**DIRETORIA ADMINISTRATIVA E FINANCEIRA**

**GERÊNCIA DE SUPRIMENTOS E GESTÃO DE CONTRATOS**

Objeto: Registro de preços para eventual contratação de empresa especializada na prestação de serviço de segurança de borda, denominado Security Service Edge (SSE), através de processo licitatório, abrangendo licenciamento de uso em nuvem, processamento de dados no Brasil, implantação, configuração da solução de segurança, treinamento (passagem de conhecimento), suporte técnico, garantia por 12 (doze) meses, fornecimento de toda documentação técnica gerada durante o período de implantação da solução e acompanhamento contínuo de adoção da plataforma.

A **BB TECNOLOGIA E SERVIÇOS S.A.,** no uso de suas atribuições torna público aos interessados, a errata no Edital da Licitação Eletrônica 2023/15, com a seguinte alteração:

## No Anexo I do Edital:

**1) <u>Onde se lê:</u>**

3.3.1 Proxy em nuvem: processamento do tráfego web dos usuários em tempo real com destino ao Microsoft Office 365, SaaS terceiros e filtragem de URL.

**<u>Leia-se</u>**

3.3.1 Proxy em nuvem: processamento do tráfego web dos usuários em tempo real com destino ao Microsoft Office 365, AWS, ShadowIT, Filtro URL, Proteção contra domínios maliciosos, aplicações indesejadas e por fim análise e prevenção contra malwares.

**2) <u>Onde se lê:</u>**

3.5.2. A solução deve ser capaz de bloquear/liberar o uso de aplicações instaladas no desktop – a exemplo: Dropbox, Amazon Drive, dentre outras.

**Leia-se**

3.5.2 A solução deve ser capaz de identificar via reconhecimento do tráfego web e não web e bloquear/liberar o uso de aplicações instaladas no desktop – a exemplo: Dropbox, Amazon Drive, SSH, RDP, Telnet, RealVNC, Teamviewer, dentre outras.

3) **Onde se lê:**

3.5.5.2. Deve ser capaz de identificar e controlar nativamente 20.000 aplicações SaaS ou 40 Categorias nativas de aplicações SaaS;

**Leia-se**

3.5.5.2 Deve ser capaz de identificar e controlar nativamente 40.000 aplicações SaaS;

4) **Onde se lê:**

3.5.6.2.1. Caso de Uso: A solução deverá prevenir o acesso a URLs associadas às categorias de Botnets, DGA, Command Control, Sites Maliciosos e Phishing.

**Leia-se**

3.5.6.2.1. Caso de Uso: A solução deve ser capaz de interceptar requisições de DNS e bloqueá-la com destino a domínios relacionados a Command & Control, Phishing, DGA, Botnet, Spam, Spyware e Malware.

5) **Onde se lê:**

9.6.3. Possuam a certificação técnica do fabricante: Principais fabricantes de segurança cibernética – e Certified Internetwork Expert Security Certification;

**Leia-se**

9.6.3. Possuam a certificação técnica do fabricante da solução ofertada.

**6) <u>Onde se lê:</u>**

4.12.1. Por se tratar de uma plataforma SaaS, a contratada deverá alocar, durante a vigência do contrato, dois recursos técnicos, de forma remota, para acompanhamento da adoção, boas práticas, revisão do ambiente periodicamente, apresentação de novas funcionalidades da plataforma e apoio junto a problemas.

**<u>Leia-se</u>**

4.12.1. Por se tratar de uma plataforma SaaS, a contratada deverá alocar, durante a vigência do contrato, recursos técnicos, de forma remota, para acompanhamento da adoção, boas práticas, revisão do ambiente periodicamente, apresentação de novas funcionalidades da plataforma e apoio junto a problemas.

**<u>No Anexo I do Edital, ficam incluídos os itens abaixo:</u>**

3.5.3.11 - Deve ser capaz de reconhecer o tráfego de rede para identificar mais de 400 aplicações.

3.5.11.5 - A integração com Youtube deve ser nativa e não depender da API do Google.

3.5.12.1 - A integração com Youtube deve ser nativa e não depender da API do Google.

3.5.18.4 - Minimamente, a solução deverá apresentar as seguintes capacidades de controle, a depender do suporte da aplicação:

3.5.18.4.1. Create.

3.5.18.4.2. Delete.

3.5.18.4.3. Download.

3.5.18.4.4. Edit.

3.5.18.4.5. Restore.

3.5.18.4.6. Send.

3.5.18.4.7. Upload.

3.5.18.4.8. Move.

3.5.18.4.9. Reboot.

3.5.18.4.10. Shutdown.

3.5.18.4.11. Attach.

3.5.18.4.12. Detach.

3.5.18.4.13. Login.

3.5.18.4.14. Logout.

3.5.18.4.15. Purchase.

3.5.18.4.16. Start.

3.5.18.4.17. Stop.

3.5.18.4.18. Terminate.

3.5.18.4.19. Print.

3.5.36 - A solução deverá prover monitoramento passivo das resoluções de DNS realizadas pelos clientes e aplicar as ações de liberação, bloqueio ou Sinkhole a uma requisição.

