IBM QRadar on Cloud

Diese Servicebeschreibung beschreibt den Cloud-Service, den IBM für den Kunden erbringt. Als Kunde werden der Vertragspartner und seine berechtigten Benutzer sowie 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 on Cloud 100 EPS

Das Angebot IBM QRadar on Cloud ist eine innovative Security-Intelligence-Lösung aus der IBM Cloud, die auf dem Produkt IBM Security QRadar SIEM basiert. Sie ermöglicht die Erfassung, Korrelation und Speicherung von Ereignissen, die sowohl in Vor-Ort- als auch in Cloudumgebungen generiert werden. Maßnahmen für Sicherheits- und Bedrohungsmanagement können auf die gleiche Weise wie mit einem vor Ort bereitgestellten QRadar SIEM-Produkt durchgeführt werden. Im Rahmen des Angebots bietet IBM außerdem eine Infrastrukturüberwachung rund um die Uhr (auf 24x7-Basis) und installiert die neueste Softwareversion oder kritische Patches, sobald sie verfügbar sind.

Dieser Cloud-Service enthält einen aktiven, durchsuchbaren Speicher für die Dauer von neunzig (90) Tagen.

1.2 Optionale Features oder Services

1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

Ein Service-Upgrade, mit dem die Kapazität für die Erfassung und Verarbeitung von Protokollereignissen um weitere 1000 EPS erweitert wird, aber nur temporär für eine bestimmte Anzahl von Monaten. Der Kunde kann dieses Upgrade mehrfach, bis maximal zu der Anzahl EPS erwerben, die vom Angebot unterstützt wird. Mit diesem Feature erhalten Kunden, die während des Jahres Belastungsspitzen bewältigen müssen, die Möglichkeit, solche Anforderungen über ein temporäres Kapazitätsupgrade abzufangen. Nach Ablauf der Laufzeit werden die temporären Kapazitätserweiterungen wieder aus der Kundenumgebung entfernt.

1.2.2 IBM QRadar on Cloud Data Capacity 100 EPS

Mit dem Datenkapazitätsupgrade wird zusätzlicher Speicher hinzugefügt und der Analysezeitraum verlängert. Das Kapazitätsupgrade ermöglicht den Kunden für jedes erworbene 100-EPS-Upgrade die Datenspeicherung von bis zu einem vollen Jahr.

1.2.3 IBM QRadar on Cloud Flows Add-On

Wird mit IBM QRadar SIEM und Flussprozessoren integriert, um Sichtbarkeit auf Netzwerkschicht 3 und Ablaufanalyse bereitzustellen und den Kunden beim Aufspüren, Erkennen und Reagieren auf Aktivitäten in seinem Netz zu unterstützen.

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Proaktives Aufspüren und Erkennen von Sicherheitslücken in Netzgeräten und Anwendungen, Hinzufügen von Kontexten und Unterstützung bei der Priorisierung von Aktivitäten zur Fehlerbehebung und Risikominderung.

1.2.5 IBM QRadar on Cloud Log Archival

Ermöglicht dem Kunden die Archivierung von Ereignisdaten aus dem Cloud-Service während der Subscription-Laufzeit. IBM wird mit dem Kunden zusammenarbeiten, um ausgewählte Ereignisse zu Archivierungszwecken in den Objektspeicher zu schreiben. Auf Anforderung des Kunden wird IBM innerhalb von drei (3) Geschäftstagen nach der Anforderung archivierte Ereignisdaten für einen Zeitraum von dreißig (30) Tagen in die Cloud-Service-Instanz des Kunden zurückladen. Diese Daten stehen dem Kunden für 48 Stunden zur Verfügung, bevor sie wieder in den Objektarchivierungsspeicher zurückübertragen werden. Innerhalb von drei Monaten kann der Kunde bis zu zwei Anforderungen stellen. Das Kapazitätsupgrade ermöglicht den Kunden für jedes erworbene 100-EPS-Upgrade die Datenspeicherung von bis zu einem vollen Jahr.

1.2.6 IBM QRadar on Cloud Optimization Service

Für diesen remote erbrachten Subscription-Service wird IBM eine Review-Besprechung mit dem Kunden abhalten, um den aktuellen Status der Cloud-Service-Instanz des Kunden zu beurteilen, und dem Kunden die Ergebnisse in Form eines QRadar on Cloud Health Status-Berichts bereitstellen, in dem Bereiche mit Verbesserungspotenzial identifiziert werden.

