Inbetriebnahme QRadar Installation in zehn (10) Tagen

Anhang A Leistungsbeschreibung (SOW) zu Ihrem IBM Angebot

Dienstleistung zum Festpreis

Inhaltsverzeichnis

Ersteller: Dr. Jobst H. Köhne, Leading Solution Sales Professional, IBM SWG Services Security Systems (ISSS)
Vertriebsbeauftragter Deutschland, Österreich und Schweiz / Sales Representative IMT DACH
Kontakt: jkoehne@de.ibm.com

1 Überblick und Ziel der Dienstleistungen

Die IBM unterstützt Sie dabei, Ihre QRadar Infrastruktur zu etablieren und die sicherheitsrelevanten Protokolldaten und Netzwerkaktivitäten innerhalb der Organisation in einer einzigen QRadar Logdatenbank, dem sog. Central Repository, zuverlässig zu speichern. Es bildet die zentrale Datengrundlage für die QRadar Suchfunktionen, die Möglichkeiten zur Filterung und Korrelationsanalyse und die Alarmfunktionen. Mit Hilfe dieser Funktionen verschafft QRadar Ihnen einen tiefen und umfassenden Einblick in den aktuellen Stand Ihrer eigenen physischen Informationsarchitektur. Das hochentwickelte und spezialisierte Überwachungswerkzeug vermag akute Angriffe und Bedrohungen der IT Sicherheit zu erkennen, Richtlinienverletzungen anzuzeigen und hilft Ihnen dabei, akute und latente operative Schwachstellen zu identifizieren.

Implementierungsvariante:

Die Implementierungsleistungen basieren auf der Möglichkeit einer verteilten Installation mit bis zu vier (4) spezialisierten Appliances, um eine Lastverteilung erreichen zu können. Dies umfasst jedoch keine Hochverfügbarkeit (Spiegelung) und keine Wiederherstellung nach einem Totalausfall.

2 Annahmen und Voraussetzungen

a. IBM kann den geplanten Zeitplan einhalten, wenn die kommerziellen und rechtlichen Vereinbarungen rechtzeitig getroffen sind und alle relevanten Informationen und Ansprechpartner verfügbar sind. IBM bittet um zwei (2) Wochen Vorlauf bei Absage oder Verschiebung von Service Einsätzen. Ihr Projektmanager wird auftretende Schwierigkeiten in dieser Hinsicht unverzüglich an IBM weiterleiten.

b. Für die Einrichtung von Logquellen kann es erforderlich sein, dass Sie für IBM Benutzerkonten bereitstellen, welche ggf. Administratorrechte haben.

c. Die Leistungen werden nur an einem Standort erbracht. Falls auch Konfigurationsleistungen für entfernt liegende Appliances in anderen Standorten erbracht werden sollen, richten Sie bitte vor Beginn des Projektes eine Möglichkeit zum Fernzugriff auf die betreffende Konsole in den anderen Standorten via SSH, HTTPS sowie auf das KVM/IMM2 Modul ein.

d. Bei dieser verteilten Installation benötigen die Geräte (Managed Hosts) eine maximale Lizensierung (bis zu 30.000 Ereignissen pro Sekunde) und es sind bis zu zwei (2) Appliances vorgesehen, welche als sogenannte „event processors“ konfiguriert werden.

e. Dieses Angebot ist nicht geeignet für folgende Situationen:

1. Konfiguration für Appliances in einer virtuellen Umgebung oder reine Softwarelizenzen (Der Kunde stellt die Hardware zur Verfügung)
2. Konfiguration von Katastrophenszenarien zum Wiederanlauf nach Totalverlust,
3. Konfiguration von Hochverfügbarkeit für weitere Geräte
4. Konfigurationen mit mehr als einem Compliance Package,
5. IBM Projektmanagement Leistungen,
6. Integration von nicht standardisierter oder individuell angepassten Integrationslösungen (z.B. kundeneigenen Werkzeugen, GRC Systemen oder nicht unterstützten Backuplösungen),
7. Konfiguration des QRadar Risk Managers.
8. Konfiguration des QRadar Vulnerability Managers,
9. Konfiguration von Incident Forensics,
10. Konfiguration von Data-Nodes.

f. Ist die Verwendung von 10Gbit Schnittstellen geplant, so müssen Sie im Vorfeld die passenden SFP+ Transceiver bestellen.

