# IBM Application Security on Cloud

Die Nutzungsbedingungen bestehen aus diesen IBM Nutzungsbedingungen – SaaS-spezifische Angebotsbedingungen (nachfolgend „SaaS-spezifische Angebotsbedingungen“ genannt) und einem Dokument mit dem Titel IBM Nutzungsbedingungen – Allgemeine Bedingungen (nachfolgend „Allgemeine Bedingungen“ genannt), das unter der folgende Adresse zu finden ist: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Im Falle eines Widerspruchs haben die SaaS-spezifischen Angebotsbedingungen Vorrang vor den Allgemeinen Bedingungen. Durch die Bestellung von IBM SaaS, den Zugriff darauf oder die Nutzung von IBM SaaS erklärt der Kunde sein Einverständnis mit diesen Nutzungsbedingungen.

Die Nutzungsbedingungen unterliegen dem IBM International Passport Advantage Vertrag, dem IBM International Passport Advantage Express Vertrag oder dem IBM Internationalen Vertrag über ausgewählte IBM SaaS-Angebote (nachfolgend „Vertrag“ genannt) und bilden zusammen mit dem jeweils anwendbaren Vertrag die vollständige Vereinbarung.

## 1. IBM SaaS

Diese SaaS-spezifischen Angebotsbedingungen gelten für die folgenden IBM SaaS-Angebote:

- IBM Application Security Analyzer
- IBM Application Security on Cloud Consulting Services

## 2. Gebührenmetriken

Die IBM SaaS-Angebote werden unter den folgenden Gebührenmetriken entsprechend der Angabe im Auftragsdokument verkauft:

a. **Job** ist eine Maßeinheit für den Erwerb von IBM SaaS. Ein Job ist ein Objekt innerhalb von IBM SaaS, das nicht weiter unterteilt werden kann und einen Datenverarbeitungsprozess einschließlich aller zugehörigen Unterprozesse darstellt. Der Kunde muss ausreichende Berechtigungen erwerben, um die Gesamtzahl der Jobs abzudecken, die während des Messzeitraums, der im Berechtigungsnachweis (Proof of Entitlement = PoE) oder Auftragsdokument angegeben ist, von IBM SaaS verarbeitet oder verwaltet werden.

b. **Anwendungsinstanz** ist eine Maßeinheit für den Erwerb von IBM SaaS. Für jede Instanz einer Anwendung, die mit IBM SaaS verbunden wird, muss eine Berechtigung erworben werden. Wenn eine Anwendung aus mehreren Komponenten besteht, die jeweils für einen bestimmten Zweck und/oder eine bestimmte Benutzerbasis einsetzbar sind und mit IBM SaaS verbunden oder von IBM SaaS verwaltet werden können, zählt jede Komponente als separate Anwendung. Test-, Entwicklungs-, Staging- und Produktionsumgebungen für eine Anwendung werden ebenfalls als separate Instanzen der Anwendung betrachtet, die jeweils eine Berechtigung benötigen. Mehrere Anwendungsinstanzen in einer einzelnen Umgebung werden als separate Instanzen der Anwendung betrachtet, die jeweils eine Berechtigung benötigen. Der Kunde muss ausreichende Berechtigungen erwerben, um die Anzahl der Anwendungsinstanzen abzudecken, die während des Messzeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, mit IBM SaaS verbunden werden.

   Für die Zwecke dieses IBM SaaS-Angebots gelten folgende Definitionen:

   - Für dynamisches Testen: eine Website, die über eine öffentliche oder private URL adressierbar ist. Jede Anwendungsinstanz umfasst die Berechtigung für eine Site mit bis zu 1.000 Seiten in einer einzelnen Domäne.
   - Für statisches Testen: eine Codeeinheit, die in einer einzigen Programmiersprache ausführbar ist. Jede Anwendungsinstanz umfasst die Berechtigung für das Scannen von Codeeinheiten mit bis zu 1.000.000 Zeilen.
   - Für Mobile-Testen: eine Binärcodeeinheit, die auf einem mobilen Gerät ausführbar ist. Jede Art von Plattform (z. B. iOS und Android) stellt eine eigene Anwendungsinstanz dar.

c. **Instanz** ist eine Maßeinheit für den Erwerb von IBM SaaS. Eine Instanz ermöglicht den Zugriff auf eine bestimmte IBM SaaS-Konfiguration. Der Kunde muss ausreichende Berechtigungen für alle IBM SaaS-Instanzen erwerben, die während des Messzeitraums, der im Berechtigungsnachweis (PoE) oder Auftragsdokument angegeben ist, zum Zugriff und zur Nutzung bereitgestellt werden.

