ATA DA CONSULTA TÉCNICA 001/2026

Contratação de empresa para prestação de serviços de SOC (Security Operations Center), SIEM (Security Information and Event Management), Implementação e Serviço Técnico Especializado, para o período de 36 (trinta e seis) meses – Processo SEI nº 7010.2026/0000504-9.

(PERGUNTAS E RESPOSTAS)

No dia quatro de março de dois mil e vinte e seis, a Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo – PRODAM-SP torna públicas as respostas aos questionamentos e sugestões apresentados pelas empresas abaixo, na Consulta Técnica referenciada:

Empresa: **"ADVANTA SISTEMAS DE TELECOMUNICAÇÕES E SERVIÇOS DE INFORMÁTICA LTDA."**

Sugestão: *Adicionar o item: "a CONTRATADA deve possuir certificação ISO 20.000, 27001 e 27701." -> A fim de garantir a qualidade da prestação de serviços de SOC.*
Resposta: Em resposta à sugestão, informamos que estamos verificando a viabilidade da inclusão do item.

Sugestão: *Alterar o Item 2.1.1. Para: "O serviço deve garantir operação de SOC em regime 24x7x365, com alta disponibilidade, redundância e continuidade operacional, suportado por modelo de operação distribuída, independente da presença física contínua em múltiplos locais, desde que os profissionais estejam alocados em diferentes localidades e que os controles de segurança, governança e níveis de serviço sejam plenamente atendidos." -> A solicitação de 2 SOC's físicos precede a pandemia e não gera ganhos reais de segurança e produtividade para a operação. O modelo de trabalho híbrido e baseado em soluções de nuvem gera a redundância necessária para manter a continuidade do serviço de SOC.*
Resposta: Em atendimento à sugestão, informamos que, tendo em vista a criticidade dos serviços operados pela PRODAM, a redundância do SOC é parte importante do projeto de SOC, sendo ele em nuvem ou On Premises e, portanto, não será alterado.

Sugestão: *Adicionar o item 2.2.1.1: "A solução proposta deverá utilizar tecnologias como SIEM, SOAR, Inteligência Artificial ou outras tecnologias para correlacionar dados de múltiplas fontes, identificar padrões de ataque, detectar anomalias em tempo real e aprimorar a resposta." -> Permitir a abertura para soluções de correlação de eventos a fim de gerar mais inteligência e ganhos reais na identificação de ameaças e resposta a incidentes.*

Resposta: Em atendimento à sugestão, informamos que foi ajustado.

Sugestão: *Adicionar o item: "Não são permitidas soluções open source, sejam elas puras ou baseadas majoritariamente em componentes de código aberto." -> Para operações 24x7, segurança, missão crítica ou ambientes produtivos regulados, isso aumenta o risco operacional.*
Resposta: Em atendimento à sugestão, informamos que foi texto foi incluído.

Sugestão: *Alterar o Item 2.2.8 para: "Deve possuir regras criadas automaticamente pela solução baseadas em IA ou Machine Learning a fim de automatizar o processo de busca de ameaças." -> A fim de gerar a automação das regras de segurança e aumentar a confiabilidade da solução.*
Resposta: Em atendimento à sugestão, informamos que foi texto foi incluído.

Sugestão: *Remover o Item 2.2.10 e seus subitens -> Utilizar o SIEM como ferramenta de governança de identidade é inverter completamente o papel da ferramenta. SIEM observa eventos, já uma ferramenta de IAM define intenção, política e responsabilidade. Sem IAM, o SIEM só consegue dizer o que aconteceu, nunca se deveria ter acontecido. Aí identidade vira análise forense contínua, não controle.*
Resposta: Em atendimento à sugestão, informamos que a utilização do SIEM também será sobre informações coletadas em logs de Active Directory e tende a possibilitar a criação das regras previstas nos referidos itens. Além disso, o recurso de IAM não está previsto neste edital.

Sugestão: *Alterar o item 2.2.28: Adicionar ao item a quantidade de ativos a qual a solução deve ser licenciada, referente ao quantitativo de EPS. Ou listar toda a infraestrutura que a solução de correlação de eventos deva suportar -> Alteração necessária para permitir a concorrência de soluções que não sejam cotadas por EPS ou armazenamento.*
Resposta: Em atendimento à sugestão, informamos que a solicitação é baseada em padrão de mercado, visando ampla concorrência.

Sugestão: *Alterar o item 2.2.40 para: "A solução deve ser capaz de coletar e armazenar todos os logs de ativos de rede e dos dispositivos de segurança, mantendo os dados disponíveis para buscas por no mínimo 2 anos. -> A coleta de dados por 2 anos permite análise retroativa automática dos dados a fim de buscar comprometimentos anteriores a descobertas de novas ameaças.*
Resposta: Em atendimento à sugestão, informamos que o texto foi ajustado.

Sugestão: *Alterar o item 2.2.42 e remover os seus subitens: "A autodetecção da solução deverá ser capaz de possibilitar a busca de eventos." -> O formato de buscas de eventos*

pode ser diverso e o seu principal objetivo deve ser permitir a transparência dos dados, não importando o modelo de busca.
Resposta: Em atendimento à sugestão, informamos que o texto foi ajustado, de acordo com as necessidades da PRODAM.

Sugestão: *Alterar o item 2.2.44 para: "Suportar a criação de interpretadores (parsers) para a integração de logs não suportados nativamente ou API para integração com a solução." -> A fim de permitir soluções que necessitem apenas de integração com as ferramentas sem construção de regras.*
Resposta: Em atendimento à sugestão, informamos que o texto foi ajustado.

Sugestão: *Alterar o item 2.2.45 para: Suportar a criação de interpretadores (parsers) ou conexões de API customizados para no mínimo 20 sistemas proprietários; - > A fim de permitir soluções que necessitem apenas de integração com as ferramentas sem construção de regras.*
Resposta: Em atendimento à sugestão, informamos que o texto foi ajustado.

