Servicebeschreibung

IBM QRadar Advisor with Watson

Diese Servicebeschreibung bezieht sich auf den von IBM für den Kunden bereitgestellten Service. Als Kunde werden das Unternehmen, seine berechtigten Benutzer und die Empfänger des Cloud-Service bezeichnet. Das maßgebliche Angebot und der Berechtigungsnachweis (Proof of Entitlement = PoE) werden als separate Auftragsdokumente zur Verfügung gestellt.

1. Cloud-Service

1.1 IBM QRadar Advisor with Watson Service

IBM QRadar Advisor with Watson bringt die kognitive Analyse auf die QRadar Security Platform und unterstützt Kunden und Sicherheitsanalysten dabei, Bedrohungen schnell zu untersuchen und darauf zu reagieren. 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 schneller reagieren und bessere 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 Bedrohungsentitäten im Zusammenhang mit der ursprünglichen Sicherheitsverletzung, wie z. B. schädlichen Dateien, verdächtigen IP-Adressen, Rogue Entities und der Beziehung zwischen ihnen, 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.

Der Cloud-Service setzt voraus, dass der Kunde über eine aktive IBM Security QRadar-Implementierung verfügt und der Aktivierungscode 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 fünfzehn (15) Abfragen pro Tag für jeweils 1000 Ereignisse pro Sekunde, für die der Kunde berechtigt ist. Über diese Grenze hinausgehende Abfragen werden vom Cloud-Service verarbeitet, werden aber ohne Priorität behandelt und langsamer zurückgeschickt.

1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial („Cloud-Service zu Testzwecken“) stellt die Funktionalität von IBM QRadar Advisor with Watson auf Testbasis zur Verfügung. Der Kunde erhält während des im Auftragsdokument oder in einer anderen Dokumentation angegebenen Zeitraums Zugriff auf den Cloud-Service zu Testzwecken. Nach Ablauf dieses Zeitraums endet sein Zugriff. Während des Testzeitraums kann der Kunde maximal 5 Abfragen pro Tag zu Sicherheitsverletzungen senden. Der Cloud-Service zu Testzwecken wird ohne Gewähr und im gegenwärtigen Zustand (auf 'as-is'-Basis) bereitgestellt und darf vom Kunden nur für interne Tests und nicht produktionsbezogene Zwecke genutzt werden. Die Antwortzeiten auf Abfragen können während der Testphase abhängig vom aktuellen Datenverkehrsvolumen variieren.

2. Sicherheitsbeschreibung

Dieser Cloud-Service orientiert sich an den unter http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp verfügbaren IBM Datensicherheits- und Datenschutzrichtlinien für IBM SaaS sowie etwaigen weiteren Bedingungen in diesem Abschnitt. Änderungen der IBM Datensicherheits- und Datenschutzrichtlinien führen nicht zu einer Beeinträchtigung der Sicherheit des Cloud-Service.

Dieser Cloud-Service kann zur Verarbeitung ausgewählter Inhalte verwendet werden, die personenbezogene Daten enthalten, wenn der Kunde als der für die Verarbeitung Verantwortliche sich davon überzeugt hat, dass die technischen und organisatorischen Sicherheitsmaßnahmen den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen sind. Der Kunde ist sich dessen bewusst, dass dieser Cloud-Service keine Funktionen zum Schutz von sensiblen

personenbezogenen Daten oder von Daten bietet, die zusätzlichen regulatorischen Anforderungen unterliegen. IBM hat keine Kenntnis von der Art der Daten, die in den Inhalten enthalten sind, und kann keine Einschätzung bezüglich der Eignung der Cloud-Services oder der getroffenen Sicherheitsmaßnahmen abgeben.

