

## IBM X-Force Threat Intelligence

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

### 1. Cloud-Service

IBM X-Force Threat Intelligence ermöglicht den programmgesteuerten Zugriff auf IBM X-Force Exchange über eine REST-konforme API, die Informationen in JavaScript Object Notation (JSON) zurückgibt. Der Cloud-Service unterstützt außerdem die Standards Structured Threat Information eXpression (STIX) und Trusted Automated eXchange of Indicator Information (TAXII). Der Cloud-Service ist für die Bereitstellung der folgenden Schlüsselfunktionen ausgelegt, die den Benutzer wie folgt unterstützen:

- a. Beim Zugriff auf Informationen über Untersuchungen bestimmter Sicherheitsbedrohungen, die als 'Sammlungen' bezeichnet werden und sich aus unstrukturierten und strukturierten Inhalten zusammensetzen
- b. Beim Zugriff auf Beschreibungen über die Art des Vorfalls (z. B. Malware, Datenschutzverletzung oder Sicherheitslücke) sowie die zugehörigen überwachbaren Informationen, die für den Vorfall relevant sind
- c. Bei der Beschaffung aktueller und umfassender Sicherheitsinformationen über die Bedrohungsindikatoren, die in den meisten Fällen als Ausgangspunkt für weitere Nachforschungen dienen, und der Kontexte zum Verständnis dieser Indikatoren
- d. Bei der Integration von Daten (gemäß der nachstehenden Definition) mit den Angeboten des Kunden, um Informationen über Sicherheitsbedrohungen bestmöglich zu nutzen

### 1.1 Angebote

Folgende Angebote stehen für den Kunden zur Wahl:

#### 1.1.1 IBM X-Force Exchange Commercial API

IBM X-Force Exchange Commercial Application Programming Interface (API) ermöglicht die automatisierte Nutzung der Bedrohungsdaten von IBM X-Force Exchange, der cloudbasierten IBM Plattform für die gemeinsame Nutzung von Bedrohungsdaten. Das Angebot wird in Paketen mit jeweils zehntausend Elementen verkauft.

#### 1.1.2 IBM X-Force Exchange Commercial API Enterprise

IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise ermöglicht die automatisierte Nutzung der Bedrohungsdaten von IBM X-Force Exchange, der cloudbasierten IBM Plattform für die gemeinsame Nutzung von Bedrohungsdaten. Das Angebot wird instanzweise verkauft. Eine Instanz bietet uneingeschränkten Zugriff auf IP und URL nach Kategoriefeed, IP- und URL-Berichte, Feeds zu Sicherheitslücken sowie alle TAXII-Feeds. Anforderungen bezüglich Indikatoren, die nicht in X-Force Exchange enthalten sind, sind auf 100.000 Elemente pro Monat begrenzt.

#### 1.1.3 IBM Advanced Threat Protection Feed by X-Force

IBM Advanced Threat Protection Feed by X-Force stellt den Benutzern eine definierte Gruppe umsetzbarer Indikatoren für die direkte Aufnahme in Sicherheitstools und Lösungen zur Verfügung. Der Feed ermöglicht den Zugriff auf umsetzbare 'Indicators of Compromise' (IPs und URLs), von Analysten abgeleitete 'Indicators of Compromise' und unsere DNS-Frühwarnungsindikatoren (DNS Early Warning). Die Feeds sind in mehreren Formaten verfügbar, einschließlich STIX/TAXII, JSON, Textliste und CSV.

#### 1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

Dieser Cloud-Service wird kostenlos zur Verfügung gestellt und bietet Kunden die Möglichkeit, wesentliche Bedrohungsdaten und Aktivierungsfeatures in die Threat Intelligence Insights-Anwendung auf Cloud Pak for Security zu integrieren. Mit diesem Paket erhalten Kunden Zugriff auf die kostenlos angebotenen X-Force Threat Intelligence-Inhalte, einschließlich X-Force-Empfehlungen, Bedrohungen und zugehöriger IOCs (IPs, URLs, Sicherheitslücken, Hashes). Außerdem können Kunden manuell die Am-I-Affected-Funktion ausführen, um böswillige Bedrohungen in ihrer Umgebung zu suchen und zu

identifizieren. Voraussetzung für diesen Cloud-Service ist die IBM Security Threat Intelligence Insights-Anwendung, die als Bestandteil von IBM Cloud Pak for Security verfügbar ist.

### 1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security ist ein Premium-Paket, das Kunden die Möglichkeit gibt, der Threat Intelligence Insights-Anwendung auf Cloud Pak for Security die nächste Generation der X-Force-Bedrohungsdaten und Funktionen hinzuzufügen. Umfassende Bedrohungsdaten, die vom IBM Incident Response and Analysis Team (IRIS) kuratiert werden, bieten Zugriff auf tiefliegende Malware, Bedrohungsgruppen, Berichte über Analysen von Bedrohungsaktivitäten und Branchenanalysen, Empfehlungen zur Problembeseitigung, Kompromittierungsindikatoren (Indicators of compromise, IOCs) und vieles mehr. Mit dem Advanced-Paket können Kunden die Am-I-Affected-Funktion permanent und automatisch ablaufen lassen sowie wesentliche Bedrohungen in der Benutzerumgebung proaktiv priorisieren und identifizieren. Voraussetzung für diesen Cloud-Service ist die IBM Security Threat Intelligence Insights-Anwendung, die als Bestandteil von IBM Cloud Pak for Security verfügbar ist.

