- Nº do processo: 4014.2025.DEMLPA.PE.0043.MPPE
- Nº do edital: 4014.2025.DEMLPA.PE.0043.MPPE
- Objeto: Ata de Registro de Preços para contratação de empresa para futura e eventual execução de SERVIÇOS DE SOLUÇÃO DE INFOVIA, com fornecimento e instalação de Links MPLS e operação de SDWAN (com BGP Self Healing) para conexão entre Recife e demais localidades, conforme Anexo I, Termo de Referência deste Edital.
- Início das propostas: 31/10/2025 08:00:00
- Termino das propostas: 18/12/2025 09:00:00

- Protocolo: 8FB24676-0360-484C-BA1C-49B2BE1D499A
- CNPJ / CPF: 05250796000154
- Tipo do Registro: Pedido de esclarecimento
- Razão social / Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
- Data do registro: 12/12/2025 18:51:19
- Descrição: QUESTIONAMENTO 09:

  Item 10.5.6.10.9.3. Apresentar o score de risco de cada ator associado ao potencial de distribuição de informação do ator;
  Entendemos que não é prática padrão das soluções de CTI disponibilizar nativamente um score de risco para cada ator, uma vez que esse tipo de classificação costuma ser fornecido por ferramentas especializadas, como ASM, SIEM, SOAR, entre outras; contudo, compreendemos que, caso a solução de CTI ofereça API que permita integração com essas plataformas capazes de calcular e atribuir scores de risco, o requisito de “apresentar o score de risco de cada ator associado ao potencial de distribuição de informação do ator” poderá ser devidamente atendido por meio dessa interoperabilidade. Está correto nosso entendimento?

  QUESTIONAMENTO 10:

  Item 10.5.6.6.8 Deve fazer análise de credenciais detectadas (utilizando modelo de machine learning) para excluir falsos positivos em tempo real, mostrando apenas casos de credenciais reais;
  Entendemos que o item “Deve fazer análise de credenciais detectadas (utilizando modelo de machine learning) para excluir falsos positivos em tempo real, mostrando apenas casos de credenciais reais” tem como objetivo reduzir o volume de alertas irrelevantes e otimizar a triagem de incidentes relacionados a vazamento de credenciais. No entanto, por questões legais e éticas, não é prática comum — nem recomendada — que empresas realizem testes ativos de acesso com essas credenciais para validar sua veracidade. Assim, compreendemos que, caso a solução permita a aplicação de filtros configuráveis, como regras de complexidade de senha, presença de padrões específicos em e-mails, domínios, URLs ou termos-chave, bem como a exclusão de

combinações conhecidas como irrelevantes, o requisito estaria atendido por meio de mecanismos que reduzem significativamente os falsos positivos sem violar diretrizes legais — está correto nosso entendimento?

QUESTIONAMENTO 11:

Item 10.5.6.10.10.8 Azure Blobs
Entendemos que o item “monitorar Azure Blobs, Digital Ocean Spaces, Documentos S3, Google API docs, Documento Windows NET” tem como objetivo identificar exposições indevidas de informações sensíveis armazenadas nessas plataformas, porém compreendemos que não é necessário que a solução acesse diretamente essas fontes primárias. Assim, entendemos que, desde que seja possível identificar e indexar essas informações por meio de fontes alternativas, como motores de busca, repositórios públicos ou outras formas de coleta em ambientes acessíveis externamente, o requisito estará atendido — está correto nosso entendimento?