Solicitação de Esclarecimentos - Edital PE/14/2023

De : Eraldo Sousa <elima@e-safer.com.br> qua., 27 de dez. de 2023 15:58
Assunto : Solicitação de Esclarecimentos - Edital PE/14/2023 1 anexo
Para : cdl@proderj.rj.gov.br

Prezados responsáveis pelo processo licitatório,

Esperamos que esta mensagem os encontre bem. Dirigimo-nos a Vossas Senhorias em relação ao Edital de PE/14/2023, publicado em 15/12/2023, que trata do Registro de Preços visando à contratação de empresa de Tecnologia da Informação para o fornecimento de solução de segurança para proteção de dispositivos finais (antivírus), aplicações em nuvem, servidores de e-mail e detecção/resposta unificada a eventos de segurança que envolvam a solução, contemplando o treinamento para operacionalização e o suporte técnico para as soluções contratadas.

Após uma análise cuidadosa do referido edital, surgiram algumas dúvidas que julgamos pertinentes para garantir uma participação esclarecida e justa no processo licitatório. Acreditamos que a obtenção de esclarecimentos adicionais contribuirá para a compreensão mais precisa dos requisitos e condições estabelecidos.

Dessa forma, gostaríamos de solicitar a gentileza de esclarecimentos sobre os seguintes pontos:

Item	Esclarecimento
2.3.2. O EDR deve analisar arquivos, execuções de memória e tráfego de rede dos endpoints; verificar continuamente os discos rígidos (HD's) e demais mídias de armazenamento de forma transparente ao usuário;	Referênte aos Scans sobre demanada é possível realizar isso através da funcionalidade On-Demand Scan
2.3.3. Identificar e proteger contra as várias vulnerabilidades dos sistemas operacionais e aplicações dos endpoints;	Crowdstrike Falcon não depende de uma única tecnologia para evitar ataques. Em vez disso, ele usa uma variedade de métodos complementares e sobrepostos que fornecem a oferta mais abrangente para substituição de AV do setor. • Prevenção baseada em IOA (indicadores de ataque) • Indicadores de Comprometimento (IOC) • Machine Learning (para criar modelos preditivos que podem detectar atividades maliciosas nunca antes vistas com alta precisão) • Táticas e Técnicas Conhecidas de MITRE ATT&CK® • Existe um modulo adicional, Spotlight, voltado a gestão de vulnerabilidades nos Hosts.
2.3.9. A solução deverá possuir filtro de reputação de websites e arquivos, ferramentas de varredura, detecção, análise e remoção de malware e riskware e demais formas de vírus e códigos maliciosos conhecidos, ameaças desconhecidas e ataques do tipo fileless (malware sem arquivo);	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
2.3.12. A solução ofertada deverá dispor de uma base de conhecimento e documentação da ferramenta em um portal com acesso público;	A solução possui toda sua base de conhecimento e documentação restrita aos clientes com acesso a console. O acesso a quaisquer informações pode ser disponibilizado conforme necessário. Como o acesso as informações de documentação e base de conhecimento é garantido e pode ser fornecido, entendemos que o item é atendido. Está correto o nosso entendimento?
2.3.17. A solução deve permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou agendado, incluindo ao menos os formatos: PDF, CSV e XLS, com o envio automático do relatório via e-mail;	Conceituamente a solução ofertada tem o cuidado de garantir que os Dashboards são atualizados em tempo real, para que os dados dos paineis sejam atualizados com agilidade e nossos clientes tenham visibilidade do que está acontecendo em seu ambiente com a maior brevidade possível. Também possuímos automações via workflows para serem acionados dinamicamente conforme ocorrem as detecções. Ao exportar relatórios de formas variadas toda a dinâmica é perdida. A solução possui a capacidade de exportar as informações em CSV e gerar relatórios em PDF. A proteção não será reduzida por não possuir 3 formas de gerar relatórios e os formatos disponíveis oferecem uma excelente experiência para gestores e administradores do ambiente. Dessa forma afirmamos que a solução atende ao requisito é atendido. Está correto o nosso entendimento?
2.3.28. A solução deve mostrar a quantidade de licenças contratadas e a quantidade delas que estão em uso;	Nosso entendimento é que deve ter um controle das licenças em uso. Esse trabalho é feito de forma quinzenal pela contratada através de sessões interativas que apresentam itens sobre o panorama de segurança, incluindo relatórios de uso da solução, boas práticas, saúde dos sensores, recomendações, estatísticas gerais da solução, uso de licenças e outros itens de interesse. Portanto este item é atendido de forma mais completa. Está correto o nosso entendimento?
3.1.1.1. Windows 8.1 (32/64-bit);	O uso de sistemas operacionais legados trazem riscos extremamente críticos a operação, sendo um dos maiores vetores de ataque. O fabricante Microsoft não desenvolve ou mantém correções de vulnerabilidades críticas para estes sistemas operacionais, tornando-os alvos fáceis em ataques cibernéticos bastante simplificados. O risco de manter esses sistemas operacionais é bem crítico e soluções que alegam proteção para estes são questionáveis. Os fabricantes de