## 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 Sheet(s), 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=1ECC13601F5911E69AAAC4D0C72C126B>

## 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](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:

- „Instanz“ ist jeder Zugriff auf eine bestimmte Konfiguration der Cloud-Services.
- „Element“ ist das Vorkommen eines bestimmten Objekts, das vom Cloud-Service verwaltet oder verarbeitet wird bzw. mit der Nutzung des Cloud-Service in Zusammenhang steht. Bei diesem Service versteht man unter einem Element jedes Ergebnis, das von einer einzelnen Abfrage zurückgegeben wird.
- „Verwalteter virtueller Server“ (Managed Virtual Server, MVS) besteht aus Verarbeitungseinheiten sowie Speicher und Ein-/Ausgabefunktionalität und führt angeforderte Prozeduren, Befehle oder Anwendungen aus, die von den Cloud-Services verwaltet werden.

## 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 Prüfung

Der Kunde wird i) Aufzeichnungen und Ausgaben von Systemtools aufbewahren und auf Anforderung bereitstellen, soweit dies für IBM und ihre beauftragten externen Prüfer erforderlich ist, um die Einhaltung der Vereinbarung durch den Kunden zu überprüfen, und ii) unverzüglich alle erforderlichen Berechtigungen bestellen und zu den zum jeweiligen Zeitpunkt gültigen Preisen von IBM bezahlen und andere Verbindlichkeiten, die sich aufgrund der Prüfung ergeben und in einer Rechnung von IBM angegeben sind, begleichen. Die Verpflichtungen im Rahmen dieses Abschnitts bleiben während der Laufzeit des Cloud-Service und eines Zeitraums von zwei Jahren danach in Kraft.

## 5.2 Daten

### 5.2.1 Begriffsbestimmungen

Der Cloud-Service umfasst den Zugriff auf IBM Daten und Community-Daten oder deren Nutzung. IBM stellt die über den Cloud-Service verfügbaren Daten und alle Inhalte anderer Anbieter ohne jegliche Gewährleistung zur Verfügung und haftet nicht für etwaige Verluste, die dem Kunden möglicherweise entstehen, wenn er auf die Daten und Inhalte anderer Anbieter zugreift oder sie verwendet. Dabei gelten folgenden Begriffsbestimmungen:

- Daten** sind Informationen, Inhalte, Dateien, Text, Grafiken, Software, Code, Nachrichten, Ausgaben von Suchabfragen, Eingaben für Suchabfragen, Inhalte in Diskussionsforen, Methoden oder sonstige Materialien, auf die über den Cloud-Service zugegriffen werden kann.
- IBM Daten** sind Daten, die dem Kunden von IBM über den Cloud-Service zur Verfügung gestellt werden, ausgenommen Community-Daten. IBM, ihre Lizenzgeber oder Lieferanten behalten sämtliche Rechte, Eigentumsrechte und Rechtsansprüche an den IBM Daten.
- Community-Daten** sind Daten, die dem Kunden über den Cloud-Service von anderen Cloud-Service-Benutzern zur Verfügung gestellt werden.

### 5.2.2 IBM Daten

IBM erteilt dem Kunden nur über den Cloud-Service eine eingeschränkte, nicht ausschließliche, nicht übertragbare Lizenz für den Zugriff auf die IBM Daten - (i) zu seiner persönlichen Nutzung, um ihn bei der Recherche und Untersuchung von Sicherheitsbedrohungen zu unterstützen, oder (ii) um die IBM Daten in seine Angebote zu integrieren. Es ist dem Kunden nicht gestattet, den gesamten Inhalt der IBM Daten oder des Cloud-Service oder wesentliche Teile davon zu kopieren oder einen entsprechenden Versuch zu unternehmen. Der Kunde muss alle Copyrightvermerke, Informationen und Beschränkungen, die in den IBM Daten enthalten oder ihnen beigefügt sind, einhalten und darf keine in den IBM Daten enthaltenen Texte, Copyrights oder sonstigen Eigentumsvermerke entfernen. Es ist dem Kunden nicht gestattet, die Zugriffsbeschränkungen für den Cloud-Service zu umgehen oder einen entsprechenden Versuch zu unternehmen.

