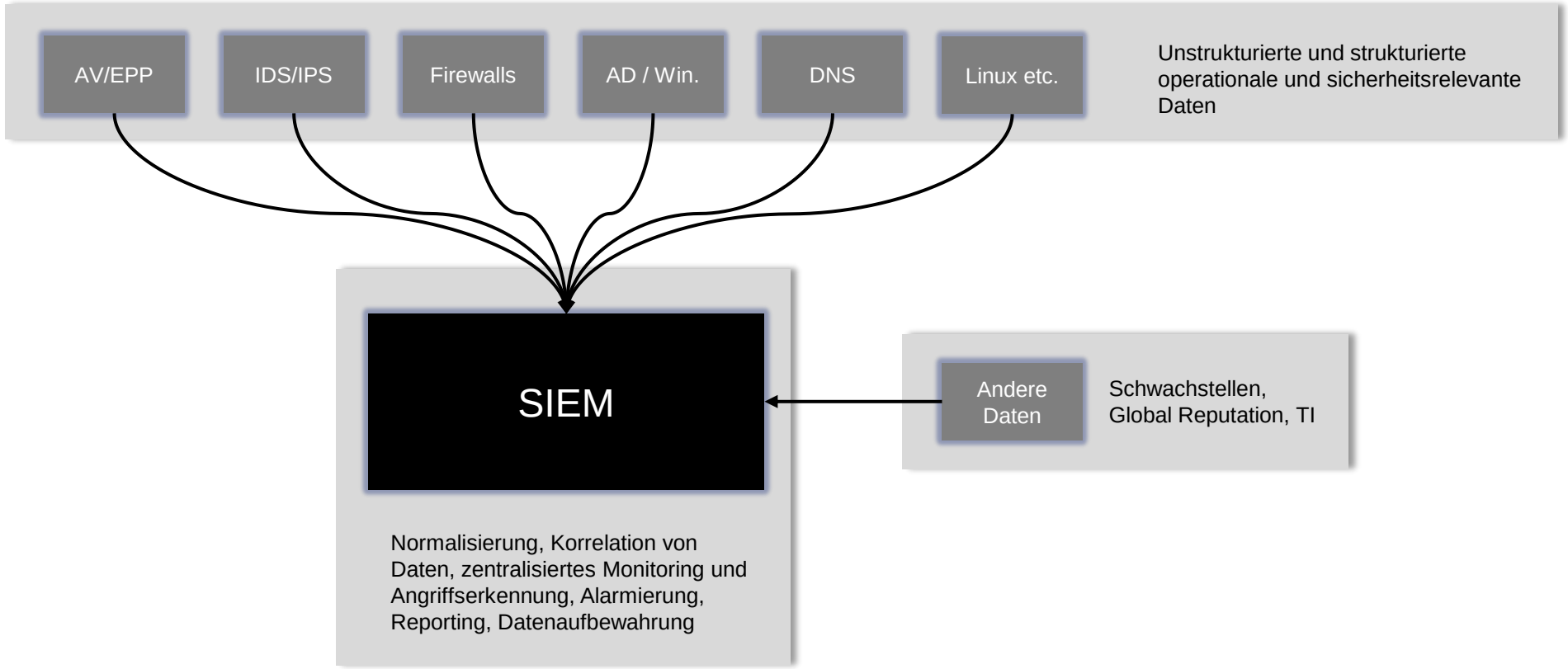
Welcome to the NG Cyber Defense Platform Jungle

Eugen Möller, Lead Consultant Cyber Defense
Sven Wiebusch, Lead Consultant Security

