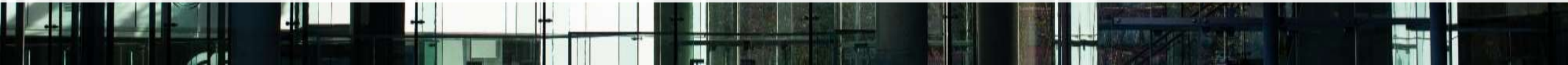
SCHWACHSTELLENMANAGEMENT UND ZERO TRUST

it-sa 2022

Peter Camillo Schmidt
Werner-Eckert-Str. 16-18, 81829 München, Germany
Computacenter AG & Co. oHG
M: +49 173 1590182
E: petercamillo.schmidt@computacenter.com

Computacenter



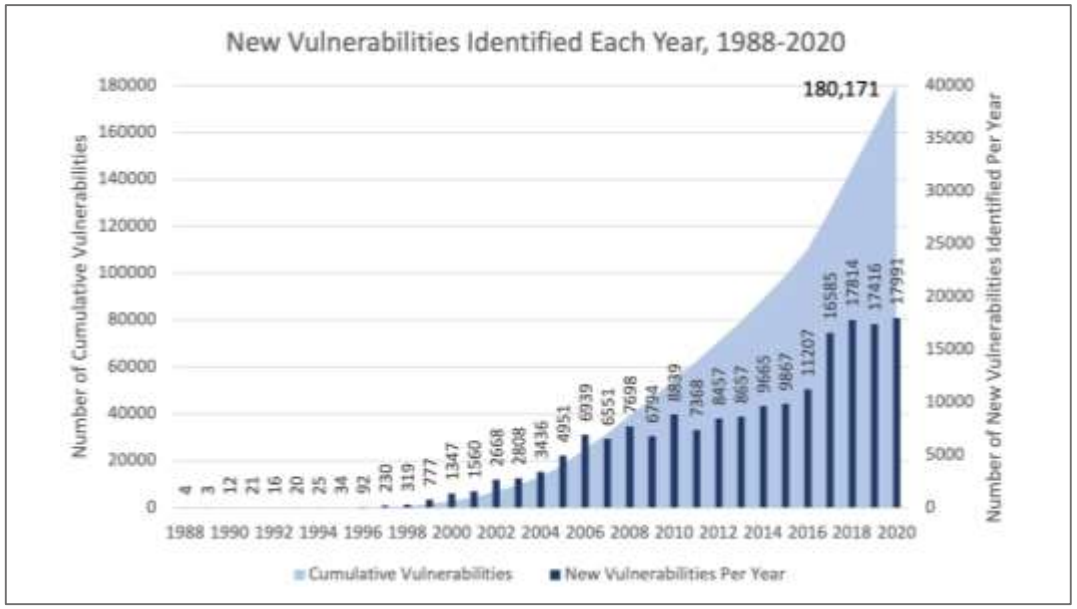
SCHWACHSTELLENMANAGEMENT IST EIN WICHTIGES CONTROL DER CYBER SECURITY

Top 6 Controls zur Cyber Security – https://www.cisecurity.org/controls/

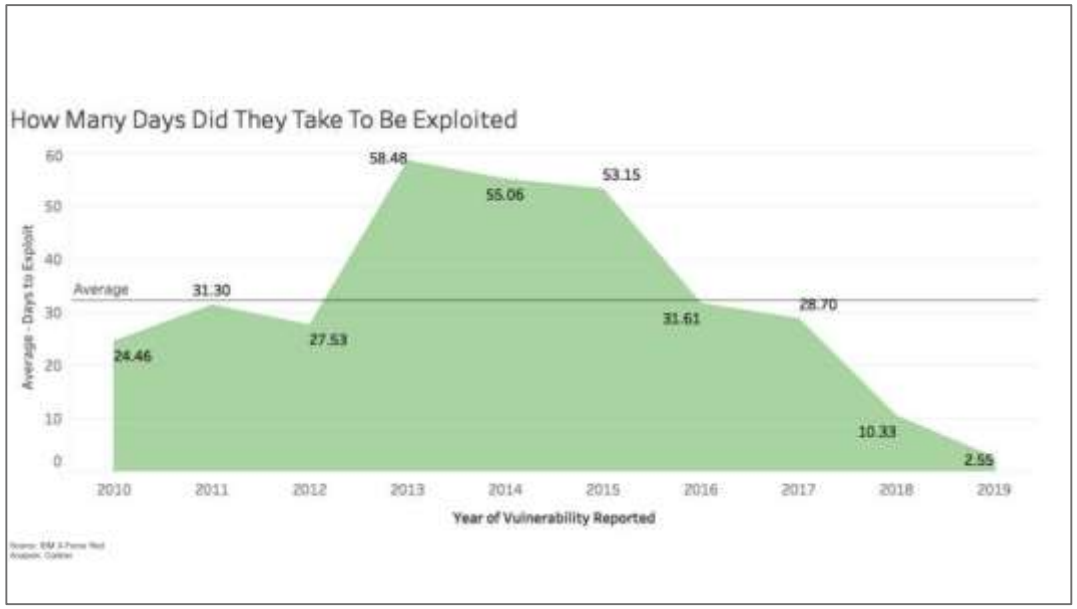
Gartner: Schwachstellenmanagement unter den Top 10 Security Projects