Wenn der Kunde IBM Daten in seine Produkte integriert, ist er dafür verantwortlich, in der Endbenutzervereinbarung (a) die kollektive Haftung des Kunden und seiner Drittlieferanten bezüglich unmittelbarer Schäden auf einen angemessenen Betrag zu begrenzen und ausdrücklich klarzustellen, dass die Drittlieferanten jegliche Haftung für Folgeschäden oder andere mittelbare Schäden sowie stillschweigende Gewährleistungen ausschließen, (b) die Endbenutzer des Kunden darauf hinzuweisen, sämtliche Ansprüche oder Schäden im Zusammenhang mit der Endbenutzervereinbarung ausschließlich gegen den Kunden zu richten, (c) die Verwendung der Daten getrennt von den Produkten oder Services des Kunden zu untersagen und (d) die Unterlizenzierung oder anderweitige Verteilung der Daten zu untersagen.

Darüber hinaus wird der Kunde, wenn er IBM Daten in seine Angebote integriert, neben den Schäden, für die er ggf. nach geltendem Recht oder den Bedingungen der Vereinbarung haftbar ist, IBM für alle Ansprüche Dritter entschädigen, freistellen und schadlos halten, die sich (a) aus der Nichteinhaltung der Bedingungen des vorstehenden Absatzes oder (b) aufgrund von Zusicherungen, Äußerungen, Behauptungen oder Gewährleistungen hinsichtlich der IBM Daten, die nicht von IBM autorisiert sind, ergeben.

Soweit vorstehend nicht ausdrücklich festgelegt, ist es dem Kunden untersagt, die IBM Daten zu kopieren, zu ändern, zu reproduzieren, zu übertragen, zu verkaufen, zum Verkauf anzubieten, zu vermieten, zu verleasen, Lizenzen oder Unterlizenzen dafür zu vergeben, weiterzugeben oder auf andere Weise Dritten zur Verfügung zu stellen.

### **5.2.3 Community-Daten**

Der Kunde ist für seine Interaktionen mit anderen Benutzern des Cloud-Service, einschließlich Zugriff auf Community-Daten, verantwortlich. Bestimmte Community-Daten können in einer Sammlung oder Bedrohung zur gemeinsamen Nutzung verfügbar sein. In Bezug auf öffentlich verfügbare Community-Daten hat der Eigentümer der Daten den Cloud-Service-Benutzern eine nicht ausschließliche, weltweite, abgegoltene Lizenz erteilt, die Community-Daten oder Teile davon zu nutzen, zu kopieren, zu reproduzieren, zu ändern, weiterzugeben und/oder davon abgeleitete Werke zu erstellen („Öffentliche Lizenz“). Wenn der Kunde Community-Daten in Übereinstimmung mit der öffentlichen Lizenz kopiert, reproduziert, weitergibt oder anderweitig verfügbar macht, muss er eine Quellenangabe für die Community-Daten hinzufügen. Der Kunde darf Daten, die in einer Sammlung oder Bedrohung verfügbar gemacht werden, nur für seine internen, nicht kommerziellen Zwecke nutzen. Der Kunde kann mit Community-Daten in Berührung kommen, die gegen IBM Richtlinien und diese Servicebeschreibung verstoßen oder auf andere Weise beleidigend sind.

Community-Daten können Benutzerprofilinformationen von anderen Cloud-Service-Benutzern enthalten. Es ist dem Kunden nicht gestattet, die Profilinformationen für andere Zwecke als zur Kommunikation über Bedrohungsinformationen mit anderen Cloud-Service-Benutzern per Data-Mining zu filtern, zu kopieren oder anderweitig zu verwenden.

Community-Daten können Links auf Websites enthalten, die nicht von IBM betrieben werden. IBM ist für die Inhalte, Produkte, Materialien oder Verfahren (einschließlich Datenschutzmaßnahmen) auf solchen Websites nicht verantwortlich. Der Kunde ist sich dessen bewusst, dass er durch den Zugriff auf Community-Daten ggf. auf Websites Dritter gelangt, die er beleidigend, unanständig oder auf andere Weise anstößig findet.

Wenn die Daten nach Meinung des Kunden personenbezogene Daten enthalten, die falsch sind oder aus anderen Gründen entfernt werden sollten, kann der Kunde über das Contribute-Feature in einem X-Force IP Report Kontakt mit IBM aufnehmen.

## **6. Übergeordnete Bedingungen**

### **6.1 Cloudflare, Inc. - Unterauftragsverarbeiter**

Folgende Bestimmung hat Vorrang vor gegenteiligen Bestimmungen in den Datensicherheits- und Datenschutzrichtlinien für Cloud-Services zwischen den Vertragsparteien: Dieser Cloud-Service verwendet Cloudflare, Inc. als einen der Unterauftragsverarbeiter von Inhalten. Cloudflare verarbeitet Inhalte in nicht verschlüsselter Form, um die Bereitstellung des Cloud-Service zu optimieren. Cloudflare ist PCI-konform als Level-1-Service-Provider und strebt Konformität mit ISO 27001 und SOC 2 an. (D. h., der Cloud-Service ist nicht vollständig PCI-konform).