   Bei den einzelnen Instanzberechtigungen besteht keine Begrenzung hinsichtlich der Anzahl der ausgeführten Jobs oder der Anwendungsinstanzen (verbundenen Anwendungen), sofern nicht mehr als 30 Jobs zu einem bestimmten Zeitpunkt verarbeitet werden.

d. **Kundenprojekt** (Engagement) ist eine Maßeinheit für den Erwerb der Services. Ein Kundenprojekt besteht aus Professional Services und/oder Schulungsservices im Zusammenhang mit IBM SaaS. Der Kunde muss ausreichende Berechtigungen zur Abdeckung aller Kundenprojekte erwerben.

## 3. Gebühren und Abrechnung

Der für IBM SaaS zu bezahlende Betrag ist in einem Auftragsdokument angegeben.

### 3.1 Anteilige Monatsgebühren

Die im Auftragsdokument angegebene anteilige Monatsgebühr wird anteilig basierend auf der Nutzung ermittelt.

### 3.2 Zusatzgebühren

Wenn die tatsächliche IBM SaaS-Nutzung während des Messzeitraums die im Berechtigungsnachweis angegebene Berechtigung überschreitet, wird dem Kunden die Nutzungsüberschreitung gemäß dem Auftragsdokument in Rechnung gestellt.

### 3.3 Einrichtungsgebühren

Die Einrichtung (Setup) wird dem Kunden gemäß der Angabe im Auftragsdokument in Rechnung gestellt.

## 4. Laufzeit und Verlängerungsoptionen

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

Bei automatischer Verlängerung wird IBM SaaS automatisch um die im Berechtigungsnachweis angegebene Laufzeit verlängert, es sei denn, der Kunde teilt IBM mindestens 30 Tage vor dem Ablaufdatum schriftlich mit, dass er keine Verlängerung wünscht.

Bei fortlaufender Nutzung steht IBM SaaS auf monatlicher Basis ununterbrochen zur Verfügung, bis der Kunde unter Einhaltung einer Frist von 30 Tagen schriftlich kündigt. IBM SaaS bleibt nach Ablauf der 30-Tage-Frist bis zum Ende des Kalendermonats verfügbar.

## 5. Technische Unterstützung

Während der Subscription-Laufzeit und nachdem IBM dem Kunden mitgeteilt hat, dass sein Zugriff auf IBM SaaS freigeschaltet ist, wird technische Unterstützung über Onlineforen und als Standardunterstützung während des Zeitraums bereitgestellt, in dem beim Kunden nutzungsabhängige Gebühren anfallen. Die Kunden können in IBM SaaS ein Support-Ticket einstellen oder eine Chatsitzung öffnen, um Unterstützung zu erhalten. IBM stellt das IBM Software as a Service Support Handbook zur Verfügung, das Kontaktinformationen für die technische Unterstützung sowie weitere Informationen und Prozesse enthält.

| 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 |

| Fehlerklasse | Definition der Fehlerklasse | Angestrebte Reaktionszeiten | Deckungszeiten |
|---|---|---|---|
| 2 | **Erhebliche Auswirkung auf den Geschäftsbetrieb:** Die Nutzung eines geschäftsrelevanten 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 |

### 5.1 Zugriff auf Kundendaten

IBM kann zur Diagnose von Problemen mit dem Service und um das Scannen von Kundenanwendungen mithilfe des Service zu vereinfachen, auf Kundendaten zugreifen. Der Datenzugriff erfolgt ausschließlich zum Zwecke der Fehlerbehebung oder zur Unterstützung von IBM Produkten oder Services.

