((TÍTULO))((NG))**ATA DA CONSULTA TÉCNICA Nº 004/2022**
((TEXTO)) ((NG)) **ATA DE REGISTRO DE PREÇOS, ENVOLVENDO CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA O FORNECIMENTO DE SERVIÇO DE SUBSCRIÇÃO DE SOLUÇÃO CORPORATIVA DE PREVENÇÃO DE AMEAÇAS DE NOVA GERAÇÃO (EDR - ENDPOINT DETECTION AND RESPONSE), CONTEMPLANDO INSTALAÇÃO, CONFIGURAÇÃO, TREINAMENTO E SUPORTE ESPECIALIZADO DA SOLUÇÃO, PELO PERÍODO DE 36 (TRINTA E SEIS) MESES.**((CL))

(PERGUNTAS E RESPOSTAS)

No dia quatro do mês de fevereiro de dois mil e vinte e três, 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: ((NG)) **"BRICON**"((CL)).
Pergunta 1: O texto descrito a seguir encontra-se no "Teste de Bancada" na página 51, item 2.5, porém não foi descrito na especificação técnica: "A capacidade de AV, ou NGAV, deve estar completamente operacional após instalação do agente no endpoint, sem a necessidade de reinicialização do sistema operacional."Entendemos que esta trata-se de uma característica fundamental da solução a ser adquirida, pois simplifica e agiliza a sua implementação evitando a interrupção do ambiente computacional, mantendo assim o bom desempenho da operação em produção. Entendemos que por ser uma característica do "agente", ou "sensor", este item deva ser incluído como subitem (ex.: 2.3.8, na página 11) do item 2.3 Características dos Agentes ou Sensores. Desta forma mantem-se a correlação entre a especificação técnica e o que está sendo solicitado para comprovação no "Teste de Bancada". Está correto o nosso entendimento?.
Reposta: Este item será corrigido, retirando esta obrigação de "não reinicialização do sistema operacional". Desta forma aumentando a competitividade junto ao mercado.
Pergunta 2: Os itens 2.8.1 a 2.8.5, na página 23, descrevem as capacidades necessárias de inteligência de ameaças da solução a ser ofertada para monitorar ameaças, mapear atores maliciosos, identificar as vulnerabilidades utilizadas, os métodos de instalação, ações e objetivos, com breve descrição dos grupos maliciosos, além de permitir a extração de indicadores de comprometimento (IOCs). Para permitir as capacidades de inteligência de ameaças solicitadas nos itens 2.8.1 a 2.8.5 em uma console única, com gerência de administração centralizada, totalmente integrada e de um único fabricante, conforme solicitado no Termo de Referência, entendemos como imprescindível que a solução utilize o módulo de detecção de threat intelligence (inteligência de ameaças) do mesmo fabricante da plataforma de EDR, correlacionando artefatos, domínios, IPs ou comandos a partir de machine learning de forma automática, evitando assim a necessidade de serviços apartados e integrações com outras soluções de mercado. Está correto o nosso entendimento?
Reposta: Não está correto o entendimento. A questão de administração centralizada de um único fabricante já consta no Termo de Referência. Além disso, a utilização do termo específico "threat intelligence" pode limitar a participação de outros fabricantes. Entendemos ainda que essas funcionalidades estão descritas no item 2.8.
Pergunta 3: Sobre o emulador citado no item 2.9.3, página 23, e item 8.3, página 58. Entendemos que a solução permite a verificação das hashes no VirusTotal e/ou Hybrid Analysis após uma detecção, independente do sistema operacional, bastando apenas a emulação de uma versão de Windows e Linux, não havendo a necessidade de emular todos os sistemas listados nos itens 2.9.3.1, 2.9.3.2 e 2.9.3.3, bem como listados no item 8.3 do Teste de Bancada, na página 58. Está correto o nosso entendimento?