Sugestão: *Remover texto do item 2.2.54.2: "logon fora do expediente" -> Utilizar o SIEM como ferramenta de governança de identidade é inverter completamente o papel da ferramenta. SIEM observa eventos, já uma ferramenta de IAM define intenção, política e responsabilidade. Sem IAM, o SIEM só consegue dizer o que aconteceu, nunca se deveria ter acontecido. Aí identidade vira análise forense contínua, não controle.*
Resposta: Em atendimento à sugestão, informamos que a utilização do SIEM também será sobre informações coletadas em logs de Active Directory e tende a possibilitar a criação das regras previstas nos referidos itens. Além disso, o recurso de IAM não está previsto neste edital.

Sugestão: *Remover item 2.2.55.4: Soluções que utilizam análise automatizadas de ameaças não necessitam de ajustes finos constantes das regras.*
Resposta: Em atendimento à sugestão, informamos que o item será mantido, tendo em vista a necessidade de ajuste de regras.

Sugestão: *Remover itens 2.2.75.2; 2.2.75.3; 2.2.75.6; 2.2.75.7; 2.2.75.8; 2.2.83.3; 2.2.83.7 : Utilizar o SIEM como ferramenta de governança de identidade é inverter completamente o papel da ferramenta. SIEM observa eventos, já uma ferramenta de IAM define intenção, política e responsabilidade. Sem IAM, o SIEM só consegue dizer o que aconteceu, nunca se deveria ter acontecido. Aí identidade vira análise forense contínua, não controle.*
Resposta: Em atendimento à sugestão, informamos que a utilização do SIEM também será sobre informações coletadas em logs de Active Directory e tende a possibilitar a

criação das regras previstas nos referidos itens. Além disso, o recurso de IAM não está previsto neste edital.

Sugestão: *Remover item 2.2.78: A fim de permitir a participação de soluções que não se baseiam em construções manuais de regras para o ambiente.*
Resposta: Em atendimento à sugestão, informamos que o item será mantido, tendo em vista a necessidade de ajuste de regras.

Sugestão: *Remover o item 2.2.64: Ferramentas de scan de vulnerábilidades devem ser gerenciadas a parte dos dados encaminhados ao correlacionador de eventos. A solução de vulnerabilidades deve ser suportada pela CONTRATADA.*
Resposta: Em atendimento à sugestão, informamos que o texto foi removido.

Sugestão: *Remover o item 2.2.66: A ferramenta deve suportar as ferramentas da Contratante sem limitações aos modelos de coleta de dados.*
Resposta: Em atendimento à sugestão, informamos que o texto foi removido.

Empresa: "PPN TECNOLOGIA"

Sugestão: 2.1.1. O serviço deve contemplar dois ou mais Centros de Operações de Segurança (SOC) em locais distintos, operando em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano);
1. Considerando-se que a Seção 5 (INDICADORES DE NÍVEL DE SERVIÇOS) estabelece rigorosos Indicadores de Nível de Serviço, validar a necessidade de multiplicidade de locais, que eleva consideravelmente os custos operacionais da solução e pode impactar a competitividade do certame.
Resposta: Em atendimento à sugestão, informamos que, tendo em vista a criticidade dos serviços operados pela PRODAM, a redundância do SOC é parte importante do projeto de SOC e, portanto, não será alterado.

Questionamentos: 2.1.2. A CONTRATADA deve prover níveis de segurança elevados, utilizando no SOC ferramentas para garantir a segurança dos dados manipulados, contemplando, no mínimo, os seguintes controles de segurança física e lógica
2. As soluções descritas nos subitens destinam-se exclusivamente à proteção do ambiente operacional do SOC da CONTRATADA ou também devem ser implantadas nos ambientes do CONTRATANTE?
3. Caso o entendimento seja pela aplicação nos ambientes do CONTRATANTE, o custo de licenciamento de todas as soluções citadas já deve estar incluso na proposta comercial? Ou a contratante já possui essas licenças e a contratada deverá apenas realizar a gestão e operação?

Resposta: Em atendimento ao questionamento, informamos que as soluções descritas no referido item se destinam exclusivamente à proteção do ambiente operacional da CONTRATADA.

Questionamentos: 2.1.2.1. Solução de proteção de endpoints;

3. A solução de proteção de endpoints deve obrigatoriamente possuir capacidades de EDR/XDR para resposta ativa a incidentes, ou uma solução de EPP (Antivírus tradicional) é suficiente?

Resposta: Em atendimento aos questionamentos, informamos o Antivírus corresponde ao que foi solicitado.

4. Existe exigência quanto a funcionalidades mínimas, tais como detecção comportamental, resposta a incidentes, integração com SIEM/SOAR ou mapeamento a frameworks reconhecidos (ex.: MITRE ATT&CK)?

5. A solução deve ser aplicada apenas aos ativos utilizados na operação do SOC ou também aos endpoints do CONTRATANTE monitorados pelo serviço?

6. Caso o ambiente da CONTRATANTE esteja contemplado, qual a volumetria estimada de endpoints (estações de trabalho, servidores e dispositivos móveis) que deverão ser cobertos pela solução?

Resposta: Em atendimento aos questionamentos, informamos que a solução descrita no referido item se destina exclusivamente à proteção do ambiente operacional da CONTRATADA.

Questionamentos: 2.1.2.2. Solução de prevenção contra vazamento de informações (DLP);

5. O DLP deve operar apenas no ambiente do SOC da CONTRATADA ou também sobre os dados e fluxos de informação do CONTRATANTE?

Resposta: Em atendimento aos questionamentos, informamos que a solução descrita no referido item se destina exclusivamente à proteção do ambiente operacional da CONTRATADA.

6. O controle de DLP solicitado deve abranger quais camadas: Endpoint (bloqueio de USB/impressão), Network (tráfego de rede/web) ou Cloud/SaaS (compartilhamento em nuvem)?

Resposta: O controle necessário se fará somente sobre os Endpoints.

