IBM QRadar Advisor with Watson

Esta Descrição de Serviço descreve o Serviço em Nuvem. Os documentos de transação aplicáveis fornecem precificação e detalhes adicionais sobre o pedido do Cliente.

1. Serviço em Nuvem

O IBM QRadar Advisor with Watson estende a análise cognitiva à Plataforma de Segurança QRadar , ajudando os Clientes e os analistas de segurança a investigarem e responderem às ameaças. Ele alimenta o corpus de conhecimento do Watson for Cyber Security, alcançando dados não estruturados (incluindo websites de segurança, blogs e papéis de pesquisa, dentre outros) e correlacionando com incidentes de segurança locais. Fazendo isso, ele pode ajudar a descobrir ameaças ocultas e a automatizar insights para respostas e tomada de decisão. O QRadar Advisor with Watson permite que um analista de segurança envie dados de um ataque à segurança para o Watson a fim de executar a descoberta de ameaça, usando a sua base de conhecimento de centenas de milhares de origens de dados não estruturados e estruturados, e mapeando isso de volta para entidades de ameaças relacionadas ao ataque original, como arquivos maliciosos, endereços IP suspeitos, entidades não autorizadas e os relacionamentos entre eles. Isso pode ser especialmente valioso para determinar se um ataque à segurança está ou não associado a uma campanha de malware conhecida. Neste caso, o Watson fornecerá conhecimentos importantes sobre o malware empregado, as vulnerabilidades exploradas e o escopo da ameaça (incluindo terminais adicionais possivelmente impactados), dentre outros insights.

1.1 Ofertas

O Cliente pode escolher uma das ofertas disponíveis a seguir.

1.1.1 IBM QRadar Advisor with Watson

O IBM QRadar Advisor with Watson requer que o Cliente tenha uma implementação ativa do IBM QRadar, seja em um ambiente local nas dependências do Cliente ou em uma implementação em nuvem, além de ter instalado o software de ativação do Serviço em Nuvem nessa implementação para que o Cliente acesse as funcionalidades dele. O Serviço em Nuvem contém um 'limite flexível' no número de consultas de ataques à segurança que esse Cliente poderá enviar ao Serviço em Nuvem a uma taxa de 1,5 solicitações por dia por 100 Eventos Por Segundo (arredondado para cima até a solicitação mais próxima) à qual o Cliente tem direito. Consultas enviadas além desse limite não serão processadas pelo Serviço em Nuvem pelo restante do dia.

1.1.2 BM QRadar Advisor with Watson – Enterprise

O IBM QRadar Advisor with Watson – Enterprise é mais adequado para implementações de grande centro de operações de segurança (SOC – Security Operation Center) que geralmente excedem duzentos e cinquenta mil Eventos Por Segundo ou mais. O Cliente deve instalar o software de ativação do Serviço em Nuvem em sua implementação do IBM QRadar adquirida separadamente para acessar a funcionalidade do Serviço em Nuvem. O IBM QRadar Advisor with Watson – Enterprise está disponível sob uma métrica de encargo baseada em Instância que não depende da escala da implementação do IBM QRadar do Cliente. O Cliente está limitado a 25 envios na fila a qualquer momento.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

O IBM QRadar Advisor with Watson – Starter Pack deve ser usado por usuários iniciantes do QRadar Advisor with Watson. Este Serviço em Nuvem possui a funcionalidade completa do QRadar Advisor with Watson, conforme descrito na seção 1.1.1 acima, mas está disponível apenas como a primeira compra do QRadar Advisor with Watson pelo Cliente e não é renovado.

1.2 Serviços Opcionais

1.2.1 IBM QRadar Advisor with Watson – Test Environment

O IBM QRadar Advisor with Watson – Test Environment é para Clientes que desejam implementar o Serviço em Nuvem com o seu ambiente de teste interno e pode ser usado apenas para testes de não

produção. O IBM QRadar Advisor with Watson – Test Environment deve ser complementado por uma subscrição para o Serviço em Nuvem de nível de produção.

