Resposta aos Questionamentos - NETWORK SECURE SEGURANCA DA INFORMACAO LTDA.

QUESTIONAMENTO 01:

Item 10.5.6.4.6.5.3. Quantidade ilimitada de usuários;
Entendemos que algumas soluções de Threat Intelligence adotam modelos de precificação baseados na quantidade de usuários ativos que terão acesso à plataforma ou aos seus recursos. Como a edital não menciona explicitamente esse número, acreditamos que seria importante obter uma estimativa da quantidade de pessoas que utilizarão a solução, a fim de esclarecer possíveis variações de custo e garantir que a proposta esteja alinhada com a realidade operacional da CONTRATANTE. Está correto o nosso entendimento?

Resposta: Considere pelo menos 2 usuários com acesso a administração plataforma. Para o monitoramento, considere qualquer credencial @mppe.mp.br.

QUESTIONAMENTO 02:
Quantidade de ativos/domínios:
Entendemos que algumas soluções de Threat Intelligence adotam modelos de precificação baseados na quantidade de ativos monitorados, como marcas, empresas e domínios vinculados à CONTRATANTE. Como a edital não especifica explicitamente esses quantitativos, acreditamos que seria importante obter uma estimativa média desses elementos, a fim de esclarecer possíveis variações de custo e garantir que a proposta esteja alinhada com a realidade operacional da CONTRATANTE. Está correto o nosso entendimento?

Resposta: Deverá considerar o domínio mppe.mp.br e todo e qualquer usuário criado a partir do domínio @mppe.mp.br.

QUESTIONAMENTO 03:
Quantidade de interações:
Entendemos que, embora algumas soluções incluam a possibilidade de realizar interações com atores maliciosos como parte de suas capacidades investigativas, seria relevante, para fins de precificação e planejamento operacional, obter uma estimativa média da quantidade de solicitações desse tipo atualmente realizadas pela CONTRATANTE. Essa informação ajudaria a dimensionar corretamente os recursos necessários e garantir que a proposta esteja alinhada com o volume real de demandas. Está correto o nosso entendimento?

Resposta: Deverá considerar o domínio mppe.mp.br e todo e qualquer usuário criado a partir do domínio @mppe.mp.br.

QUESTIONAMENTO 04:
Item 10.5.6.4.6.6.3. Realizar ações em lote;
Entendemos que o item "Realizar ações em lote" tem como objetivo principal permitir maior agilidade e eficiência no tratamento de múltiplos incidentes ou indicadores, otimizando o tempo da equipe de resposta. No entanto, ressaltamos que a execução direta de ações em lote por

interface gráfica pode representar riscos operacionais, como a aplicação inadvertida de comandos em massa sem a devida validação contextual. Assim, compreendemos que, caso a solução disponibilize uma API documentada e segura que permita a execução dessas ações de forma programática e controlada, inclusive com possibilidade de integração com orquestradores ou playbooks, o requisito estaria plenamente atendido — está correto nosso entendimento?

Resposta: Sim.

QUESTIONAMENTO 05:
Item 10.5.6.4.12.2. Interface para visualização de gráficos com dados relacionados às etapas do ciclo de vida das detecções;
Entendemos que o item "Interface para visualização de gráficos com dados relacionados às etapas do ciclo de vida das detecções" busca oferecer visibilidade sobre o andamento e tratamento das detecções ao longo do tempo, porém destacamos que não é comum — nem o foco principal — de soluções especializadas em CTI (Cyber Threat Intelligence) fornecerem nativamente esse tipo de visualização gráfica, uma vez que esse tipo de análise e apresentação costuma ser realizado por ferramentas complementares como SIEM, SOAR ou plataformas de BI. Assim, compreendemos que, ao disponibilizarmos uma API robusta e documentada que permita a extração estruturada desses dados para integração com tais ferramentas, o requisito estaria devidamente atendido — está correto nosso entendimento?

Resposta: A interface em questão refere-se a uma consulta gráfica de quantas credenciais sofreram algum tipo de detecção da plataforma, sobre uma determinada linha temporal.

QUESTIONAMENTO 06:
Item 10.5.6.10.10.9. Digital Ocean Spaces
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?

Resposta: Não, a plataforma deverá possuir recursos de busca "ativo" nas plataformas indicadas nos subitens - 10.5.6.10.10.7 a 10.5.6.10.10.13, identificando repositórios públicos que possam estar divulgando informações do domínio "mppe". Não serão aceitas soluções que "esperem" que o dado nas plataformas indicadas seja disponibilizado na deep web para alertar o SOC.

QUESTIONAMENTO 07:
Item 10.5.6.10.10.11. Google API docs

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?

Resposta: Não, a plataforma deverá possuir recursos de busca "ativo" nas plataformas indicadas nos subitens - 10.5.6.10.10.7 a 10.5.6.10.10.13, identificando repositórios públicos que possam estar divulgando informações do domínio "mppe". Não serão aceitas soluções que "esperem" que o dado nas plataformas indicadas seja disponibilizado na deep web para alertar o SOC.

QUESTIONAMENTO 08:
Item 10.5.6.10.10.12. Documento Windows NET
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?