Reposta: Não está correto o entendimento. O teste deverá ser realizado nas plataformas relacionadas no Termo de Referência para garantir que a solução funcione nos diversos ambientes da CONTRATANTE. Porém, as versões dos sistemas operacionas serão revisadas**.**

Pergunta 4: Conforme descrito item 2.7 da página 22, e seus subitens, entendemos que a CONTRATANTE necessitará de um solução que atenda toda a camada threat intelligence e indicadores de IOCs, como também necessitará de monitoramento pelo fabricante em escala 24x7 e um time global capacitado para abastecer os IOCs de forma centralizada e remota, utilizando a mesma console de gerenciamento, não sendo aceita a aquisição de serviços apartados ou até mesmo ferramentas adicionais de terceiros para análise continua e proteção eficaz. Está correto o nosso entendimento?

Reposta: Não está correto o entendimento. A solução deverá ser capaz de monitorar e evidenciar de forma automática, sem intervenção humana. O termo utilizado no item 2.7.1 "software com serviço gerenciado" corresponde a um software com gerenciamento centralizado e dashboads que permitam a análise. Este termo será revisto para evitar dúvidas. Não haverá cotratação de serviços de monitoramento.

Pergunta 5: No item 2.7 Investigação e detecção de ameaças, na página 22, e seus subitens, entendemos que para não deixar a investigação e detecção de ameaças somente de forma automatizada, identificando apenas ameaças e atores maliciosos conhecidos, o serviço deverá ser prestado através de análise humana e continua, 24x7, em busca de anomalias e estratégias de atacantes que fogem do escopo de tecnologia de segurança padrão;
Está correto o nosso entendimento?

Reposta: Não está correto o entendimento. A solução deverá ser capaz de monitorar e evidenciar de forma automática, sem intervenção humana. O termo utilizado no item 2.7.1 "software com serviço gerenciado" corresponde a um software com gerenciamento centralizado e dashboads que permitam a análise. Este termo será revisto para evitar dúvidas. Não haverá cotratação de serviços de monitoramento.

Pergunta 6: No item 2.7 Investigação e detecção de ameaças, na página 22, e seus subitens, entendemos que para a sua eficácia os serviços de Hunting devem contemplar pelo menos as seguintes áreas de conhecimento: i. Análise de Malware; ii. Teste de penetração; iii. Forense de rede; iv. Forense de disco; v. Reposta a incidente; vi. Inteligência de ameaças
Está correto o nosso entendimento?

Reposta: Não está correto o entendimento. A solução deverá ser capaz de monitorar e evidenciar de forma automática, sem intervenção humana. O termo utilizado no item 2.7.1 "software com serviço gerenciado" corresponde a um software com gerenciamento centralizado e dashboads que permitam a análise. Este termo será revisto para evitar dúvidas. Não haverá cotratação de serviços de monitoramento

Pergunta 7: No item 2.7 Investigação e detecção de ameaças, na página 22, e seus subitens, entendemos que a equipe especializada da Contratada deverá realizar com frequência busca histórica de dados em busca de evidências de intrusão;
Está correto o nosso entendimento?

Reposta: Não está correto o entendimento. A solução deverá ser capaz de monitorar e evidenciar de forma automática, sem intervenção humana. O termo utilizado no ite 2.7.1 "software com serviço gerenciado" corresponde a um software com gerenciamento centralizado e dashboads que permitam a análise. Este termo será revisto para evitar dúvidas. Não haverá cotratação de serviços de monitoramento.

Pergunta 8: No item 2.7 Investigação e detecção de ameaças, na página 22, e seus subitens, entendemos que a console única da solução, com gerência de administração centralizada, deverá apresentar, no mínimo, os seguintes dashboards: I. Total de indícios de ameaças geradas; II. Total de indícios de ameaças investigadas; III. Total de detecções acionadas;
Está correto o nosso entendimento?

Reposta: Não está correto o entendimento. Os itens solicitados já estão descritos no Termo de Referência item 2.7**.**

Empresa: ((NG)) **"DISRUPTEC BRASIL**"((CL)).