Darüber hinaus wird IBM dem Kunden auf Anforderung die folgenden Beratungsleistungen für bis zu acht (8) Tage innerhalb eines Jahres bereitstellen:

- Unterstützung beim Hinzufügen weiterer Protokollquellen zum Cloud-Service
- Konfiguration weiterer Suchvorgänge, Berichte und Dashboards
- Weitere Optimierung der bestehenden QRadar-Implementierung
- Vermittlung von Wissen zu relevanten QRadar-Themen

1.3 Setup-Services

Die folgenden Setup-Services werden remote erbracht und können separat bestellt werden. Jeder bestellte Service verfällt 90 Tage nach dem Erwerb, 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.

1.3.1 IBM QRadar on Cloud Deployment Service

Dieser Service bietet vierzig (40) Stunden an Professional Services, in denen IBM einige oder alle der folgenden Maßnahmen durchführen wird:

IBM wird eine Prüfung der SIEM-Architektur (bis zu sechzehn Stunden) durchführen, um die Berichtspflichten des Kunden zu definieren, und dem Kunden die Prüfungsergebnisse in einem Lösungsarchitekturbericht zur Verfügung stellen, der dazu beitragen soll, die Anforderungen des Kunden zu definieren und zu erfassen.

Dieser Bericht enthält Folgendes:

- Die definierten Berichtspflichten des Kunden, um ihn bei Compliance-, Auditing- und Security-Intelligence-Anforderungen zu unterstützen
- Die Security-Intelligence-Anforderungen, Anwendungsfälle und Apps, bei deren Implementierung IBM den Kunden ggf. unterstützt (bis zu zehn (10) Anwendungsfälle und bis zu zwei (2) Apps)
- Allgemeine Informationen zu den Protokoll- und Datenflussquellen des Kunden, die zur Unterstützung der Anwendungsfälle benötigt werden
- Überlegungen zur Netzinfrastruktur, beispielsweise hinsichtlich Firewalls und Ports

Auf der Grundlage des Lösungsarchitekturberichts wird IBM die folgenden Tätigkeiten ausführen, sofern die verbleibende Zeit dies zulässt:

- Konfigurieren der Ereignissammlung für bis zu drei (3) Instanzen aus bis zu zehn (10) Protokollquellentypen im Cloud-Service. Diese Aktivität beinhaltet die Vermittlung von Wissen an die zuständigen Mitarbeiter des Kunden, sodass sie bei Bedarf weitere Protokollquellen hinzufügen können. Im Rahmen dieses Service werden nur Protokollquellen berücksichtigt, die von den QRadar-Standardeinheitenunterstützungsmodulen (Device Support Modules, DSMs) unterstützt werden
- Erstoptimierung, dazu gehören a) die Aktivierung von Standardregeln, gespeicherten Suchen, Zeitreihendiagrammen mit kumulierten Werten sowie Berichten; b) die Identifizierung und Entfernung von Störquellen; und c) die Konfiguration von Offlinespeicher über NFS, CIFS oder iSCSI
- Implementierung von bis zu zehn (10) Anwendungsfällen und zwei (2) Apps aus IBM QRadar App Exchange gemäß der Beschreibung im Lösungsarchitekturdokument

1.3.2 IBM QRadar on Cloud Custom Parser Service

Dieser Service beinhaltet die Entwicklung eines angepassten Parsers/uDSM für die Unterstützung der vom Standard abweichenden Protokollquellentypen des Kunden, die an den Cloud-Service gesendet werden sollen, und schließt folgende Tätigkeiten ein:

- Erstellen eines angepassten Parsers für einen einzelnen vom Standard abweichenden Protokollquellentyp (wird remote ausgeführt)
- Erstellen, Konfigurieren und Zuordnen eines uDSM
- Bereitstellen und Testen des angepassten uDSM
- Syntaktisches Analysieren (Parsen) von bis zu fünfundzwanzig Nachrichtentypen für die Protokollquelle

