IBM Cloud Services Agreement

IBM Cloud Service Description: IBM AppScan Dynamic Analyzer for Bluemix

Except as noted below the terms of the IBM Bluemix Service Description or Terms of Use, as applicable, apply.

The following is the Service Description for your Order:

1. Cloud Service Description

   This service identifies security issues at the code level of web applications hosted on Bluemix. It allows a user to scan for security vulnerabilities without the need to supply the application code. At the end of the security scan the service generates a security report that includes details of detected vulnerabilities, the potential security risks to the application caused by these vulnerabilities, with suggestions for how to fix them.

   To start using the service:
   ● Provide the starting URL of the web application's Bluemix hosted staging site, create a scan name and start the scan.
   ● Once the scan is completed a report will be generated and available for download.

2. Entitlement and Billing Information

2.1 Charge Metrics

   The Cloud Service is offered in accordance with the following charge metric:

   Application Instance - An Application Instance is an instance of an application connected to or managed by the Cloud Service. An application in multiple environments, such as test, development, staging, and production, is counted as separate instances. Multiple copies of an application running in the same environment are also counted as separate instances. You will be charged for each Application Instance connected to or managed during the billing period.

3. Safe Harbor Framework

   The Cloud Service does not comply with the US-EU and US-Swiss Safe Harbor Frameworks.

4. Service Unique Terms

   The Cloud Service can be used to help Customer meet compliance obligations, which may be based on laws, regulations, standards or practices. Any directions, suggested usage, or guidance provided by the Service does not constitute legal, accounting, or other professional advice, and Customer is cautioned to obtain its own legal or other expert counsel. Customer is solely responsible for ensuring that Customer and Customer’s activities, applications and systems comply with all applicable laws, regulations, standards and practices. Use of this Service does not guarantee compliance with any law, regulation, standard or practice.

   The Cloud Service performs invasive and non-invasive tests on the website and web application Customer chooses to scan, which testing entails certain risks, including without limitation the following:
   a. Customer’s computer systems while running applications under test may hang or crash, resulting in temporary system unavailability or loss of data;
   b. the performance and throughput of Customer’s systems, as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded during testing;
   c. excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;
   d. data may be changed or deleted as a result of probing vulnerabilities;
   e. alarms may be triggered by intrusion detection systems;
   f. emails may be triggered by the email function of the web application being tested;
g. the cloud service may intercept the traffic of the monitored network for the purpose of looking for events.

The Cloud Service is not designed for use in a production environment due to the inherent risks described above. Further, in the event that Customer inputs authenticated log-in credentials for the application under test into the Service, Customer should only input such credentials for test accounts and not for production users. Use of production user credentials may result in personal data being transmitted via the Service.

IT IS CUSTOMER’S RESPONSIBILITY TO DETERMINE IF THE SERVICE IS APPROPRIATE OR SAFE FOR CUSTOMER’S WEBSITE, WEB APPLICATION, MOBILE APPLICATION OR TECHNICAL ENVIRONMENT.

The Cloud Service is designed to identify a variety of potential security and compliance issues in web applications and web services. It does not test all vulnerabilities or compliance risks, nor does it act as a barrier to security attacks. Security threats, regulations and standards continually change, and the Service may not reflect all such changes. The security and compliance of Customer’s web application, systems and employees, and any remedial actions, are Customer’s responsibility alone. It is solely within Customer’s discretion to use or not use any of the information provided by the Service.

Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. CUSTOMER IS RESPONSIBLE FOR ENSURING THAT CUSTOMER DOES NOT USE THE SERVICE TO SCAN ANY WEBSITES AND/OR APPLICATIONS OTHER THAN WEBSITES AND/OR APPLICATIONS OWNED BY CUSTOMER OR THOSE THAT CUSTOMER HAS THE RIGHT AND AUTHORITY TO SCAN.