Computacenter

Welcome to the NG Cyber Defense Platform Jungle

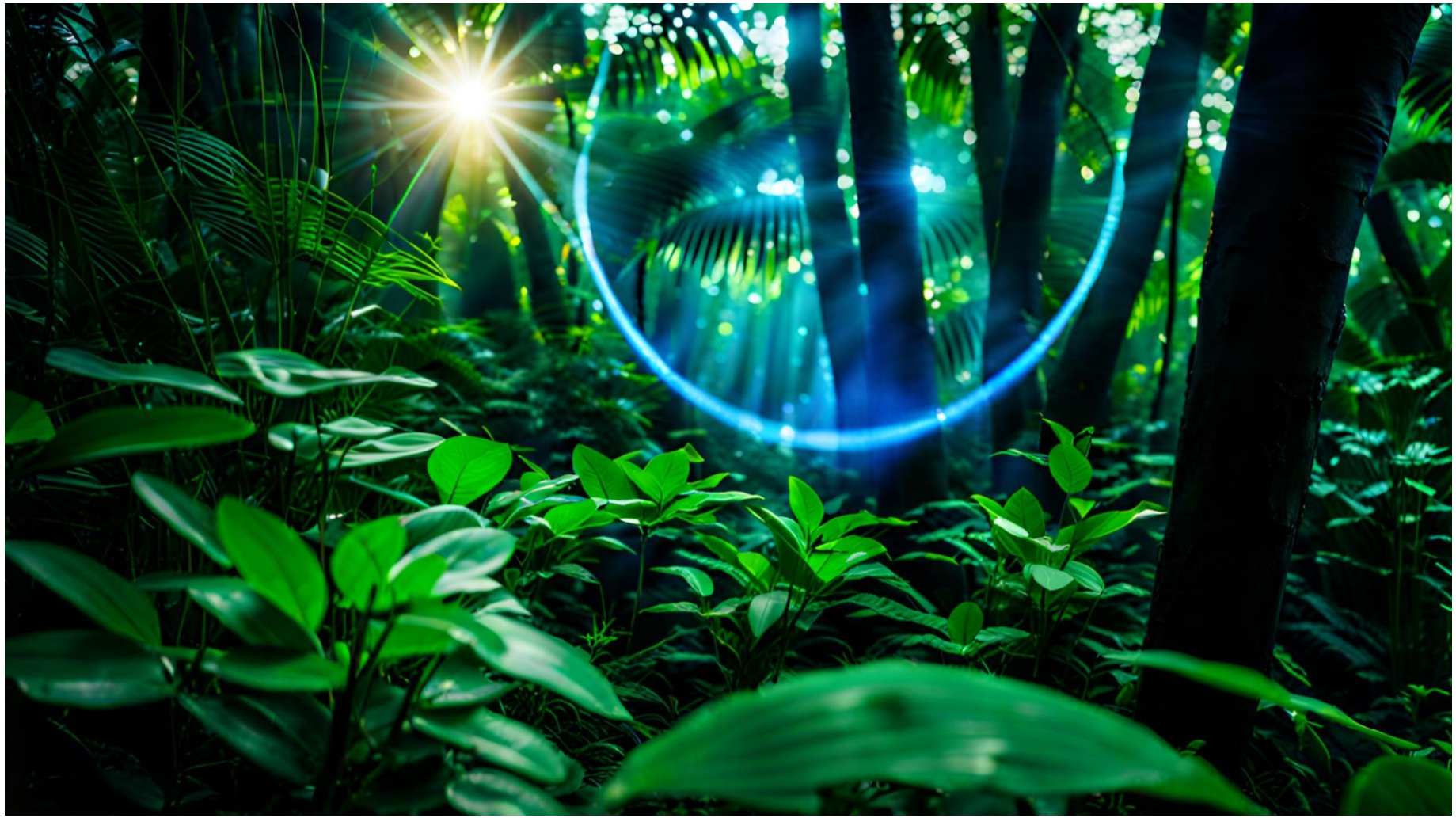
Früher war alles besser …



Halle 9 I Stand 419 – Download des Vortrags:

Welcome to the NG Cyber Defense Platform Jungle

Heute …

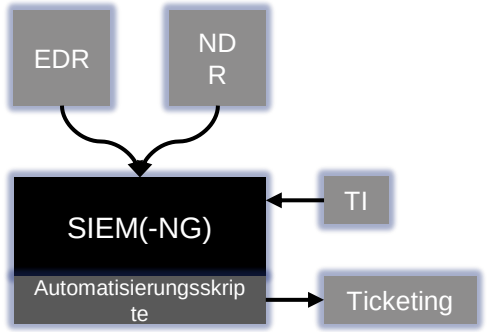


Quelle: runway gen3 prompt by Holger Viehoefer

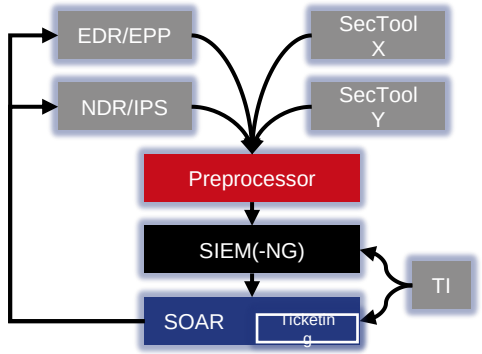
Welcome to the NG Cyber Defense Platform Jungle