3 Verantwortlichkeiten der IBM

Die Verantwortungen für die folgenden Aktivitäten liegen bei IBM und ergänzen ggf. die Leistungen, die im Bestellschein beschrieben sind.

3.1 *Aktivität 1: Review der Kundenumgebung und QRadar Installation*

Während dieser Aktivität wird IBM die Aufstellung und Inbetriebnahme der Appliance vornehmen oder eine Konsole installieren, welche mit bis zu drei (3), von dieser aus gesteuerten, Geräten arbeitet. Diese Leistung umfasst im Einzelnen:

Vorgang	Aufgabe	Leistungen
Server Appliance Installation	Initial-Konfiguration	Konfiguration der folgenden Netzwerkparameter : • Hostname • Eigene IP Adresse der QRadar Appliance • IP Adresse des Default Gateway • IP Adresse der DNS Server • IP Adresse des E-Mail Servers • Passwörter • Einsetzen des Aktivierungsschlüssels
	Test der Verbindungen	• Prüfen der Verbindung mit den Protokollen HTTPS und SSH • Prüfen der grundlegenden Netzdienste
System Setup	Einstellungen von System und Konsole	• Lokale Firewall (auf der Appliance) • Management der internen Kollektor-schnittstellen • Einstellung der Systemzeit • Haltezeiten für die QRadar Datenbank und Einstellungen & Auswahl d. Optionen d. Filter • SNMP Einstellungen • Ausführen und Einstellen der automatischen Updates der Software der Appliance • Installation der neuesten sinnvollen Patches und Fixes • Anlegen von bis zu 5 Benutzern und Rollen • Einstellungen an der Konsole • DNS Einstellungen • Grundeinstellungen zu Reports • Einschalten bzw. Deaktivieren der akkumulierenden Zeitreihengrafiken nach Kundenvorgabe • Einstellung der Sicherungsdateien
	Sammeln von Netzdaten-abfolgen (Flows) und -ereignissen	• Zuordnung von Prozessen im Deployment Editor • Konfigurationseinstellungen am internen Kollektor

Kundenindividuelle Anpassungen und Durchsatzsteigerung	Netzwerk Hierachie	• Beratung und Erfassung der Anforderungen • Anlage und Test von Netzwerkhierarchien; bis zu 50 Objekte • Kundendemonstration und ggf. Anpassung gemäß der Anforderungen • Konfiguration der Sicherungsdatei für Netzwerkhierarchien
	Logquellen im Netz (Assets)	• Beratung und Erfassung der Anforderungen • Überprüfen der automatischen Registrierung von Servern (Logquellen) • Konfiguration von bis zu zehn (10) Logquellentypen

IBM übergibt zu dieser Aktivität keine Liefergegenstände.

3.2 *Aktivität 2: Sammeln von Logdaten*

Während dieser Aktivität unterstützt IBM Sie dabei, mit Ihrer neuen All-In-One Appliance, Logdaten von je bis zu drei Instanzen von bis zu zehn Typen von Logdatenquellen zu sammeln.
Es werden nur solche Typen von Logdatenquellen berücksichtigt, die im Produktumfang von QRadar durch einen Standardgeräteadapter (DSM; Device Support Module) unterstützt sind. Es werden keine kundenindividuellen Logdatenstromparser entwickelt oder QRadar Universalgeräteadapter zusammengestellt und konfiguriert (keine uDSMs). Das Sammeln von Logdaten und Netzdatenabfolgen (Flows) ist beschränkt auf die Möglichkeiten der QRadar Konfigurationsrichtlinien, die in der aktuellen Version des DSM Konfigurationshandbuchs beschrieben sind.

IBM übergibt zu dieser Aktivität keine Liefergegenstände.

3.3 *Aktivität 3: Sammeln von Netzdatenabfolgen (Flows)*

Während dieser Aktivität unterstützt IBM Sie dabei, mit Ihrer neuen neuen All-In-One Appliance, Flows von je bis zu drei Instanzen, von im QRadar Produktumfang als Standard unterstützen Netzdatenquellen zu sammeln.