## 6. Zusätzliche Bedingungen für die IBM SaaS-Angebote

Durch Sicherheitsscans werden unter Umständen nicht alle Sicherheitsrisiken in einer Anwendung aufgedeckt. Ferner sind Sicherheitsscans nicht für die Nutzung in gefährlichen Umgebungen bestimmt oder vorgesehen, die einen ausfallsicheren Betrieb voraussetzen, einschließlich, aber nicht beschränkt auf Luftfahrzeugnavigation, Luftverkehrskontrollsysteme, Waffensysteme, lebenserhaltende Systeme, Atomanlagen oder andere Anwendungen, bei denen das Nichterkennen von Sicherheitsrisiken zu Todesfällen, Personen- oder Sachschäden führen kann. IBM übernimmt keine Gewähr für die unterbrechungs- oder fehlerfreie Ausführung von Sicherheitsscans.

IBM SaaS kann verwendet werden, um den Kunden bei der Einhaltung seiner Compliance-Verpflichtungen zu unterstützen, die auf Gesetzen, Verordnungen, Normen oder Verfahren beruhen können. Sämtliche Anweisungen, empfohlenen Vorgehensweisen oder Anleitungen, die vom Service bereitgestellt werden, stellen keine rechtliche, betriebswirtschaftliche oder anderweitige fachliche Beratung dar, und dem Kunden wird dringend geraten, sich von juristisch oder fachlich kompetenter Stelle beraten zu lassen. Der Kunde ist allein dafür verantwortlich, sicherzustellen, dass von ihm selbst und durch die von ihm ausgeübten Tätigkeiten sowie durch seine Anwendungen und Systeme alle anwendbaren Gesetze, Verordnungen, Normen oder Verfahren eingehalten werden. Durch die Verwendung des Service ist die Einhaltung von Gesetzen, Verordnungen, Normen oder Verfahren nicht garantiert.

IBM SaaS führt invasive und nicht invasive Tests für die Website, die Webanwendung oder die mobile Anwendung durch, die der Kunde für den Scanvorgang auswählt. Das unbefugte Eindringen in oder Zugreifen auf Computersysteme ist durch bestimmte Gesetze verboten. Der Kunde autorisiert IBM zur Ausführung der Services gemäß der Beschreibung in diesem Dokument und bestätigt, dass der Zugriff der Services auf seine Computersysteme mit seiner Zustimmung erfolgt. IBM kann diese vom Kunden erteilte Autorisierung Dritten offenlegen, falls dies für die Ausführung der Services als notwendig erachtet wird.

Die Tests bergen bestimmte Risiken, einschließlich der folgenden:

a. Auf den Computersystemen des Kunden kann es während der Ausführung der zu testenden Anwendungen zu Blockierungen oder Ausfällen kommen, die eine vorübergehende Nichtverfügbarkeit der Systeme oder Datenverluste zur Folge haben können.

b. Während der Tests können Leistung und Durchsatz der Kundensysteme als auch der zugeordneten Router und Firewalls vorübergehend beeinträchtigt sein.

c. Unter Umständen werden große Mengen an Protokollnachrichten generiert, wodurch übermäßig viel Plattenspeicherplatz durch Protokolldateien belegt wird.

d. Durch das Testen auf Sicherheitslücken könnten Daten verändert oder gelöscht werden.

e. Durch Intrusion Detection Systems (Warnsysteme gegen Angriffe von außen) könnten Alarmnachrichten ausgelöst werden.

f. Von der E-Mail-Funktion der getesteten Webanwendung könnten E-Mails ausgelöst werden.

g. IBM SaaS könnte den Datenverkehr des überwachten Netzes abfangen, um nach Ereignissen zu suchen.

Alle von IBM in einem Service-Level-Agreement zugestandenen Rechte oder Rechtsansprüche, die sich auf die Websites oder Anwendungen beziehen, die einem Test unterzogen werden, sind während der Testaktivitäten ausgesetzt.

Falls authentifizierte Anmeldedaten für die zu testende Anwendung im Service verwendet werden, sollten nur die Anmeldedaten von Testkonten und nicht von Produktionsbenutzern eingegeben werden. Die Verwendung der Anmeldedaten von Produktionsbenutzern kann zur Folge haben, dass personenbezogene Daten über den Service übertragen werden.

IBM SaaS kann für das Scannen von Webproduktionsanwendungen konfiguriert werden. Wenn vom Kunden der Scantyp „Produktion“ festgelegt wird, werden die Scans so ausgeführt, dass die oben aufgeführten Risiken reduziert werden. In bestimmten Situationen kann IBM SaaS jedoch zu Leistungseinbußen oder Instabilität innerhalb der getesteten Produktionssites und Infrastruktur führen. IBM übernimmt keinerlei Gewährleistung oder Haftung in Bezug auf die Eignung von IBM SaaS für das Scannen von Produktionssites.

