IBM QRadar Advisor with Watson

Diese Servicebeschreibung beschreibt den Cloud-Service. Die anwendbaren Auftragsdokumente enthalten Preisangaben und weitere Einzeleinheiten zur Bestellung des Kunden.

1. Cloud-Service

IBM QRadar Advisor with Watson bringt die kognitive Analyse auf die QRadar Security Platform und unterstützt Kunden und Sicherheitsanalysten bei der Untersuchung und Reaktion auf Bedrohungen. Dabei kommt der Wissenskorpus von Watson for Cyber Security ins Spiel, indem unstrukturierte Daten (z. B. Sicherheitswebsites, Blogs und Forschungsartikel) genutzt und mit lokalen Sicherheitsvorfällen in Beziehung gesetzt werden. Auf diese Weise können versteckte Bedrohungen aufgedeckt und die Erkenntnisgewinnung automatisiert werden, um angemessen reagieren und Entscheidungen treffen zu können. Mithilfe von QRadar Advisor with Watson kann ein Sicherheitsanalyst eine Sicherheitsverletzung an Watson senden, um eine Bedrohungserkennung anhand der Wissensdatenbank von Watson mit Hunderttausenden von unstrukturierten und strukturierten Datenquellen durchzuführen und das Ergebnis mit Bedrohungselementen im Zusammenhang mit der ursprünglichen Sicherheitsverletzung, wie z. B. schädlichen Dateien, verdächtigen IP-Adressen, betrügerischen Elementen (sog. Rogue Entities) und der Beziehung zwischen diesen, abzugleichen. Diese Vorgehensweise kann besonders geeignet sein, wenn es darum geht, festzustellen, ob eine Sicherheitsverletzung mit einer bekannten Malware-Kampagne in Zusammenhang steht. Ist dies der Fall, stellt Watson Hintergrundinformationen zur eingesetzten Malware, den ausgenutzten Schwachstellen und zum Umfang der Bedrohung (einschließlich der möglicherweise ebenfalls betroffenen Endpunkte) sowie andere Erkenntnisse zur Verfügung.

1.1 Angebote

Folgende Angebote stehen für den Kunden zur Wahl.

1.1.1 IBM QRadar Advisor with Watson

IBM QRadar Advisor with Watson setzt voraus, dass der Kunde über eine aktive IBM QRadar-Implementierung verfügt, entweder in einer lokalen On-Premises-Umgebung oder in einer Cloudimplementierung, und dass die Aktivierungssoftware des Cloud-Service dort installiert ist, damit der Kunde auf die Funktionalität des Cloud-Service zugreifen kann. Der Cloud-Service enthält eine „weiche Grenze“ für die Anzahl der Abfragen zu Sicherheitsverletzungen, die der Kunde an den Cloud-Service senden kann. Sie liegt bei 1,5 Anfragen pro Tag für jeweils 100 Ereignisse pro Sekunde (aufgerundet auf die nächste Anfrage), für die der Kunde berechtigt ist. Über diese Grenze hinausgehende Abfragen werden vom Cloud-Service während des restlichen Tages nicht verarbeitet.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise eignet sich besonders für große Security Operations Centers (SOC), in denen zweihundertfünfzigtausend Ereignisse pro Sekunde oder mehr in der Regel überschritten werden. Um Zugriff auf die Funktionalität des Cloud-Service zu erhalten, muss die Aktivierungssoftware des Cloud-Service auf der separat erworbenen IBM QRadar-Implementierung installiert werden. IBM QRadar Advisor with Watson – Enterprise ist unter der instanzbasierten Gebührenmetrik verfügbar, die nicht vom Umfang der IBM QRadar-Implementierung des Kunden abhängig ist. Der Kunde kann zu keiner Zeit mehr als 25 Einträge in die Warteschlange stellen.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

Das IBM QRadar Advisor with Watson – Starter Pack richtet sich an Erstbenutzer von QRadar Advisor with Watson. Dieser Cloud-Service beinhaltet die vollständige Funktionalität von QRadar Advisor with Watson, die oben in Abschnitt 1.1.1 beschrieben wird, steht aber nur für Kunden zur Verfügung, die QRadar Advisor with Watson zum ersten Mal erwerben, und kann nicht verlängert werden.

1.2 Optionale Services

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment richtet sich an Kunden, die beabsichtigen, den Cloud-Service in ihrer internen Testumgebung bereitzustellen, und kann nur für Tests außerhalb des

Produktionsbetriebs eingesetzt werden. IBM QRadar Advisor with Watson – Test Environment muss durch eine Subscription für den Cloud-Service im Produktionsbetrieb ergänzt werden.