Pergunta 1: No item 2.5 do Teste de Bancada, pag. 51, encontramos o texto a seguir, porém o mesmo texto não foi descrito na especificação técnica: A capacidade de AV, ou NGAV, deve estar completamente operacional após instalação do agente no endpoint, sem a necessidade de reinicialização do sistema operacional. Este texto deveria estar descrito também na especificação técnica do Termo de Referência, como sendo uma característica do agente, ou sensor, como subitem do item 2.3, pag. 10. Com isso, mantem-se a coerência entre o descrito na especificação técnica do Termo de Referência e o que está sendo solicitado no Teste de Bancada**;**
Concordam com o nosso entendimento?
Reposta: Este item será corrigido, retirando esta obrigação de "não reinicialização do sistema operacional". Desta forma aumentando a competitividade junto ao mercado
Pergunta 2: O item 2.7, pag. 22, descreve a Investigação e detecção de ameaças. Entendemos que para garantir a efetividade e melhores práticas da investigação e detecção de ameaças de forma integrada e centralizada, com o objetivo de conter as novas ameaças ainda desconhecidas, que surgem a cada dia, e correlacionar os eventos a atores maliciosos, este serviço deverá ser fornecido e operado em regime 24x7 pelo mesmo fabricante da solução de EDR a ser fornecida pela CONTRATADA à CONTRATANTE**.**
Concordam com o nosso entendimento?
Reposta: Não está correto o entendimento. A solução deverá ser capaz de monitorar e evidenciar de forma automática, sem intervenção humana. O termo utilizado no item 2.7.1 “software com serviço gerenciado” corresponde a um software com gerenciamento centralizado e dashboads que permitam a análise**.**
Pergunta 3: tem 2.9 Capacidades de emulação de execução de código pag. 23. No item 2.9.3, é solicitado que a solução deva emular execução, no mínimo, nos seguintes sistemas operacionais: 2.9.3.1 Windows 10 2.9.3.2 LINUX Ubuntu, RedHat, CentOS 2.9.3.3 Windows Server 2012 Não há necessidade de emular especificamente estas distribuições de um mesmo sistema operacional e, inclusive, sistema operacional legado em vias de obsolescência. Entendemos que não há solução no mercado que atenda esta característica, ou, se houver, talvez seja atendida desta forma somente por algum fabricante específico, sem que haja a real necessidade disso, restringindo a participação de outros fabricantes e limitando a competitividade do processo. Na realidade entendemos que a solução deva fazer a verificação independente do sistema operacional e emular uma versão de Windows e Linux.
Concordam com o nosso entendimento?
Reposta: Não está correto o entendimento. O teste deverá ser realizado nas plataformas relacionadas no Termo de Referência para garantir que a solução funcione nos diversos ambientes da CONTRATANTE. Porém, as versões dos sistemas operacionas serão revisadas.
Pergunta 4: No item 7.3 Responsabilidade do Fabricante das soluções vencedoras, pag. 38, há o seguinte subitem: 7.3.1 Deverão acompanhar 30% de implementação nas dependências da PRODAM e conjunto com a equipe de analistas de segurança da informação da PRODAM. A implementação é responsabilidade da CONTRATADA, com sua capacidade técnica comprovada através das declarações do Fabricante e demais atestados solicitados nos itens 14.1 a 14.4, além da CONTRATADA estar sujeita às penalidades previstas no item 10, em especial no subitem 10.5. Cabe ressaltar que a CONTRATADA conta com o acompanhamento e suporte técnico da Fabricante durante todo o processo de implementação. Neste caso entendemos que não há a necessidade do acompanhamento em 30% da implementação nas dependências da PRODAM por parte do fabricante, eliminando a necessidade deste subitem. Concordam com o nosso entendimento e exclusão do subitem 7.3.1?
Resposta: está correto o entendimento. Devido à complexidade ao ambiente do parque tecnológico da Prefeitura de São Paulo, bem como sistemas críticos que envolvem seus ativos, é imprescindível o acompanhamento presencial de um especialista da CONTRATADA até o momento descrito no termo de referência. Portanto, estaremos alterando o termo de referencia para que a responsabilidade seja da CONTRATADA**.**
Empresa: ((NG)) **“GERTECH**”((CL)).