3.5.37 - A solução deverá ser capaz de interpretar o tráfego de rede e identificar aplicações não autorizadas como Ultrasurf.

3.5.38 - A solução deverá suportar a interceptação do tráfego de ferramentas de desenvolvimento e gestão via linha de comando, permitindo controles aplicados a AWS Cli, Android Studio, Azure CLI, Boto, Curl, Fastlane e Git.

3.5.38 - A solução deverá suportar o uso futuro para o DLP de Endpoint.

3.6.19.4 - A solução deverá ser capaz de aplicar o conceito de confiança zero para mais de 30.000 aplicações SaaS, corporativas ou terceiras, garantindo que a BBTS tenha controle granular sobre as atividades desejadas para cada uma delas.

3.6.19.5 - O controle baseado no conceito de confiança zero, deve minimamente suportar as seguintes aplicações corporativas:

3.6.19.5.1 - Amazon AWS (S3, EC2, Cloud Trail, Cloud Watch, CodeBuild, CodeCommit, CodePipeline, Amazon Devops Guru, Amazon Drive, Amazon EKS, Amazon DynamoDB).

3.6.19.5.2 - Microsoft Azure (Azure Admin, Azure Devops).

3.6.19.5.3 - Google Workspace (Google Mail, Google Chat, Google Hangouts, Google Drive, Google Admin, Google API Console, Google Accounts, Google Biquery, Google Calendar).

3.6.19.5.4 - Facebook Workplace;

3.6.19.5.5 – SalesForce

3.6.19.6 - Para aplicações SaaS desenvolvidas pela BBTS ou de desenvolvimento nacional, a solução deverá apresentar capacidade de customização de interpretador para registro de ações, a exemplo: Upload, Download, Search, dentre outros.

3.6.25 - A solução deverá apresentar os incidentes em painéis especializados, contendo eventos subdivididos por:

3.6.25.1. DLP;

3.6.25.2. Malware;

3.6.25.3. Análise comportamental dos usuários;

3.6.25.4. Sites maliciosos.

3.8 - Solução Cloud API:

3.8.1. A solução deve se integrar com o provedor de serviço, através do intercâmbio de informações por meio do método de Interface de Programação de Aplicação (API).

3.8.1.1. A integração deverá ser nativa sem exigir a instalação de equipamentos on-premise para redirecionamento do tráfego ou emprego de clientes para redirecionamento do tráfego.

3.8.2. A proteção ofertada pela solução deverá cobrir o uso das aplicações por meio dos seguintes métodos:

3.8.2.1. Browser;

3.8.2.2. Mobile;

3.8.2.3. Aplicativo de Desktop;

3.8.3. Dentre as capacidades mínimas para este módulo, a solução deverá:

3.8.3.1. Realizar o inventário e inspecionar o conteúdo armazenado no Microsoft One Drive, Microsoft Sharepoint, independente de quando ele tenha sido criado ou carregado.

3.8.3.2. Classificar o documento quanto a exposição perante a usuários internos e usuários externos no Microsoft Sharepoint e Microsoft One Drive.

3.8.3.3. Identificar e proteger conteúdo sensível armazenado no serviço SaaS, de acordo com perfil do motor de DLP.

3.8.3.4. Proteger contra armazenamento de artefatos maliciosos no Microsoft One Drive e Sharepoint.

3.8.3.5. Garantir controle de acesso por meio de ações como restrição de acesso, revogação do compartilhamento e quarentenar conteúdo sensível.

3.8.3.6. Prover painel consolidado e acionável com as informações levantadas pela solução.

3.8.4. A solução deverá possuir motor especializado contra vazamento de dados, garantindo as capacidades mínimas que seguem:

3.8.4.1. Deverá possuir identificadores pessoais brasileiros nativos, dentre eles CPF, CNPJ, Nome, Título de Eleitor, CNH e RG.

3.8.4.2. Deverá suportar a criação de dicionários customizados para fins de detecção de documentos com palavras chaves contra vazamentos de dados.

3.8.4.3. Deve possuir a capacidade de detectar informações confidenciais em, no mínimo, 500 tipos de arquivos distintos.

3.8.5. A solução deverá empregar o monitoramento do comportamento do usuário para identificação das seguintes anomalias:

3.8.5.1. Detecção de Ameaça Interna: Deve ser capaz de identificar comportamento anômalos através de movimentação não comum de dados(upload/download), alteração no histórico de comportamento de um determinado usuário da BBTS, monitoramento de atividades não comuns e por fim a identificação de compartilhamento de credenciais.