1.3 Acceleration Services

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Im Rahmen dieses remote erbrachten Subscription-Service wird IBM dem Kunden die folgenden Beratungsleistungen an bis zu 5 Tagen innerhalb eines Jahres bereitstellen:

- Bewertung des SOC-Prozesses des Kunden einschließlich Untersuchung und/oder des Prozesses zur Störfallbehebung (Incident Response)
- Erneute Bewertung von Referenzsets
- Anpassung der automatischen Analyse von Verstößen großen Ausmaßes
- Anwendungsfallentwicklung
- Empfehlungen für SOC-Prozessänderungen, die QRadar Advisor with Watson einschließen
- Anleitungen zur bestmöglichen Beurteilung und Integration der Daten aus QRadar Advisor with Watson in die vorhandenen Prozesses des Kunden
- Vermittlung von Wissen zu relevanten QRadar Advisor with Watson-Themen

HINWEIS: Abhängig vom Status der QRadar-Implementierung des Kunden können die folgenden Aktivitäten in diesen Service integriert werden:

- Zustandsprüfung der QRadar-Implementierung des Kunden
- Weitere Optimierung der bestehenden QRadar-Implementierung
- Unterstützung beim Hinzufügen weiterer Protokollquellen zur QRadar-Implementierung des Kunden

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Dieser Setup-Service wird remote erbracht und beinhaltet vierzig (40) Stunden an Professional Services, die 90 Tage nach dem Erwerb verfallen, sofern nichts anderes vermerkt ist, unabhängig davon, ob das Stundenkontingent (sofern zutreffend) aufgebraucht wurde. Im Rahmen der Services wird dem Kunden ein IBM Engagement Manager zur Seite gestellt, der Kick-off-Telefongespräche terminiert.

IBM wird einige oder alle der folgenden Maßnahmen durchführen:

- Bewertung des SOC-Prozesses des Kunden einschließlich Untersuchung und/oder des Prozesses zur Störfallbehebung (Incident Response)
- Implementierung von QRadar Advisor with Watson in der Kundenumgebung
  - Installation von QRadar Advisor with Watson
  - Zuordnung einheitlicher Eigenschaften zu QRadar Advisor with Watson
  - Implementierung von Referenzsets
  - Anpassung der automatischen Analyse von Verstößen großen Ausmaßes
  - Anleitung bezüglich Anwendungsfall
  - Empfehlungen für SOC-Prozessänderungen, die QRadar Advisor with Watson einschließen

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

Dieser Setup-Service richtet sich an Kunden mit weniger als 5.000 Ereignissen pro Sekunde (EPS).

Im Rahmen dieses remote erbrachten Service wird IBM dem Kunden die folgenden Beratungsleistungen (oder eine Kombination dieser Leistungen) an bis zu 16 Stunden innerhalb eines Zeitraums von 90 Tagen bereitstellen:

- Installation von QRadar Advisor with Watson
- Berechtigungsmanagement für QRadar Advisor with Watson
- Konfiguration von QRadar Advisor with Watson, die Folgendes umfassen kann:
  - Konfiguration eines sicheren Proxy-Servers
  - Übermittlung von X-Force Exchange-Berechtigungsnachweisen
  - Erstellung von autorisierten Service-Token

- Konfiguration von Aufbewahrungsrichtlinien für das Speichern von Analyseergebnissen
- Zuordnung von benutzerdefinierten Ereigniseigenschaften
- Export von Referenzsets
- Zuordnung von Bedrohungsdaten
- Konfiguration von Assetkennungen
- Nutzungsoptimierung

- Automatisches Untersuchen von Verstößen und Anzeigen der Ergebnisse (mindestens ein Anwendungsfall/Showcase)
- Untersuchung der Erkenntnisse anhand des Beziehungsdiagramms

2. Datenblätter für Datenverarbeitung und Datenschutz

Die Ergänzenden Bedingungen zur Auftragsverarbeitung von IBM unter http://ibm.com/dpa (EB-AV) und die Datenblätter für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheets, nachfolgend „Datenblätter“ oder „Anlagen zu den EB-AV“ genannt) unter den nachstehenden Links enthalten zusätzliche Datenschutzinformationen für die Cloud-Services und deren Optionen in Bezug auf die Arten der Inhalte, die verarbeitet werden können, die damit verbundenen Verarbeitungstätigkeiten, die Datenschutzfunktionen und die Besonderheiten hinsichtlich der Aufbewahrung und Rückgabe der Inhalte. Die EB-AV finden Anwendung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und i) die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) oder ii) eines der unter http://ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze auf diese Verarbeitung Anwendung findet.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206

3. Service-Levels und technische Unterstützung

3.1 Service-Level-Agreement

IBM stellt dem Kunden das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) bereit. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service anwenden (siehe die nachstehende Tabelle). Der Prozentsatz der Verfügbarkeit wird berechnet als Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Serviceausfallminuten in dem betreffenden Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in dem Vertragsmonat. Die Definition von Serviceausfall, der Prozess zur Bearbeitung von Ansprüchen und die Kontaktaufnahme mit IBM bei Problemen mit der Serviceverfügbarkeit sind im IBM Cloud Service-Supporthandbuch unter https://www.ibm.com/software/support/saas_support_overview.html enthalten.