7. A definição das regras de classificação de dados e políticas de conformidade será de responsabilidade da contratada (consultoria) ou a contratante fornecerá as regras prontas para implementação técnica?

Resposta: Em atendimento ao questionamento, informamos que a definição das regras ficará a cargo da CONTRATADA.

8. Existe expectativa de cobertura específica para dados pessoais e dados pessoais sensíveis (LGPD), dados classificados ou sigilosos, ou outros tipos de informação?

Resposta: Refere-se à proteção de dados pessoais sensíveis.

2.1.2.3. Solução de proteção de e-mails;

7. A proteção deve contemplar apenas no ambiente do SOC da CONTRATADA ou também sobre os dados e fluxos de informação do CONTRATANTE?

Resposta: Em atendimento aos questionamentos, informamos que a solução descrita no referido item se destina exclusivamente à proteção do ambiente operacional da CONTRATADA.

8. A solução de e-mail deve incluir proteção contra ameaças avançadas como Sandboxing (análise de anexos em ambiente isolado), proteção contra ataques de personificação (Business Email Compromise - BEC), phishing avançado, spear phishing, malware, ransomware?

Resposta: Em atendimento aos questionamentos, informamos que os recursos descritos não fazem parte da solicitação do edital.

9. A solução deverá ser integrada via Gateway (MX Record) ou via API diretamente na suite de e-mails (Office 365/Google Workspace)?

Resposta: Em atendimento aos questionamentos, informamos que os recursos descritos não fazem parte da solicitação do edital.

10. Caso o ambiente da CONTRATANTE esteja contemplado, qual é a quantidade de caixas postais que deverão ser cobertas pela solução?

Resposta: Em atendimento aos questionamentos, informamos que a solução descrita no referido item se destina exclusivamente à proteção do ambiente operacional da CONTRATADA.

2.2. Serviço de Coleta e Correlação de Eventos de Segurança (SIEM)

11. Serão aceitas soluções baseadas em plataformas de Código Aberto (Open Source)?

12. A solução de SIEM ofertada deve obrigatoriamente contar com Suporte Técnico do Fabricante (Enterprise Support)?

Resposta: Em atendimento aos questionamentos, informamos que a solução solicitada não poderá ser em código aberto e deverá obrigatoriamente possuir contrato de Suporte Técnico.

2.2.29.1. Será definida uma reserva de Eventos Por Segundos (EPS) prevendo um crescimento de 50% de acréscimo ao ano sobre o valor inicialmente contratado, com utilização sob demanda, podendo chegar a 15.000 EPS, durante a vigência contratual, sem garantia de execução em sua totalidade.

13. Solicitamos esclarecimentos quanto à volumetria de Eventos Por Segundo (EPS) que deve compor a proposta comercial para o serviço de SIEM, visto que o Termo de Referência 2 apresenta indicadores distintos. Nosso entendimento é que deve ser orçado o volume de 4.000 EPS por mês (item 2.2.28) para vigência de 36 meses, perfazendo um total de 144 pacotes de 1.000 EPS (item 1.1). O eventual crescimento de 50% durante a

vigência do contrato seria um acréscimo de 72.000 EPS ou a proposta deve limitar-se a 15.000 EPS?

Resposta: Em atendimento ao questionamento, informamos que o texto foi revisto para simplificar o entendimento. De todo modo, o valor que deve compor a proposta é do valor unitário do pacote de 1.000 (mil) EPS e o valor total possível de pacotes a serem contratados (15.000 EPS ou 15 pacotes mensais multiplicados pelo número de meses do contrato – 36 meses)

9.1.3 Para fins de comprovação de pertinência e compatibilidade, será considerado válido o(s) atestado(s) que comprove(m) a execução de, no mínimo, 50% (cinquenta por cento) do total de EPS previsto no item 2 da Tabela de Composição de Itens constante deste Termo de Referência, correspondendo a 72 (setenta e dois pacotes de 1000 EPS na execução total do contrato).

14. Solicitamos revisar a volumetria de 72.000 EPS uma vez que mostra-se extremamente expressiva e incomum em ambientes de TI municipais, sendo geralmente encontrada apenas em infraestruturas críticas de nível nacional ou globais. Manter tal exigência pode limitar o universo de possíveis licitantes.

Resposta: Em atendimento ao questionamento, informamos que o texto foi revisto para simplificar o entendimento.

Sobre o modelo de contratação

15. Considerando a alta complexidade do objeto, a diversidade de tecnologias envolvidas e natureza multidisciplinar dos serviços de SOC, recomendamos a admissão de consórcios e subcontratação. Tal medida visa garantir que a Administração Pública não seja limitada por barreiras de mercado e preserve a competitividade e isonomia entre os licitantes, assegurando que o prestador de serviço possa integrar as melhores soluções tecnológicas disponíveis.

Resposta: Em atenção à sugestão, informamos que a Contratação de empresa para prestação de serviços de SOC (Security Operations Center), SIEM (Security Information and Event Management), Implementação e Serviço Técnico Especializado exige uniformidade técnica, responsabilidade única e garantia de continuidade operacional. A participação de consórcios ou a subcontratação, com diferentes empresas se responsabilizando por partes distintas da solução, pode acarretar riscos de incompatibilidade entre os componentes, dificuldade na responsabilização técnica por falhas ou problemas operacionais, fragmentação no suporte, dificultando a resolução de incidentes e comprometimento do SLA (Acordo de Nível de Serviço), de modo que, diante de tais riscos técnicos e operacionais será mantida a vedação à participação de consórcios no certame e não será permitida a subcontratação do objeto contratual.

Empresa: "TELETEX IT SOLUTIONS"

Questionamento: *1. Em relação ao item 2.1.2 e aos subitens 2.1.2.1, 2.1.2.2 e 2.1.2.3, entende-se que as soluções de proteção de endpoints, DLP e proteção de e-mails são requisitos referentes à infraestrutura do SOC da proponente, ou seja, tais soluções não fazem parte do fornecimento à CONTRATANTE. Está correto esse entendimento?*
Resposta: Em atendimento ao questionamento, informamos que o entendimento está correto.