Pergunta 1: No Termo de Referência, o item 3 (pag. 29), descreve as características do Suporte, Manutenção e Garantia do fabricante da solução. No subitem 3.1.11.4. (pag. 30) que os serviços de suporte técnico do software poderão ser prestados de forma remota, porém no item 3.1.11.11 (pag.31) informa que: A CONTRATADA deverá disponibilizar um especialista técnico uma vez por semana, de forma presencial, para análise do ambiente, discussão e implementação das melhores práticas; Os Serviços de Suporte Técnico, Manutenção e Garantia do Fabricante são prestados exclusivamente de forma remota, garantindo que as questões de implementação, operação e gerenciamento sejam resolvidas o mais rápido possível, de acordo com os níveis de severidade apresentados no item 3.1.11.12. Em concordância com os demais subitens do item 3, entendemos que no item 3.1.11.11 no lugar do atendimento ser efetuado de forma presencial, ele poderá ser feito de forma remota. Está correto o nosso entendimento?
Resposta: Não está correto o entendimento. Devido à complexidade ao ambiente do parque tecnológico da Prefeitura de São Paulo, bem como sistemas críticos que envolvem seus ativos, é imprescindível o acompanhamento presencial de um especialista da CONTRATADA até o momento descrito no termo de referência.
Pergunta 2: No Termo de Referência, no item 10, (pag. 44), no subitem 10.4 está descrito: Caso haja atraso na disponibilização de profissionais para suporte on-site, haverá multa de 1% ao dia de atraso, calculado sobre o valor mensal do contrato; O Suporte on-site não foi contemplado neste Termo de Referência, não tendo sido estipulado o "Tempo de Atendimento", desta forma não é possível estabelecer o que pode ser considerado como atraso, passível de multa. Desta forma este item não se aplica, tornando-o sem efeito e eliminando assim a sua necessidade.
Concordam com o nosso entendimento referente à exclusão deste item?
Resposta: Não está correto o entendimento. O item 3.1.11.11 prevê a disponibilidade presencial de um profissional da CONTRATADA.
Pergunta 3: No Termo de Referência, no item 10.6 (pag. 45), está descrito: Caso não ocorra a visita semestral estabelecido, haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato; Na especificação do Termo de Referência não foi descrita a necessidade de visita semestral, sendo assim tanto esta multa, quanto este item, não se aplicam, eliminando assim a sua necessidade. Concordam com o nosso entendimento referente à exclusão deste item?
Resposta: O entendimento está correto. Porém, o texto será alterado para especificar a necessidade de visita semestral para análise do ambiente.
Empresa: ((NG)) **"ISH**"((CL)).
Pergunta 1: Destacamos que para poder atender o edital de maneira a entregar um produto compatível com as soluções que já existem no ambiente, precisamos que os itens abaixo sejam retirados por não serem features de mercado naturais para EDR:
2.11 Gestão de Vulnerabilidades. 2.12 Inventário de ativos, usuários e aplicações. Os demais itens demarcados no documento, são itens inerentes a Antivírus, e não EDR, motivo esse que também sugerimos revisão
Resposta: O Termo de Referência visa a busca por uma solução de EDR que agreguem outras funcionalidades para melhor gestão da segurança do ambiente PRODAM, portanto os itens serão mantidos**.**
Empresa: ((NG)) **"CENTURYDATA**"((CL)).
Pergunta 1: 1.9 não serão aceitas soluções que utilizem base local de assinaturas, também conhecida como Base de Vacinas, para reconhecer ameaças, mesmo que este seja apenas um dos métodos de detecção da solução; Pergunta: No nosso entendimento toda a ferramenta presente no mercado possui sua base de assinatura, pois é computacionalmente barata e requer pouco hardware. Contudo, a solução que estamos propondo (SentinelOne) assim como os demais players do mercado possui essa base de assinatura, mas o seu carro chefe é detecção por comportamento. Dito isso, o SentinelOne estaria desqualificado?
Resposta: De acordo com o descrito, entendemos que o produto não atende, tendo em vista que funciona por meio de base local de assinatura. A intenção do edital não é a contratação de um serviço de Antivírus por assinatura.