	solução de segurança que mantém soluções compatíveis com este legado são sempre baseadas em hashes e assinaturas. Atualmente 71% dos ataques não utilizam nenhum malware. Outro fator que a migração do Windows 8.1 para Windows 10 é relativamente simples e rápido. Portanto, a efetividade em proteger esses dispositivos legados dessas soluções é extremamente baixa. Nosso entendimento é que a solução deve proteger os dispositivos minimamente suportados pelos respectivos fabricantes. A solução proposta possui a suportabilidade alinhada com o suporte dos respectivos fabricantes. Está correto o nosso entendimento?
3.1.2.10. A solução deve permitir a constituição de políticas genéricas aplicáveis a máquinas, grupos de usuários ou máquinas;	Nosso entendimento é que as políticas de segurança devem sempre acompanhar os dispositivos, independente do usuário que esteja utilizando o mesmo. Portanto as políticas devem ser distribuídas de forma uniforme entre os dispositivos ou grupos específicos de dispositivos. Está correto o nosso entendimento?
3.1.2.12. A solução deverá gerar relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;	Conceituamente a solução ofertada tem o cuidado de garantir que os Dashboards são atualizados em tempo real, para que os dados dos paineis sejam atualizados com agilidade e nossos clientes tenham visibilidade do que está acontecendo em seu ambiente com a maior brevidade possível. Também possuímos automações via workflows para serem acionados dinamicamente conforme ocorrem as detecções. Ao exportar relatórios de formas variadas toda a dinâmica é perdida. A solução possui a capacidade de exportar as informações em CSV e gerar relatórios em PDF. Os dashboards são totalmente customizavéis e possuem capacidade para montar painéis com quaisquer dados da solução. Os painés ou dashboards oferecem diferentes formas de interagir com os dados, possibilitando filtrar e visualizar as informações, montar gráficos e tabelas e uso de widgets. Os dados também podem ser consumidos via API, ampliando as possibilidades de relatórios e armazenamento da organização. Pela forma dinâmica de tratar e interagir com os dados e formatos disponíveis da solução proposta fornecem uma excelente experiência para gestores, administradores do ambiente e profissionais de segurança. Dessa forma concluímos que a solução atende ao requisito é atendido. Está correto o nosso entendimento?
3.1.2.13. A solução deverá gerar relatórios e gráficos pré-definidos nos formatos pdf, docx e xlsx;	Conceituamente a solução ofertada tem o cuidado de garantir que os Dashboards são atualizados em tempo real, para que os dados dos paineis sejam atualizados com agilidade e nossos clientes tenham visibilidade do que está acontecendo em seu ambiente com a maior brevidade possível. Também possuímos automações via workflows para serem acionados dinamicamente conforme ocorrem as detecções. Ao exportar relatórios de formas variadas toda a dinâmica é perdida. A solução possui a capacidade de exportar as informações em CSV e gerar relatórios em PDF. Os dashboards são totalmente customizavéis e possuem capacidade para montar painéis com quaisquer dados da solução. Os painés ou dashboards oferecem diferentes formas de interagir com os dados, possibilitando filtrar e visualizar as informações, montar gráficos e tabelas e uso de widgets. Os dados também podem ser consumidos via API, ampliando as possibilidades de relatórios e armazenamento da organização. Pela forma dinâmica de tratar e interagir com os dados e formatos disponíveis da solução proposta fornecem uma excelente experiência para gestores, administradores do ambiente e profissionais de segurança. Dessa forma concluímos que a solução atende ao requisito é atendido. Está correto o nosso entendimento?
3.1.2.16. A solução deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;	Conceituamente a solução ofertada tem o cuidado de garantir que os Dashboards são atualizados em tempo real, para que os dados dos paineis sejam atualizados com agilidade e nossos clientes tenham visibilidade do que está acontecendo em seu ambiente com a maior brevidade possível. Também possuímos automações via workflows para serem acionados dinamicamente conforme ocorrem as detecções. Ao exportar relatórios de formas variadas toda a dinâmica é perdida. A solução possui a capacidade de exportar as informações em CSV e gerar relatórios em PDF. A proteção não será reduzida por não possuir 3 formas de gerar relatórios e os formatos disponíveis oferecem uma excelente experiência para gestores e administradores do ambiente. Dessa forma afirmamos que a solução atende ao requisito é atendido. Está correto o nosso entendimento?
3.1.2.19. A solução deve permitir ter como fonte de atualização um compartilhamento de rede em pelo menos um dos seguintes formatos: UNC, NFS e SMB;	Uma das principais limitações do modelo de EDR baseado em assinaturas é sua incapacidade de lidar com ameaças desconhecidas. Mais de 70% dos ataques atuais não utilizam malware, portanto, soluções tradicionais baseadas em assinaturas são ineficazes. As soluções mais modernas devem ser baseadas no comportamento de ameaças, independentes de existirem vacinas/assinaturas ou se a ameaça utiliza componentes legítimos disponíveis no próprio sistema operacional. A proteção deve utilizar tecnologias com Machine Learning e sem uso de nenhum tipo de vacinas/assinaturas. Atualmente 08 dos 10 maiores bancos utilizam a solução ofertada e estatisticamente são os maiores alvos de ataques cibernéticos. Testaram de maneira exaustiva a solução e optaram pela aquisição da mesma. Nosso entendimento é que a solução deve oferecer o maior nível de proteção possível, com máxima efetividade de proteção contra ameaças, incluindo as