1.3 Serviços de Aceleração

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Para este serviço de subscrição fornecido remotamente, a IBM fornecerá para o Cliente qualquer um dos serviços de consultoria a seguir por até cinco dias no período de um ano:

- Avaliação do processo SOC do Cliente, incluindo investigação e/ou processo de resposta de incidente;
- Reavaliação das respostas de conjuntos de referência;
- Ajuste das análises automáticas para ofensas de alta magnitude;
- Desenvolvimento de caso de uso;
- Fornecimento de recomendações para mudanças do processo SOC que incorporam o QRadar Advisor with Watson;
- Orientação sobre como entender melhor e incorporar os dados do QRadar Advisor with Watson aos processos existentes do Cliente;
- Fornecimento de transferência de conhecimento sobre assuntos pertinentes ao QRadar Advisor with Watson.

NOTA: as seguintes atividades podem ser incorporadas nesse serviço com base no status da implementação do QRadar do Cliente:

- Execução de uma Verificação de Funcionamento na implementação do QRadar do Cliente;
- Realização de ajustes adicionais na implementação do QRadar existente;
- Auxílio com a inclusão de origens de log adicionais na implementação do QRadar do Cliente.

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Este serviço de configuração é fornecido remotamente e inclui quarenta (40) horas de serviços profissionais que expiram em noventa (90) dias a partir da data de compra, a menos que seja indicado de outra forma, independentemente de todas as horas (se aplicável) terem ou não sido utilizadas. Os serviços incluirão um Gerente de Compromisso designado pela IBM que agendará as chamadas de lançamento.

A IBM tomará algumas ou todas as ações seguintes:

- Avaliação do processo SOC do Cliente, incluindo investigação e/ou processo de resposta de incidente;
- Implementação do QRadar Advisor with Watson no ambiente do Cliente:
    - Instalação do QRadar Advisor with Watson;
    - Mapeamento das propriedades unificadas para o QRadar Advisor with Watson;
    - Implementação de respostas de conjuntos de referência;
    - Ajuste das análises automáticas para ofensas de alta magnitude;
    - Orientação de caso de uso;
    - Fornecimento de recomendações para mudanças do processo SOC que incorporam o QRadar Advisor with Watson.

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

Este serviço de configuração foi desenvolvido para Clientes com menos de 5.000 eventos por segundo (EPS).

Para este serviço fornecido remotamente, a IBM fornecerá ao Cliente qualquer um dos serviços de consultoria a seguir (ou uma combinação deles) por até 16 horas dentro de um período de 90 dias:

- Instalação do QRadar Advisor with Watson.
- Gerenciamento de permissões para o QRadar Advisor with Watson.

- Configuração do QRadar Advisor with Watson, que pode incluir:
  - Configuração do servidor proxy seguro;
  - Envio de credenciais de troca do X-Force;
  - Criação de tokens do serviço autorizado;
  - Configuração de políticas de retenção para armazenar resultados de análise;
  - Mapeamento de propriedades de evento customizadas;
  - Exportação de conjuntos de referências;
  - Mapeamento de inteligência de ameaça;
  - Configuração de identificação de ativos;
  - Otimização de uso;
- Investigação automática de ofensa e resultados (pelo menos uma demonstração de caso de uso).
- Exploração de insights com o gráfico de relacionamento.

2. Planilhas de Proteção e Processamento de Dados

O Adendo de Processamento de Dados (DPA - Data Processing Addendum) da IBM em http://ibm.com/dpa e a(s) Planilha(s) de Proteção e Processamento de Dados (referida(s) como planilha(s) de dados ou Apêndice(s) do DPA) nos links abaixo fornecem informações adicionais sobre a proteção de dados para os Serviços em Nuvem e suas opções relacionadas aos tipos de Conteúdo que podem ser processados, às atividades de processamento envolvidas, aos recursos de proteção de dados e às especificidades sobre retenção e devolução de Conteúdo. O DPA aplica-se aos dados pessoais presentes no Conteúdo, se e até o limite em que seja aplicável: i) o Regulamento Geral sobre a Proteção de Dados da União Europeia (EU/2016/679) (RGPD); ou ii) outras leis de proteção de dados identificadas em http://ibm.com/dpa/dpl.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206