JÄHRLICH WERDEN TAUSENDE SCHWACHSTELLEN ENTDECKT UND ANGREIFER BENÖTIGEN WENIGE TAGE, UM EXPLOITS ZU FINDEN

Pro Jahr kommen Tausende neuer Schwachstellen hinzu

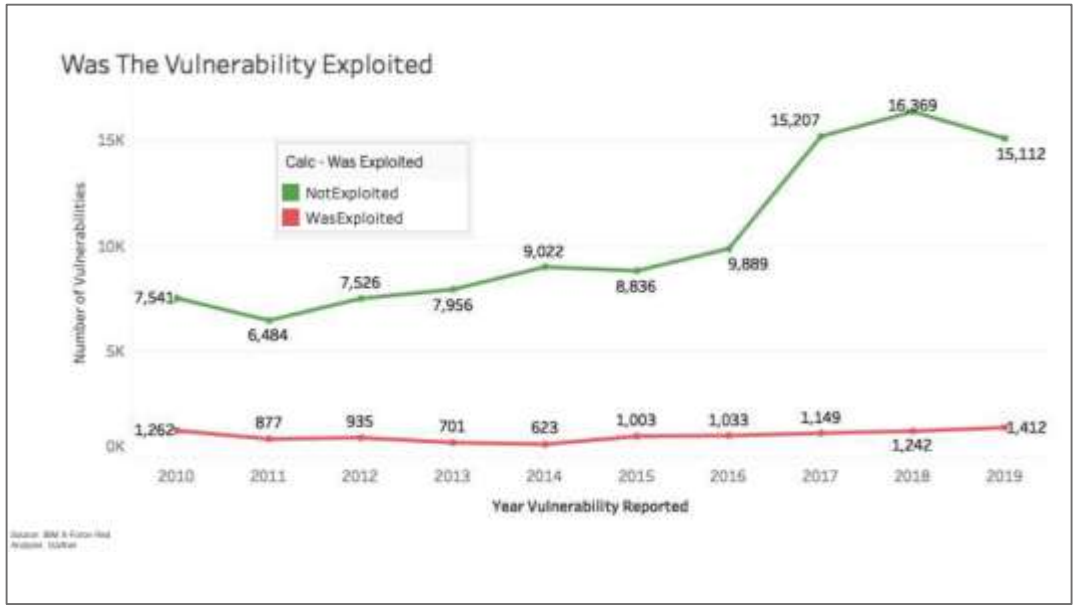


Exploits werden innerhalb weniger Tage entwickelt

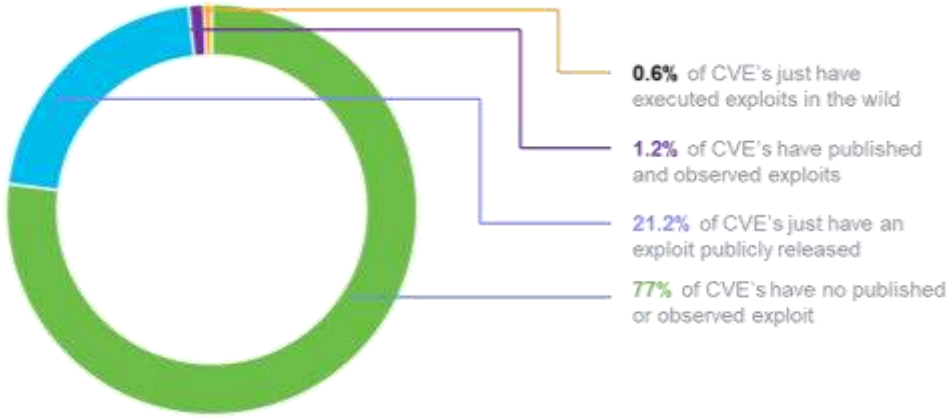


NICHT ALLE SCHWACHSTELLEN SIND KRITISCH

Anzahl der Schwachstellen mit Exploit ist stabil und niedrig



Anzahl der wirklich kritischen Schwachstellen ist noch geringer

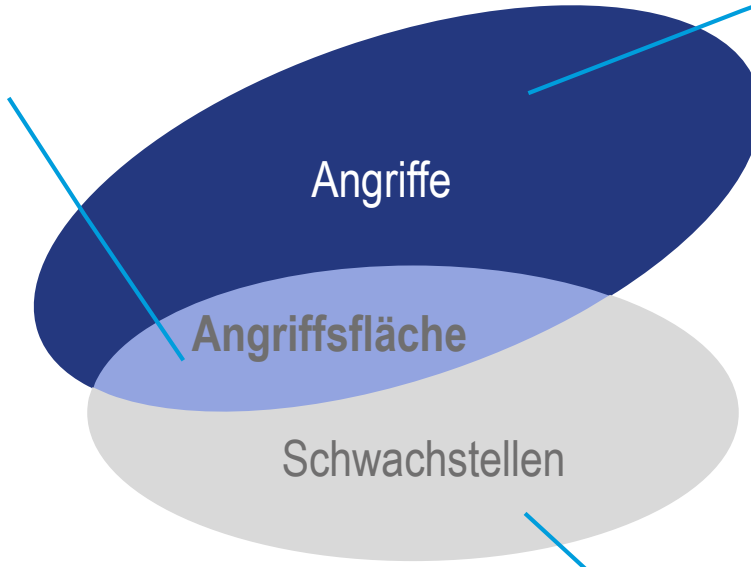


Source: Cisco / Kenna

ZIEL DES SCHWACHSTELLENMANAGEMENT

REDUKTION DER ANGRIFFSFLÄCHE

Das Ziel des Schwachstellenmanagements ist die Verringerung der Angriffsfläche



Angreifer können bestimmte Schwachstellen ausnutzen

Es gibt viele Schwachstellen, die mit Scannern leicht zu identifizieren sind – nicht alle sind kritisch!

DIE HERAUSFORDERUNG LIEGT IN DER BEWÄLTIGUNG VON KOMPLEXITÄT UND ORGANISATIONSPERFORMANCE…

…UND AUSSERDEM MUSS ES JEMAND MACHEN

Komplexität

Ein Scan liefert als Ergebnis oftmals mehrere 100.000 Schwachstellenereignisse

Organisationsperformance

- Systemeigner lassen sich nicht immer gut identifizieren
- IT Betrieb hat SLA getriebene Ziele

