TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Berlin, 13.06.2019

Ohne Cloud kein CSSP

Daniel Kramer - Veronym Holding GmbH
DACH Cybersecurity Advisor

Impuls

Impulse zur Cloud

Flexibilität

Leistungsstark

Schnell

weltweite Verfügbarkeit

Kosteneffizient

Sicher

Plattformunabhängigkeit

Budgetschonend

Service Entwurf

Mission: Wir möchten wesentlich dazu beitragen, die Online-Welt zu einem sicheren Ort zu machen.

Zielsetzung war die Bereitstellung einer breiten Palette von Cyber-Schutzmechanismen, unter der Voraussetzung, dass eine Inbetriebnahme des Service auf jedem Endgerät, ohne fachkundiges IT Personal innerhalb weniger Minuten erfolgen kann. Die Unternehmensgröße spielt dabei keine Rolle (1-n).

Organisationsform: **Cloud Security Service Provider** (CSSP)

Application layer access control (FWaaS)
Vulnerability Protection
Anti-Spyware
URL Filtering
File Blocking
Data Filtering
Antivirus mit Anbindung an die weltgrößte Cloud-Malware-Analyse-Umgebung und Malware-Datenbank
Security Reporting

Platform Challenge

- Eine exakte Vorhersage über die Nutzerwachstumskurve ist nicht möglich
- Eine Plattform zu bauen, die von Beginn an groß genug ist und jede Individualität abdeckt, ist nicht wirtschaftlich
- In Echtzeit auf schwankendes Nutzeraufkommen und Datenverkehr zu reagieren ist Voraussetzung
- Der Service muss sofort und weltweit verfügbar sein

Platform Challenge - Lösung

- Die Entwicklung des Service erfolgte, von der ersten Codezeile an, innerhalb der Cloud.
- Benötigte Instanzen mit speziellen Entwicklungsumgebungen wurden bei Bedarf hochgefahren, Tests durchgeführt, Ergebnisse ermittelt und Teilprojekte abgeschlossen.
- Lasttests unterschiedlicher Qualitäten konnten per Knopfdruck gestartet und dadurch wichtige Erkenntnisse innerhalb von Minuten bewertet werden.
- Das massive Datenaufkommen durch das Auswerten von Logfiles aus bis zu 6 Datenquellen erforderte ein hohes Aufkommen an Speicherkapazität, schon in der Entwicklungsphase. Unterschiedliche Cloud-Speicherqualitäten für “hot-“ und “colddata” kamen zum Einsatz.
- Vorgefertigte Cloud Module für die Umwandlung verschiedener Datenformate (CSV/RAW -> JSON- > Apache Parquet) beschleunigten die Entwicklungszeit unverhofft erheblich.

