IBM Resilient Security Orchestration, Automation and Response on Cloud

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

1. Cloud-Service

Die IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud bietet Unternehmen die Möglichkeit, Prozesse und Technologien, die an der Reaktion auf Sicherheitsvorfälle (Incident Response) beteiligt sind, zu koordinieren und zu automatisieren und die Mitarbeiter dabei einzubinden.

Die IBM Resilient SOAR Platform on Cloud optimiert das Incident-Response- und Privacy-Response-Management, damit Unternehmen automatisiert, schneller und flexibler auf Ereignisse und Sicherheitsvorfälle reagieren können. Die Resilient SOAR Platform on Cloud ist die Basis für eine erfolgreiche Abwehr von Cyberangriffen, die Unternehmen Folgendes ermöglicht:

- Erstellung von Reaktionsplänen, die auf Branchenstandards und bewährten Verfahren basieren
- Einfachere Integration mit Sicherheits- und IT-Tools sowie Koordination der Reaktionen auf Ereignisse und Sicherheitsvorfälle
- Zusammenarbeit im gesamten Unternehmen, indem alle Beteiligten Zugriff auf die Tools erhalten, die sie benötigen, um ihre Rollen und Aufgaben im Rahmen der Incident-Response-Maßnahmen wahrzunehmen

Die IBM Resilient SOAR Platform wurde für Unternehmen unterschiedlicher Größe und Komplexität konzipiert und kann mit mehreren optionalen Add-ons erworben werden. Der Kunde ist nicht zur Nutzung von Funktionen berechtigt, die nicht in dem von ihm erworbenen Angebot oder Add-on angegeben sind.

1.1 Angebote

Folgende Angebote stehen für den Kunden zur Wahl:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration bietet die Basis für die Abwehr von Cyberangriffen. Kunden können Reaktionspläne erstellen, die auf Branchenstandards und bewährten Verfahren basieren, diese auf einfache Weise mit Sicherheits- und IT-Tools integrieren sowie Reaktionen auf Ereignisse und Sicherheitsvorfälle koordinieren. Der Cloud-Service vereinfacht die Zusammenarbeit im Unternehmen und gibt allen Beteiligten die Möglichkeit, ihre Rollen und Aufgaben im Rahmen der Maßnahmen zur Reaktion auf Sicherheitsvorfälle wahrzunehmen.

Mit den spezialisierten Fallmanagementfunktionen der Plattform können Sicherheitsteams bei Ereignissen und Sicherheitsvorfällen im Bereich Cybersicherheit zusammenarbeiten. Dynamic Playbooks können auf rasch entstehende Attacken abgestimmt werden und die Teams können Prozesse schnell wiederholen, um die Effektivität durch Anpassen der Playbooks, Datenfelder und Anzeigenlayouts zu verbessern. Durch Simulationen können die Reaktionsprozesse weiter verfeinert werden. Integrierte und installierbare Integrationen ermöglichen die Aufbereitung von Daten, um Kontext für die Entscheidungsfindung eines Sicherheitsteams zu sammeln und Korrekturmaßnahmen entsprechend der Anzahl der pro Monat erworbenen Aktionen zu koordinieren. E-Mail-Auswertung und Parsing sind weitere einfache Methoden für die Eskalation über andere Tools. Zugriffsschutz kann durch SAML-Authentifizierung gewährleistet werden. Transparenz und Risikoanalyse werden durch Analyseverfahren und Reporting unterstützt. Dieses Angebot ist für alle anderen unten aufgeführten Add-ons erforderlich.

1.2 Optionale Services

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions ist für die Koordinationsfunktionen der Plattform notwendig. Integrierte und installierbare Integrationen, einschließlich Integrationen mit mehreren Threat Intelligence Feeds, ermöglichen die automatisierte Aufbereitung von Daten zum Erfassen von Kontext für die Entscheidungsfindung eines Sicherheitsteams sowie die Koordination von Korrekturmaßnahmen.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy ermöglicht Kunden die Beurteilung und Reaktion auf Datenschutzverstöße. Die von diesem Angebot generierten Reaktionspläne werden auf die Datentypen, die Anzahl der Aufzeichnungen und die anwendbaren regulatorischen Vorschriften angepasst. Die Kunden erhalten zudem Zugriff auf eine integrierte Wissensdatenbank mit globalen Bestimmungen zur Anzeigepflicht von Datenschutzverstößen, die sie dabei unterstützen soll, ihre Incident-Response-Pläne weiter anzupassen.

