One Pager – IBM Q1 (SWG)

Herausforderungen des Kunden

Durch die Zunahme von High-Profile Attacken, einer wachsenden Gefahr durch mobile Schwachstellen und immer komplexeren Bedrohungen, müssen sich auch die Security Landschaften innerhalb der Automobil-, Luft und HighTech Industrie immer schneller anpassen. Firmen müssen rasch Bedrohungen identifizieren, Betriebsspionage erkennen, Geschäftsrisiken vorhersehen und dabei umfangreiche Compliancebestimmungen einhalten.
Die Anforderungen an eine umfassende Security Infrastruktur sind vielfältig:

Threats & Security Visibility:
Betrug, Spionage, gezielte Exploits, Cyber-Kriminalität und Social Media Gefahren müssen intelligent sichtbar gemacht und bekämpft werden. Ohne eine breite Beobachtung und Integration können Bedrohungen übersehen werden. Dabei werden Tools benötigt, die den gesamten Risk Management Lifecycle adressieren.

Compliance & Policy:
Compliance erfordert die Erfassung und Auswertung von Milliarden von Logdateien und Einträgen pro Tag. Diese Regulierungen haben Auswirkungen auf den gesamten vertikalen Markt, auf Configuration Audits und manuelle Prozesse.

Lösung

Die Q1 Security Intelligence Platform liefert eine integrierte und automatisierte Security Lösung, die eine umfassende 360° Sicht über das gesamte Netzwerk bietet, unabhängig der Größe und Komplexität der Infrastruktur. Durch die einzigartige „One-Console“ Herangehensweise, wird der gesamte IT Security Lifecycle abgedeckt, d.h. vor, während und nach einer Attacke:

Prediction/Prevention Phase:

Risk Management	- QRadar Risk Manager
Compliance Management	- QRadar Risk Manager
Vulnerability Management	- QRadar Risk Manager
Configuration Management	- QRadar Risk Manager

Reaction / Remediation Phase:

Security Information & Event Management	- QRadar SIEM
Network/User Anomaly Detection	- Network / Virtual Activity Collectors
Log Management	- QRadar Log Manager

Nutzen für den Kunden

- Ermächtigt Security Professionals, Attacken, Exploits und Policy-Verstöße umfassend abzuwehren, zu verhindern, beseitigen und analysisieren
- Die flexible Architektur erlaubt Organisationen ihre Security Intelligence Infrastruktur mit nahtlos integrierten Anwendungen innerhalb einer einizigen Bedienungsoberfläche einfach zu skalieren
- Durch fortgeschrittene und forensische Analyse- und Korrelationsmethoden können abnormale Aktivitäten identifiziert werden, egal ob im Netzwerk, durch Anwendungen, Benutzeraktivität, mobile Endgeräte oder physische Security Devices – und das unabhängig ob cloud-basiert oder lokal
- Aufbau eines Sicherheitsprofils im Vorfeld einer Attacke durch automatisiertes Erkennen der Quellen und Auswirkungen potenzieller Bedrohungen sowie Reporting

Anknüpfungspunkte für Kundengespräch

- Welche Gefahren und Bedrohungen sehen Sie sich im Speziellen ausgesetzt?
- Wie werden Gefahren im Vorfeld eines Exploits identifiziert?
- Wie gehen Sie mit den Gefahren von Social Media um?
- Wie decken Sie den gesamten Security-Zyklus ab, d.h. vor, während und nach einer Attacke? Wie gewährleisten Sie ein integriertes Monitoring?
- Wie wird Security Management bereichs- und länderübergreifend standardisiert und ausgebaut?
- Gibt es eine direkte Toolunterstützung bei Anomaly Detection / Behaviour Monitoring?

Zielgruppe

- Chief Security Officer (CSO)
- Corporate Security Office
- Entwicklungsleiter im Bereich IT Security

Ansprechpartner

- SWG ()