Descrição de Serviço em Nuvem IBM

IBM Security AppScan Mobile Analyzer

A seguir está a Descrição de Serviço para o seu Pedido:

1. Serviço em Nuvem

A oferta de Serviço em Nuvem é descrita abaixo e é especificada em um Documento de Transação para as ofertas autorizadas selecionadas. O Documento de Transação consistirá da Cotação e do Certificado de Titularidade (PoE), o que confirma a data de início e o termo dos Serviços em Nuvem. A fatura começará após o fornecimento do Serviço em Nuvem.

1.1 IBM Security AppScan Mobile Analyzer

Este serviço identifica problemas de segurança no nível de código de aplicativos móveis Android. Ele permite que um desenvolvedor verifique se há vulnerabilidades de segurança sem a necessidade de fornecer o código fonte do aplicativo. No fim da varredura, o serviço gera um relatório de segurança que inclui detalhes de vulnerabilidades detectadas, os riscos de segurança em potencial para o aplicativo móvel causados por essas vulnerabilidades, com sugestões sobre como corrigi-los.

2. Descrição de Segurança

2.1 Políticas de Segurança

A IBM tem uma equipe de segurança de informação e também mantém políticas de privacidade e segurança que são comunicadas aos funcionários da IBM. A IBM requer treinamento de privacidade e segurança para o pessoal que suporta datacenters IBM. As políticas e as normas de segurança da IBM são revisadas e reavaliadas anualmente. Os incidentes de segurança da IBM são gerenciados de acordo com um procedimento abrangente de resposta a incidente.

2.2 Controle de Acesso

O acesso aos dados de clientes, se necessário, é permitido apenas pelos representantes de suporte e equipe de operações de serviço IBM, de acordo com os princípios de segregação de funções. A equipe IBM usa autenticação de dois fatores para um host de gerenciamento de "gateway". Quando do acesso aos dados do Cliente, todas as conexões são canais criptografados.

2.3 Integridade e Disponibilidade de Serviço

Modificações nos sistemas operacionais e no software de aplicativo são controladas pelo processo de gerenciamento de mudanças da IBM. Mudanças nas regras do firewall também são controladas pelo processo de gerenciamento de mudanças e são revisadas pela equipe de segurança IBM antes da implementação. A IBM monitora o datacenter 24 horas por dia, 7 dias por semana. A varredura de vulnerabilidade interna e externa é conduzida regularmente por administradores autorizados e fornecedores terceiros para ajudar a detectar e resolver exposições potenciais de segurança do sistema. Sistemas de detecção de malware (antivírus, detecção de invasão, varredura de vulnerabilidade e prevenção de invasão) são usados em todos os datacenters IBM. Os serviços de datacenter da IBM suportam uma variedade de protocolos de entrega de informações para a transmissão de dados através de redes públicas. Exemplos incluem HTTPS/SFTP/FTPS/S/MIME e VPN de site a site. Os dados de backup destinados a armazenamento externo são criptografados antes do transporte.

2.4 Criação de Log de Atividade

A IBM mantém logs de sua atividade para sistemas, aplicativos, repositórios de dados, middleware e dispositivos de infraestrutura de rede aptos e configurados para atividade de criação de log. Para minimizar a possibilidade de violação e para permitir análise central, alerta e relatório, a criação de log de atividade é executada em tempo real para os repositórios de criação de log. Os dados são subscritos para evitar violação. Os logs são analisados em tempo real e através de relatórios de análise periódica para detectar comportamento anormal. A equipe de operações é alertada sobre as anomalias e entra em contato com um especialista em segurança on-call 24 horas por dia, 7 dias por semana, quando necessário.

2.5 Segurança Física

A IBM mantém normas de segurança física projetadas para restringir o acesso físico não autorizado a datacenters IBM. Existem apenas pontos de acesso limitados nos datacenters, que são controlados por autenticação de dois fatores e monitorados por câmeras de segurança. O acesso somente é permitido para a equipe autorizada que possui acesso aprovado. A equipe de operações verifica a aprovação e emite um badge de acesso que concede o acesso necessário. Os funcionários que recebem esse badge devem entregar outros badges de acesso e somente podem possuir o badge de acesso do datacenter durante o período de sua atividade. O uso de badges é registrado. Os visitantes que não sejam da IBM são registrados ao entrar nas instalações e são acompanhados durante a permanência nas instalações. Áreas de entrega, docas de carregamento e outros pontos em que pessoas desautorizadas possam entrar nas instalações são controlados e isolados.

2.6 Conformidade

A IBM certifica suas práticas de privacidade anualmente como consistente com o U.S. Department of Commerce's Safe Harbor Principles (Princípios de Porto Seguro do Departamento de Comércio dos EUA): Aviso, Escolha, Transferência Progressiva, Acesso e Exatidão, Segurança e Supervisão/Aplicação. A IBM executa auditorias SSAE 16 padrão de indústria (ou seu equivalente) anualmente nos datacenters de produção. A IBM revisa atividades relacionadas a segurança e privacidade para o cumprimento dos requisitos de negócios da IBM. Avaliações e auditorias são realizadas regularmente pela IBM para confirmar a conformidade com suas políticas de segurança de informações. Os funcionários da IBM e os funcionários do fornecedor são submetidos a treinamento completo de segurança e conscientização de força de trabalho anualmente. A equipe é lembrada de seus objetivos de cargo e de sua responsabilidade de atender à conduta ética de negócios, confidencialidade, e às obrigações de segurança da IBM anualmente.

3. Informações de Autorização e Faturamento

3.1 Métricas de Encargos

O Serviço em Nuvem é disponibilizado sob a métrica de encargo a seguir, conforme especificado no Documento de Transação:

- Instância de aplicativo é uma unidade de medida pela qual o IBM SaaS pode ser obtido. É necessária uma autorização de Instância de aplicativo para cada instância de um Aplicativo conectado ao IBM SaaS. Caso um aplicativo tenha vários componentes, cada um deles terá um propósito e/ou uma base do usuário diferente e cada um poderá ser conectado ao IBM SaaS ou gerenciado por ele, portanto, cada um desses componentes será considerado um Aplicativo separado. Além disso, os ambientes de teste, desenvolvimento, exibição e produção de um Aplicativo são considerados instâncias distintas do Aplicativo e cada um deles deve ter uma autorização. Várias instâncias do Aplicativo em um único ambiente são consideradas instâncias distintas do Aplicativo e cada uma deve ter uma autorização. Devem ser obtidas autorizações suficientes para cobrir o número de Instâncias do aplicativo conectadas ao IBM SaaS durante o período de medição especificado no Certificado de Titularidade (PoE) ou no Documento de Transação do Cliente.

3.2 Encargos e Faturamento

A quantia a pagar pelo Serviço em Nuvem é especificada em um Documento de Transação.

3.3 Pagamento por utilização

As opções de pagamento por utilização serão faturadas no mês seguinte da utilização do serviço no encargo especificado no Documento de Transação.

4. Suporte Técnico

O suporte técnico para o Serviço em Nuvem fica disponível durante o período de subscrição.

As Horas de Suporte de Operação são como segue:

Informações sobre as horas de disponibilidade, sistemas de relatório de problemas on-line e outros processos e veículos de comunicação do suporte técnico estão descritos no IBM Software as a Service Support Handbook.

Suporte após o Horário de Expediente:

O Suporte Após Horário Comercial (fora das horas operacionais regulares estabelecidas acima) está disponível para problemas de Gravidade 1 em dias úteis, fins de semana e feriados. Problemas de Gravidade 1 exigem que o cliente esteja disponível para ajudar a diagnosticar problemas durante o

período de 24 horas por dia, 7 dias por semana, caso contrário, o problema será rebaixado para a Gravidade 2.