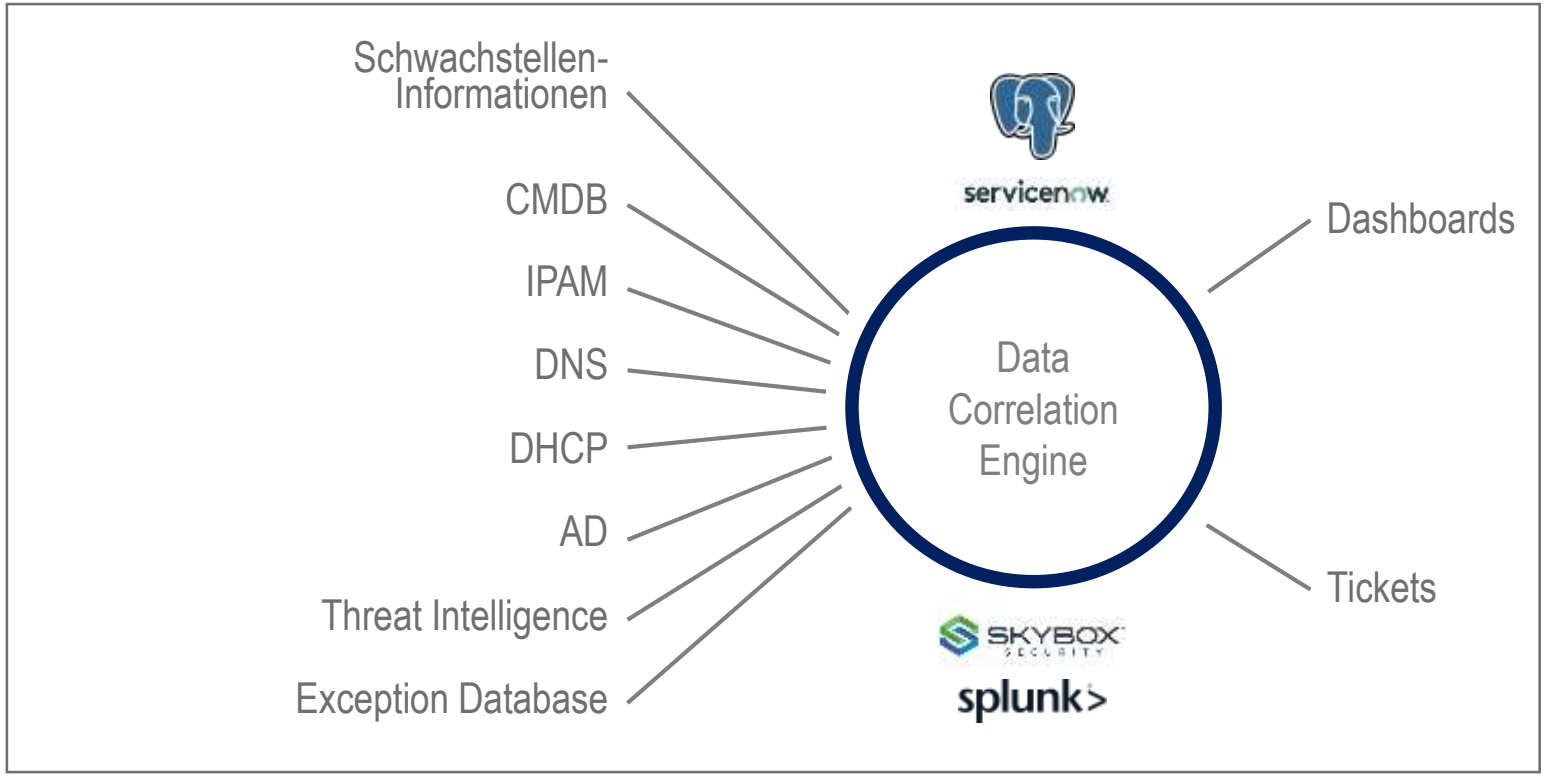
Betriebsmodell

Zwischen Scan und dem Einspielen eines Patches klafft noch eine Lücke

DIE COMPUTACENTER PROPOSITION I

AUFBAU EINER DATA CORRELATION ENGINE

Aufbau einer Data Correlation Engine



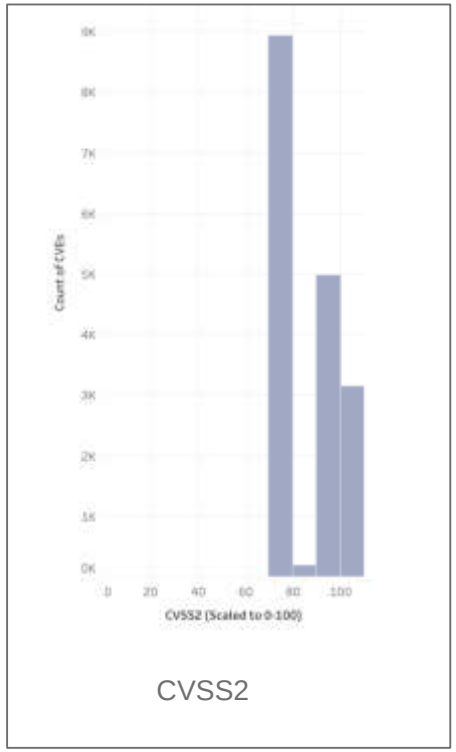
Vorteile

- Asset Owner: Korrelation der Schwachstellendaten mit CMDB und DDI Daten
- Kritische Schwachstellen: Korrelation der Schwachstellendaten mit Threat Intelligence
- Reporting: Erstellung aussagekräftiger Reports bis hin zum Self Service