Sugestão: *2. Transcrevo a redação do item 2.1.7.1.2*
Descrição: **Conduzir análises de políticas e regras aplicadas a firewall, WAF, IPS, Endpoints, etc, realizar análises forenses e de tráfego de rede para identificar e mitigar riscos e aprimorar a elaboração de Playbooks de Resposta a Incidentes de Segurança da Informação.**
Sugere-se um novo texto baseado nos fundamentos que descrevemos abaixo:
Nova Descrição: Conduzir análises estratégicas de políticas e regras de segurança aplicadas a firewalls, WAF, IPS, endpoints e ativos de rede, utilizando enriquecimento automático de dados para correlacionar eventos brutos com o contexto de identidade, geolocalização e criticidade do ativo. Realizar análises forenses e de tráfego de rede sobre dados enriquecidos por threat intelligence, visando à identificação proativa de riscos e à redução de falsos positivos. Utilizar os dados contextuais para o aprimoramento e a orquestração de playbooks de resposta a incidentes, garantindo que as ações de mitigação sejam baseadas no score de risco e no impacto ao negócio.
Resposta: Em atendimento à sugestão, informamos que o texto foi ajustado.

Sugestão: *3. Analisando todos os requisitos que compõem o TR concluímos que o objetivo não é a entrega de um SOC apenas operacional. Espera-se um SOC estratégico, alinhado à governança e à gestão de risco aplicada à operação, com aderência a normas e boas práticas reconhecidas (ISO/IEC 27001/27002, NIST), abrangendo criação e validação de políticas, atendimento a requisitos de evidência e capacidade de produção de relatórios executivos (KPIs e KRIs), entre outros.*
Diante disso, para o item 2.1.7 (subitens 2.1.7.[1–8].1) , sugerimos a comprovação de um profissional certificado CISSP na estrutura do SOC.
Para os analistas, além de 01 certificação EC-Council CSA, sugerimos que a equipe seja composta, no mínimo, por: 05 profissionais com certificação CompTIA Security+ (certificação de entrada); 01 profissional com CompTIA CySA+ (certificação intermediária); 01 profissional com CASP+ ou SecurityX (certificação avançada); e 01 profissional com CEH — Certified Ethical Hacker (da EC-Council).
As certificações sugeridas são vendor-neutral (não vinculadas a fabricantes específicos) e comprovam competências transversais necessárias à prestação dos serviços de SOC/SIEM/resposta a incidentes, independentemente da tecnologia adotada. Além

disso, contribuem para a imparcialidade técnica e para a livre competição, além de serem credenciais amplamente aceitas e requisitadas no mercado.
Resposta: Em atendimento à sugestão, informamos que os itens foram revisados de acordo com a necessidade da CONTRATANTE.

Sugestão: *4. O item 2.2.25 está com a seguinte redação atual :*
Descrição : **Possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos via protocolo SYSLOG**
Sugere-se um novo texto baseado nos fundamentos que descrevemos abaixo: Nova Descrição : Possuir capacidade de integração nativa com soluções de segurança e de infraestrutura, suportando múltiplos métodos de ingestão de dados, incluindo Syslog, APIs REST nativas, webhooks, conectores diretos para ambientes de nuvem (AWS, Azure e GCP) e aplicações SaaS, além de protocolos como WMI, WinRM, FTP/SFTP e SNMP, bem como suporte a formatos de dados estruturados, como JSON, XML e CEF.

Resposta: Em atendimento à sugestão, informamos que os itens foram revisados de acordo com a necessidade da CONTRATANTE.

Questionamento: *5. Por meio da leitura dos itens/subitens 2.2.28, 2.2.29, 2.2.29.1 e 2.2.29.2, entende-se que a cobrança será realizada a partir de 4.000 EPS na ativação da solução, podendo chegar a 15.000 EPS durante a vigência contratual, sem garantia de execução em sua totalidade.*
Por sua vez, no item 9.1, que trata da qualificação técnica, solicita-se atestado(s) técnico(s) que comprove(m) a execução de, no mínimo, 50% (cinquenta por cento) do total de EPS previsto no item 2 da Tabela de Composição de Itens constante deste Termo de Referência, correspondendo a 72 (setenta e dois) pacotes de 1.000 EPS na execução total do contrato.
Ou seja, embora o TR indique que a demanda pode chegar a 15.000 EPS durante a vigência contratual, exige-se atestado técnico com comprovação de 72.000 EPS. Entendemos que seria mais coerente solicitar atestado técnico de, no máximo, 15.000 EPS.
Resposta: Em atendimento ao questionamento, informamos que os itens foram revistos para simplificar o entendimento.

Sugestão: *6. Sugerimos acrescentar um item dedicado ao tema de sandbox, por exemplo item 2.2.88.*
2.2.88 A solução deve disponibilizar integração nativa com serviço de sandbox em nuvem, globalmente reconhecido, para detonação e análise dinâmica de arquivos suspeitos de forma ilimitada. O ambiente deve permitir a execução dinâmica em tempo real para detecção de ameaças avançadas, incluindo exploits zero-day, rootkits e

malwares desconhecidos, garantindo que a inteligência gerada seja automaticamente propagada para os mecanismos de detecção e resposta da plataforma.
Resposta: Em atendimento à solicitação, informamos que a sugestão não foi adotada visando ampla competitividade.

Sugestão: *7. Para o item 2.3.13 . Da forma como o item está redigido, permite redefinições a qualquer momento, com retrabalho potencialmente ilimitado e imprevisibilidade de custos e prazos, ainda que sem extrapolar o escopo dos serviços. É necessário calibrar o texto para garantir a exequibilidade do item. Sugestão para a redação do item 2.3.13: Redefinições durante a implementação serão formalizadas por escrito e justificadas tecnicamente, com atualização do planejamento/cronograma, mantendo-se a premissa de que não haverá alteração de escopo.*
Resposta: Em atendimento à sugestão, informamos que o texto foi revisto.