Pergunta 2: 2.5 A capacidade de AV, ou NGAV, deve estar completamente operacional após instalação do agente no endpoint, sem a necessidade de reinicialização do sistema operacional. Pergunta: Para que todos os recursos estejam funcionando devidamente , se faz necessário reiniciar o equipamento após a instalação. Da mesma forma, o agente realiza apenas um SCAN na máquina para identificar os arquivos legados. Dito isso, é um critério de desqualificação? Todos os fabricantes recomendam realizar a reinicialização do sistema.
Resposta: Este item será corrigido, retirando esta obrigação de "não reinicialização do sistema operacional". Desta forma aumentando a competitividade junto ao mercado**.**
Pergunta 3: 2.6 A solução contratada deverá ser compatível com a solução existente de Endpoint Protect da Trellix, instalada nos Desktops e Servidores corporativos. Pergunta: Como recomendação de mercado e até dos players, não é recomendável a instalação de dois antivírus na máquina. O SentinelOne não é compatível para evitar situação de não detectar alguma ameaça devido à incompatibilidade com outro antivírus. Dito isso, a PRODAM tem intenção de manter dois antivírus nos equipamentos? O SentinelOne é um XDR, por isso toda a parte de EDR e EPP estão presentes na ferramenta
Resposta: A intenção não é ter dois antivírus nos equipamentos. O objeto do edital não visa a contratação de um serviço de Antivírus e sim de um EDR.
Pergunta 4: 3.35 Para dispositivos de armazenamento em massa, deve permitir acesso granular com no mínimo, as seguintes permissões: 2 a) Leitura somente; b) Escrita e leitura; c) Escrita leitura e execução; d) Bloqueio total. Pergunta: Uma dúvida, a busca é por um EDR/XDR ou um DLP? O SentinelOne consegue realizar bloqueio em USB e Bluetooth, mas a nível granular que estão solicitando, recomendo um DLP para realizar esse tipo de bloqueio.
Resposta: A intenção não é contratar DLP. O objeto do edital visa a contratação de um serviço de EDR.
Pergunta 5: 3.38 A política de firewall deve permitir a utilização de múltiplas regras de firewall; Pergunta: O termo referência é por um EDR ou um Firewall de borda? O SentinelOne possui um firewall de camada 4 para alguns protocolos.
Resposta: Não está correto o entendimento. A solução deve permitir criação de regra para controlar o tráfego pelo qual a estação/servidor possa se comunicar com o restante da rede.
Empresa: ((NG)) **“DEFCON1**”((CL)).
Pergunta 1: 1º questionamento: Na página 41 o item 8.1 descreve: A Contratada deverá oferecer garantia, suporte e licenças da solução e suas funcionalidades contratadas por um prazo mínimo de 36 (trinta e seis) meses, a contar da data de sua efetiva instalação. Durante o período de cobertura, a CONTRATADA deverá prestar suporte para todos os componentes do objeto deste edital, incluindo configuração técnica do produto; Questionamento: A Fabricante fornece a garantia e o suporte a partir do momento da disponibilização das licenças à CONTRATANTE, desta forma o prazo de 36 (trinta e seis) meses é contado a partir da entrega das licenças à CONTRATANTE, independente da data de instalação das licenças. Não há como desvincular a data de início da garantia e do suporte da data da efetiva entrega das licenças, pois a partir da entrega das licenças inicia a obrigatoriedade da fabricante em disponibilizar atualizações de versões e prestar o suporte, expirando a sua responsabilidade em prestar estes serviços, caso não haja renovação, em 36 (trinta e seis meses) a partir desta entrega. Caso os 36 (trinta e seis) meses sejam contados somente a partir da instalação, fato é que haverá um período em que a CONTRATANTE não poderá contar com o suporte e a garantia de atualização de versões por parte da fabricante da solução. De acordo com o fato acima exposto sugerimos o seguinte texto para este item: A Contratada deverá oferecer garantia, suporte e licenças da solução e suas funcionalidades contratadas por um prazo mínimo de 36 (trinta e seis) meses, a contar da data da entrega das licenças à CONTRATANTE, com seu respectivo aceite da entrega. Durante o período de cobertura, a CONTRATRATADA deverá prestar suporte para todos os componentes do objeto deste edital, incluindo configuração técnica do produto; Estão de acordo com a nossa sugestão de texto, em benefício da CONTRATANTE?
Resposta: o texto será corrigido para: A Contratada deverá oferecer garantia, suporte e licenças da solução e suas funcionalidades contratadas por um prazo mínimo de 36 (trinta e seis) meses, a contar da data de sua efetiva entrega e ativação (conforme item 16). Serão