Es liegt in der Verantwortung des Kunden, zu entscheiden, ob der Service für seine Website, seine Webanwendung, seine mobile Anwendung oder seine technische Umgebung geeignet ist und den Sicherheitsanforderungen entspricht.

IBM SaaS ist für die Erkennung einer Vielzahl potenzieller Sicherheits- und Compliance-Probleme in mobilen Anwendungen, Webanwendungen und Web-Services ausgelegt. Es werden weder alle Sicherheitslücken oder Compliance-Risiken überprüft noch fungiert der Service als Schutz vor Sicherheitsattacken. Da sich Sicherheitsbedrohungen, Regelungen und Standards ständig ändern, kann der Service nicht alle Änderungen berücksichtigen. Die Sicherheit und Compliance der Webanwendung des Kunden, seiner Systeme und Mitarbeiter sowie alle Abhilfemaßnahmen liegen in der alleinigen Verantwortung des Kunden. Der Kunde entscheidet alleine über die Nutzung der vom Service bereitgestellten Informationen.

Das unbefugte Eindringen in oder Zugreifen auf Computersysteme ist durch bestimmte Gesetze verboten. Der Kunde ist dafür verantwortlich, sicherzustellen, dass mit dem Service nur seine eigenen Websites und/oder Anwendungen oder diejenigen Websites und/oder Anwendungen gescannt werden, für die er entsprechend berechtigt ist.

Es wird ausdrücklich darauf hingewiesen, dass die im Datenschutzabschnitt der IBM Nutzungsbedingungen – Allgemeine Bedingungen beschriebenen Kundeninhalte auch Daten enthalten können, die bei Anwendungspenetrationstests für IBM ggf. zugänglich sind.

## 6.1 Systeme im Eigentum Dritter

Der Kunde erklärt sich in Bezug auf Systeme (die für die Zwecke dieser Regelung unter anderem auch Anwendungen und IP-Adressen einschließen), die sich im Eigentum Dritter befinden und nach Maßgabe der vorliegenden Bedingungen getestet werden, damit einverstanden:

a. vor Beginn der IBM Tests auf den Systemen Dritter eine unterzeichnete Erklärung vom Eigentümer jedes einzelnen Systems einzuholen, in der IBM zur Bereitstellung der Services auf dem jeweiligen System autorisiert wird und der Eigentümer seine Zustimmung zu den im Abschnitt „Permission to Perform Testing“ aufgeführten Bedingungen erteilt, und IBM eine Kopie der Zustimmungserklärung vorzulegen;

b. allein dafür verantwortlich zu sein, die Systemeigentümer über die Risiken, Schwachstellen und Sicherheitslücken zu informieren, die auf diesen Systemen durch die von IBM remote durchgeführten Tests aufgedeckt werden; und

c. den Informationsaustausch zwischen den Systemeigentümern und IBM zu veranlassen und zu ermöglichen, soweit dies von IBM für notwendig erachtet wird.

Der Kunde erklärt sich damit einverstanden:

- IBM unverzüglich zu informieren, wenn bei einem der Systeme, die nach Maßgabe der vorliegenden Bedingungen getestet werden, ein Eigentümerwechsel stattfindet;

- die Ergebnisse oder die Tatsache, dass die Services von IBM ausgeführt wurden, nicht ohne die vorherige schriftliche Zustimmung von IBM außerhalb des Kundenunternehmens offenzulegen; und
- IBM in vollem Umfang für alle Verluste und Verbindlichkeiten zu entschädigen, die IBM aufgrund von Ansprüchen Dritter entstehen, die darauf zurückzuführen sind, dass der Kunde die Anforderungen in diesem Abschnitt „Systeme im Eigentum Dritter“ nicht einhält, und für alle Forderungen oder Ansprüche Dritter, die gegen IBM, ihre Unterauftragnehmer oder Erfüllungsgehilfen aufgrund (a) der Überprüfung der Systeme auf Sicherheitsrisiken, Schwachstellen oder Sicherheitslücken nach Maßgabe der vorliegenden Bedingungen, (b) der Bereitstellung der Testergebnisse für den Kunden oder (c) der Verwendung oder Offenlegung der Ergebnisse durch den Kunden geltend gemacht werden.