IBM übergibt zu dieser Aktivität keine Liefergegenstände.

3.4 *Aktivität 4: Anpassung an Kundenumgebung (Initiales Tuning)*

Während dieser Aktivität wird IBM Sie dabei unterstützen, die Einstellung der Parameter Ihrer neuen Appliance vorzunehmen. Der Schwerpunkt wird dabei auf der Inbetriebnahme von im Produktumfang mitgelieferten und vorbereiteten Inhalten liegen. Dazu zählen Regeln, Richtlinien, Reports und deren Feineinstellungen, die dem Ziel dienen, möglichst weißes Rauschen und falsche Alarme von echten Bedrohungen zu unterscheiden. IBM leitet Ihre Mitarbeiter an, die Feineinstellungen der Schwellen und Filter für Berichte selbst vorzunehmen.

Ihr Team wird aktiv an den Entscheidungen, welche vorbereiteten Alarme und Berichtselemente aktiviert werden, beteiligt und in die Lage versetzt, schnell und einfach Feineinstellungen für QRadar vorzunehmen.

Das initiale Tuning umfasst:

a. Identifizieren und Beseitigen von Rauschquellen,

b. Aktivierung von vorgefertigten Regeln, gespeicherten Suchabfragen und Grafiken von akkumulierten Zeitreihen,

c. Auswahl und Einplanung von Standardberichten einschließlich Anpassung gemäß der Kundenanforderungen,

d. Anpassen von QRadar Konsolenansichten (Dashboards) gemäß der Kundenwünsche,

IBM übergibt zu dieser Aktivität keine Liefergegenstände.

3.5 *Aktivität 5: Weitere Integrationsschritte - Advanced Tuning*

Während dieser Aktivität wird IBM Sie dabei unterstützen, Ihre Appliance weiter auf seine geschäftlichen Anforderungen und Sicherheitsrichtlinien auszurichten. Sie können dabei eine Aufgabe aus folgenden zwei (2) Optionen auswählen:

a. Sicherung und Ablage der Logdaten, zum Beispiel über NFS,

b. Identifikation sowie Aktivierung aus Kundensicht wichtiger Reports, nach vorheriger gemeinsamer Absprache.

IBM übergibt zu dieser Aktivität ein Dokument mit den Konfigurationsentscheidungen.

4 Verantwortlichkeiten des Kunden

Ergänzend zu den allgemeinen Mitwirkungspflichten, die im Bestellschein beschrieben sind, folgen spezifische Beistellungen, ohne die der IBM Einsatz nicht erfolgreich sein kann.

Sie werden rechtzeitig zum Projektbeginn vor Eintreffen der IBM Berater folgende Voraussetzungen schaffen:

a. Die folgende Checkliste zur Installation der Appliance durcharbeiten:
- Nehmen Sie Kontakt mit dem IBM Support auf – richten Sie Ihren Zugang ein.
- Erfragen Sie Ihren Lizenzschlüssel und halten Sie diesen bereit.
- Notieren Sie die Aktivierungsschlüssel, die sich aufgeklebt auf der Appliance oder bei den Begleitpapieren befinden.
- Installieren Sie die Hardware Appliances in ein Rack (Geräterahmen) mit der richtigen Anschlusspannung.
- Sorgen Sie für Monitor und Tastatur für jede Appliance oder eine äquivalente KVM/IMM2 (Tastatur, Video, Maus) Lösung.
- Verbinden Sie die QRadar Appliances mit der Netzwerkinfrastruktur.
- Stellen Sie einen aktiven IP-Netzanschluss für jede Appliance sicher.
- Legen Sie die IP-Netzeinstellungen für die Appliance fest (Hostname, IP Addresse, Subnet Mask, Default Gateway, NTP/DNS/Mail Servers, usw. – siehe Handbuch).
- Ist die Verwendung von 10Gbit Schnittstellen geplant, so müssen Sie im Vorfeld die passenden SFP+ Transceiver bestellen.

b. Die folgende Checkliste zur Vorbereitung eines Steuerungs-PC´s abschließen:
- Ein Arbeitsplatzrechner muss bereit gestellt werden, um die QRadar Konsole aufzurufen.
- Der Zugriff zur QRadar Konsole via TCP Ports 22, 10000, 80 und 443 muss von dem Arbeitsplatzrechner aus gewährleistet sein (Hinweis: Falls die Verbindung über Firewalls verläuft oder spezielle Anforderungen an DSM bestehen, sehen Sie im Handbuch nach oder fragen Sie den IBM Support.).
- Das Kommandozeilen- und Skriptausführungsprogramm „secure shell“ (SSH) und das Programm „secure copy“ (SCP/SFTP) müssen installiert und einsatzbereit auf dem Arbeitsplatzrechner sein, der den Zugriff auf die Konsole hat.
- Ebenso muss auf dem Arbeitsplatzrecher installiert und einsatzbereit sein:
  - Die aktuellste Version des Internetbrowsers Mozilla Firefox (bevorzugt), des Internetbrowsers Internet Explorer 8.0 or 9.0 mit der Option „Compatibility View“ (aktiviert) oder die aktuellste Version des Internetbrowsers Google Chrome,
  - Java Runtime Environment Version 1.6 oder höher,
  - Adobe Flash 10.x.

c. Einen Ihrer Mitarbeiter als IBM's ersten Ansprechpartner für den betreffenden Standort benennen.

d. IBM darüber informieren, ob eine Sicherheitsüberprüfung und –freigabe für die IBM Mitarbeiter notwendig ist. Bitte planen Sie ggf. genügend Zeit für einen Freigabevorgang ein.

e. Systemadministratoren abstellen, die in der Lage und berechtigt sind, alle nötigen Logquellsysteme so zu konfigurieren, dass diese ihre Logdaten an die QRadar Kollektoren senden, sodass QRadar wiederum in die Lage versetzt wird, deren Logdaten zu sammeln und abzulegen. Zu den Typen von Logdatenquellen können Ereignisprotokolle (Events/Logs), Netzdatenabfolgen (Network Activity/Netflows) und IBM QRadar QFlow Appliances, je nach Ihrer Vorgabe, gehören.

f. Vorarbeiten zur Konfiguration der Logquellen gemäß Installationshandbuch (siehe QRadar Configuring DSM guide) abschließen.

g. Die Konfiguration ggf. vorhandener Netflows so vorbereiten, dass sie ihre Daten an die IP-Adresse senden können, die für die All-In-One Appliance festgelegt wurde.

h. Eine Liste erstellen, die die Logquellen, den Typ und die Verbindungsparameter für den Anschluss an QRadar enthält.

i. Festlegen der Netzhierarchie: Subnet Name, Description, IP/CIDR Werte, Risk Weight.

j. Festlegen der besonders wichtigen Logquellen mit ihren Angaben und Parametern, dem Hostnamen, den IP-Addressen und den Typen (z.B. Domain Controller, Mailserver, Webserver, DNS-Server, Netzwerkscanner, Firewalls, usw.).

5 Aufwände und Vergütung

Die hier beschriebenen Dienstleistungen einschließlich anfallender Reisezeiten werden zum

Festpreis von 18500,- € zzgl. MwSt. bzw. 22200,- SFR zzgl. USt.

erbracht.

Reisekosten und Spesen werden zusätzlich in Rechnung gestellt und sind im Bestellschein geregelt.

Die Leistungen werden nach Terminabstimmung mindestens zwei (2) Wochen vor Beginn mit dem Kunden vorzugsweise innerhalb von zwei (2) Wochen, an einem einzigen Standort des Kunden, erbracht.

Die Leistung gilt nach spätestens zehn (10) Personentagen als erbracht.

Bitte beachten Sie die im Bestellschein beschriebenen sonstigen rechtlichen und finanziellen Rahmenbedingungen, die je nach Land und Kunde voneinander abweichen können.

Ersteller: Dr. Jobst H. Köhne, Leading Solution Sales Professional, IBM SWG Services Security Systems (ISSS)
Vertriebsbeauftragter Deutschland, Österreich und Schweiz / Sales Representative IMT DACH
Kontakt: jkoehne@de.ibm.com