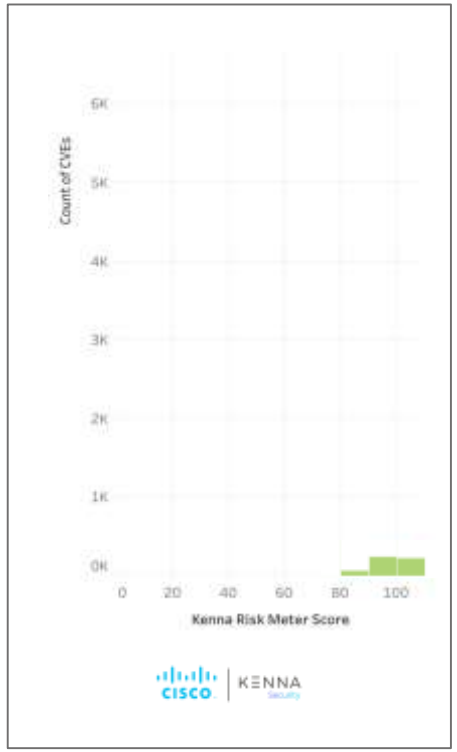
MEHRWERT PREDICTIVE PRIORITIZATION

DRAMATISCHER EINBRUCH DER ANZAHL ZU BEHANDELNDER SCHWACHSTELLEN

17.279 CVEs	627 CVEs	Die Nadel im Heuhaufen

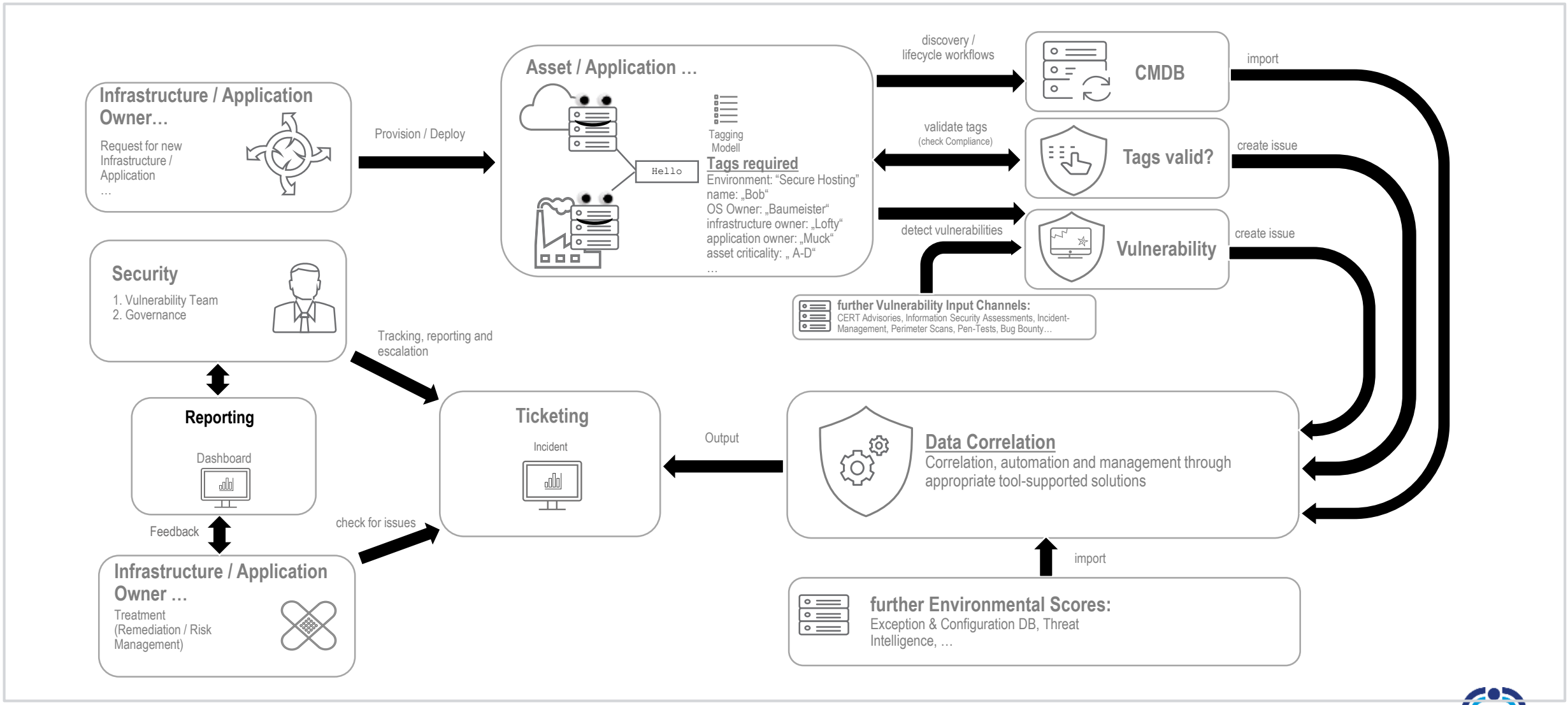


CVSS2



- Informationen werden wie AV Updates aus dem Internet bezogen und können in der Correlation Engine OnPrem verarbeitet werden.
- Service kann gemeinsam mit Tenable über einen Cisco Rahmenvertrag als Gesamtlösung bezogen werden.

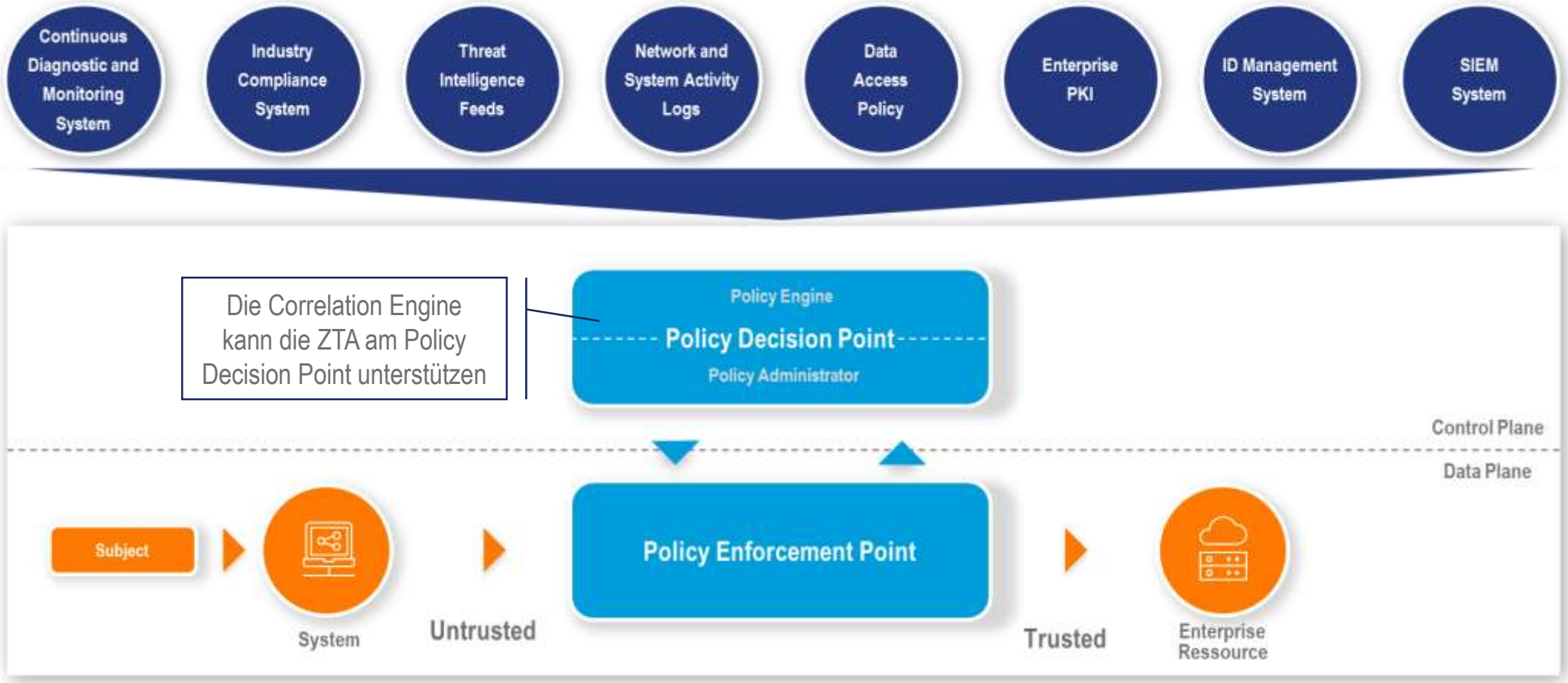
SCHRITTWEISE EINFÜHRUNG DER DATA CORRELATION ENGINE



CORRELATION ENGINE UND ZERO TRUST

LOGISCHE BAUSTEINE EINER ZERO TRUST ARCHTEKTUR

COMPUTACENTER ORIENTIERT SICH AN NIST SP 800-207



DEDICATED CLIENT – EIN BEISPIEL FÜR EINEN ZERO TRUST USE CASE