2. Inhalte und Datenschutz

Das Datenblatt für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheet, nachfolgend „Datenblatt“ genannt) enthält relevante Informationen über den Cloud-Service in Bezug auf die Art der Inhalte, die für die Verarbeitung freigegeben sind, die damit verbundenen Verarbeitungsaktivitäten, die Datenschutzfunktionen und die Besonderheiten hinsichtlich der Aufbewahrung und Rückgabe der Inhalte. Alle Einzelheiten oder Erläuterungen und Bedingungen, einschließlich der Verantwortlichkeiten des Kunden, im Zusammenhang mit der Nutzung des Cloud-Service und der Datenschutzfunktionen, sofern anwendbar, werden in diesem Abschnitt beschrieben. Abhängig von den vom Kunden gewählten Optionen und dessen Nutzung des Cloud-Service können mehrere Datenblätter zur Anwendung kommen. Das Datenblatt ist ggf. nur in englischer Sprache und nicht in einer Landessprache verfügbar. Trotz lokaler Gesetze oder Gepflogenheiten bestätigen die Vertragsparteien, dass sie Englisch verstehen und diese Sprache für den Erwerb und die Nutzung der Cloud-Services geeignet ist. Die folgenden Datenblätter beziehen sich auf den Cloud-Service und die verfügbaren Optionen. Der Kunde bestätigt, dass i) IBM die Datenblätter von Zeit zu Zeit nach eigenem Ermessen ändern kann und dass ii) diese Änderungen frühere Versionen ersetzen. Alle Änderungen an den Datenblättern werden mit der Absicht durchgeführt, i) bestehende Verpflichtungen von IBM zu verbessern oder transparenter zu gestalten, ii) die Umsetzung neu eingeführter Standards und anwendbarer Gesetze sicherzustellen oder iii) zusätzliche Verpflichtungen seitens IBM aufzunehmen. Durch Änderungen an den Datenblättern wird der Datenschutz in Bezug auf einen Cloud-Service nicht verringert.

Link(s) zu den anwendbaren Datenblättern:

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7

Der Kunde ist dafür verantwortlich, die verfügbaren Datenschutzfunktionen für einen Cloud-Service zu bestellen, zu aktivieren und anzuwenden, und übernimmt die Verantwortung für die Nutzung der Cloud-Services, wenn er dieser Verpflichtung nicht nachkommt. Dies gilt auch für die Erfüllung von Datenschutzanforderungen sowie anderer rechtlicher Anforderungen in Bezug auf Inhalte.

Die Ergänzenden Bedingungen zur Auftragsverarbeitung (EB-AV) von IBM unter http://ibm.com/dpa und die zugehörigen Anlagen finden Anwendung und ergänzen diese Vereinbarung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) auf diese Verarbeitung Anwendung findet. Die für diesen Cloud-Service anwendbaren Datenblätter dienen als Anlagen zu den EB-AV. Sofern die EB-AV Anwendung finden, richtet sich die Verpflichtung von IBM, Änderungen bezüglich der Unterauftragsverarbeiter bekannt zu geben, und das Recht des Kunden, Einspruch gegen eine solche Änderung einzulegen, nach den Regelungen in den EB-AV.

3. Service-Level-Agreement

Das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) wird von IBM, so wie im Berechtigungsnachweis angegeben, für den Cloud-Service bereitgestellt. Das SLA stellt keine Gewährleistung dar. Es wird nur Kunden zur Verfügung gestellt und gilt ausschließlich für Produktionsumgebungen.

3.1 Gutschriften für Ausfallzeiten

Der Kunde muss innerhalb von 24 Stunden, nachdem er zum ersten Mal festgestellt hat, dass ein Vorfall mit kritischen Auswirkungen auf den Geschäftsbetrieb aufgetreten und der Cloud-Service nicht verfügbar ist, ein Support-Ticket der Fehlerklasse 1 beim IBM Help-Desk für technische Unterstützung öffnen. Der Kunde ist verpflichtet, IBM in angemessener Weise bei der Diagnose und Lösung des Problems zu unterstützen.