Der Cloud-Service ermöglicht den Kunden lediglich das Einstellen und Verwalten der folgende Inhalte, die gemäß den anwendbaren Datenschutzgesetzen zum Teil ggf. als personenbezogene Daten gelten:

- Quell-/Ziel-IP-Adressen
- URLs
- Domänen
- Dateihashes

2.1 Sicherheitsfunktionen und Verantwortlichkeiten

Mit dem Cloud-Service werden die folgenden Sicherheitsfunktionen implementiert:

Im Rahmen des Cloud-Service werden Inhalte bei der Datenübertragung (in Transit) zwischen dem IBM Netz und der IBM Security QRadar-Implementierung des Kunden verschlüsselt. Im Cloud-Service ruhende Inhalte (at Rest), die zur Übertragung vorgesehen sind, werden nicht verschlüsselt.

An den Cloud-Service gesendete Inhalte bleiben nach ihrer Verarbeitung weder im Cloud-Service erhalten noch werden sie dort gespeichert.

3. Technische Unterstützung

Technische Unterstützung für den Cloud-Service wird per E-Mail, in Online-Foren und über ein Onlinesystem für die Problemmeldung, wie nachstehend beschrieben, bereitgestellt. Die technische Unterstützung ist Bestandteil des Cloud-Service und nicht als separates Angebot erhältlich.

Fehlerklasse	Definition der Fehlerklasse	Angestrebte Reaktionszeiten	Deckungszeiten
1	**Kritische Auswirkung auf den Geschäftsbetrieb/Serviceausfall:** Geschäftskritische Funktionen sind nicht funktionsfähig oder eine kritische Schnittstelle ist ausgefallen. Dies betrifft normalerweise eine Produktionsumgebung und weist darauf hin, dass der Zugriff auf die Services nicht möglich ist, mit kritischen Auswirkungen auf betriebliche Abläufe. In diesem Fall ist eine sofortige Lösung erforderlich.	Innerhalb von 1 Stunde	24x7
2	**Erhebliche Auswirkung auf den Geschäftsbetrieb:** Die Nutzung eines Service-Features oder einer Servicefunktion ist stark eingeschränkt oder es besteht die Gefahr, dass der Kunde Abgabefristen nicht einhalten kann.	Innerhalb von 2 Stunden während der Geschäftszeiten	Mo-Fr zu den Geschäftszeiten
3	**Geringe Auswirkung auf den Geschäftsbetrieb:** Der Service oder die Funktionalität kann genutzt werden und das Problem hat keine kritische Auswirkung auf betriebliche Abläufe.	Innerhalb von 4 Stunden während der Geschäftszeiten	Mo-Fr zu den Geschäftszeiten
4	**Minimale Auswirkung auf den Geschäftsbetrieb:** Eine Anfrage oder eine Frage nicht technischer Art.	Innerhalb 1 Arbeitstages	Mo-Fr zu den Geschäftszeiten

Für Kunden, die an der Betaversion des Cloud-Service teilnehmen und noch mit Version 7.2.7 der QRadar Platform arbeiten, können einige Probleme im Zusammenhang mit der technischen Unterstützung möglicherweise nicht behoben werden. Betroffene Kunden müssen ein Upgrade auf

Version 7.2.8 durchführen und das neueste Patch installieren, um volle technische Unterstützung zu erhalten.

4. Informationen zur Berechtigung und Abrechnung

4.1 Gebührenmetriken

Der Cloud-Service ist mit der im Auftragsdokument angegebenen Gebührenmetrik verfügbar:

a. **100 Ereignisse pro Sekunde** ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein Ereignis ist das Auftreten eines bestimmten Vorkommnisses, das vom Cloud-Service verarbeitet wird oder mit der Nutzung des Cloud-Service in Zusammenhang steht. Es müssen ausreichende Berechtigungen erworben werden, um die Gesamtzahl der Ereignisse pro Sekunde (aufgerundet auf die nächsten hundert) abzudecken, die während des Messzeitraums eintreten, der im Berechtigungsnachweis oder Auftragsdokument angegeben ist.

