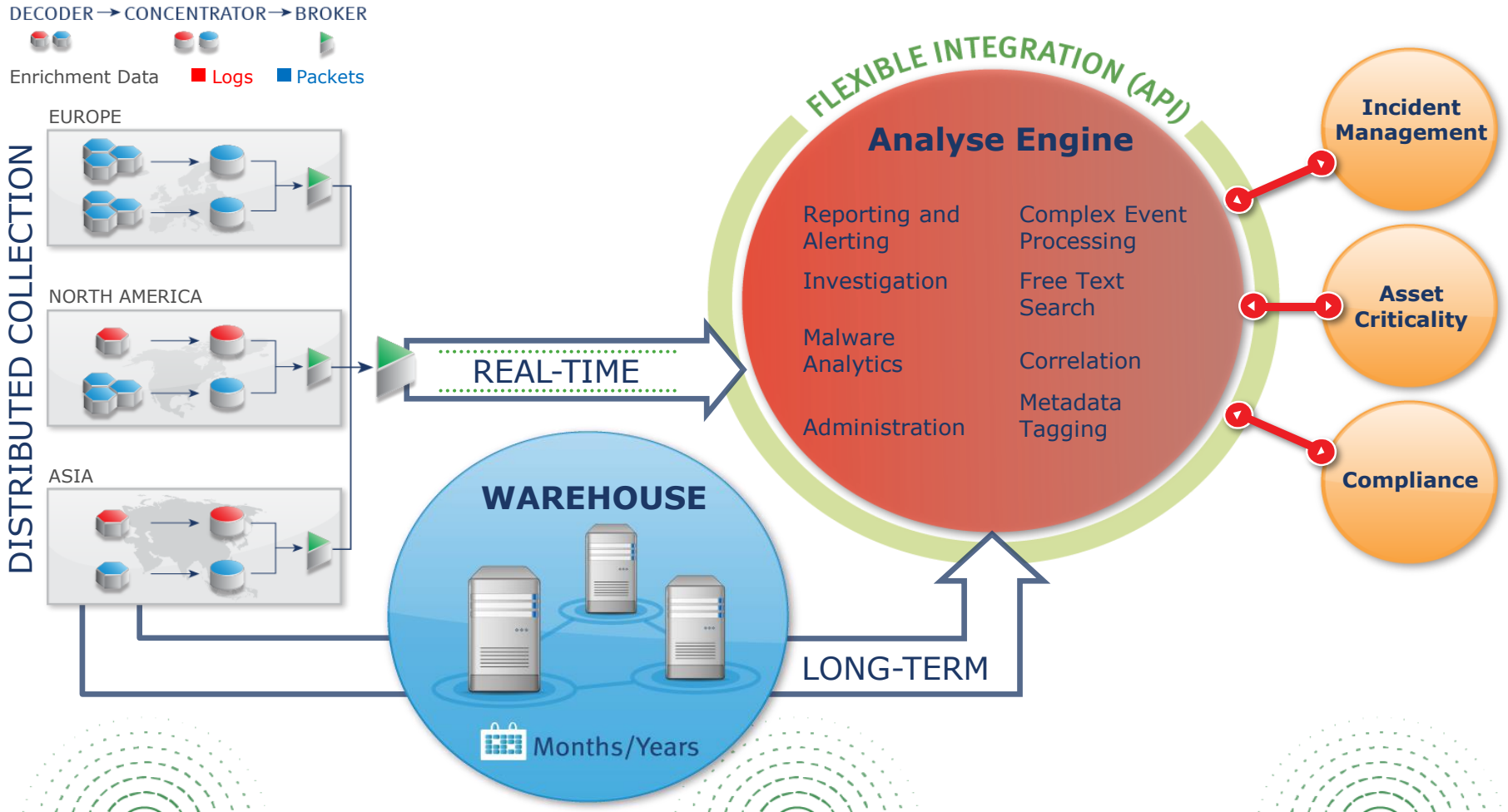
- Velocity
- Page Sequence
- Origin
- Contextual Information

Beispiel 3: Daten anreichern – intern und extern

FIGURE 2: AUTOMATED ENRICHMENT OF EVENT DATA



Security Analytics Architektur



Intelligence Driven Security
- Zusammenfassung

Intelligence Driven Security

Intelligence: Aufklärung, Information, Einsicht

- Ausgangspunkt für jeden Cyber- Sicherheits Ansatz ist die Analyse der Risiken
- Grundlage für eine effektive Cyber-Abwehr ist die genaue Kenntnis und ein umfassendes Verständnis über die Vorgänge im Unternehmen (Netzwerk, Anwendungen)
- Neben der Analyse der „Dynamischen Daten" ist die Infrastruktur Compliance eine wichtige Voraussetzug (Schwachtellen, Konfiguration)
- Kontext / Big Data: erst in der Kombination unabhängiger Vorgänge ergeben sich Anhaltspunkte für mögliche Angriffe
- Daten aus dem Unternehmen müssen zur Analyse mit externen Informationen zusammengebracht werden

RSA

Advanced Security Management Szenario

Governance Risk Compliance

Chance Risk

Was sind meine Unternehmenswerte?

Risk Mgmt.

Enterprise Mgmt. Policy Mgmt.

Business Continuity Mgmt. Vendor Mgmt.

Compliance Mgmt. Threat Mgmt.

AUDIT Mgmt. Incident Mgmt.

MANAGEMENT DASHBOARD
ARCHER eGRC

Business Context

SECURITY ANALYTICS

Wer sind die ANGREIFER

- Hacktivisten
- Kriminelle
- Staaten

MALWARE

Threat Feeds

Network

Logs

3rd Party Feeds

SEE EVERYTHING IN YOUR COMPLIANCE DOMAIN

VISIBILITÄT, VERSTÄNDNIS, HANDLUNGSFÄHIGKEIT

INTELLIGENT CONTROLS

RSA eFraud Network

IP Information 10.0.1.195

RiskEngine

Network

Channel Information

Behavioral profile

Device profile

Fraud Intelligence

RSA case management feedback

CERTIFIED SECURED BY RSA PARTNER

Maßnahmen

Danke

Axel Daum | Manager Channel Germany | RSA – The Security Division of EMC
axel.daum@rsa.com | +49 160 904 914 50