Sugestão: *8. Para o item 2.1.7.7.2: em quais tipos de incidentes/cenários serão estabelecidos procedimentos padronizados para a realização de auditoria forense ? (por exemplo, delimitar que será em cenários de ransomware ou outro de interesse). Ademais, entendemos que se trata de cenários pós-incidente (post-mortem). Está correto esse entendimento?*
Resposta: Em atendimento ao questionamento, informamos que o entendimento está correto.

Empresa: “TELEFONICA BRASIL S/A”

Sugestão: *Referenciando a Consulta Técnica nº 001/2026 cujo objeto compreende a PRESTAÇÃO DE SERVIÇOS PARA FORNECIMENTO DE: SOC (SECURITY OPERATIONS CENTER) SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) SERVIÇOS TÉCNICOS ESPECIALIZADOS seguem nossas considerações e análises.*
Validamos o documento e confirmamos que atendemos 100% do TR. Não obstante, nossa equipe de pré-vendas incluiu, em anexo, a sugestão para inserção em um capítulo adicional.

SOCaaS:
- Correlaciona eventos
- Analisa múltiplas fontes
- Coordena resposta
- Visão estratégica

EDR/XDR:
- Gera eventos ricos do endpoint
- Foco profundo em host
- Executa contenção local
- Visão tática e operacional

12 SERVIÇO DE DETECÇÃO E RESPOSTA EM TEMPO REAL
12.1 Características gerais
12.1.1 O serviço de Detecção e Resposta em Tempo Real corresponde ao serviço de monitoramento de contínuo de endpoints, como computadores e servidores, dispositivos de rede, dados de aplicativos, utilizando bases de dados em nuvem, recursos de inteligência artificial e aprendizado de máquina para oferecer uma abordagem abrangente na detecção de ameaças e oferecendo respostas automatizadas e análise de dados em larga escala. Doravante, será denominada solução de EDR/XDR;
12.1.2 A CONTRATADA é responsável pela administração, operação, suporte, e integração do produto com as demais ferramentas de forma a atender plenamente ao objeto;
12.1.3 Deve ser baseada em soluções em nuvem e oferecida pela CONTRATADA como serviço;
12.1.4 Deve integrar e unificar dados de múltiplas fontes, como agentes de proteção de endpoints, servidores, redes, e infraestrutura em nuvem do CONTRATANTE com objetivo de fornecer uma visão abrangente das atividades no ambiente computacional do CONTRATANTE;
12.1.5 Deve possuir módulo de investigação de ameaças integrado ao produto e ao ecossistema de tecnologias ofertadas pela CONTRATADA;

12.1.6 Deve possuir ambiente de emulação de arquivos considerados maliciosos, suportando os sistemas operacionais em uso no ambiente computacional do CONTRATANTE, no mínimo., conforme a Tabela 20;
12.1.7 Deve monitorar de forma contínua e ininterruptamente bases de conhecimento próprias e de parceiros sobre novas ameaças que possam afetar o ambiente computacional do CONTRATANTE, bem como os meios de prevenir e mitigá-las;
12.1.8 Deve possuir console de administração baseada em interface web, compatível com os navegadores mais recentes, sem a necessidade de instalação de plugins ou componentes adicionais;
12.1.9 O acesso à console de administração deve ser feito via sessões SSL/TLS, com certificados válidos e compatíveis os navegadores mais recentes;
12.1.10 A console de administração deve possuir visibilidade completa do ambiente computacional em que os agentes de proteção estejam instalados, independente de localização geográfica;
12.1.11 ;Deve possuir dashboards e relatórios com modelos prontos com as seguintes visualizações, no mínimo:
12.1.11.1 Agentes ativos com versão, sistema operacional e status de atualização;
12.1.11.2 Detecções por objetivo de ataque;
12.1.11.3 Detecções por técnica ou tática de ataque;
12.1.11.4 Detecções por severidade, criticidade ou impacto;
12.1.11.5 Top 10 detecções por máquina;
12.1.11.6 Top 10 detecções por usuário.
12.1.12 Deve apresentar a superfície de ataque do ambiente computacional do CONTRATANTE, conforme as fontes de dados conectadas, compreendendo:
12.1.12.1 Estações de trabalho, servidores e dispositivos móveis do CONTRATANTE;
12.1.12.2 Usuários, incluindo os com permissões administrativas;
12.1.12.3 Aplicações acessadas;
12.1.12.4 Ativos mantidos pelo CONTRATANTE sob custódia de provedores de nuvem;
12.1.12.5 Domínios e subdomínios do CONTRATANTE;
12.1.12.6 Endereços IP públicos associados ao CONTRATANTE e respectivos hosts;
12.1.12.7 Serviços e portas públicas, e hosts públicos.
12.1.13 A solução de EDR/XDR deve analisar o comportamento de usuários, de forma nativa ou de ferramenta integrada, ofertada pela CONTRATADA, aplicando mecanismos de UEBA (User behavior analytics);
12.1.13.1 Deve identificar comportamentos anômalos ou suspeitos de usuários, com ações de remediação;
12.1.13.2 Deve apresentar alertas de ameaças direcionadas, identificando possíveis ações maliciosas, respondendo automaticamente às ameaças.
12.1.14 Deve prover auditoria detalhada de ações e configurações realizadas na solução de EDR/XDR, bem como nos agentes de proteção de endpoint;

