Pregão Eletrônico Nº PE.EPE.90.004/2025

OBJETO: *Aquisição de bens:*

(i) 02 (dois) equipamentos *(physical appliances)* de Firewall de Aplicação Web (WAF).

Contratação de serviços:

(i) Licenciamento para os 02 (dois) equipamentos de Firewall de Aplicação Web (WAF) contemplando a garantia, o suporte do fabricante, as atualizações e as assinaturas necessárias para o seu pleno funcionamento, pelo período de 36 (trinta e seis) meses;

(ii) Instalação e configuração para os equipamentos de Firewall de Aplicação Web (WAF), a ser prestado em parcela única;

(iii) Suporte técnico remoto especializado, por telefone ou website próprios, provido pela **CONTRATADA**, para os equipamentos de Firewall de Aplicação Web (WAF) pelo período de 36 (trinta e seis) meses;

(iv) Treinamento especializado na instalação, configuração e uso dos equipamentos de Firewall de Aplicação Web (WAF), devendo ser ministrado para 06 (seis) alunos, em 01 (uma) turma, com carga horária mínima de 24 (vinte e quatro) horas.

QUESTIONAMENTO:

"De acordo com as especificações técnicas gostaríamos de verificar de podermos atender conforme planilha demonstrando cada linha:

Suporte ao protocolo WCCP	Utilizar outros métodos para redirecionamento.
Malware detection, DLP, Web defacement protection	Bloqueio de uploads perigosos e comportamentos maliciosos.
Machine learning para mapear estrutura da aplicação	Perfilamento manual ou por aprendizado básico (learning mode).
Perfil dinâmico de utilização e adaptação automática	Requer intervenção manual para adaptação.
Reconhecimento de Zero Day	Depende de assinaturas e regras criadas.
Inspeção de tráfego in/out: malware,	DLP parcial;

DLP, cloaking	
Perfil gerado via scanner XML	Perfil é criado via observação de tráfego.
Ofuscação de parâmetros sensíveis	Permite apenas mascaramento parcial com rewrite, mas sem rotação automática.

- Suporte ao protocolo WCCP: *Utilizar outros métodos para redirecionamento;*

RESPOSTA Nº 01: Deve ter suporte ao protocolo WCCP conforme o item 1.4.2 da Especificação Técnica.

- Malware detection, DLP, Web defacement protection: *Bloqueio de uploads perigosos e comportamentos maliciosos;*

RESPOSTA Nº 02: Deve ser capaz de prover as funcionalidades requeridas conforme o item 1.7.2 da Especificação Técnica.

- Machine learning para mapear estrutura da aplicação: *Perfilamento manual ou por aprendizado básico (learning mode);*

RESPOSTA Nº 03: O item 1.7.3 da Especificação Técnica estabelece que o aprendizado deve ser automático.

- Perfil dinâmico de utilização e adaptação automática: *Requer intervenção manual para adaptação;*

RESPOSTA Nº 04: Conforme o item 1.7.4 da Especificação Técnica, a adaptação deve ser automática e a intervenção manual opcional.

- Reconhecimento de Zero Day: *Depende de assinaturas e regras criadas;*

RESPOSTA Nº 05: Conforme o item 1.7.20 da Especificação Técnica, a solução deve ser capaz de reconhecer e remediar Zero Day Attacks.

- Inspeção de tráfego in/out, malware, DLP, cloaking: *DLP parcial;*

RESPOSTA Nº 06: Conforme o item 1.7.25 da Especificação Técnica, a solução deve ser capaz de inspecionar o fluxo de saída com capacidade de impedir o vazamento de informações confidenciais.

- Perfil gerado via scanner XML: *Perfil é criado via observação de tráfego;*

RESPOSTA Nº 07: O item 1.7.47 da Especificação Técnica indica que a solução deve ser capaz de gerar perfil de proteção automaticamente por meio de relatórios gerados em XML a partir de scanner de vulnerabilidade de terceiros.

- Ofuscação de parâmetros sensíveis: *Permite apenas mascaramento parcial com rewrite, mas sem rotação automática;*

RESPOSTA Nº 08: A solução deve implementar mecanismo de ofuscação robusto o suficiente para evitar ataques Man-in-the-Browser (MiTB). Aceita-se, no lugar de rotação, a geração aleatória do valor do parâmetro ofuscado.