Einige bewährte Ansätze

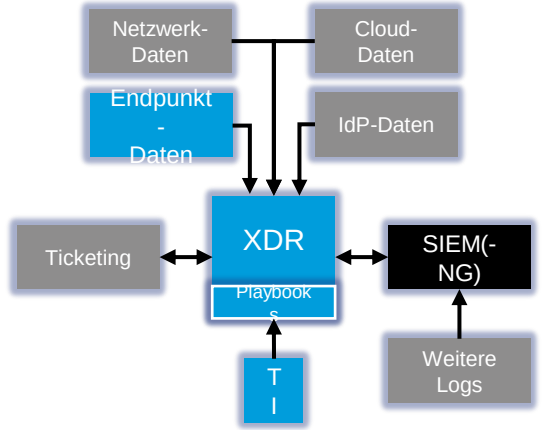
Gartner “SOC Visibility Triad”



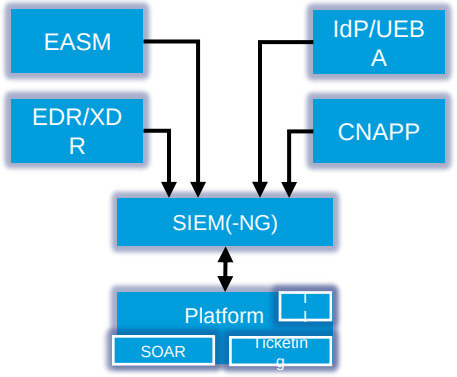
SOAR-basiertes Best-of-Breed



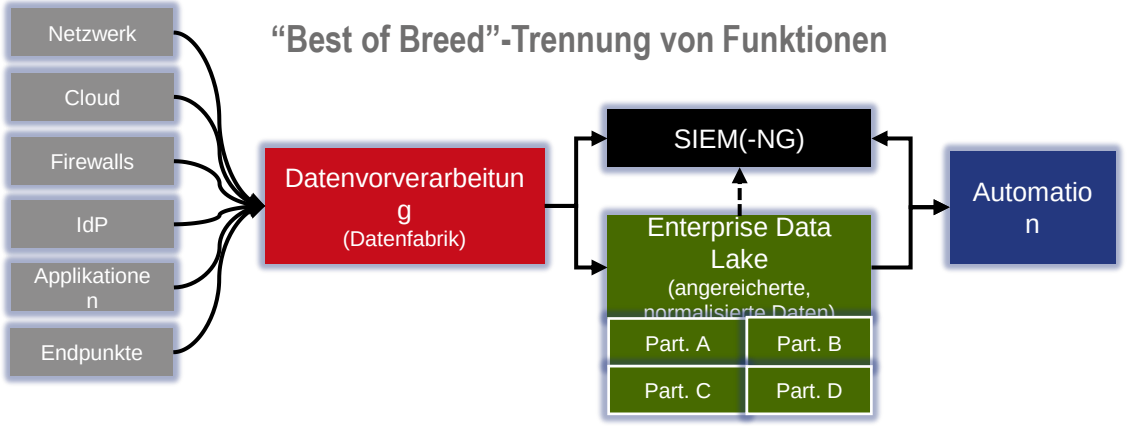
Klassischer AV-Hersteller bietet E|XDR



All-in-One-Plattform



“Best of Breed”-Trennung von Funktionen



Halle 9 I Stand 419 – Download des Vortrags:

Welcome to the NG Cyber Defense Platform Jungle

Doch welcher Ansatz ist „der Richtige“?

Altbewährtes oder Bleeding Edge?

Best-of-Breed oder möglichst konsolidiert?

Ist Hersteller- und Portfoliostabilität ein Thema?

Welche Bereiche möchten wir abdecken?

Viel selbst basteln und integrieren oder Out-of-the-Box?

Wie flexibel, modular oder skalierbar soll es werden?