consequentemente alterdos os itens de aceite. Durante o período de cobertura, a CONTRATADA deverá prestar suporte para todos os componentes do objeto deste edital, incluindo configuração técnica do produto.

Pergunta 2: 2º Questionamento: No item 10 Penalidades, nas páginas 44 e 45, os subitens 10.1, 10.2, 10.3, 10.4 e 10.6 tratam-se de itens relacionados especificamente ao Suporte Técnico, sendo assim as penalidades devem ser aplicadas relacionadas a prestação dos serviços mensais de Suporte Técnico, e não relacionadas ao valor mensal do contrato como um todo. Desta forma nos subitens 10.1, 10.2, 10.3, 10.4 e 10.6, onde está escrito "valor mensal do contrato" a redação adequada seria "valor mensal do suporte técnico". Estão de acordo com nosso entendimento?

Resposta: não esta correto o entendimento. A penalidade será cobrada pelo valor mensal do contrato, conforme o termo de referencia**.**

Pergunta 3: 3º Questionamento No item 10 Penalidades, na página 44, o subitem 10.5 trata-se de um item relacionado especificamente à instalação da solução, sendo assim a penalidade deve ser aplicada relacionada a prestação do serviço de instalação. Desta forma nos subitens 10.5, onde está escrito "valor mensal do contrato" a redação adequada seria "valor da instalação". Estão de acordo com nosso entendimento?

Resposta: não esta correto o entendimento. A penalidade será cobrada pelo valor do contrato, conforme o termo de referencia**.**

Pergunta 4: 4º questionamento: Na página 45, o item 12.1 descreve: O pagamento das Subscrições será efetuado em parcelas mensais de igual valor, a partir da emissão do termo de aceite pela CONTRATANTE. Questionamento: As Subscrições são fornecidas pela Fabricante no ato da assinatura do instrumento contratual entre a CONTRATANTE e a CONTRATADA, ocasião em que é colocado o pedido de compras junto à Fabricante, sendo a cobrança da Fabricante efetuada a partir desta data; sendo assim o pagamento das Subscrições deverá ser efetuado pela CONTRATANTE em parcelas mensais de igual valor, a partir da entrega das Subscrições pela Fabricante e CONTRATADA à CONTRATANTE, mediante o seu respectivo aceite da entrega. Desta forma sugerimos a utilização do seguinte texto: O pagamento das Subscrições será efetuado em parcelas mensais de igual valor, a partir da entrega das Subscrições pela CONTRATADA e emissão do termo de aceite da entrega pela CONTRATANTE. Estão de acordo com nosso entendimento? Estão de acordo com nosso entendimento?