5. Laufzeit und Verlängerungsoptionen

Die Laufzeit des Cloud-Service beginnt an dem Datum, an dem IBM dem Kunden mitteilt, dass sein Zugriff auf den Cloud-Service gemäß der Angabe im Berechtigungsnachweis freigeschaltet ist. Im Berechtigungsnachweis ist festgelegt, ob sich der Cloud-Service automatisch verlängert, auf fortlaufender Basis genutzt werden kann oder am Ende der Laufzeit abläuft.

Bei automatischer Verlängerung wird der Cloud-Service automatisch um die im Berechtigungsnachweis angegebene Laufzeit verlängert, es sei denn, der Kunde teilt IBM mindestens 90 Tage vor dem Ablaufdatum schriftlich mit, dass er keine Verlängerung wünscht.

Bei fortlaufender Nutzung steht der Cloud-Service auf monatlicher Basis ununterbrochen zur Verfügung, bis der Kunde unter Einhaltung einer Frist von 90 Tagen schriftlich kündigt. Der Cloud-Service bleibt nach Ablauf der 90-Tage-Frist bis zum Ende des Kalendermonats verfügbar.

6. Aktivierungssoftware

Für den Cloud-Service ist Aktivierungssoftware erforderlich, die der Kunde auf seine Systeme herunterlädt, um die Nutzung des Cloud-Service zu ermöglichen. Die Aktivierungssoftware darf nur in Verbindung mit dem Cloud-Service verwendet werden. Die Aktivierungssoftware wird im gegenwärtigen Zustand (auf „as-is“-Basis) bereitgestellt.

Die Aktivierungssoftware für den Cloud-Service steht über die IBM Security App Exchange unter https://exchange.xforce.ibmcloud.com/hub für den Kunden zum Download zur Verfügung.

7. Zusätzliche Bedingungen

7.1 Allgemeines

Der Kunde erklärt sich damit einverstanden, dass IBM in Werbe- oder Marketingmaterial öffentlich auf den Kunden als Subskribent der Cloud-Services verweisen darf.

7.2 Aktivierungssoftware

Für den Cloud-Service ist Aktivierungssoftware erforderlich, die der Kunde auf seine Systeme herunterlädt, um die Nutzung des Cloud-Service zu ermöglichen. Die Aktivierungssoftware darf nur in Verbindung mit dem Cloud-Service verwendet werden. Die Aktivierungssoftware wird im gegenwärtigen Zustand (auf „as-is“-Basis) bereitgestellt.

Die Aktivierungssoftware für den Cloud-Service steht über die IBM Security App Exchange unter https://exchange.xforce.ibmcloud.com/hub für den Kunden zum Download zur Verfügung.

7.3 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 beachtet 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.

7.4 Ablauf des Cloud-Service

Vor dem Ablauf oder der Beendigung des Cloud-Service können Daten vom Kunden über die vom Cloud-Service bereitgestellten Berichterstellungs- oder Exportfunktionen extrahiert werden.

7.5 Sicherheitsdaten

Im Rahmen des Cloud-Service, der eine Berichterstattung beinhaltet, wird IBM anonymisierte und/oder aggregierte Informationen, die aus dem Cloud-Service erfasst wurden, aufbereiten und verwalten („Sicherheitsdaten“). Die Sicherheitsdaten lassen keine Rückschlüsse auf den Kunden oder eine Person zu, außer wie unten in Absatz (d) vorgesehen. Der Kunde erklärt sich außerdem damit einverstanden, dass IBM die Sicherheitsdaten nur für folgende Zwecke verwenden und/oder kopieren darf:

a. Veröffentlichung und/oder Weitergabe der Sicherheitsdaten (z. B. in Datensammlungen und/oder Analysen im Zusammenhang mit Cybersicherheit)

b. Entwicklung oder Verbesserung von Produkten oder Services

c. Durchführung interner Recherchen oder mit Dritten

d. Rechtmäßige Weitergabe von bestätigten Informationen über externe Täter