3. Níveis de Serviço e Suporte Técnico

3.1 Acordo de Nível de Serviço

A IBM fornece ao Cliente o seguinte acordo de nível de serviço (SLA - Service Level Agreement) de disponibilidade. A IBM aplicará o mais alto Crédito de Disponibilidade aplicável com base na disponibilidade cumulativa do Serviço em Nuvem, conforme mostrado na tabela abaixo. A porcentagem de disponibilidade é calculada como o número total de minutos em um mês contratado, menos o número total de minutos de Tempo de Inatividade do Serviço no mês contratado, dividido pelo número total de minutos no mês contratado. A definição de Tempo de Inatividade do Serviço, o processo de reivindicação e como contatar a IBM com relação a problemas de disponibilidade do serviço estão no manual de suporte de Serviço em Nuvem da IBM disponível em https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilidade	Crédito (% de encargo de subscrição mensal*)
Menor que 99,9%	2%
Menor que 99,0%	5%
Menor que 95,0%	10%

* O encargo de subscrição é o preço contratado para o mês que é objeto da reivindicação.

3.2 Suporte Técnico

O suporte técnico para o Serviço em Nuvem, incluindo detalhes de contato do suporte, níveis de gravidade, horário de disponibilidade do suporte, tempos de resposta e outras informações e processos de suporte, são localizados selecionando o Serviço em Nuvem no guia de suporte IBM disponível em https://www.ibm.com/support/home/pages/support-guide/.

4. Encargos

4.1 Métricas de Encargos

A(s) métrica(s) de encargos para o Serviço em Nuvem é(são) especificada(s) no Documento de Transação.

A(s) métrica(s) de encargo a seguir aplica(m)-se a este Serviço em Nuvem:

- Evento por Segundo (EPS) é uma ocorrência de um EPS específico processado ou relacionado ao uso dos Serviços em Nuvem. Para o propósito desse Serviço em Nuvem, os Eventos por Segundo são aqueles coletados e processados pela implementação do IBM QRadar do Cliente.
- Instância corresponde a cada acesso a uma configuração específica dos Serviços em Nuvem.
- Compromisso é um serviço profissional ou de treinamento relacionado aos Serviços em Nuvem.

5. Termos Adicionais

Para Contratos de Serviço em Nuvem (ou contratos de nuvem base equivalentes) firmados antes de 1º de janeiro de 2019, aplicam-se os termos disponíveis em https://www.ibm.com/acs.

5.1 Software de Ativação

O Serviço em Nuvem contém os seguinte Software de Ativação:

- IBM QRadar com o aplicativo Watson (https://exchange.xforce.ibmcloud.com/hub)

5.2 Uso Lícito do Serviço em Nuvem

O Serviço em Nuvem foi projetado para ajudar o Cliente a melhorar o ambiente e dados de segurança do Cliente. O uso do Serviço em Nuvem pode envolver diversas leis ou regulamentos, incluindo aqueles relacionados a privacidade, proteção de dados, trabalho, comunicações eletrônicas e armazenamento. O Serviço em Nuvem somente pode ser usado para propósitos lícitos e de forma lícita. O Cliente concorda em usar o Serviço em Nuvem em conformidade com as leis, os regulamentos e as políticas aplicáveis, e assume toda a responsabilidade pelo cumprimento de tal conformidade. O Cliente declara que obterá ou obteve quaisquer consentimentos, permissões ou licenças necessários para habilitar o uso lícito do Serviço em Nuvem.

6. Termos de Substituição

6.1 Uso de Dados

Os termos a seguir prevalecem sobre qualquer disposição em contrário na seção Proteção de Dados e de Conteúdo dos termos básicos do Serviço em Nuvem entre as partes: a IBM não usará nem divulgará os resultados decorrentes do uso do Serviço em Nuvem pelo Cliente que são exclusivos de seu Conteúdo (Insights) ou que de outra forma identifiquem o Cliente. A IBM pode, no entanto, usar Conteúdo e outras informações (exceto Insights) que resultem do Conteúdo no curso do fornecimento do citado Serviço em Nuvem, removendo identificadores pessoais; de modo que qualquer dado pessoal não possa mais ser atribuído a um indivíduo específico sem o uso de informações adicionais. A IBM usará tais dados somente para pesquisas, testes e desenvolvimento de ofertas.