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams ermöglicht Benutzermanagement und Datentrennung über mehrere Teams hinweg. Sensible Informationen sind nur zugänglich, soweit unbedingt erforderlich, indem der Zugriff durch Arbeitsbereiche und anpassbare rollenbasierte Zugriffssteuerung eingeschränkt wird. Das Benutzer- und Gruppenmanagement kann durch Nutzung des Active Directory für die Benutzerberechtigung vereinfacht werden. Separate Gruppe können außerdem so konfiguriert werden, dass sie über eine eigene Organisation verfügen.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP bietet Fallmanagement- sowie Prozess-, Anpassungs- und Playbook-Managementfunktionen für mehrere Organisationen. Ereignisse und Sicherheitsvorfälle aus mehreren Organisationen können in einer einzigen Warteschlange angezeigt werden, die Analysten von Managed Security Service Providern (MSSP) eine Gesamtübersicht ihrer Kunden bereitstellt. Mit Playbooks, die pro Organisation konfiguriert sind, können sowohl standardisierte als auch angepasste Prozesse auf einfache Weise verwaltet werden.

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production ist eine separate Instanz der IBM Resilient SOAR Platform, die vom Kunden nur für interne nicht produktionsbezogene Aktivitäten eingesetzt werden darf, wie beispielsweise Tests, Leistungsoptimierung, Fehlerdiagnose, internes Benchmarking, Staging, Qualitätssicherung und/oder Entwicklung intern verwendbarer Zusätze oder Erweiterungen für den Cloud-Service über veröffentlichte Anwendungsprogrammierschnittstellen.

1.3 Acceleration Services

Die Angebote IBM Security Expert Labs (SEL) for Resilient Services sind remote erbrachte Services, die von einem Resilient-Experten in Form einer Architektur- und Implementierungsberatung für die Resilient-Bereitstellung durchgeführt werden. Das als Cloud-Service oder als On-Premises-Software verfügbare Angebot IBM Resilient Security, Orchestration and Response ist Voraussetzung für jeden dieser Services.

1.3.1 IBM SEL for Resilient Base Starter Service

Während eines 5-tägigen remote durchgeführten Kundenprojekts wird IBM folgende Leistungen erbringen:

- Unterstützung bei der Definition der IBM Security Resilient-Architektur
- Installation und Konfiguration von IBM Security Resilient (soweit zutreffend)
- Schulung für Analysten und Designer zu Konfiguration und Umsetzung der aktuellen Incident-Response-Pläne des Kunden unter Berücksichtigung der wesentlichen Anforderungen des Kundenunternehmens
- In IBM Security Resilient konfigurierte Playbooks, die auf den spezifischen Prozessen des Kundenunternehmens basieren
- Vorgehensweise zur Verfolgung definierter KPIs und Metriken entsprechend dem Bedarf des Kundenunternehmens und den branchenspezifischen Best Practices
- Ermittlung von Integrationsmöglichkeiten für die Unterstützung, Automatisierung und Orchestrierung von End-to-End-Prozessen

1.3.2 IBM SEL for Resilient Premium Starter Service

Während eines 3-tägigen remote durchgeführten Kundenprojekts wird IBM folgende Leistungen erbringen:

- Unterstützung bei der Definition der IBM Security Resilient-Architektur

- Installation von IBM Security Resilient (soweit zutreffend)
- Erstkonfiguration von IBM Security Resilient in der Kundenumgebung
- Schulung für Analysten und Designer zu Konfiguration und Umsetzung der aktuellen Incident-Response-Pläne des Kunden unter Berücksichtigung der wesentlichen Anforderungen des Kundenunternehmens

1.3.3 IBM SEL for Resilient Additional Day

Zusätzlich zum Base- oder Premium Starter-Service wird IBM im Rahmen eines 1-tägigen remote durchgeführten Kundenprojekts eine vorab mit dem Kunden vereinbarte Aktivität im Zusammenhang mit IBM Security Resilient durchführen. Zum Beispiel:

- Weitere Unterstützung bei der Installation oder Konfiguration von IBM Security Resilient oder Erweiterungen (soweit zutreffend)
- Weitere Schulung oder Unterstützung von Analysten, um die Einsatzbereitschaft von IBM Security Resilient als zentrale SOAR-Lösung des Kunden sicherzustellen
- Hilfestellung für Designer bei der Konfiguration und dem Einsatz ihrer 'Playbooks', die die wesentlichen Anforderungen des Kundenunternehmens berücksichtigen
- Durchführung einer schnellen Prüfung der IBM Security Resilient-Umgebung, um Bereiche mit Verbesserungspotenzial aufzuzeigen

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://www.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=A47500205B1911E6865BC3F213DB63F7

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 Technischer Support

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:

- „Berechtigter Benutzer“ ist ein bestimmter Benutzer, dem auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) Zugriff auf die Cloud-Services erteilt wird.
- „Gleichzeitig angemeldeter Benutzer“ ist ein Benutzer, der auf beliebige Weise direkt oder indirekt (z. B. über ein Multiplexing-Programm, eine Einheit oder einen Anwendungsserver) zu einem bestimmten Zeitpunkt gleichzeitig mit anderen Benutzern auf den Cloud-Service zugreift. Eine Person, die mehrmals zur gleichen Zeit auf den Cloud-Service zugreift, zählt nur als ein einziger gleichzeitig angemeldeter Benutzer.
- „Kundenprojekt“ (Engagement) ist ein Professional Service oder Schulungsservice im Zusammenhang mit den 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. Für die Zwecke dieses Cloud-Service versteht man unter einem Element eine Aktion. Eine Aktion ist eine Koordinierungs- oder Automatisierungsanforderung des Cloud-Service an ein anderes Softwareprogramm.

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 Anforderungen in Bezug auf Add-On-Berechtigungen

Der Kunde muss die gleiche Anzahl an Berechtigungen des gleichen Typs sowohl für den Basis-Cloud-Service als auch jeden Add-On-Cloud-Service erwerben.

5.3 Nutzungsbeschränkungen

Jeder Kunde darf maximal einhunderttausend (100.000) Abfragen pro Monat an den Bedrohungsservice (Threat Service) stellen. Eine entsprechende Abfrage wird erstellt, indem der Kunde im aktivierten Bedrohungsservice einem Sicherheitsvorfall ein Artefakt hinzufügt. Wenn der Sicherheitsvorfall jeweils an den zwei (2) darauffolgenden Tagen geöffnet und aktiv bleibt, wird automatisch eine neue Abfrage an den Bedrohungsservice generiert.

Jeder Kunde darf maximal einhundert (100) Benachrichtigungs-E-Mails pro Tag und berechtigten/gleichzeitig angemeldeten Benutzer generieren. Die Benachrichtigungs-E-Mails werden von der Resilient-Plattform basierend auf einer vom Kunden kontrollierten Konfiguration generiert.

5.4 Zusätzliche Informationen zu Datenverarbeitung und Datenschutz

Es wird ausdrücklich darauf hingewiesen, dass die IBM Resilient SOAR Platform on Cloud folgende Aspekte nicht abdeckt:

- Inhalte im Ruhezustand werden nicht verschlüsselt.
- Die Plattform ist nicht für die Verarbeitung besonderer Kategorien personenbezogener Daten ausgelegt.
- Personenbezogene Daten dürfen nur auf Anforderung in Textfelder mit freiem Format eingegeben werden.

Ausführliche Informationen zur Verschlüsselung und zu den Arten personenbezogener Daten, die verarbeitet werden, sind unter der URL für das Datenblatt zu finden, auf das oben in Abschnitt 2 verwiesen wird.

6. Übergeordnete Bedingungen

6.1 Nutzung von Daten

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, die sich im Rahmen des Cloud-Service aus den Inhalten ergeben (ausgenommen Erkenntnisse), für die Verbesserung des Cloud-Service zu verwenden. Des Weiteren ist IBM berechtigt, Bedrohungs-IDs und weitere Sicherheitsinformationen, die in Inhalten eingebettet sind, zum Zweck der Erkennung von Sicherheitsbedrohungen und zum Schutz vor Sicherheitsbedrohungen weiterzugeben.