Wie groß ist unser Budget?

Multi-Vendor oder alles auf eine Karte?

Wie viele UIs möchten wir bedienen müssen?

Haben wir 3rd-Party-Abhängigkeiten?

Müssen (regulat.) Vorgaben beachtet werden?

Hohe Erkennungsrate, hohe Abdeckung, wenige False Positives?

OnPrem, Cloud oder hybrid?

Welche Schnittstellen zum Bestand sind uns wichtig?

Haben wir eigene Kapazitäten, die Lösungen zu beherrschen?

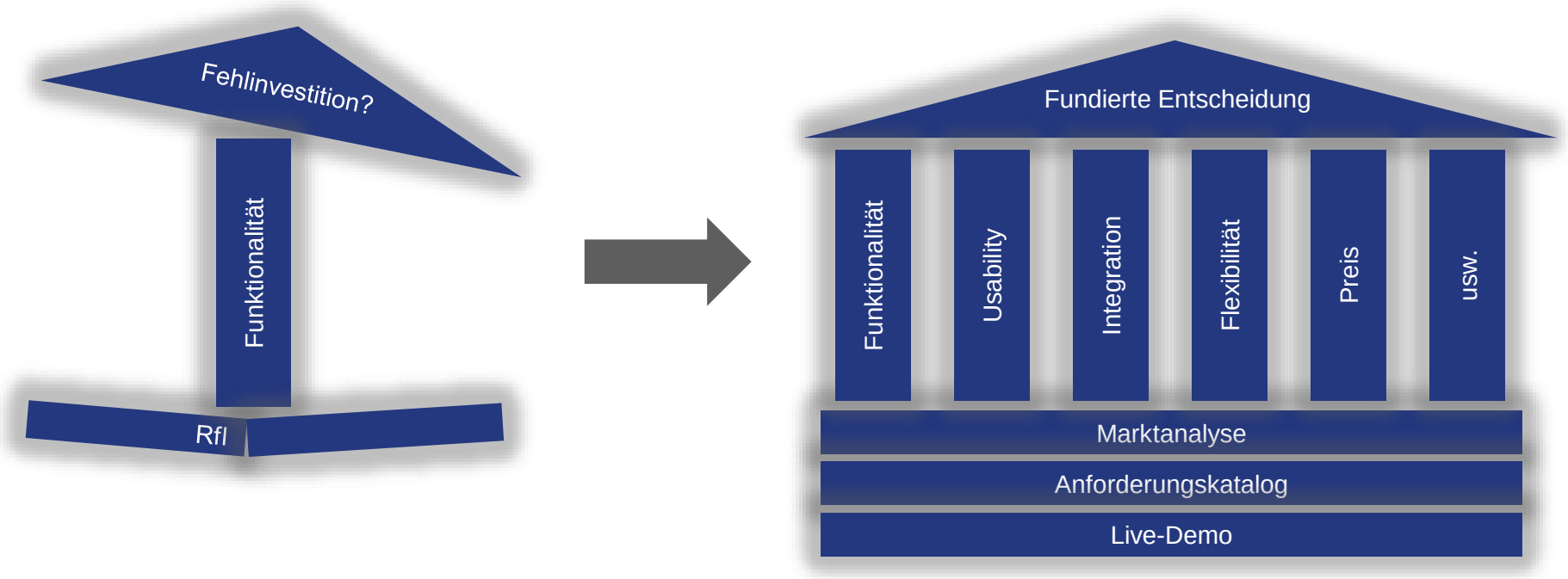
Haben wir eigene Kapazitäten, (ständig) Lösungen zu evaluieren?

Mit wie vielen Herstellern möchten wir uns befassen?

Welcome to the NG Cyber Defense Platform Jungle

Bewährtes Vorgehen

- Festlegung der grundlegenden SOC-Strategie (Scope, Services, Menschen, Prozesse, Technologien usw.)
- Ableitung der erforderlichen Tools (Was haben wir schon, was kann weg, was braucht es zusätzlich?)
- Detaillierte Anforderungsdefinition (Was ist uns wirklich wichtig?)
- Professionelle Marktbetrachtung



Halle 9 I Stand 419 – Download des Vortrags:

Besuchen Sie uns gern in Halle 9 I Stand 419

Download des Vortrags unter: