AUTOMATED VM

Ralf Nemeyer
Principal Consultant
Werner-Eckert-Straße 16-18, 81829 München, Germany
Mobile: +49 173 8929293
E-Mail: ralf.nemeyer@computacenter.com
WWW: www.computacenter.de

Peter Camillo Schmidt
Senior Consultant
Werner-Eckert-Straße 16-18, 81829 München, Germany
Mobile: +49 173 1590182
E-Mail: petercamillo.schmidt@computacenter.com
WWW: www.computacenter.de

COMPUTACENTER AUTOMATED VULNERABILITY MANAGEMENT

ÜBERBLICK DER LÖSUNGEN

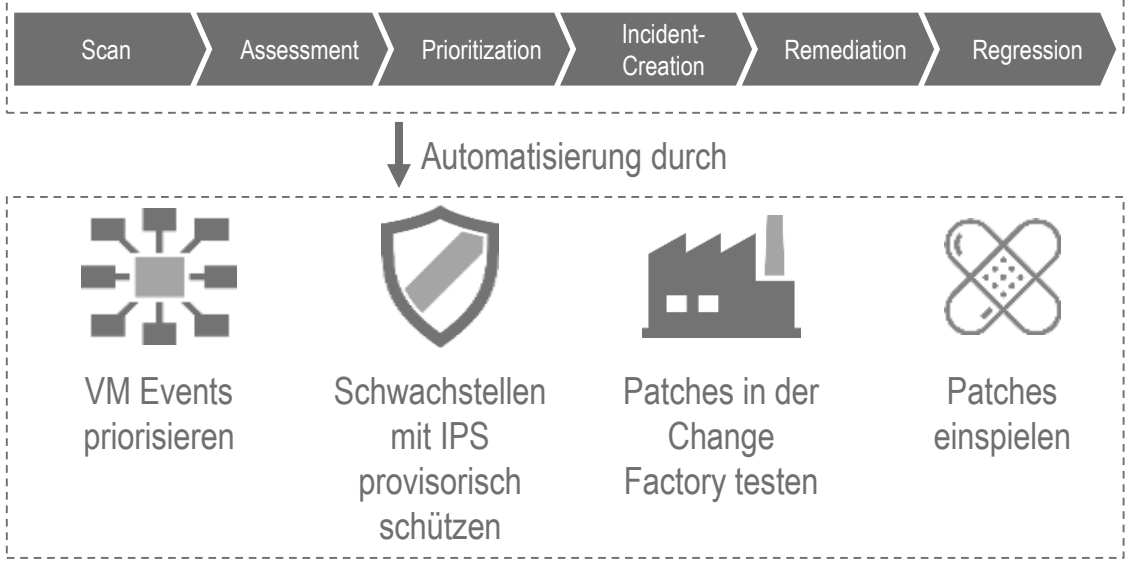
Situation

State of the Art Vulnerability Management Systeme liefern mit hoher Qualität die Schwachstellen der IT Landschaft. Diese Schwachstellen sind abzusichern, um vor Angriffen zu schützen. Laut SANS Institut gehört dies zu den Top 5 Maßnahmen zum Schutz vor Cyber Attacken.

Problem

Die Absicherung der IT Systeme ist eine komplexe Aufgabenstellung. Oftmals scheitert sie daran, dass die Systemeigner zu wenig Zeit zur Verfügung haben.

Lösung: Automatisierung des Prozesses



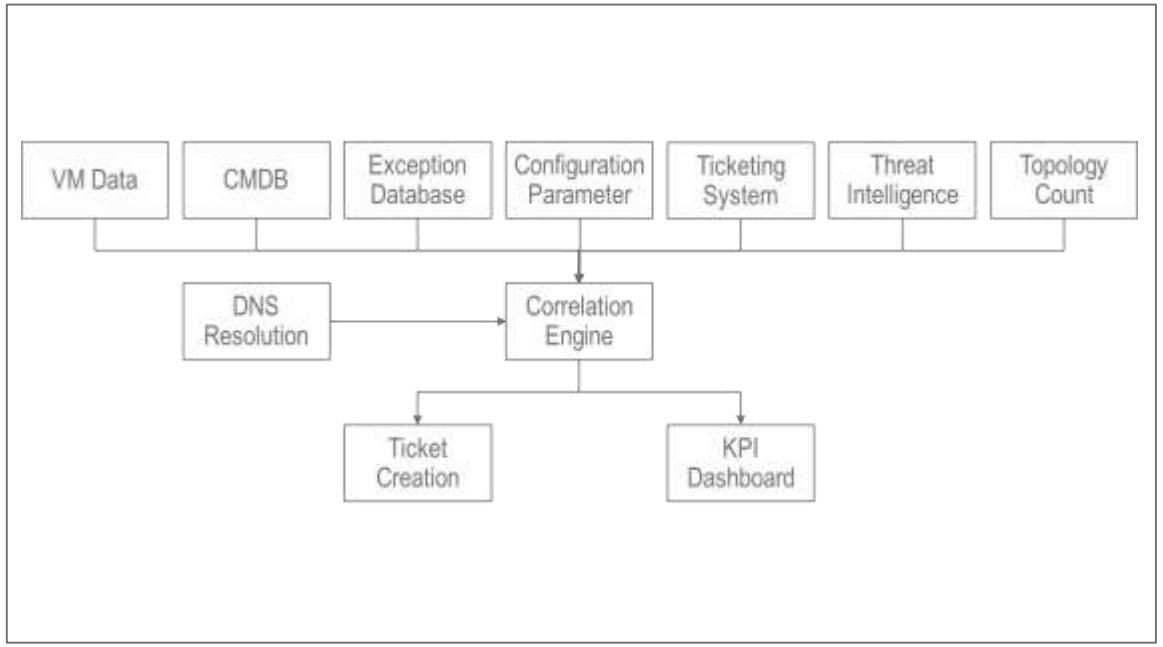
Use Cases

- Automatisierung des Schwachstellenmanagements bei internationaler Großbank
- Automatisierung des Schwachstellenmanagements bei Automobilhersteller
- Automatisierung des Schwachstellenmanagements bei internationalem Versicherungskonzern

KERN DER LÖSUNG IST EINE CORRELATION ENGINE

STEUERUNG DER ERZEUGUNG VON TICKETS

Anreicherung der VM Daten durch zusätzliche Datensilos



Identifikation von Asset Ownern

In großen Organisationen ist dies ein MUSS.

Priorisierung von Schwachstellen

Sinnvoll, wenn bestehende Remediation Prozesse mit unterschiedlichen Prioritäten angesteuert werden können, z.B.:

- Reguläres Patching: alle 3 Monate
- Service Fenster: wöchentlich
- Emergency Patching

ASPEKTE DER REMEDIATION PHASE

IN DER VERGANGENHEIT GAB ES OFTMALS STRIKTE TRENNUNGEN

Software Verteilung

Patchverteilung ist manchmal für Application Owner eine Hilfestellung

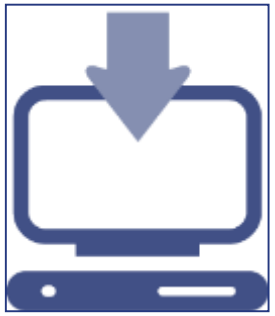
Change Factory

Nachbau kritischer Systeme bei einem Dienstleister zur Unterstützung von Application Tests

Virtual Patching

Import von CVE referenzierten Schwachstellen und IP Adressen in IPS oder NAC Umgebungen

TECHNISCHE UMGEBUNGEN MIT SPEZIELLEN HERAUSFORDERUNGEN



Clients

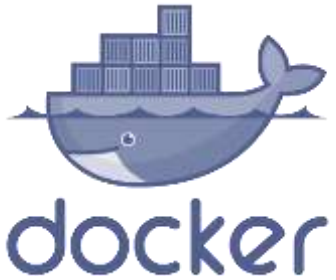
- Systemowner identifizieren
- Abdeckung der Clients im Scan-Zyklus (Teilzeitjobs, Mobile Mitarbeiter)
- Tracking der Systeme

Mobile Devices

- Definiere Policies
- Ordne Severities zu
- Reporte an MDM
- Remediate über MDM

Azure AWS ...

- Identifikation der Eigner
- Realtime Scanning
- Remediation Prozess



- Image Scans
- Compliance Scans
- Remediation Prozess

BETRIEB

KONTINUIERLICHE VERBESSERUNG DER EFFIZIENZ

Situation

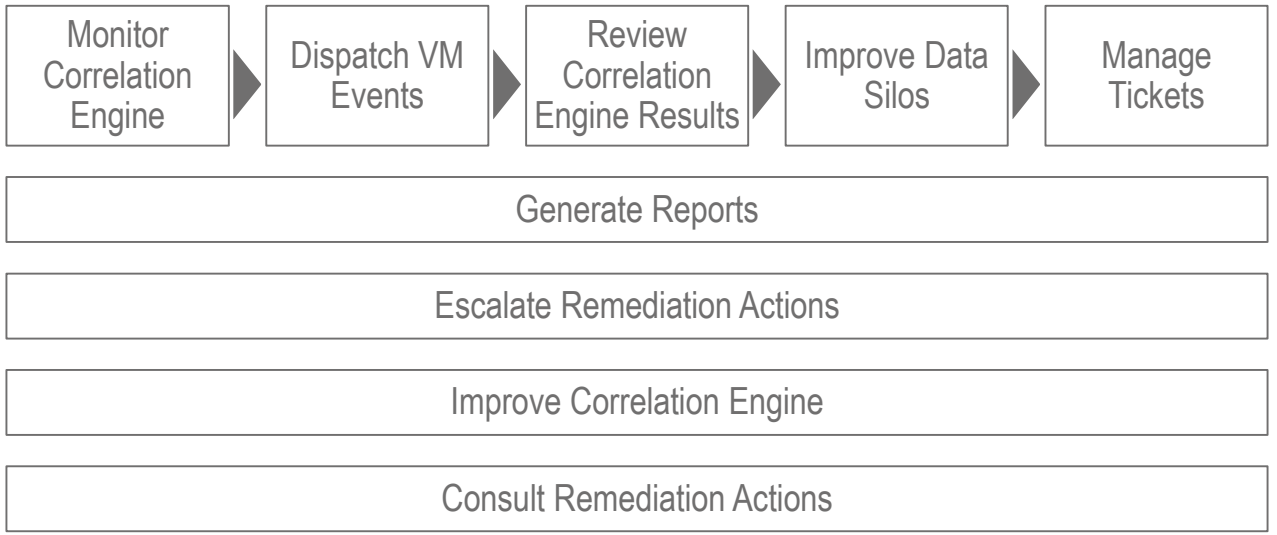
Trotz aller Automatisierung verbleiben Tätigkeiten, die im Rahmen des kontinuierlichen Betriebs umzusetzen sind.

Die Aufgaben des Betriebs erfordern die Unterteilung in einen Basisbetrieb und einen Betrieb, der sich über verschiedene Möglichkeiten zur auszeichnen kann und die Gesamt Performance verbessern kann.

Problem

Die Verbesserung der Performance erfordert Know How.

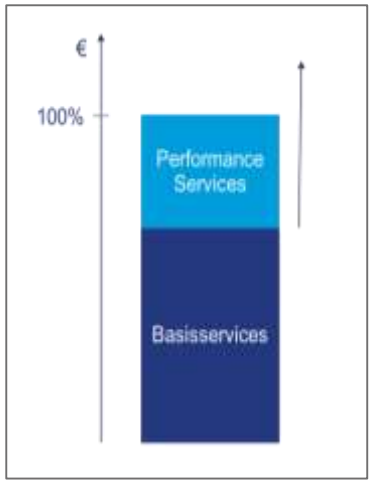
Lösung: Betriebsprozess und Aufteilung der Services



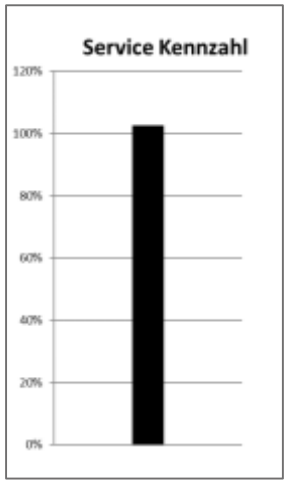
KPI BASED BILLING

ERFOLGSABHÄNGIGE SERVICE ERBRINGUNG

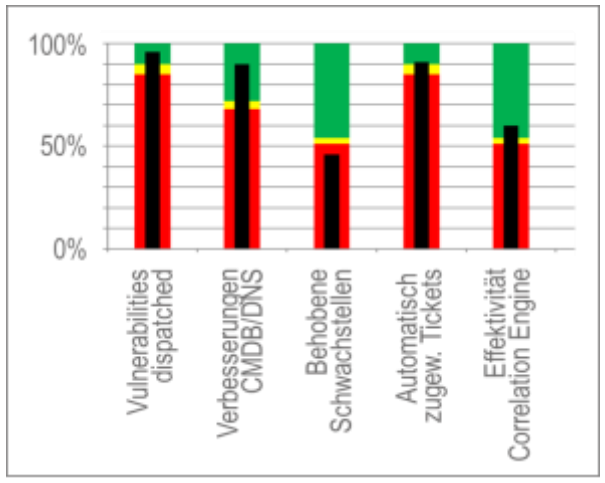
Performance Services und Basis Services



Service Kennzahl



Drill Down in die KPIs



Zeitliche Entwicklung der KPIs