Resposta: Não, a plataforma deverá possuir recursos de busca "ativo" nas plataformas indicadas nos subitens - 10.5.6.10.10.7 a 10.5.6.10.10.13, identificando repositórios públicos que possam estar divulgando informações do domínio "mppe". Não serão aceitas soluções que "esperem" que o dado nas plataformas indicadas seja disponibilizado na deep web para alertar o SOC.

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?

Resposta: Não, a plataforma deverá possuir recursos de busca "ativo" nas plataformas indicadas nos subitens - 10.5.6.10.10.7 a 10.5.6.10.10.13, identificando repositórios públicos que possam estar

divulgando informações do domínio “mppe”. Não serão aceitas soluções que “esperem” que o dado nas plataformas indicadas seja disponibilizado na deep web para alertar o SOC.

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?

Resposta: Não. A utilização do recurso de teste automatizado de credenciais tem como o objetivo verificar se realmente se o vazamento é procedente ou se trata de informações desatualizadas que ainda circulam na deep web ou em fóruns similares, com o objetivo de diminuir o reporte de falsos positivos.

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?

Resposta: Não, a plataforma deverá possuir recursos de busca “ativo” nas plataformas indicadas nos subitens - 10.5.6.10.10.7 a 10.5.6.10.10.13, identificando repositórios públicos que possam estar divulgando informações do domínio “mppe”. Não serão aceitas soluções que “esperem” que o dado nas plataformas indicadas seja disponibilizado na deep web para alertar o SOC.

QUESTIONAMENTO 12:

Itens 10.5.3.4.12.4.2 e 10.5.3.4.12.4.15

Para atendimento do requisito de Penetration Test com publicação em site oficial e relatório público de testes independentes, o MPPE aceita: (a) publicação do sumário executivo do pentest do

ambiente implantado no contrato (com relatório completo sob NDA), ou (b) exige especificamente pentest do produto/fabricante publicado no site do fabricante? O que o MPPE considera 'site oficial' (fabricante / contratada / órgão) e qual o nível mínimo de detalhe esperado no relatório público?

Resposta: Serão aceitos certificados publicados no próprio site do fabricante da solução ofertada, indicando que ela passou pelo pentest conduzido por agente externo.

QUESTIONAMENTO 13:
Item 5.3 – 10.5.3.4.12.3 e subitens (fontes mínimas de coleta/integração)
Para fins de dimensionamento e planejamento de implantação, solicita-se informar o quantitativo atual (aproximado) das soluções/fontes citadas no item 10.5.3.4.12.3 e subitens.

Resposta: Serão aceitos certificados publicados no próprio site do fabricante da solução ofertada, indicando que ela passou pelo pentest conduzido por agente externo.

QUESTIONAMENTO 14:
Item 15.10.2.1.2.2.
Considerando que o objeto envolve a operação de um SOC (Security Operations Center), entende-se que a certificação ISO/IEC 27001, quando utilizada como requisito, deve estar diretamente vinculada ao ambiente e aos processos do SOC (ex.: monitoramento, correlação e tratamento de eventos, gestão de incidentes, gestão de acessos privilegiados, registro e retenção de evidências, gestão de mudanças, continuidade e melhoria contínua).
Isso porque uma ISO/IEC 27001 genérica (com escopo amplo e sem relação com a operação do SOC) pode não refletir a maturidade e o controle efetivo sobre as rotinas críticas do serviço contratado, enquanto uma certificação com escopo aderente ao SOC dá mais segurança à Administração quanto à existência de um SGSI aplicado exatamente onde o risco é maior: no processamento de logs, dados sensíveis e na tomada de decisão operacional durante incidentes.
Diante disso, solicitamos confirmar: a Administração exige que a ISO/IEC 27001 apresentada tenha escopo explicitamente aplicável ao SOC (ou às atividades essenciais do SOC), e que o certificado seja do ambiente/unidade responsável pela execução do serviço, e não apenas corporativo/genérico?

Resposta: Sim. Só serão aceitos certificados ISO 27001 ou SOC2 da equipe de SOC da empresa.

PEDRO HENRIQUE GONCALVES ARAGAO DA C LIMA:1878263
Assinado digitalmente por PEDRO HENRIQUE GONCALVES ARAGAO DA C LIMA:1878263
ND: C=BR, O=ICP-Brasil, OU=Autoridade Certificadora da Justica - AC-JUS, OU=24100909000180, OU=Videoconferencia, OU=Cert-JUS Poder Publico - A3, OU=Ministerio Publico do Estado de Pernambuco - MPPE, OU=Tecnico Ministerial - Telecomunicacoes, CN=PEDRO HENRIQUE GONCALVES ARAGAO DA C LIMA:1878263
Razão: Eu sou o autor deste documento
Localização:
Data: 2025.12.16 09:15:57-03'00'
Foxit PDF Reader Versão: 2025.2.1

gov.br
Documento assinado digitalmente
BRUNO HENRIQUE MONTENEGRO FERREIRA
Data: 15/12/2025 22:55:10-0300
Verifique em https://validar.iti.gov.br

gov.br
Documento assinado digitalmente
HENRIQUE LUIZ HOLANDA DE MELO JUNIOR
Data: 16/12/2025 08:09:20-0300
Verifique em https://validar.iti.gov.br