IBM QRadar on Cloud

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

1.1 Ofertas

O Cliente pode escolher dentre as seguintes ofertas disponíveis.

1.1.1 IBM QRadar on Cloud

A oferta IBM QRadar on Cloud entrega uma solução de inteligência de segurança avançada a partir da Nuvem da IBM com base no produto IBM Security QRadar SIEM. Ela permite ao Cliente coletar, correlacionar e armazenar eventos gerados tanto em ambientes locais quanto em nuvem e executar gerenciamento de segurança e ameaças conforme fariam com um produto QRadar SIEM no local. Como parte da oferta, a IBM também fornece monitoramento de infraestrutura 24 horas por dia, 7 dias na semana e aplica o nível de software mais recente ou os patches essenciais sempre que estiverem disponíveis.

Este Serviço em Nuvem inclui noventa (90) dias de armazenamento ativo, pesquisável e tem direito a quantidades de 100 Eventos por Segundo (EPS).

1.2 Serviços Opcionais

1.2.1 IBM QRadar on Cloud Temporary Upgrade

Um serviço de aprimoramento que fornece uma capacidade adicional de 1.000 EPS para coletar e processar eventos de log, mas apenas por uma quantidade temporária de meses. O Cliente pode comprar diversas unidades deste aprimoramento até o nível máximo de EPS que a oferta pode suportar. A intenção desta parte é permitir a um Cliente que necessite de cobertura durante períodos de "pico" ao longo do ano atenda esta necessidade através do aprimoramento temporário de capacidade . No término deste período, estas quantias adicionais de capacidade temporária serão removidas do ambiente do Cliente.

1.2.2 IBM QRadar on Cloud Data Capacity

O aprimoramento de capacidade de dados inclui armazenamento adicional e amplia o período de análise. O aprimoramento de capacidade fornece aos Clientes até 1 ano completo de dados de eventos armazenados para cada compra de aprimoramento de 100 Eventos Por Segundo (EPS).

1.2.3 IBM QRadar on Cloud Flows Add-On

Integra-se com o IBM QRadar SIEM e com os processadores de fluxo para fornecer análise de fluxo e de visibilidade de rede Layer 3 a fim de ajudar o Cliente a perceber, detectar e responder a atividades em sua rede.

Este Serviço em Nuvem inclui noventa (90) dias de armazenamento ativo, pesquisável e tem direito a quantidades de 10.000 Fluxos por Minuto (FPM).

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Detecta e descobre proativamente as vulnerabilidades de segurança de dispositivos e aplicativos de rede, adicionando contexto e suportando a priorização de atividades de remediação e mitigação.

1.2.5 IBM QRadar on Cloud Log Archival

Permite ao Cliente arquivar dados de eventos do Serviço em Nuvem durante o período de subscrição. A IBM trabalhará com o Cliente para registrar os eventos designados no armazenamento de objetos para fins de arquivamento. Mediante solicitação do Cliente, a IBM irá remontar até 30 (trinta) dias de dados de eventos arquivados na instância do Serviço em Nuvem do Cliente dentro de três (3) dias úteis a partir dessa solicitação. Esses dados permanecerão disponíveis para o Cliente por 48 horas antes de serem devolvidos ao armazenamento de objetos arquivados. O Cliente pode fazer até duas solicitações por

período de três meses. O aprimoramento de capacidade fornece aos Clientes até 1 ano completo de dados armazenados para cada aprimoramento de 100 EPS comprado.

1.2.6 IBM QRadar on Cloud Flows Add-On Data Capacity

O aprimoramento de capacidade de dados inclui armazenamento adicional e expande o período de análise, fornecendo ao Cliente até 1 ano completo de dados de fluxo armazenados para cada compra de armazenamento de 10.000 FPM.

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

Esta oferta permite que os Clientes arquivem dados de fluxo do Serviço em Nuvem durante o período de subscrição. A IBM irá trabalhar com o Cliente para gravar registros de fluxo designados no armazenamento de objetos para propósitos de arquivamento. Mediante solicitação do Cliente, a IBM irá remontar até (30) dias de dados de fluxo arquivados na instância do Cliente do Serviço em Nuvem, em até três (3) dias úteis dessa solicitação. Esses dados permanecerão disponíveis para o Cliente por 48 horas antes de serem devolvidos ao armazenamento de objetos arquivados. O Cliente pode fazer até duas solicitações por período de três meses. O aprimoramento de capacidade fornece aos Clientes até 1 ano completo de dados armazenados para cada upgrade de 10.000 FPM comprado.

1.2.8 IBM QRadar on Cloud for Non-Production Environment

A oferta IBM QRadar on Cloud for Non-Production Environment entrega uma instância de teste dedicada do Serviço em Nuvem. Ela permite aos Clientes coletar, correlacionar e armazenar eventos gerados tanto em ambientes locais quanto em nuvem e executar o gerenciamento de segurança e de ameaças, conforme fariam com um produto QRadar SIEM implementado no local em um ambiente de teste dedicado. Como parte da oferta, a IBM também fornece monitoramento de infraestrutura 24 horas por dia, 7 dias na semana e aplica o nível de software mais recente ou os patches essenciais sempre que estiverem disponíveis. O Cliente pode usar esse Serviço em Nuvem somente para propósitos de teste de não produção.