	conhecidas e desconhecidas. A solução proposta é baseada técnicas comportamentais, utilizando tecnologias de Machine Learning e oferece proteção superior, capaz de proteger contra ataques avançados, ataques sem escrita de arquivos (file less), que não utilizam malware, que não possuem assinaturas pelos fabricantes tradicionais. Outros ganhos também são percebidos, como não é necessário reboot do sistema operacional e nem atualizar assinaturas, o custo operacional também é reduzido de forma substancial. Dessa forma a solução ofertada oferece uma solução superior ao requisito, está correto o nosso entendimento?
3.1.2.23. Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;	A solução ofertada funciona em tempo real com os dispositivos protegidos e dispensa o uso de configurações de tempo de comunicação. Dados de telemetria e detecções de ameaças são transmitidos de maneira otimizada para a console de forma constante, com uso médio de 10Mb dia por dispositivo. Dessa forma entendemos que o item é atendido de forma superior ao requisitado. Está correto o nosso entendimento?
3.1.2.24. Deve permitir a escolha do intervalo de tempo necessário para que uma estação seja considerada off-line;	A solução ofertada considera o dispositivo offline com 2 minutos sem comunicação, intervalo cuidadosamente estudo para garantir a máxima proteção e visibilidade sobre o ambiente. Dessa forma entendemos que o item é atendido de forma superior ao requisitado. Está correto o nosso entendimento?
3.1.2.26. Deve permitir a configuração do número de tentativas inválidas de login para o bloqueio de usuários;	Entendemos que o referido item tem como objetivo proteger a console de administração contra ataques de força bruta. A solução proposta possui lógica própria para detectar ataques dessa natureza. E ao invés de operar com esse conceito tradicional, a solução emprega o uso de autenticação MFA (multifator) para proteger os acessos a console. Dessa forma entendemos que o item é atendido de forma superior ao requisitado. Está correto o nosso entendimento?
3.1.2.28. Deve permitir a configuração da duração do bloqueio;	A solução ofertada funciona com o conceito de isolamento do dispositivo que pode ocorrer de forma manual ou automática de acordo com as detecções. Possui flexibilidade para ajustar em quais níveis de detecção um dispositivo deve ser isolado da rede. Uma vez isolado o dispositivo deve permanecer com a comunicação bloqueada exceto para a console da solução, até que a ameaça seja investigada. Depois de concluída a investigação o analista responsável poderá retirar ou não o isolamento de forma manual e controlada. A partir dessa perspectiva, entendemos que um dispositivo envolvido em detecções maliciosas não deve ser desbloqueado de forma automática, sem prévia análise, em nenhuma circustância.. Está correto o nosso entendimento?
3.1.2.31. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;	A solução ofertada dispensa a preocupação com volume de logs ou eventos. A solução possui capacidade ilimitada para eventos e dados da telemetria, evitando que logs ou dados de interesse sejam rotacioados, acarretando em perda de informações críticas para investigação. Para as detecções os dados são armazenados por 90 dias e para os dados de telemetria, utilizados em investigações e caça ameaças (threat hunting) são de 7 dias. Mais do que suficiente para detectar anomalias e investigações suspeitas. Dessa forma entendemos que o item é atendido de forma superior ao requisitado. Está correto o nosso entendimento?
3.1.2.50. Deve permitir integração com Active Directory para acesso a console de administração;	Pela natureza da solução, são empregados conceitos de confiança zero (zero trust). Cerca de 80% dos ataques em 2023 utilizaram credenciais válidas e a maior superfície é liderada pelo Active Directory. Dessa forma a solução poderia ser comprometida facilmente nesses ataques utilizando credenciais válidas. A solução proposta possui capacidade de gerenciar os usuários em base própria, com recursos de de permissionamento granular baseados em RBAC (Role Based Access Control). A solução ainda conta com proteção extra, baseada em autenticação MFA. O que reduz em 99% o risco de acessos indevidos a console de administração. Adicionalmente a solução possui recursos de integração via SSO (Single SignOn) para as principais soluções avançadas de identidade em nuvem, como o Azure AD. Dessa forma acreditamos que o requisito é superado e atendido de forma superior. Está correto o nosso entendimento?
3.1.2.55. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.1.2.63. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;	Uma das principais limitações do modelo de EDR baseado em assinaturas é sua incapacidade de lidar com ameaças desconhecidas. Mais de 70% dos ataques atuais não utilizam malware, portanto, soluções tradicionais baseadas em assinaturas são ineficazes. As soluções mais modernas devem ser baseadas no comportamento de ameaças, independentes de existirem vacinas/assinaturas ou se a ameaça utiliza componentes legítimos disponíveis no próprio sistema operacional. A proteção deve utilizar tecnologias com Machine Learning e sem uso de nenhum tipo de vacinas/assinaturas. Atualmente, 08 dos 10 maiores bancos utilizam a solução ofertada e estatisticamente são os maiores alvos de ataques cibernéticos. Testaram de maneira exaustiva a solução e optaram pela aquisição da mesma. Nosso entendimento é que a solução deve oferecer o maior nível de proteção possível, com máxima efetividade de proteção contra ameaças, incluindo as conhecidas e desconhecidas. A solução proposta é baseada técnicas comportamentais, utilizando tecnologias de Machine Learning e oferece proteção superior, capaz de proteger contra ataques avançados, ataques sem escrita de arquivos (file less), que não utilizam malware, que não possuem assinaturas pelos fabricantes tradicionais. Outros ganhos também são percebidos, como não é necessário reboot do sistema operacional e nem atualizar assinaturas, o custo operacional também é reduzido de forma substancial. Dessa forma a solução ofertada oferece uma solução superior ao requisito, está correto o nosso entendimento?