## 6.2 Cookies

Der Kunde ist sich dessen bewusst und stimmt zu, dass IBM während des normalen Betriebs und im Rahmen des Supports für IBM SaaS über Tracking und andere Technologien personenbezogene Daten des Kunden (sowie seiner Mitarbeiter und Auftragnehmer) erfassen kann, die mit der IBM SaaS-Nutzung in Zusammenhang stehen. Auf diese Weise kann IBM Nutzungsstatistiken und -informationen über die Effektivität von IBM SaaS zusammenstellen, die dazu beitragen sollen, das Benutzererlebnis zu verbessern und/oder Interaktionen mit dem Kunden anzupassen. Der Kunde bestätigt, dass er die Zustimmung der betroffenen Personen einholen wird oder eingeholt hat, damit IBM die erfassten personenbezogenen Daten für die vorstehenden Zwecke innerhalb von IBM, durch andere IBM Unternehmen und durch ihre Unterauftragnehmer in allen Ländern, in denen wir und unsere Unterauftragnehmer geschäftlich tätig sind, in Übereinstimmung mit der geltenden Gesetzgebung verarbeiten darf. IBM wird den Weisungen der Mitarbeiter und Auftragnehmer des Kunden nachkommen, die sich auf den Zugriff auf ihre erfassten personenbezogenen Daten, deren Aktualisierung, Korrektur oder Löschung beziehen.

Im Rahmen der IBM SaaS-Angebote, die eine Berichterstattung beinhalten, wird IBM anonymisierte und/oder aggregierte Informationen, die aus IBM SaaS 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

## 6.3 Bevorzugte Standorte

Soweit möglich, orientieren sich die Steuern an dem Standort/den Standorten, für den/die IBM SaaS erbracht wird. IBM weist die Steuern gemäß der Geschäftsadresse aus, die bei der Bestellung von IBM SaaS als primärer Standort angegeben wird, es sei denn, der Kunde stellt IBM zusätzliche Informationen bereit. Der Kunde ist dafür verantwortlich, diese Informationen auf dem aktuellen Stand zu halten und IBM über Änderungen zu informieren.

## 6.4 Personenbezogene Daten, regulierte Inhalte und Services

Dieses IBM SaaS-Angebot ist nicht für besondere Sicherheitsanforderungen in Bezug auf regulierte Inhalte, wie personenbezogene Daten oder sensible personenbezogene Daten, ausgelegt. Es liegt in der Verantwortung des Kunden, zu entscheiden, ob dieses IBM SaaS-Angebot seine Anforderungen im Hinblick auf die Art der Inhalte, die er in Verbindung mit IBM SaaS verwendet, erfüllt.

IBM agiert nicht als Anbieter von Services, die von der Federal Communications Commission (FCC) oder von einzelstaatlichen Regulierungsbehörden (State Regulators) reguliert werden, und beabsichtigt nicht die Bereitstellung von Services, die einer Regulierung durch die FCC oder einzelstaatliche Regulierungsbehörden unterliegen. Falls die FCC oder eine einzelstaatliche Regulierungsbehörde Regulierungsauflagen für Services einführt, die von IBM unter diesen Nutzungsbedingungen bereitgestellt werden, kann IBM (a) Produkte auf Kosten des Kunden ändern, austauschen oder ersetzen und/oder (b) die Art und Weise, in der die betreffenden Services für den Kunden bereitgestellt werden, ändern, um die Anwendung der Regulierungsauflagen auf IBM zu vermeiden (IBM kann z. B. als Bevollmächtigter des Kunden handeln, um entsprechende Services von einem Netzbetreiber zu erwerben).

# Anhang A

## 1. Allgemeine Beschreibung von IBM Application Security on Cloud

IBM Application Security on Cloud ermöglicht es dem Kunden, Sicherheitslücken (z. B. SQL-Injection, Cross-Site Scripting und Datenlecks) für eine Reihe von Anwendungen von einem einzigen Ort aus zu identifizieren. Der Service beinhaltet verschiedene Scanning-Verfahren für Anwendungssicherheit, die Sicherheitsprobleme in den Anwendungen aufdecken.