Verfügbarkeit	**Gutschrift (in Prozent (%) der monatlichen Subscription-Gebühr*)**
Unter 99,9 %	2 %
Unter 99,0 %	5 %
Unter 95,0 %	10 %

* Die Subscription-Gebühr ist der vertraglich vereinbarte Preis für den Monat, der Gegenstand des Anspruchs ist.

3.2 Technische Unterstützung

Eine Beschreibung der technischen Unterstützung für den Cloud-Service, einschließlich Support-Kontaktinformationen, Fehlerklassen, Unterstützungszeiten, Reaktionszeiten und sonstiger Unterstützungsinformationen und -prozesse, finden Sie durch Auswahl des Cloud-Service im IBM Support Guide, der unter https://www.ibm.com/support/home/pages/support-guide/ verfügbar ist.

4. Gebühren

4.1 Gebührenmetriken

Die Gebührenmetriken für den Cloud-Service sind im Auftragsdokument angegeben.

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Ereignis pro Sekunde“ (Event Per Second, EPS) ist das Auftreten eines bestimmten EPS, das von den Cloud-Services verarbeitet wird oder mit der Nutzung der Cloud-Services in Zusammenhang steht. Für die Zwecke dieses Cloud-Service sind die „Ereignisse pro Sekunde“ die Ereignisse, die von der IBM QRadar-Implementierung des Kunden erfasst und verarbeitet werden.
- „Instanz“ ist jeder Zugriff auf eine bestimmte Konfiguration der Cloud-Services.
- „Kundenprojekt“ (Engagement) ist ein Professional Service oder Schulungsservice im Zusammenhang mit den Cloud-Services.

5. Zusätzliche Bedingungen

Für Vereinbarungen für Cloud-Services (oder vergleichbare Cloud-Basisvereinbarungen), die vor dem 1. Januar 2019 unterzeichnet wurden, finden die Bedingungen unter https://www.ibm.com/acs Anwendung.

5.1 Aktivierungssoftware

Der Cloud-Service enthält die folgende Aktivierungssoftware:

- IBM QRadar with Watson App (https://exchange.xforce.ibmcloud.com/hub)

5.2 Rechtmäßige Nutzung des Cloud-Service

Der Cloud-Service ist dazu ausgelegt, den Kunden bei der Verbesserung seiner Sicherheitsumgebung und -daten zu unterstützen. Bei der Nutzung des Cloud-Service kann eine Reihe von Gesetzen oder Bestimmungen zu beachten sein, einschließlich solcher, die sich auf den Datenschutz, die Datensicherheit, arbeitsrechtliche Angelegenheiten sowie die elektronische Kommunikation und die Speicherung beziehen. Der Cloud-Service darf nur für gesetzlich zulässige Zwecke und in rechtmäßiger Weise verwendet werden. Der Kunde willigt ein, den Cloud-Service gemäß den anwendbaren Gesetzen, Bestimmungen und Richtlinien zu verwenden und die gesamte Verantwortung für deren Einhaltung zu übernehmen. Er versichert, dass er alle Einverständniserklärungen, Genehmigungen oder Lizenzen einholen wird oder eingeholt hat, die für die rechtmäßige Nutzung des Cloud-Service erforderlich sind.

6. Übergeordnete Bedingungen

6.1 Nutzung von Daten

Folgende Bestimmung hat Vorrang vor gegenteiligen Bestimmungen im Abschnitt „Inhalte und Datenschutz“ der Basisbedingungen für Cloud-Services zwischen den Vertragsparteien: IBM wird die Ergebnisse, die sich aus der Nutzung des Cloud-Service durch den Kunden ergeben und sich eindeutig auf Kundeninhalte beziehen (Erkenntnisse) oder den Kunden anderweitig identifizieren, weder verwenden noch offenlegen. IBM ist jedoch berechtigt, Inhalte und andere Informationen (ausgenommen Erkenntnisse), die sich im Laufe der Erbringung des Cloud-Service aus den Inhalten ergeben, zu verwenden, sofern persönliche Kennungen entfernt werden und personenbezogene Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden können. IBM wird diese Daten ausschließlich für Forschungs- und Testzwecke sowie für die Angebotsentwicklung verwenden.