4.1 Suporte de Fórum

Todos os clientes do Serviço em Nuvem recebem suporte de fórum que é monitorado regularmente pelos representantes de suporte e desenvolvedores IBM.

a. Faça Perguntas:

https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. Visualizar Posts Atuais:

https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

4.2 Suporte Padrão

O suporte padrão está disponível durante o período de tempo em que o cliente incorre em encargos Pay as you Go. A partir do Serviço em Nuvem, os clientes podem submeter um chamado de suporte ou abrir uma sessão de bate-papo para obter assistência. Para obter mais informações sobre os procedimentos de suporte, consulte o portal da web de suporte da IBM no endereço: https://support.ibmcloud.com ou o IBM SaaS Software Support Handbook no endereço: http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

Gravidade	Definição de Gravidade	Objetivos de Tempo de Resposta	Cobertura do Tempo de Resposta
1	**Impacto crítico nos negócios/inatividade do serviço:** Funcionalidades essenciais para os negócios ficam inoperáveis ou ocorre falha na interface essencial. Geralmente, se aplica a um ambiente de produção e indica uma incapacidade de acessar serviços resultando em um impacto crítico nas operações. Essa condição requer uma solução imediata.	Dentro de 1 hora	24 horas por dia, 7 dias por semana
2	**Impacto significativo nos negócios:** O uso de um recurso de negócios de serviço ou de uma função do serviço fica gravemente restringido ou o Cliente corre o risco de perder prazos finais de negócios.	Dentro de 2 horas em horário comercial	Horário comercial de segunda a sexta-feira
3	**Impacto menor nos negócios:** Indica que o serviço ou a funcionalidade está utilizável e não há um impacto crítico nas operações.	Dentro de 4 horas em horário comercial	Horário comercial de segunda a sexta-feira
4	**Impacto mínimo nos negócios:** Uma solicitação de consulta ou não técnica	Dentro de 1 dia útil	Horário comercial de segunda a sexta-feira

5. Conformidade com o Safe Harbor

A IBM não determinou a conformidade deste Serviço em Nuvem com o US-EU and US-Swiss Safe Harbor Frameworks.

6. Informações Adicionais

O Serviço em Nuvem é projetado para identificar uma variedade de problemas de conformidade e segurança potenciais em aplicativos móveis e serviços da web móveis. O Serviço em Nuvem não testa todas as vulnerabilidades ou riscos de conformidade, nem age como barreira para ataques à segurança. Ameaças, regulamentos e normas de segurança mudam continuamente e o Serviço pode não refletir todas essas mudanças. A segurança e conformidade do aplicativo móvel, sistemas e funcionários do Cliente, e quaisquer ações corretivas, são de responsabilidade apenas do Cliente. Fica exclusivamente a critério do Cliente usar ou não qualquer uma das informações fornecidas pelo Serviço.

6.1 Locais de Benefícios Derivados

Onde aplicável, os tributos são baseados no(s) local(is) que o Cliente identifica como recebedor(es) dos benefícios dos Serviços em Nuvem. A IBM aplicará tributos com base no endereço de negócios listado ao solicitar um Serviço em Nuvem como o local de benefício primário, a menos que o Cliente forneça informações adicionais à IBM. O Cliente é responsável por manter tais informações atualizadas e por fornecer quaisquer mudanças à IBM.

6.2 Cookies

O cliente está ciente e concorda que a IBM pode, como parte da operação e suporte normais do Serviço em Nuvem, coletar suas informações pessoais (seus funcionários e fornecedores) relacionadas ao uso do Serviço em Nuvem, por meio de rastreamento e de outras tecnologias. A IBM faz isso para reunir estatísticas e informações de uso sobre a efetividade de nosso Serviço em Nuvem para fins de melhoria da experiência do usuário e/ou customizar interações com o cliente. O Cliente confirma que obterá ou obteve consentimento para permitir que a IBM processe as informações pessoais coletadas para o propósito acima na IBM, outras empresas IBM e suas subcontratadas, onde quer que a IBM ou seus subcontratados façam negócios, em conformidade com a lei aplicável. A IBM atenderá às solicitações dos funcionários e contratados do Cliente para acessar, atualizar, corrigir ou excluir as informações pessoais coletadas.