Der Anspruch aus einem Support-Ticket aufgrund der Nichteinhaltung eines SLA muss innerhalb von drei (3) Arbeitstagen nach Ablauf des Vertragsmonats geltend gemacht werden. Die Entschädigung für einen berechtigten Anspruch aus einem SLA wird als Gutschrift gewährt und mit einer künftigen Rechnung für den Cloud-Service verrechnet. Sie basiert auf dem Zeitraum, in dem das Produktionssystem nicht zur Verarbeitung des Cloud-Service zur Verfügung stand („Ausfallzeit“). Die Erfassung der Ausfallzeit beginnt mit der Meldung des Vorfalls durch den Kunden und endet, wenn der Cloud-Service wiederhergestellt ist. Als Ausfallzeit zählen nicht: Zeiten für vorab geplante oder angekündigte Unterbrechungen zur Durchführung von Wartungsarbeiten; Gründe, die IBM nicht zu vertreten hat; Probleme mit dem Inhalt, der Technologie, den Entwürfen oder Anweisungen des Kunden oder Dritter; nicht unterstützte Systemkonfigurationen und Plattformen oder andere Fehler des Kunden; vom Kunden verursachte Sicherheitsvorfälle oder vom Kunden durchgeführte Sicherheitstests. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service während jedes einzelnen Vertragsmonats anwenden (siehe die nachstehende Tabelle). Die Gesamtentschädigung für einen beliebigen Vertragsmonat wird 10 Prozent (%) von einem Zwölftel (1/12) der Jahresgebühr für den Cloud-Service nicht überschreiten.

3.2 Service-Levels

Verfügbarkeit des Cloud-Service in einem Vertragsmonat

Verfügbarkeit in einem Vertragsmonat	**Entschädigung (in Prozent (%) der monatlichen Subscription-Gebühr* für den Vertragsmonat, der Gegenstand des Anspruchs ist)**
Unter 99,9 %	2 %
Unter 99 %	5 %
Unter 95 %	10 %

* Wurde der Cloud-Service von einem IBM Business Partner erworben, so wird die monatliche Subscription-Gebühr auf der Basis des zum jeweiligen Zeitpunkt gültigen Listenpreises für den Cloud-Service berechnet, der in dem Vertragsmonat wirksam war, der Gegenstand des Anspruchs ist, mit einem Abschlag von 50 Prozent (%). Eine eventuelle Rückvergütung von IBM wird direkt an den Kunden geleistet.

Die Verfügbarkeit, ausgedrückt als Prozentsatz, wird wie folgt berechnet: Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Ausfallminuten in einem Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in einem Vertragsmonat.

4. Technische Unterstützung

Technische Unterstützung für den Cloud-Service wird per E-Mail, in Online-Foren und über ein Onlinesystem für die Problemmeldung bereitgestellt. Der von IBM unter https://www-01.ibm.com/software/support/saas_support_guide.html zur Verfügung gestellte „Software as a Service Support Guide“ enthält Kontaktinformationen für die technische Unterstützung sowie weitere Informationen und Prozesse. Die technische Unterstützung wird mit dem Cloud-Service angeboten und ist nicht als separates Angebot erhältlich.

5. Informationen zur Berechtigung und Abrechnung

5.1 Gebührenmetriken

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

- „Kundenprojekt“ (Engagement) ist eine Maßeinheit für den Erwerb der Services. Ein Kundenprojekt besteht aus Professional Services und/oder Schulungsservices im Zusammenhang mit dem Cloud-Service. Der Kunde muss ausreichende Berechtigungen zur Abdeckung aller Kundenprojekte erwerben.
- „Ereignisse pro Sekunde“ (Events Per Second = EPS) 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. Der Kunde muss ausreichende Berechtigungen erwerben, um die Anzahl der Ereignisse pro Sekunde

abzudecken, die während des Messzeitraums, der im Berechtigungsnachweis oder Auftragsdokument angegeben ist, vom Cloud-Service erfasst und verarbeitet werden sollen.