Resposta: Não está correto o entendimento. Entendemos que o pagamento deverá ser feito após o aceite da solução, confirmando que a solução está em pleno funcionamento. Tal ação visa evitar prejuízos ao erário público**.**

Pergunta 5: 5º questionamento: Na página 45, o item 12.3 descreve: O pagamento da Subscrição das Licenças e o Serviço de Suporte e Garantia, será efetuado pago em parcelas mensais de igual valor, a partir da emissão do termo de aceite da instalação e configuração, pela CONTRATANTE. Questionamento: As Subscrições e o Serviço de Suporte e Garantia são fornecidos pela Fabricante no ato da assinatura do instrumento contratual entre a CONTRATANTE e a CONTRATADA, ocasião em que é colocado o pedido de compras junto à Fabricante, sendo a cobrança da Fabricante efetuada a partir desta data; sendo assim o pagamento das Subscrições e do Serviço de Suporte e Garantia deverão ser efetuados pela CONTRATANTE em parcelas mensais de igual valor, a partir da entrega das Subscrições e do Serviço de Suporte e Garantia pela Fabricante e CONTRATADA à CONTRATANTE, a partir do aceite da entrega. Desta forma sugerimos a utilização do seguinte texto: O pagamento das Subscrições e do Serviço de Suporte e Garantia serão efetuados em parcelas mensais de igual valor, a partir da entrega das Subscrições e do Serviço de Suporte e Garantia pela CONTRATANTE à CONTRATADA, a partir da emissão do termo de aceite da entrega. Estão de acordo com nosso entendimento

Resposta: Não está correto o entendimento. Entendemos que o pagamento deverá ser feito após o aceite da solução, confirmando que a solução está em pleno funcionamento. Tal ação visa evitar prejuízos ao erário público.

Empresa: ((NG)) **"YSSY"**((CL)).

Pergunta 1: O termo de referência pede a mesma licença para o EDR para servidores e estações de trabalho. Identificamos que apenas dois fabricantes no mercado têm este formato. A maioria dos fabricantes, inclusive o que desejamos entrar – Sophos, que é líder no MQ do Gartner e no Wave do Forester – não tem este modelo, sendo que o licenciamento e as funcionalidades são diferentes para servidores e estações de trabalho, que tem comportamento e necessidades de proteção de um EDR muito diferentes. Desta forma, nossa sugestão é a retirada desta exigência, mantendo as funciolidades desejadas para estações de trabalho e para servidores, incluindo o teste de bancada para ambos.
Resposta: sim, será revisto e aceitos agentes especificos para servidores e desktop, possibitando a ampla concorrencia junto ao mercado.
Empresa: ((NG)) **"TELEFÔNICA**"((CL)).
Pergunta 1:
2.2.10 A gerência de administração da solução deve ter capacidade de separar os endpoints gerenciados através de grupos via seleção manual e a criação de grupos com adição de endpoints de forma automática com base em no mínimo, os critérios abaixo:
2.2.10.2 Endereços IP; Não atende
Resposta: item será mantido por ser importante a gestão da solução
2.2.10.3 Endereço de rede (CIDR); Não atende
Resposta:item será mantido por ser importante a gestão da solução
2.2.10.4 Hostname parcial ou completo; Não atende
Resposta: item será mantido por ser importante a gestão da solução
2.2.10.7 Versão do agente. Não atende
Resposta: item será mantido por ser importante a gestão da solução
2.3.2 O agente deve suportar os seguintes sistemas operacionais
Resposta: item será mantido por ser importante a gestão da solução
2.3.2.2 Linux:
CentOS a partir da versão 6; Atende parcialmente: CentOS: 7.8 - 8.4
RESPOSTA: estaremos alterando o termo de referencia para as verões a partir de CentOS 7.8 8.4
Oracle Linux a partir da versão 7; Atende parcialmente: OL: 7.9 8.4
Resposta: conforme o termo de referencia, o item deve ser comprovado pelo teste de bancada.
SUSE Linux Enterprise 12.2 – 12.5 e 15.3; Atende parcialmente: SUSE: 15.3 e 42.3
Resposta: estaremos retirando do termo de referencia.
2.3.6 Para instalação do agente em desktops e servidores que não estejam no domínio corporativo, a CONTRATADA deverá fornecer junto a solução ferramenta de deployment para instalação do agente. Esta solução tem que ser configurada com a senha administrativa destes desktops ou servidores para a instalação do agente. Necessária solução adicional
Resposta:seu entendimento esta correto.
2.4.15 Deve ser capaz de forçar a utilização de ASLR, de modo a mitigar ataques que exploram corrupção de memória; Sim, dificil comprovar
Resposta: conforme o termo de referencia, o item deve ser comprovado pelo teste de bancada.
2.4.18 Deve ser capaz de impedir ataques que sobrescrevam SEH (Structured Exception Handling); Sim, dificil comprovar.
Resposta: conforme o termo de referencia, o item deve ser comprovado pelo teste de bancada.
2.4.19 Deve ser capaz de impedir ataques que explorem vulnerabilidades causadas por ponteiros nulos; Sim, dificil comprovar
Resposta: conforme o termo de referencia, o item deve ser comprovado pelo teste de bancada.
2.4.24 A solução deverá ter sido avaliada pelo MITRE e atender ao menos as seguintes técnicas dentro da avaliação do MITRE ATT&CK:
https://portal.checkpoint.com/dashboard/endpoint/threathunting#/search/mitre