12.1.15 Deve ser capaz de correlacionar eventos de segurança fornecendo contexto adicional sobre ameaças em potencial;
12.1.16 Deve indicar as vulnerabilidades existentes que estão sob ataque ou tentativa de exploração no ambiente computacional do CONTRATANTE, listando os equipamentos afetados;
12.1.17 Deve fornecer visibilidade abrangente das atividades de segurança no ambiente computacional do CONTRATANTE, junto com relatórios detalhados sobre incidentes, ameaças potenciais e eficácia das medidas de segurança, fortalecendo a postura de segurança do CONTRATANTE.
12.2 Ferramentas
12.2.1 O componente de software instalado nos equipamentos é o agente de proteção de endpoint e workloads com capacidade de detecção e resposta, doravante denominado como AGENTE DE PROTEÇÃO DE ENDPOINT;
12.2.2 O agente de proteção de endpoint deve ser compatível com a solução de EDR/XDR proposta pela contratada, sendo preferencialmente do mesmo fabricante, com as versões compatíveis entre si, garantindo pleno funcionamento de todas funcionalidade e atendimento do objeto;
12.2.3 A instalação do agente de proteção de endpoint nos dispositivos deve suportar a instalação via scripts ou políticas de segurança centralizadas, de modo silencioso e sem a necessidade de reiniciar os equipamentos;
12.2.4 Os agentes de proteção de endpoints devem ser capazes de proteger dispositivos contra ameaças conhecidas e desconhecidas, ameaças avançadas(APTs), ransomwares e comportamentos maliciosos, ainda que desconectado da console administrativa da solução de EDR/XDR;
12.2.5 Deve ser capaz de evitar criptografia de arquivos e modificação de arquivos do sistema operacional causados por ransomware através de mecanismos de prevenção e/ou bloqueio dessas ações, e preferencialmente a restauração para seu estado original dos arquivos afetados por ransomware;
12.2.6 Deve conter regras pré-definidas para detecções para principais famílias de ransomware, sendo capaz de prevenir e bloquear seus ataques;
12.2.7 Deve ser capaz de detectar malware desconhecido como RAT (Trojan de acesso remoto) por meio das atividades do malware e não de uma assinatura;
12.2.8 Deve proteger contra scripts CScript maliciosos e contra macros maliciosas do Office;
12.2.9 A atualização dos agentes de proteção de endpoints deve ser realizada através de sessão SSL/TLS com o servidor de atualizações, sem prejuízo nas atividades realizadas pelos usuários;
12.2.10 A solução de EDR/XDR deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas(zero-day), ataques do tipo fileless, ameaças avançadas (APTs), Ransomwares, exploits, URLs maliciosas, websites e outros

comportamentos maliciosos, sem depender exclusivamente de bases de assinaturas ou heurísticas;
12.2.11 Deve suportar os sistemas operacionais utilizados pelo CONTRATANTE, conforme tabela Tabela 20, no mínimo;
12.2.12 Deve suportar a instalação e proteção sob ambientes virtualizados de VDI (Virtual Desktop Interface);
12.2.13 A ferramenta de XDR deve possuir capacidade de realizar análises avançadas de dados e detectar ameaças de forma proativa, incluindo o uso de inteligência artificial, aprendizado de máquina e análise comportamental para identificar ações suspeitas e fornecer respostas com maior assertividade e menor tempo de resposta;
12.2.14 A ferramenta de XDR deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas(zero-day), ataques do tipo fileless, ameaças avançadas (APTs), Ransomwares, exploits, URLs e websites e outros comportamentos maliciosos, sem depender exclusivamente de bases de assinaturas ou heurísticas;
12.2.15 A ferramenta de XDR deve suportar a criação e execução de ações automatizadas configuráveis;
12.2.16 A ferramenta de XDR deve ser capaz de reportar detecções, exportando para arquivos PDF, ou XLSX, ou CSV, com no mínimo os filtros abaixo:
12.2.16.1 Severidade;
12.2.16.2 Tática;
12.2.16.3 Técnica;
12.2.16.4 Usuário;
12.2.16.5 Host;
12.2.16.6 Tipo de sistema operacional;
12.2.16.7 Versão do sistema operacional;
12.2.16.8 Último dia;
12.2.16.9 Última semana;
12.2.16.10 Últimos 30 dias;
12.2.16.11 Nome de arquivo;
12.2.16.12 Hash do processo.
12.2.17 A ferramenta de XDR deve utilizar tecnologias avançadas para analisar e detectar vulnerabilidades de segurança no ambiente do CONTRATANTE, através de algoritmos de aprendizado de máquina e análise comportamental para identificar padrões suspeitos e indicadores de comprometimento;
12.2.18 Através da console administrativa da ferramenta de XDR, deve ser possível analisar isolada ou em conjunto, artefatos considerados suspeitos, enviados a partir dos equipamentos em que o agente de proteção de endpoint estiver instalado, ou via upload, com objetivo de obter informações detalhadas e auxiliar na detecção de novos incidentes de segurança envolvendo esses artefatos ou semelhantes, através de ambiente seguro de execução simulada que permita mapear a execução, processos

iniciados, conexões, urls maliciosas ou suspeitas, e-mails maliciosos ou suspeitos, destinos e protocolos envolvidos na ameaça ou artefato suspeito;
12.2.19 As ameaças e vulnerabilidades identificadas devem possuir classificação segundo o framework de segurança NIST ou MITRE ATT&CK, bem como através da análise comportamental da comunicação do equipamento em que a ferramenta estiver instalada;
12.2.20 A ferramenta de XDR deve ser capaz de atender as técnicas e táticas do framework do MITRE ATT&CK;
12.2.21 As ameaças ou vulnerabilidades encontradas devem possuir classificação de impacto e criticidades;
12.2.22 Deve possuir políticas de uso de dispositivos removíveis e USB, com capacidade mínima de políticas de leitura ou leitura e escrita;
12.2.23 Deve possuir políticas de uso de dispositivos removíveis e USB, com análise em tempo real o dispositivo quanto a arquivos maliciosos ou considerados suspeitos;
12.2.24 Deve fornecer proteção contra URLs e websites considerados maliciosos ou de baixa reputação;
12.2.25 A lista de URLs e websites maliciosos e sua reputação deve ser atualizada pelo fabricante automaticamente;
12.2.26 Deve ser capaz de identificar acesso a URLs e websites além das portas padrão 80 e 443;
12.2.27 Deve permitir a criação de listas de exceção de URLs e websites;
12.2.28 O agente de proteção de endpoint deve ser único a ser instalado em cada dispositivo, provendo todas funcionalidades, sendo administrado pela console de administração da ferramenta de XDR;
12.2.29 O agente de proteção de endpoint não deve impactar no desempenho dos equipamentos em que estiver instalado em uso comum. Em casos de indisponibilidade por falhas, deverá ser analisado e respondido conforme o subitem 20.2.2.6;
12.2.30 O agente de proteção de endpoint deve ser capaz de efetuar a detecção e remediação em tempo real, ainda que momentaneamente desconectado da console administrativa do XDR, com capacidade de bloquear em tempo real ameaças conhecidas e desconhecidas, ataques do tipo fileless, ameaças avançadas, ransomwares, exploits, movimentação lateral, URLs, websites e comportamentos maliciosos, sem depender de bases de assinaturas ou heurísticas exclusivamente;
12.2.31 O agente de proteção de endpoint deve permitir a execução remota de scripts personalizados, através da console administrativa da solução de EDR/XDR, de forma nativa ou integrado à ferramentas de orquestração;
12.2.32 Deve permitir o acesso remoto somente a usuários ou perfis específicos;
12.2.33 Deve permitir a aplicação de políticas de firewall nos dispositivos;
12.2.34 Deve permitir o isolamento do dispositivo que o agente de proteção de endpoint estiver instalado em casos de incidente de segurança ou de infecção, permitindo acesso apenas via console de administração da ferramenta de XDR;

12.2.35 Deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação (Malicioso, Suspeito, etc.) do processo detectado;
12.2.36 A ferramenta de XDR deve ser capaz de criar políticas com abrangência individual, grupos de equipamentos, perfis, ou global;
12.2.37 Deve mapear o risco cibernético existente no ambiente computacional do CONTRATANTE, gerando indicadores e ações práticas a serem executadas, visando diminuir o espectro do risco cibernético;
12.2.38 Deve elencar os pontos de entrada que podem ser utilizados para um ataque cibernético, com base nas camadas de proteção solicitadas;
12.2.39 Deve mapear o cenário de vulnerabilidades, correlacionando informações com objetivo de apontar o risco ao ambiente computacional do CONTRATANTE de acordo com a severidade e criticidade;
12.2.40 Deve mapear as vulnerabilidades no ambiente computacional do CONTRATANTE, classificando-as conforme o nível de CVSS Score e impacto, apresentando as que estão sendo exploradas em equipamentos e através da rede;
12.2.41 Deve classificar os índices de riscos das vulnerabilidades encontradas no ambiente computacional do CONTRATANTE, apontando as que representem maior rísco e impacto;
12.2.42 Deve apresentar o nível de risco cibernético de usuários do CONTRATANTE, identificando os comportamentos anômalos:
12.2.42.1 Login atípico ou impossível;
12.2.42.2 Comprometimento de credencial;
12.2.42.3 Ataque de força bruta;
12.2.42.4 Login a partir de IPs suspeitos;
12.2.42.5 Múltiplas tentativas de logins com sucessos e falhas;
12.2.42.6 Movimentos laterais.
12.2.43 Deve listar os alertas identificados e correlacioná-los com técnicas e táticas do framework de segurança MITRE ATT&CK, de acordo com níveis de riscos de baixo a critico;
12.2.44 Deve listar ações de resposta executadas, e status de execução;
12.2.45 Deve possuir lista de indicadores de comprometimento e objetos suspeitos;
12.2.46 Deve permitir adicionar ou remover objetos sha-1, sha-256, URLs maliciosos, IPs, domínios e endereços de e-mail na lista de objetos suspeitos;
12.2.47 A ferramenta de XDR deve possuir nativamente módulo de detecção de ameaças, capaz de detectar vetores de ameaças no ambiente computacional do CONTRATANTE e ameaças em potencial;
12.2.48 A ferramenta de XDR deve ser capaz de detectar atividades suspeitas associadas a arquivos DLL, em sistemas operacionais Windows;
12.2.49 A solução proposta deve ser capaz de incorporar as técnicas MITRE ATT&CK no esquema de detecção e mostrar quais dessas técnicas foram utilizadas;

12.2.50 Deve possuir módulo de investigação capaz de coletar dados telemétricos de ameaças encontradas e investigadas, incluindo:
12.2.50.1 Endereços de rede e geolocalização;
12.2.50.2 Login de usuários;
12.2.50.3 Processos executados;
12.2.50.4 Requisições de DNS;
12.2.50.5 Uso de comandos e ferramentas administrativas;
12.2.50.6 Conexões e processos associados;
12.2.50.7 Scripts executados;
12.2.50.8 Arquivos escritos, compactados ou descompactados.
12.2.51 O módulo de investigação deve utilizar regras com modelo machine learning e inteligência artificial, em conjunto a base de inteligência de ameaças da fabricante;
12.2.52 A ferramenta de XDR deve possuir módulo de Threat hunting integrado à ferramenta de XDR, e possuir recursos de machine learning e inteligência artificial com objetivo de identificar vetores, ameaças em potencial e adversários infiltrados no ambiente computacional do CONTRATANTE;
12.2.53 A ferramenta de XDR deve ser capaz de pesquisar e apresentar potenciais e ameaças nos dispositivos em que estiver instalada, usando indicadores de comprometimento (IOC);
12.2.54 O módulo de threat hunting deve contemplar, no mínimo, as seguintes áreas:
12.2.54.1 Análise de Malware;
12.2.54.2 Forense de rede;
12.2.54.3 Forense de disco;
12.2.54.4 Reposta a incidente;
12.2.54.5 Inteligência de ameaça.
12.2.55 Deve possuir capacidades de processamento de dados massivos em busca de atividades maliciosas;
12.2.56 A ferramenta de XDR deve possuir ambiente de emulação de execução de código integrado à ferramenta de XDR, com capacidade de execução de arquivos binários, executáveis, e URLs;
12.2.57 O módulo de emulação de execução de código deve ser capaz de receber arquivos suspeitos enviados pela ferramenta de proteção de endpoints, enviados de forma automática ou manual para execução simulada;
12.2.58 O módulo de sandbox deve ser capaz de emular execução de códigos, de ao menos os sistemas operacionais abaixo:
12.2.58.1 Windows 10 e Superiores.
12.2.59 O módulo de sandbox deve incluir na análise de execução, as características:
12.2.59.1 Táticas e técnicas de acordo como modelo de ameaças MITRE ATT&CK;
12.2.59.2 Caraterísticas comportamentais suspeitas;
12.2.59.3 Imagens de execução, quando aplicável;
12.2.59.4 Detalhes do arquivo como nome, hash, tamanho, tipo;