Esse Serviço em Nuvem inclui noventa (90) dias de armazenamento ativo e pesquisável.

1.3 Serviços de Aceleração

1.3.1 IBM QRadar on Cloud Optimization Service

Para este serviço de subscrição prestado remotamente, a IBM realizará uma reunião de revisão com o Cliente a fim de avaliar o funcionamento atual da instância do Serviço em Nuvem do Cliente e fornecer os resultados ao Cliente através de um relatório de Funcionamento do QRadar on Cloud, que identificará áreas para melhoria, se houver.

Além disso, a IBM fornecerá qualquer um dos seguintes serviços de consultoria ao Cliente, a pedido do Cliente, por até oito (8) dias no período de 1 ano:

- Ajuda na inclusão de fontes de log adicionais ao Serviço em Nuvem;
- Configuração de pesquisas, relatórios e painéis adicionais;
- Execução de ajustes adicionais na implementação QRadar existente; e
- Fornecimento de instrução sobre assuntos pertinentes ao QRadar.

1.3.2 Serviços de Configuração

Os seguintes serviços de configuração são prestados remotamente e solicitados separadamente. Cada serviço solicitado expira em noventa (90) dias a partir da compra, a menos que seja indicado de outra forma, independentemente de todas as horas (se aplicável) terem sido utilizadas. Os serviços incluirão um Gerente de Compromisso designado pela IBM que agendará as chamadas de lançamento.

a. **IBM QRadar on Cloud Deployment Services**

Este serviço fornece quarenta (40) horas de serviços profissionais durante os quais a IBM executará alguns ou todos os seguintes:

A IBM conduzirá uma revisão da arquitetura SIEM de até dezesseis horas de duração para definir os requisitos de relatórios do Cliente e fornecerá suas descobertas ao Cliente em um relatório de arquitetura de solução que ajudará a definir e capturar os requisitos do Cliente.

Esse relatório incluirá:

- Os requisitos de relatórios definidos pelo Cliente para ajudar a atender os requisitos de conformidade, auditoria e inteligência de segurança do Cliente.
- Os requisitos de inteligência de segurança, casos de uso e aplicativos que a IBM pode auxiliar na implementação (até 10 (dez) casos de uso e até dois (2) aplicativos).
- Informações de alto nível sobre as fontes de log e fluxo do Cliente que serão necessárias para suportar os casos de uso.
- Considerações sobre a infraestrutura de rede, tais como firewalls e portas.

Com base no relatório da arquitetura da solução, a IBM executará as seguintes tarefas, à medida que houver tempo hábil:

- Configuração da coleta de eventos para até três (3) instâncias de até 10 (dez) tipos de fontes de log no Serviço em Nuvem. Essa atividade incluirá transferência de conhecimento para aos funcionários relevantes do Cliente a fim de que possam incluir mais fontes de log, conforme necessário. Somente fontes de log suportadas pelos QRadar Device Support Modules (DSMs) padrão serão incluídas como parte deste serviço.
- Ajuste inicial, que inclui a) ativação de regras prontas para utilização, pesquisas salvas, gráficos e relatórios de séries temporais acumulados; b) Identificação e remoção de origens de ruído; e c) configuração do armazenamento off-line através de NFS, CIFS ou iSCSI.
- Implementação dos 10 (dez) casos de uso e dos dois (2) aplicativos do IBM QRadar App Exchange documentados no documento de arquitetura da solução.

b. **IBM QRadar on Cloud Custom Parser Service**

Esse serviço fornecerá o desenvolvimento de um único analisador/uDSM customizado para suportar os tipos de fontes de log não padronizados do Cliente que devem ser enviados ao Serviço em Nuvem e inclui as seguintes tarefas:

- Criação de um analisador customizado para um tipo de fontes de log não padronizado (trabalho executado remotamente);
- Criação, configuração e mapeamento de uDSM;
- Implementação e teste do uDSM customizado; e
- Análise de até vinte e cinco tipos de mensagens para a fonte do log.

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 limente 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=FB0F42F0750011E6865BC3F213DB63F7

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 esse Serviço em Nuvem:

- Compromisso é um serviço profissional ou de treinamento relacionado aos Serviços em Nuvem.
- Eventos por Segundo (EPS) é o número de ocorrências de um evento específico por segundo processado pelos ou relacionado ao uso dos Serviços em Nuvem.
- Fluxos por Minuto é o número de fluxos por minuto gerenciado ou processado pelos Serviços em Nuvem. Um Fluxo é um registro de comunicações entre dois hosts. Os pacotes que contêm o mesmo IP de origem, IP de destino, porta de origem, porta de destino e protocolo são combinados como um registro de Fluxo.
- Ativo é um recurso tangível ou item de valor de identificação exclusiva a ser acessado ou gerenciado pelos 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 software de ativação é fornecido ao Cliente sob os termos a seguir:

Software de Ativação	Termos de Licença Aplicáveis (se houver)
Data Gateway	O Cliente pode instalar e usar somente até 10 (dez) cópias do Data Gateway