3.1.2.64. Deve permitir atualização incremental da lista de definições de vírus;	A solução proposta não trabalho com nenhum tipo de assinatura ou definições de vírus para detectar ataques. Nosso entendimento é que a solução deve oferecer o maior nível de proteção possível, com máxima efetividade de proteção contra ameaças, incluindo as conhecidas e desconhecidas. A solução proposta é baseada técnicas comportamentais, utilizando tecnologias de Machine Learning e oferece proteção superior, capaz de proteger contra ataques avançados, ataques sem escrita de arquivos (file less), que não utilizam malware, que não possuem assinaturas pelos fabricantes tradicionais. Outros ganhos também são percebidos, como não é necessário reboot do sistema operacional e nem atualizar assinaturas, o custo operacional também é reduzido de forma substancial. Dessa forma a solução ofertada oferece uma solução superior ao requisito, está correto o nosso entendimento?
3.1.2.66. Deve permitir o rollback das atualizações das listas de definições de vírus e engines.	A solução proposta não trabalho com nenhum tipo de assinatura ou definições de vírus para detectar ataques. Nosso entendimento é que a solução deve oferecer o maior nível de proteção possível, com máxima efetividade de proteção contra ameaças, incluindo as conhecidas e desconhecidas. A solução proposta é baseada técnicas comportamentais, utilizando tecnologias de Machine Learning e oferece proteção superior, capaz de proteger contra ataques avançados, ataques sem escrita de arquivos (file less), que não utilizam malware, que não possuem assinaturas pelos fabricantes tradicionais. Outros ganhos também são percebidos, como não é necessário reboot do sistema operacional e nem atualizar assinaturas, o custo operacional também é reduzido de forma substancial. Dessa forma a solução ofertada oferece uma solução superior ao requisito, está correto o nosso entendimento?
3.1.3.1. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações, Controle de dispositivos e EDR (Endpoint Detection and Response) em um único agente.	Na estratégia e arquitetura da solução proposta o componente é feita a gestão do Firewall presente no sistema operacional, tornando a solução mais leve, consistente e otimizada para focar nas ameaças. Tudo através de uma console simplificada e intuitiva. Já quanto ao HIPS (Host Intrusion Prevention System) e/ou HIDS (Host Intrusion Detection System), diversas das soluções líderes de mercado avaliadas por entidades renomadas como Gartner, Forrester, Mitre, SE LABS e etc., trazem a disposição de seus componentes e funcionalidades de forma diferente, ou seja, oferecem os mesmos recursos em formas superiores e ou equivalentes, por meio de novos motores ou implementações mais modernas. A solução entrega a funcionalidade/proteção de maneira equivalente/superior por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Está correto o nosso entendimento?
3.1.3.2.4. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção.	No panorama atual de segurança cibernética estamos lidando com ameaças extremamente avançadas onde a limpeza de arquivos não é garantida nem mesmo pelos fabricantes de tecnologias. Portanto a limpeza de arquivos e artefatos é sempre incerta. Tecnologias ou processos que alegam a respectiva limpeza são questionáveis e trazem riscos na resposta a incidentes. Os artefatos maliciosos devem ser removidos ou colocados em quarentena para analise adicional, empregado conceitos de detonação do conteúdo (Sandbox) para análises avançadas (Estáticas, Dinamicas). As soluções tradicionais focadas em recursos de verficar arquivos baseados em hashes e assinaturas falharam, cerca de 71% dos ataques atuais não utilizam malware. Portanto, a efetividade em efetuar varreduras em arquivos compactados é questionável, independente de quantos níveis tal artefato foi compactado. A solução proposta é baseada em comportamento, utilizando técnicas modernas de Machine Learning, detectando as ameaças em seu real contexto, na execução, na escrita; Sejam ameaças conhecidas ou desconhecidas. Seja utilizando ferramentas presentes no sistema operacional (Living off the Land). Com base nesse breve contexto e a forma de como a solução trabalha acreditamos que o item é superado. Está correto o nosso entendimento?
3.1.3.2.8. Deverá ser possível configurar os níveis de camadas de compressão para a varredura de arquivos comprimidos;	As soluções tradicionais focadas em recursos de verficar arquivos baseados em hashes e assinaturas falharam, cerca de 71% dos ataques atuais não utilizam malware. Portanto, a efetividade em efetuar varreduras em arquivos compactados é questionável, independente de quantos níveis tal artefato foi compactado. A solução proposta é baseada em comportamento, utilizando técnicas modernas de Machine Learning, detectando as ameaças em seu real contexto, na execução, na escrita; Sejam ameaças conhecidas ou desconhecidas. Seja utilizando ferramentas presentes no sistema operacional (Living off the Land). Com base nesse breve contexto e a forma de como a solução trabalha acreditamos que o item é superado. Está correto o nosso entendimento?
3.1.3.2.9. Deverá realizar varredura de arquivos comprimidos do tipo OLE, sendo possível configurar as camadas de compressão;	As soluções tradicionais focadas em recursos de verficar arquivos baseados em hashes e assinaturas falharam, cerca de 71% dos ataques atuais não utilizam malware. Portanto, a efetividade em efetuar varreduras em arquivos compactados é questionável, independente de quantos níveis tal artefato foi compactado. A solução proposta é baseada em comportamento, utilizando técnicas modernas de Machine Learning, detectando as ameaças em seu real contexto, na execução, na escrita; Sejam ameaças conhecidas ou desconhecidas. Seja utilizando ferramentas presentes no sistema operacional (Living off the Land). Com base nesse breve contexto e a forma de como a solução trabalha acreditamos que o item é superado. Está correto o nosso entendimento?
3.1.3.2.16. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no sistema;	A solução proposta chega a ser 15 vezes mais rápida e leve do que as soluções tradicionais. A solução proposta não depende de escaneamento (conhecidos também como OnAccess Scans) mas é baseada em comportamento das ameaças, execução, contexto. Mas ainda assim possui o recurso de escaneamento de unidades de disco, pastas e arquivos. Nesse modelo tradicional o consumo de recursos do sistema é mais afetado pelo processamento, no consumo da CPU. Sendo assim os ajustes de configuração na limitação do uso de recursos é baseada em CPU. Com base neste breve contexto entendemos que a solução supera o requisito, está correto?