12.2.59.5 Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
12.2.59.6 Leitura e escrita de arquivos em disco;
12.2.59.7 Leitura e alteração de chaves de registro;
12.2.59.8 Detalhes de processos iniciados durante a execução.
12.2.60 A CONTRATADA deve oferecer programa de treinamento oficial da ferramenta de XDR para a equipe técnica designada pelo CONTRATANTE limitado a turma de até 3 profissionais;
12.2.61 Deve ser capaz de receber de forma automática, atualização das bases de dados dos módulos ou recursos de segurança, sem intervenção do administrador da ferramenta;
12.2.62 Os agentes de proteção de endpoints devem possuir o recurso de firewall de host, permitindo aplicar regras de isolamento ou segregação de tráfego através da console administrativa, para um equipamento isolado, grupos ou perfis de equipamentos;
12.2.63 Deve ter a capacidade de controlar o tráfego baseado nos tipos de Protocolos, Endereços IP e intervalo de portas;
12.2.64 Deve ser capaz de definir regras de tráfego com base em políticas de micro-segmentação ou segmentação lógica equivalente;
12.2.65 A solução de EDR/XDR deve ser capaz de detectar ações de varreduras de portas e fingerprint (Network Scan, Port Scan, TCP Null Scan, SYN Scan, Xmas Scan, OS Fingerprint), através do agente de proteção de endpoint, ou combinado com outro componente ofertado pela contratada;
12.3 Processo de gestão de serviço de XDR
12.3.1 A CONTRATADA é responsável por integrar e centralizar os dados de segurança de várias fontes, considerando o ambiente computacional do CONTRATANTE, bem como novos elementos a serem inseridos no ambiente de segurança do CONTRATANTE;
12.3.1.1 Os dados consolidados deve incluir informações sobre vulnerabilidades identificadas, nome do ativo, grupo de serviço, prioridade e criticidade.
12.3.2 A CONTRATADA é responsável por emitir relatórios periódicos com a saúde do ambiente computacional em que a ferramenta de XDR está instalada, contendo:
12.3.2.1 Comunicação com agentes: dias sem contato, último contato;
12.3.2.2 Políticas aplicadas: proteção, resposta, controle de dispositivos, firewall;
12.3.2.3 Versão: atualizações;
12.3.2.4 Dispositivo: sistema operacional, localidade; endereço IP.
12.3.3 A CONTRATADA deverá continuamente e de forma proativa detectar vetores de ameaças ao ambiente computacional do CONTRATANTE, classificando as ameaças em potencial por sua severidade, criticidade, e impacto;
12.3.4 A CONTRATADA deverá fornecer notas explicativas e recomendações para remediação baseada nas atividades maliciosas encontradas e investigadas;

12.3.5 Deve permitir a extração de indicadores de comprometimento como hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de e-mail, nomes de arquivos associados às atividades maliciosas;
12.3.6 Deve permitir a importação de hashes MD5, SHA1, SHA256, URLs, Ips, domínios e endereços de e-mail com objetos considerados suspeitos;
12.3.7 Deve permitir a remoção de hashes MD5, SHA1, SHA256, URLs, Ips, domínios e endereços de e-mail com objetos considerados suspeitos;
12.3.8 A CONTRATADA deve fornecer relatórios completos sobre ameaças detectadas e investigadas, classificando os atores envolvidos, impacto no ambiente computacional do CONTRATANTE, conexões, processos executados, requisições e demais dados telemétricos.
12.4 Grupo técnico de gestão de serviço de XDR
12.4.1 Este grupo é exclusivo para gestão de XDR, não sendo permitido que os profissionais deste grupo sejam compartilhados com os demais serviços descritos no objeto deste termo de referência;
12.4.2 A CONTRATADA é responsável pelo dimensionamento da equipe necessária para realizar tal serviço, sem impacto ao acordo de níveis de serviço, conforme item Erro! Fonte de referência não encontrada.;
12.4.3 Durante a vigência do contrato, a CONTRATADA deve manter os profissionais com os requisitos abaixo:
12.4.3.1 Diploma de curso de nível superior de graduação na área de tecnologia da informação, acrescido de certificado de curso de pós-graduação em área de tecnologia da informação de, no mínimo, 360 (trezentas e sessenta) horas, fornecidos por instituição reconhecida pelo Ministério da Educação (MEC);
12.4.3.2 Conhecimento avançado em segurança da informação, com experiência comprovada de no mínimo 1 (um) ano em operação, sustentação e suporte a ambientes similares ao do CONTRATANTE;
12.4.3.3 Manter válidos e atualizados certificações propostas na tabela 11.
12.4.4 A CONTRATADA deverá apresentar a documentação comprobatória contendo:
12.4.4.1 Currículo vitae comprovando habilidades;
12.4.4.2 Certificações técnicas que comprovem o conhecimento.

Resposta: Informamos que o produto EDR/XDR extrapola o conteúdo do objeto deste Termo de Referência, não fazendo parte do serviço solicitado.