IBM Application Security on Cloud bietet folgende Funktionen:

- Scannen mobiler Anwendungen zur Ermittlung von Sicherheitslücken. Dabei kommen dynamische (Blackbox) und interaktive (Glass-Box) Sicherheitsanalyseverfahren zum Einsatz.
- Scannen von Produktions- und Vorproduktionswebsites im öffentlichen oder privaten Netz zur Ermittlung von Sicherheitslücken. Dabei kommen dynamische (Blackbox) Sicherheitsanalyseverfahren zum Einsatz.
- Scannen der Datenflüsse innerhalb von Web- und Desktopanwendungen zur Ermittlung von Sicherheitslücken. Dabei kommen statische (Whitebox) Sicherheitsanalyseverfahren zum Einsatz.
- Ausführliche Berichte über Sicherheitslücken, die sowohl Gesamtübersichten der Ergebnisse als auch Korrekturmaßnahmen enthalten, die von den Entwicklern Schritt für Schritt durchgeführt werden können.
- Integration mit verschiedenen DevOps-Plattformen.

### 1.1 IBM Application Analyzer

IBM Application Analyzer kann pro Anwendungsinstanz, pro Job (Scan) oder als komplette Instanz erworben werden und ermöglicht die Ausführung der folgenden Scantypen:

- Dynamic Analyzer – Testen von Vorproduktions- oder Produktionswebsites mithilfe von DAST-Verfahren
- Mobile Analyzer – Testen iOS- oder Android-Binaries mithilfe von IAST-Verfahren
- Static Analyzer – Testen von Byte- oder Quellcode-Datenflüssen mithilfe von SAST-Verfahren

### 1.2 Setup-Service

Die IBM Application Security on Cloud Consulting Services sind ein produktbezogener Setup-Service für Application Analyzer. Der Service greift auf IBM Consultants zurück, die Anleitungen und Unterstützung beim Testen auf Anwendungsrisiken und den Umgang damit geben. Die IBM Application Security on Cloud Consulting Services werden in Engagement-Blöcken erworben, die in den angegebenen Stückzahlen aufgewendet werden können, um die folgenden spezifischen Services anzufordern und in Anspruch zu nehmen:

a. **Fast Start** [Erfordert eine (1) Engagement-Einheit]

Der Fast Start-Service bietet Fachwissen und Anleitungen für die Anwendung der Test- und Risikomanagementfunktionen von Application Security on Cloud. Nachdem der Kunde seine erfolgreiche Anmeldung beim Application Security on Cloud-Portal bestätigt hat, wird IBM eine Webkonferenz von bis zu zwei (2) Stunden für zwei (2) aktive Teilnehmer durchführen, um Informationen zu grundlegenden AppSec-Konfigurationen und -Funktionen auf IBM SaaS bereitzustellen, einschließlich Scantypen, Ausführung von Scans, Überprüfung von Berichten und Installation zugehöriger Tools und Plug-ins. Der Fast Start-Service gilt nach der Beendigung (a) des Kundenwebinars, (b) der Installation der anwendbaren Tools und Plug-ins und (c) der Unterstützung des Kunden beim Setup und der Ausführung seines ersten Scans als geleistet.

b. **Assessment Review** [Erfordert zwei (2) Engagement-Einheiten]

Der Assessment Review-Service bietet Unterstützung bei der Prüfung eines Testergebnisses sowie beim Verständnis und bei der Priorisierung der Behebung von Sicherheitslücken in der Anwendung. IBM wird eine Webkonferenz von bis zu einer (1) Stunde für zwei (2) aktive Teilnehmer durchführen, um einen Überblick über die festgestellten Sicherheitslücken und das allgemeine Sicherheitsrisiko der Anwendung zu geben und die Sicherheitslücken der Anwendung ausführlich zu erörtern, insbesondere (1) wie die Anfälligkeit getestet wurde, (2) wie die Sicherheitslücken festgestellt wurden, (3) welches Risiko jede Sicherheitslücke darstellt und (4) allgemeine Korrekturempfehlungen zur Behebung der Sicherheitslücke bereitstellen. Der Review basiert ausschließlich auf dem Testergebnis und beinhaltet keine Prüfung des Quellcodes. Der Kunde wird das Testergebnis prüfen und IBM das Testergebnis vor der Webkonferenz zur Prüfung zukommen lassen. Der Assessment Review-Service gilt nach der Beendigung der Webkonferenz als geleistet.

c. **Scan for Me** [Erfordert vier (4) Engagement-Einheiten]

Im Rahmen des Scan for Me-Service wird ein IBM Experte für Anwendungssicherheit zur Verfügung gestellt, der einen Scan konfiguriert und ausführt, die Ergebnisse validiert und eine Kurzdarstellung des Berichts zur Erläuterung der Erkenntnisse gibt. Der Kunde ermöglicht einem IBM Consultant den Zugriff auf seine ASoC-Umgebung, um einen Scan zu konfigurieren und auszuführen, die Ergebnisse zu validieren, Empfehlungen zur Priorisierung von Korrekturmaßnahmen zu erteilen und eine Kurzdarstellung des Berichts zur Erläuterung der Erkenntnisse zu geben. IBM wird eine Webkonferenz von bis zu einer (1) Stunde für zwei (2) aktive Teilnehmer durchführen, um einen Überblick über die festgestellten Sicherheitslücken und das allgemeine Sicherheitsrisiko der Anwendung zu geben und die Sicherheitslücken der Anwendung ausführlich zu erörtern, insbesondere (1) wie die Anfälligkeit getestet wurde, (2) wie die Sicherheitslücken festgestellt wurden, (3) welches Risiko jede Sicherheitslücke darstellt und (4) allgemeine Korrekturempfehlungen zur Behebung der Sicherheitslücke bereitstellen. Auf Anforderung wird IBM bis spätestens 30 Tage nach dem ersten Scan erneut einen Scan unter Verwendung der ursprünglichen Scankonfiguration durchführen, um ausschließlich die Sicherheitskorrekturen, aber keine neue Funktionalität zu prüfen, die Ergebnisse auszuwerten und dem Kunden einen Bericht bereitzustellen. Der Scan for Me-Service gilt nach der Beendigung der Webkonferenz zur Überprüfung der Ergebnisse des ersten Scans oder, sofern zutreffend, der Beendigung des vom Kunden angeforderten erneuten Scans und der Bereitstellung des zugehörigen Berichts als geleistet.

d. **Advisor on Demand** [Erfordert sieben (7) Engagement-Einheiten]

Der Advisor on Demand-Service umfasst bis zu zwanzig (20) von einem IBM Consultant erbrachte Stunden, die für Aktivitäten im Zusammenhang mit IBM SaaS aufgewendet werden können. Der IBM Consultant leistet Unterstützung bei spezifischen die Anwendungssicherheit betreffenden Themen, insbesondere beim Programmmanagement, bei der Priorisierung von Sicherheitstests, bei Strategien für Korrekturmaßnahmen sowie bei der Quellcodeanalyse und -reparatur. IBM wird in Zusammenarbeit mit dem Kunden einen Projektterminplan mit den spezifischen Kundenanforderungen, einschließlich der Projektziele, relevanten Technologien, gewünschten Fristen, erwarteten Arbeitsergebnisse und der geschätzten Anzahl an Advisor on Demand-Service-Engagements ausarbeiten und erstellen. Der Kunde muss den Zugriff auf die Anwendungen und Systeme sowie die Dokumentation bereitstellen, die für die Ausführung der Services erforderlich sind. Der Advisor on Demand-Service gilt als geleistet, wenn bis zu 20 Stunden an Sicherheitsfachkenntnissen vermittelt wurden und/oder der Projektterminplan eingehalten wurde und/oder die im Projektterminplan definierten dokumentierten Arbeitsergebnisse für den Kunden bereitgestellt wurden.

e. **Anwendungspenetrationstests**

Drei Optionen:

(1) **Compliance/Entry-Level-Anwendungspenetrationstest**, der bis zu vierzig (40) Stunden an Beraterzeit umfasst und bei dem der Schwerpunkt auf Fehlern in der Single-Step-Logik und einfacheren Versionen von Injektionslücken liegt. Erfordert fünfzehn (15) Engagement-Einheiten.

(2) **Standardanwendungspenetrationstest**, der bis zu sechzig (60) Stunden an Beraterzeit umfasst und den Schwerpunkt auf Logikfehler in mehrstufigen Workflows, komplexe Versionen von Injektionslücken und die Analyse komplexer Datentypen ausweitet. Erfordert einundzwanzig (21) Engagement-Einheiten.

(3) **Erweiterter Anwendungspenetrationstest**, der bis zu achtzig (80) Stunden an Beraterzeit umfasst und den Schwerpunkt auf das Reverse Engineering kompilierter ausführbarer Dateien, die Analyse angepasster Netzprotokolle und die detailliere Analyse öffentlich verfügbarer Bibliotheken und Frameworks ausweitet. Erfordert siebenundzwanzig (27) Engagement-Einheiten.

Im Rahmen des Anwendungspenetrationstestservice wird ein IBM Mitarbeiter für das Testen und Beurteilen einer Anwendung, für die Bereitstellung eines Testberichts sowie für eine Kurzdarstellung des Berichts zur Erläuterung der Erkenntnisse und der damit verbundenen Risiken zur Verfügung gestellt.

IBM führt zu Projektbeginn ein Gespräch von bis zu einer (1) Stunde mit zwei (2) aktiven Teilnehmern zur Prüfung der Umgebung und Organisation des Kunden durch. Dabei werden unter anderem die Anwendungsplattform, Architektur, Frameworks, unterstützende Infrastruktur, bekannte Sicherheitsprobleme oder -bedenken hinsichtlich der Anwendung, ein vorläufiger Testplan und ein Kontaktnetz für Notfälle erörtert.

Der Anwendungspenetrationstest wird von IBM durchgeführt und beinhaltet unter anderem Folgendes: Aufdeckung allgemeiner Sicherheitslücken, wie SQL-Injection, Cross-Site Scripting, Beurteilung der Stärken und Schwächen vorhandener Sicherheitsmaßnahmen, wie beispielsweise Eingabevalidierung, Authentifizierung und Berechtigung, Prüfung auf ordnungsgemäße Umsetzung der Geschäftslogik, Validierung der ordnungsgemäßen Verwendung sicherer Protokolle, Identifizierung von Sitzungsverarbeitungsfehlern und Prüfung auf Verwendung geeigneter Sicherheitskontrollen bei der Anmeldung, Kennwortwiederherstellung, Kennwortrichtlinie und anderen Benutzermanagementfunktionen. Die Erkenntnisse werden im Bericht über den Anwendungspenetrationstest dokumentiert. IBM wird eine Webkonferenz mit einer Dauer von bis zu einer (1) Stunde für eine Kurzdarstellung des Berichts durchführen. Der Anwendungspenetrationstestservice gilt als geleistet, wenn die zugewiesene Beratungszeit aufgebraucht, die Webkonferenz abgehalten und der Abschlussbericht über den Anwendungspenetrationstest dem Kunden übergeben wurde.

### 1.2.1 Verantwortlichkeiten im Rahmen der Setup-Services

IBM wird:

- Setup-Services gemäß den vom Kunden erworbenen Engagement-Einheiten und nach Maßgabe des Berechtigungsnachweises bereitstellen; und
- ein Setup-Service gilt als erbracht, wenn die in Abschnitt 1.2 beschriebenen Kriterien erfüllt sind.

Der Kunde erklärt sich damit einverstanden:

- für die Bezahlung aller Gebühren im Zusammenhang mit den von ihm erteilten Engagement-Beauftragungen während der Vertragslaufzeit verantwortlich zu sein;
- und bestätigt, dass erworbene Engagement-Einheiten innerhalb der anfänglichen Vertragslaufzeit aufgebraucht werden müssen und verfallen, wenn sie bis zum Enddatum der Vertragslaufzeit nicht genutzt werden; und
- für alle Setup-Services mindestens 30 Tage vor dem Enddatum der Subscription eine formale Anforderung zu stellen.

Bei der Erbringung der Setup-Services kann IBM vom Kunden Informationen anfordern und ihn zu angemessener Zusammenarbeit auffordern. Verabsäumt es der Kunde, die angeforderten Informationen rechtzeitig bereitzustellen oder seinen Mitwirkungspflichten zeitnah nachzukommen, werden nach

Festlegung durch IBM Gebühren in Form von Engagement-Einheiten in dem für die Services erforderlichen Umfang fällig oder es kommt zu Verzögerungen bei der Erbringung des betreffenden Service.

Damit IBM die Tests präzise durchführen kann, erklärt der Kunde sich damit einverstanden, den Anweisungen von IBM bezüglich der Vorbereitung und Wartung der Umgebung während der Testperiode Folge zu leisten.