3.1.3.2.18. A solução deverá ter a capacidade de escanear drivers de rede mapeados nos servidores.	Nosso entendimento é o item tem o objetivo de garantir que sejam detectados artefatos maliciosos que estejam sendo executados ou gravados no sistema de arquivos. A solução proposta não depende de escaneamento (conhecidos também como OnAccess Scans) mas é baseada em comportamento das ameaças, independente de onde estejam. A tecnologia é provida aos discos conectados diretamente no servidor, e não em drives de rede mapeados. Está correto o entendimento?
3.1.3.3.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.1.3.3.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo o bloqueio de URLs com baixa reputação;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.1.3.3.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas, e deve permitir também a criação de blacklists e whitelists de URL's;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.1.3.3.5. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.1.3.3.6. A solução deve permitir que o administrador reclassifique uma URL para evitar falsos positivos.	Entendemos que o objetivo deste item é garantir que falsos-positivos sejam evitados para que não gerem detecções indevidas. A solução proposta possui recursos mais modernos para proteção e detecção, assim como possui recursos avançados para configurar exclusões baseadas em Machine Learning, IOCs (Indicadores de Comprometimento) e IOAs (Indicadores de Ataque). Assim entendemos que o item está superado, está correta a nossa conclusão?
3.1.3.6.4. A solução deve ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;	Nosso entendimento para o referido item é que devem possuir mecanismos para identificar todos os dados de interesse relacionados a uma detecção. A solução proposta possui recursos de coletar a telemetria dos dispositivos mesmo que estes não tenham gerado nenhuma detecção. Os dados da telemetria contidos são muito mais abrangentes do que o pacote de rede. Tais dados incluem: Informações do host Mapeamento de conexões de rede, portas, origem, destino, executável, processo, linha de comando Conexões externas, por país, incluindo portas e número de conexões List of external network connections (by country, including the port and the # of connections) Endereços IP externos e internos Atividades de logon de usuário Quaiquer valores ou modificações relacionadas a inicialização do dispositivo (Registro do Windows, tarefas, pastas de inicialização) Executáveis escritos e executados DLL injections Execuções a partir de navegadores Web Histórico de comandos Execução de processos Histórico de comandos executados, parâmetros, usuário, data e hora Uso de ferramentas administrativas Scripts executados