Platform Challenge - Lösung

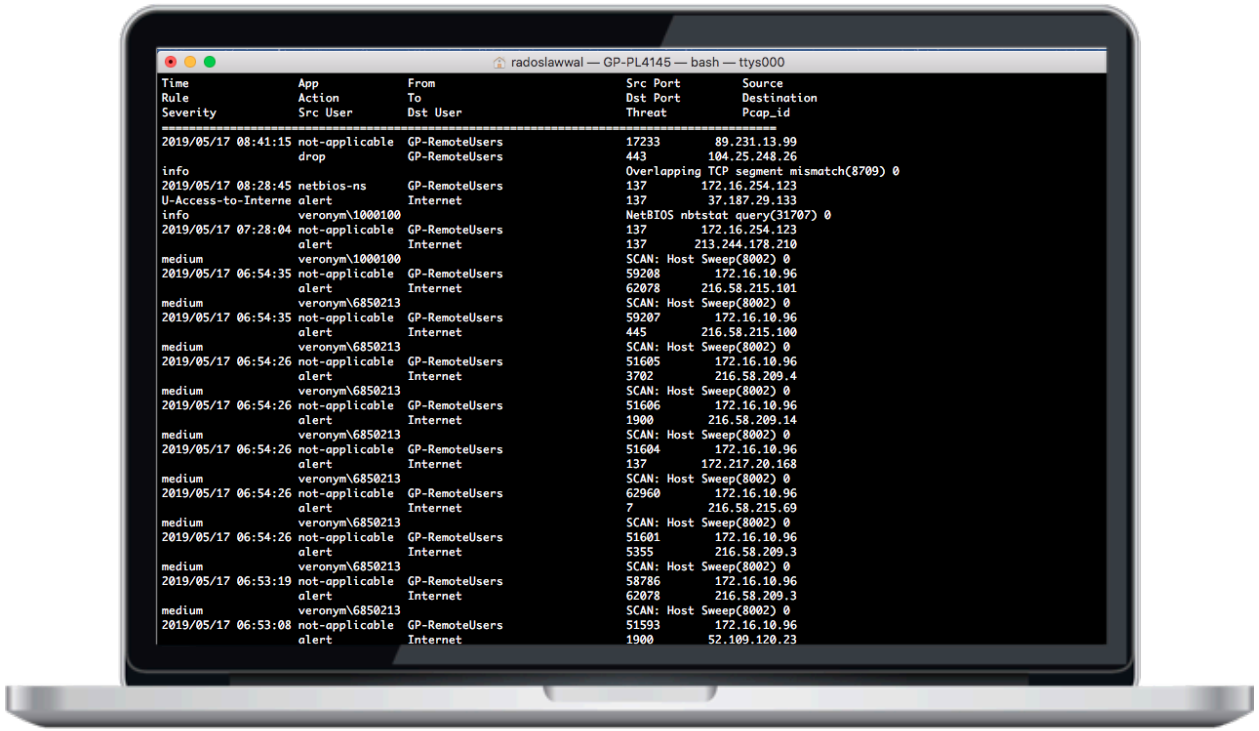
- SHOWSTOPPER

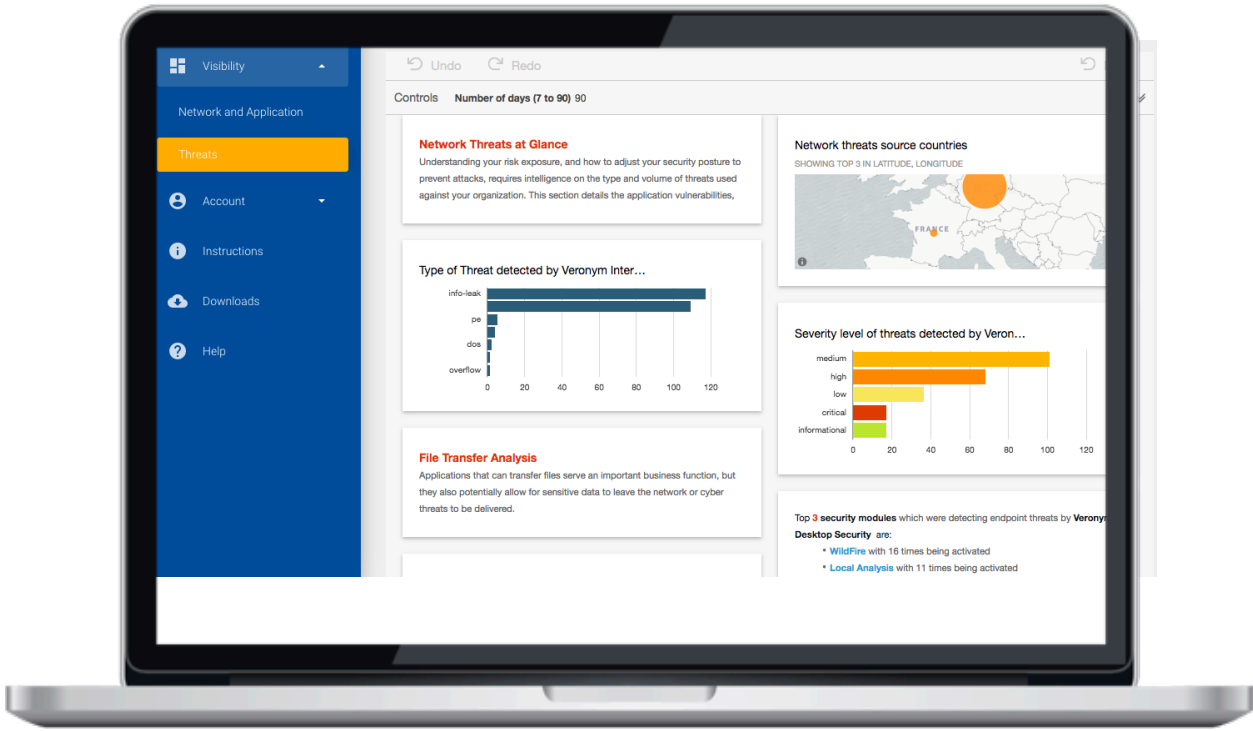
  Die Trennung des Management- vom Livetraffic muss über ein zweites Interface erfolgen

  on premise -> entweder Modelwechsel auf höhere Maschinenklasse oder Zukauf teurer Hardware, in beiden Fällen erheblicher finanzieller Aufwand und mehrere Tage/Wochen zeitlicher Verzug

  Cloud -> per Zubuchung der zweiten Interface-Option, start und stop des Services, erfolgte innerhalb weniger Minuten das Upgrade auf eine Instanz mit zwei ENI

Veronym Cybersecurity Service





Fazit

Die von uns geplante Entwicklungszeit des Service wurde anstatt nach 24 Monaten innerhalb 13 Monaten abgeschlossen.
Maßgeblich dafür waren Features aus der Cloud und Cloudcommunity.