3.8.5.2. Comprometimento de Usuários: Monitoramento de login no Microsoft Office 365 para identificação de tentativas de acesso de contas da BBTS a partir de países suspeitos e ataque de força bruta.

3.8.6. Referente ao controle de malware a solução deverá empregar as seguintes capacidades:

3.8.7. A solução deverá empregar múltiplos perfils de proteção, dentre eles:

3.8.7.1. Análise de artefatos por meio de assinaturas.

3.8.7.2. Análise de artefatos por meio de heurística.

3.8.7.3. Análise comportamental de artefatos utilizando modelos de Machine Learning para Portable Executable Files.

3.8.8. Para a integração nativa via CASB API entre o fabricante e a tenant do Microsoft Office 365, a solução deverá apresentar painéis especializados para cada um dos módulos de aplicações, dentre eles:

3.8.8.1. Microsoft One Drive:

3.8.8.1.1. A solução deverá realizar todo o inventário do conteúdo armazenado na aplicação, garantindo a apresentação do nome do arquivo, tipo de arquivo, proprietário do arquivo, com quem está compartilhado e histórico de versões do arquivo.

3.8.8.1.2. Deve identificar arquivos compartilhados com usuários externos, bem como a permissão de acesso dada pelo proprietário.

3.8.8.1.3. Apresentar e classificar os arquivos quanto a exposição, devendo identificar arquivos com acesso público, privado e interno.

3.8.8.1.4. Deve permitir ao administrador da solução, baixar o arquivo que viole uma política de detecção de vazamento de dados.

3.8.8.1.5. Deve possuir capacidade de apresentar quais usuários foram identificados com malware, a partir de um artefato malicioso.

3.8.8.1.6. Além da identificação dos compartilhamentos externos, a solução deve permitir a remoção do link de compartilhamento público e restringir o acesso ao arquivo a pessoas selecionadas.

3.8.8.1.7. Através da integração com o Microsoft Information Protection (MIP), deverá permitir a importação dos labels previamente criados e utilizá-los para auxiliar no inventário e classificação de documentos.

3.8.8.2. Microsoft Sharepoint:

3.8.8.2.1. A solução deverá realizar todo o inventário do conteúdo armazenado na aplicação, garantindo a apresentação do nome do arquivo, tipo de arquivo, proprietário do arquivo, com quem está compartilhado e histórico de versões do arquivo.

3.8.8.2.2. Deve identificar arquivos compartilhados com usuários externos, bem como a permissão de acesso dada pelo proprietário.

3.8.8.2.3. Apresentar e classificar os arquivos quanto a exposição, devendo identificar arquivos com acesso público, privado e interno.

3.8.8.2.4. Deve permitir ao administrador da solução, baixar o arquivo que viole uma política de detecção de vazamento de dados.

3.8.8.2.5. Deve possuir capacidade de apresentar quais usuários foram identificados com malware, a partir de um artefato malicioso.

3.8.8.2.6. Além da identificação dos compartilhamentos externos, a solução deve permitir a remoção do link de compartilhamento público e restringir o acesso ao arquivo a pessoas selecionadas.

3.8.8.2.7. Através da integração com o Microsoft Information Protection (MIP), deverá permitir a importação dos labels previamente criados e utilizá-los para auxiliar no inventário e classificação de documentos.

3.8.8.3. Microsoft Teams:

3.8.8.3.1. Usuários Internos e Externos.

3.8.8.3.2. Times Públicos e Privados.

3.8.8.3.3. Incidentes de DLP.

3.8.8.4. Microsoft Outlook:

3..8.4.1. Incidentes de DLP.

3.8.8.4.2. Remetentes com violações de DLP.

3.8.8.4.3. Destinatários com violações de DLP.

3.8.8.4.4. Domínios que mais receberam e-mails com violações de DLP.

Ficam alteradas as datas conforme quadro abaixo:

**ONDE SE LÊ:**

| RECEBIMENTO DAS PROPOSTAS | ABERTURA DA SESSÃO | INÍCIO DA DISPUTA DE PREÇOS |
|---|---|---|
| **Até 22/03/2023** | **22/03/2023** | **22/032023** |
| **Até às 10h00min** | **10h00min** | **10h30min** |

**LEIA-SE:**

| RECEBIMENTO DAS PROPOSTAS | ABERTURA DA SESSÃO | INÍCIO DA DISPUTA DE PREÇOS |
|---|---|---|
| **Até 05/04/2023** | **05/04/2023** | **05/04/2023** |
| **Até às 10h00min** | **10h00min** | **10h30min** |

Brasília, 14 de março de 2023.

Italo Augusto Dias de Souza

Assinado de forma digital por Italo Augusto Dias de Souza
Dados: 2023.03.14 18:16:53 -03'00'

ITALO AUGUSTO DIAS DE SOUZA
AUTORIDADE COMPETENTE DE LICITAÇÃO