	Atividades de DNS, resolução de nomes, processos Informações de rede de portas abertas (Network Listening) Arquivos e scripts escritos Uso de mídia removível Portanto, de acordo com a ampla coleta de dados de telemetria descritos, concluimos que o item é atendido de forma superior ao requisito. Está correto o nosso entendimento?
3.1.3.6.6. As regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Está correto o nosso entendimento que a solução atende ao requisito?
3.1.3.6.10. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Está correto o nosso entendimento que a solução atende ao requisito?
3.1.3.6.11. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.1.3.6.12. As regras de IPS poderão ter sua capacidade de LOG desabilitado;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. A solução possui recursos para configurar regras na plataforma para não gerar alertas de detecção, muito similar ao contexto do requisito. Está correto o nosso entendimento que a solução atende ao requisito?
3.1.3.6.13. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. A solução possui recursos para notificar os aspectos relacionados a todos os motores da plataforma, permitindo que sejam identificados quais alertas foram disparados e por qual componente. Está correto o nosso entendimento que a solução atende ao requisito?
3.1.3.6.14. As regras de IPS devem ser atualizadas automaticamente pelo fabricante.	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.1.3.7.1. As regras de controle de aplicação devem permitir as seguintes ações: liberar e bloquear;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear

	aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.1.3.7.2. A regra com permissão de liberar aplicações deve possuir as seguintes funcionalidades: permitir a execução de processos externos, não permitir a execução de processos externos e herdar direitos de execução;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.1.3.7.3. O módulo de controle de aplicações deve permitir importar e exportar regras;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.1.3.7.4. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.1.3.7.5. As regras de controle de aplicação devem permitir os seguintes métodos para	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator

identificação das aplicações: Assinatura sha-1 e sha-256 do executável;	relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.1.3.7.6. Atributos do certificado utilizado para assinatura digital do executável, Caminho lógico do executável, Base de assinaturas de certificados digitais válidos e seguros;	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.1.3.7.7. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.1.3.7.8. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.1.3.7.9. O modulo de controle de aplicativos deve possuir uma lista de aplicações malintencionadas para bloqueio e monitoramento.	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.2.3. A solução deverá permitir no mínimo a aplicação de regras de IPS/IDS e antimalware para hosts gerenciados de Docker container;	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.2.10.8. Deverá ser possível configurar os níveis de camadas de compressão para a varredura de arquivos comprimidos;	As soluções tradicionais focadas em recursos de verficar arquivos baseados em hashes e assinaturas falharam, cerca de 71% dos ataques atuais não utilizam malware. Portanto, a efetividade em efetuar varreduras em arquivos compactados é questionável, independente de quantos níveis tal artefato foi compactado. A solução proposta é baseada em comportamento, utilizando técnicas modernas de Machine Learning, detectando as ameaças em seu real contexto, na execução, na escrita; Sejam ameaças conhecidas ou desconhecidas. Seja utilizando ferramentas presentes no sistema operacional (Living off the Land). Com base nesse breve contexto e a forma de como a solução trabalha acreditamos que o item é superado. Está correto o nosso entendimento?