Resposta: não foi possivel, atraves da navegação, identificar as tecnicas listadas a seguir.
T1026, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1095, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1102, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1132, T1132.001, Não Atende
Resposta:conforme o termo de referencia, o item deve ser comprovado.
T1543, T1543.003, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1546.003, T1546.008, T1546.015, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1547, T1547.001, Não Atende
Resposta:conforme o termo de referencia, o item deve ser comprovado.
T1548, T1548.002, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1550, T1550.002, T1550.003, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1552.001, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1559, T1559.001, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1560, T1560.001, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1562, T1562.004, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1564, T1564.004, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1567, T1567.002, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1570, Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
T1574, T1574.001 Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.4.31 Deve implementar permissões específicas de forma a impedir que o acesso remoto esteja disponível somente para usuários específicos;
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.4.33 A solução deve prover a capacidade de adição de endereços específicos para mesmo quando o endpoint esteja em quarentena sejam alcançáveis, ou seja, quando houver o isolamento do endpoint o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a gerência de administração da solução; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.4.43 As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente. Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.5 Características específicas para sistemas operacionais Linux
2.5.4 Deve efetuar bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos? Verificar
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.6.9 Deve permitir a criação de fluxo de trabalho (Workflow) para automatização de processos, os quais devem incluir os seguintes recursos:
2.6.9.1 Verificação da cadeia de execução do Workflow; Não Atende

Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.6.9.2 Compreender gatilhos de execução baseados em:
a) Novos Incidentes; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
b) Novas detecções; Não Atende
RESPOSTA: conforme o termo de referencia, o item deve ser comprovado.
c) Eventos de auditoria incluindo os parâmetros: atribuição, status, comentários e políticas. Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.10.2.7 Requisições DNS; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.10.2.8 Conexões de rede incluindo portas e processos associados; Não Atende **RESPOSTA**: conforme o termo de referencia, o item deve ser comprovado.
2.10.2.10 Scripts escritos em disco; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.10.2.11 Mapa de geolocalização de conexões de rede. Não Atende
RESPOSTA: conforme o termo de referencia, o item deve ser comprovado.
2.11 Gerenciamento de vulnerabilidades, Não Atende - Não atendemos todo o capítulo, itens de 2.11.1 a 2.11.14
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.12.2 Deverá permitir o acompanhamento das alterações de senha e a atividade de login junto com o uso de outras contas; Não Atende.
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.12.3 A solução deverá obter informações sobre o uso de aplicativos, por exemplo, os aplicativos que estão instalados—incluindo onde e quem os está usando—para orientar decisões sobre quais manter e quais desinstalar Não Atende.
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.12.4.3 Mapear relacionamentos entre ativos gerenciados; Não Atende.
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.12.4.5 Acompanhar o uso de recursos do sistema ao longo do tempo; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.12.5.3 Ver quando as senhas foram alteradas pela última vez; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.12.6.2 Listar quais máquinas estão; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.
2.12.7.3 Ativo não suportado: um ativo que não pode ter a solução instalada; Não Atende
Resposta: conforme o termo de referencia, o item deve ser comprovado.