- „Zehntausend Datenflüsse (Flows) pro Minute“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein Datenfluss ist die Aufzeichnung der Kommunikation zwischen zwei Hosts. Alle Pakete, die dieselbe Quellen-IP und Ziel-IP, denselben Quellenport und Zielport sowie dasselbe Protokoll enthalten, werden zu einem Datenflussdatensatz (Flow Record) zusammengefasst. Der Kunde muss ausreichende Berechtigungen erwerben, um die höchste Anzahl der Datenflüsse in einem einminütigen Intervall (aufgerundet auf die nächsten zehntausend) abzudecken, die während des Messzeitraums, der im Berechtigungsnachweis oder Auftragsdokument angegebenen ist, vom Cloud-Service verwaltet oder verarbeitet werden.
- „256 Assets“ ist eine Maßeinheit für den Erwerb des Cloud-Service. Ein Asset ist eine bewegliche Sache oder ein Wertgegenstand, der verwaltet werden kann, einschließlich Produktions- und Transportmitteln, Einrichtungen sowie IT-Hardware und Software. Jede Ressource oder jedes Element mit einer eindeutigen Kennung innerhalb des Cloud-Service ist ein separates Asset. Der Kunde muss ausreichende Berechtigungen erwerben, um die Assets (aufgerundet auf die nächsten 256) abzudecken, auf die während des Messzeitraums, der im Berechtigungsnachweis oder Auftragsdokument angegeben ist, vom Cloud-Service zugegriffen wird oder die vom Cloud-Service verwaltet werden. Jede Assetberechtigung entspricht 256 Assets.

5.2 Setup-Gebühren

Für jeden bestellten Setup-Service wird eine einmalige Setup-Gebühr zu dem im Auftragsdokument angegebenen Preis in Rechnung gestellt.

5.3 Abrechnungshäufigkeit

Ausgehend von der gewählten Abrechnungshäufigkeit wird IBM dem Kunden die fälligen Gebühren zu Beginn des Abrechnungszeitraums in Rechnung stellen, mit Ausnahme von Gebühren für Nutzungsüberschreitungen und spezifischen Nutzungsgebühren, die rückwirkend berechnet werden.

6. 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. Verlängerungen unterliegen einer jährlichen Preiserhöhung gemäß der Angabe in einem Angebot. Falls die automatische Verlängerung nach der Benachrichtigung von IBM über die Vertriebseinstellung des Cloud-Service eintritt, endet die Verlängerungslaufzeit mit Ablauf der derzeitigen Verlängerungslaufzeit oder zum angekündigten Datum der Vertriebseinstellung, wobei das frühere Datum maßgeblich ist.

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.

7. Zusätzliche Bedingungen

7.1 Allgemeines

Es ist dem Kunden untersagt, Cloud-Services, allein oder in Kombination mit anderen Services oder Produkten, zur Unterstützung risikoreicher Aktivitäten wie Planung, Errichtung, Kontrolle oder Wartung von Nuklearanlagen, Massentransportsystemen, Luftverkehrskontrollsystemen, Fahrzeugsteuerungssystemen, Waffensystemen oder für die Luftfahrzeugnavigation oder Luftfahrzeugkommunikation oder für andere Aktivitäten zu verwenden, bei denen ein Versagen des Cloud-Service zum Tod oder zu ernsthaften Verletzungen führen kann.

7.2 Aktivierungssoftware

Dieser Cloud-Service enthält Aktivierungssoftware, die nur in Verbindung mit dem Cloud-Service während seiner Laufzeit verwendet werden darf. Die Bedingungen separater Lizenzvereinbarungen, die

der Aktivierungssoftware beigefügt sind, kommen ebenfalls zur Anwendung, soweit sie nicht durch diesen Abschnitt eingeschränkt werden. Im Falle eines Widerspruchs haben die Bedingungen dieser Servicebeschreibung Vorrang vor den beigefügten Lizenzvereinbarungen. Die Aktivierungssoftware wird im gegenwärtigen Zustand (auf „as-is“-Basis) bereitgestellt. Der Kunde darf lediglich bis zu 10 Kopien der Aktivierungssoftware installieren und verwenden.

7.3 Sichere Daten

IBM ist berechtigt, Indikatoren für potenziell schädliche Aktivität aus dem Inhalt des Kunden für die Verwendung zur Analyse von Cyberbedrohungskontexten, insbesondere URLs, IP-Adressen, Domänen und Datei-Hashwerte zu erfassen. IBM kann diese Indikatoren wiederum verwenden, um den Kunden darüber zu benachrichtigen, wenn diese Indikatoren darauf hindeuten, dass das Cyberbedrohungsrisiko des Kunden erhöht ist.