3.2.10.9. Deverá realizar varredura de arquivos comprimidos do tipo OLE, sendo possível configurar as camadas de compressão;	As soluções tradicionais focadas em recursos de verficar arquivos baseados em hashes e assinaturas falharam, cerca de 71% dos ataques atuais não utilizam malware. Portanto, a efetividade em efetuar varreduras em arquivos compactados é questionável, independente de quantos níveis tal artefato foi compactado. A solução proposta é baseada em comportamento, utilizando técnicas modernas de Machine Learning, detectando as ameaças em seu real contexto, na execução, na escrita; Sejam ameaças conhecidas ou desconhecidas. Seja utilizando ferramentas presentes no sistema operacional (Living off the Land). Com base nesse breve contexto e a forma de como a solução trabalha acreditamos que o item é superado. Está correto o nosso entendimento?
3.2.10.11. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;	As soluções tradicionais focadas em recursos de verficar arquivos baseados em hashes e assinaturas falharam, cerca de 71% dos ataques atuais não utilizam malware. Portanto, a efetividade em efetuar varreduras em arquivos compactados é questionável, independente de quantos níveis tal artefato foi compactado. A solução proposta é baseada em comportamento, utilizando técnicas modernas de Machine Learning, detectando as ameaças em seu real contexto, na execução, na escrita; Sejam ameaças conhecidas ou desconhecidas. Seja utilizando ferramentas presentes no sistema operacional (Living off the Land). Com base nesse breve contexto e a forma de como a solução trabalha acreditamos que o item é superado. Está correto o nosso entendimento?
3.2.10.12. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;	As soluções tradicionais focadas em recursos de verficar arquivos baseados em hashes e assinaturas falharam, cerca de 71% dos ataques atuais não utilizam malware. Portanto, a efetividade em efetuar varreduras em arquivos compactados é questionável, independente de quantos níveis tal artefato foi compactado. A solução proposta é baseada em comportamento, utilizando técnicas modernas de Machine Learning, detectando as ameaças em seu real contexto, na execução, na escrita; Sejam ameaças conhecidas ou desconhecidas. Seja utilizando ferramentas presentes no sistema operacional (Living off the Land). Com base nesse breve contexto e a forma de como a solução trabalha acreditamos que o item é superado. Está correto o nosso entendimento?
3.2.10.16. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no sistema;	A solução proposta chega a ser 15 vezes mais rápida e leve do que as soluções tradicionais. A solução proposta não depende de escaneamento (conhecidos também como OnAccess Scans) mas é baseada em comportamento das ameaças, execução, contexto. Mas ainda assim possui o recurso de escaneamento de unidades de disco, pastas e arquivos. Nesse modelo tradicional o consumo de recursos do sistema é mais afetado pelo processamento, no consumo da CPU. Sendo assim os ajustes de configuração na limitação do uso de recursos é baseada em CPU. Com base neste breve contexto entendemos que a solução supera o requisito, está correto?
3.2.10.18. A solução deverá ter a capacidade de escanear drivers de rede mapeados nos servidores.	Nosso entendimento é o item tem o objetivo de garantir que sejam detectados artefatos maliciosos que estejam sendo executados ou gravados no sistema de arquivos. A solução proposta não depende de escaneamento (conhecidos também como OnAccess Scans) mas é baseada em comportamento das ameaças, independente de onde estejam. A tecnologia é provida aos discos conectados diretamente no servidor, e não em drives de rede mapeados. Está correto o entendimento?
3.2.11.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.2.11.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo o bloqueio de URLs com baixa reputação;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.2.11.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas, e deve permitir também a criação de blacklists e whitelists de URL's;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.2.11.5. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?

