IBM QRadar on Cloud

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

1. Cloud-Service

1.1 IBM QRadar on Cloud

Folgende Angebote stehen für den Kunden zur Wahl.

1.1.1 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 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 Storage 100 EPS

Mit dem Datenspeicherupgrade wird zusätzlicher Speicher hinzugefügt und der Analysezeitraum verlängert. Das Kapazitätsupgrade ermöglicht den Kunden für jeden Erwerb eines 100-EPS-Upgrades 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.

1.3 Acceleration Services

1.3.1 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

1.3.2 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.

1.3.3 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

1.3.4 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. Datenblätter für Datenverarbeitung und Datenschutz

Die Ergänzenden Bedingungen zur Auftragsverarbeitung (EB-AV) von IBM unter http://ibm.com/dpa und die Datenblätter für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheet(s), nachfolgend „Datenblätter“ oder „Anlagen zu den EB-AV“ genannt) unter den nachstehenden Links enthalten zusätzliche Informationen bezüglich Datenschutz für die Cloud-Services und die Optionen in Bezug auf die Arten der Inhalte, die verarbeitet werden können, die damit verbundenen Verarbeitungsaktivitäten, 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 die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) auf diese Verarbeitung Anwendung findet.

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

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 in der Übersicht zu IBM SaaS-Support 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

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

4. Gebühren

4.1 Gebührenmetriken

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

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Kundenprojekt“ (Engagement) ist ein Professional Service oder Schulungsservice im Zusammenhang mit dem Cloud-Service.

- „Ereignisse pro Sekunde“ ist die Häufigkeit eines bestimmten Vorkommnisses pro Sekunde, das vom Cloud-Service verarbeitet wird oder mit der Nutzung des Cloud-Service in Zusammenhang steht.
- „Datenflüsse pro Minute“ ist die Anzahl Datenflüsse pro Minute, die vom Cloud-Service verwaltet oder verarbeitet wird. Ein Datenfluss ist die Aufzeichnung der Kommunikation zwischen zwei Hosts. Pakete, die dieselbe Quellen-IP und Ziel-IP, denselben Quellenport und Zielport sowie dasselbe Protokoll enthalten, werden zu einem Datenflussdatensatz (Flow Record) zusammengefasst.
- „Asset“ ist ein eindeutig identifizierter Sachwert oder Wertgegenstand, auf den der Cloud-Service zugreift oder den der Cloud-Service verwaltet.

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:

- Datengateway – Der Kunde darf lediglich bis zu zehn (10) Kopien des Datengateways installieren und verwenden.

6. Übergeordnete Bedingungen

6.1 Nutzung von Sicherheitsdaten

Folgende Bestimmung hat Vorrang vor gegenteiligen Bestimmungen im Abschnitt „Inhalte und Datenschutz“ der Basisbedingungen für Cloud-Service zwischen den Vertragsparteien: 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.