3.2.11.6. A solução deve permitir que o administrador reclassifique uma URL para evitar falsos positivos.	Entendemos que o objetivo do item é proteger os dispositivos contra ameaças originadas pela navegação em sites da web. A solução proposta possui a estratégia de entregar uma tecnologia baseada no comportamento de ameaças, tornando a solução mais confiante e sem a dependência de assinaturas e ou classificação de sites. A solução possui motor específico para tratar e bloquear ameaças como Adware, PUP (Programas Potencialmente indesejados), Drive-by-Download e etc., bem como monitorar o tráfego HTTP/HTTPS em busca de comportamento malicioso. Lembrando que a dependência em categorização de sites depende de análise prévia e classificação, muito semelhante ao conceito de assinaturas, ineficaz nos dias atuais. Toda a proteção oferecida pela solução é entregue sem depender de classificação ou filtragem de conteúdo web. Está correto o nosso entendimento?
3.2.13.1. A solução deve operar também como firewall de host, através da instalação de agentes nos endpoints protegidos;	Na estratégia e arquitetura da solução proposta o componente é feita a gestão do Firewall presente no sistema operacional, tornando a solução mais leve, consistente e otimizada para focar nas ameaças. Tudo através de uma console simplificada e intuitiva. Dessa forma concluimos que por fazer a gestão do firewall já presente no sistema operacional a solução atende ao requisito. Está correto o nosso entendimento?
3.2.13.2. A solução deve ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;	A solução proposta possui os recursos necessários para a criação de regras e efetuar o controle de tráfego. As regras podem ser criadas com base nos protocolos, endereços de origem, destino, portas de comunicação, arquivos executáveis e nomes de domínio. Concluimos que o item está de acordo com a especificação técnica. Está correto o nosso entendimento?
3.2.13.3. A solução deve ter a capacidade de controlar conexões TCP baseado nas Flags TCP;	A solução proposta possui os recursos necessários para a criação de regras e efetuar o controle de tráfego. As regras podem ser criadas com base nos protocolos, endereços de origem, destino, portas de comunicação, arquivos executáveis e nomes de domínio. Concluimos que o item está de acordo com a especificação técnica. Está correto o nosso entendimento?
3.2.13.6. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;	Entendemos que no panorama atual de segurança cibernética as regras de firewall uma vez configuradas, devem permanecer ativa em todos os momentos. Entendemos também que determinadas regras devem ser aplicadas de acordo com o contexto (Na rede interna, rede externa e redes públicas). A solução proposta trabalha de forma integrada ao Windows, utilizando o mesmo contexto para aplicar determinadas regras. Dessa forma as regras funcionam de forma dinâmica, de acordo com a localidade de onde o usuário esteja conectado. Com base no breve contexto, acreditamos que o requisito é superado. Está correto o nosso entendimento?
3.2.13.9. As regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;	Entendemos que no panorama atual de segurança cibernética as regras de firewall uma vez configuradas, devem permanecer ativa em todos os momentos. Entendemos também que determinadas regras devem ser aplicadas de acordo com o contexto (Na rede interna, rede externa e redes públicas). A solução proposta trabalha de forma integrada ao Windows, utilizando o mesmo contexto para aplicar determinadas regras. Dessa forma as regras funcionam de forma dinâmica, de acordo com a localidade de onde o usuário esteja conectado. Com base no breve contexto, acreditamos que o requisito é superado. Está correto o nosso entendimento?
3.2.14.4. A solução deve ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;	Nosso entendimento para o referido item é que devem possuir mecanismos para identificar todos os dados de interesse relacionados a uma detecção. A solução proposta possui recursos de coletar a telemetria dos dispositivos mesmo que estes não tenham gerado nenhuma detecção. Os dados da telemetria contidos são muito mais abrangentes do que o pacote de rede. Tais dados incluem: Informações do host Mapeamento de conexões de rede, portas, origem, destino, executável, processo, linha de comando Conexões externas, por país, incluindo portas e número de conexões List of external network connections (by country, including the port and the # of connections) Endereços IP externos e internos Atividades de logon de usuário Quaiquer valores ou modificações relacionadas a inicialização do dispositivo (Registro do Windows, tarefas, pastas de inicialização) Executáveis escritos e executados DLL injections Execuções a partir de navegadores Web Histórico de comandos Execução de processos Histórico de comandos executados, parâmetros, usuário, data e hora Uso de ferramentas administrativas Scripts executados Atividades de DNS, resolução de nomes, processos Informações de rede de portas abertas (Network Listening) Arquivos e scripts escritos Uso de mídia removível Portanto, de acordo com a ampla coleta de dados de telemetria descritos, concluimos que o item é atendido de forma superior ao requisito. Está correto o nosso entendimento?
3.2.14.6. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. A solução possui recursos granulares para configurar como as políticas de proteção

	são aplicadas, com base em qualquer característica do dispositivo. Está correto o nosso entendimento que a solução atende ao requisito?
3.2.14.7. As regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Está correto o nosso entendimento que a solução atende ao requisito?
3.2.14.11. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Está correto o nosso entendimento que a solução atende ao requisito?
3.2.14.12. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.2.14.13. As regras de IPS poderão ter sua capacidade de LOG desabilitado;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. A solução possui recursos para configurar regras na plataforma para não gerar alertas de detecção, muito similar ao contexto do requisito. Está correto o nosso entendimento que a solução atende ao requisito?
3.2.14.14. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;	A solução proposta entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. A solução possui recursos para notificar os aspectos relacionados a todos os motores da plataforma, permitindo que sejam identificados quais alertas foram disparados e por qual componente. Está correto o nosso entendimento que a solução atende ao requisito?
3.2.14.15. As regras de IPS devem ser atualizadas automaticamente pelo fabricante.	A solução entrega a funcionalidade de HIDS e HIPS de maneira equivalente/superior, por meio de motores avançados específicos, entretanto sem a dependência de assinaturas/vacinas e sem agentes/produtos adicionais. Outro fator relevante é que estatisticamente tais componentes estiveram presentes e disponíveis nos licenciamentos e ou aquisições nos últmos 10 anos mas não foram implementados devido a sua alta complexidade. Dessa forma concluímos que poderão ser consideradas soluções que entreguem funcionalidades e proteções equivalentes, sem assinaturas, implementação simplificada e máxima efetividade na proteção contra ameaças. Os componentes também possuem a funcionalidade de ativar ou desativar o recurso de forma simples e intuitiva, sem a necessidade de reinicializar o dispositivo nem implementar agentes adicionais. Sendo assim concluimos que o item é superado pelo fato da solução oferecer recursos mais modernos em sua implementação. Está correto o nosso entendimento?
3.2.15.1. A solução deve ter a funcionalidade de controle de aplicações;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser

	executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.15.2. A solução deve ser capaz de bloquear softwares não reconhecidos;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.15.3. A solução deve ser capaz de gerar relatório referente ao status do módulo;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.14.4. A solução deve ser capaz de gerar relatório sobre o status do agente;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança

	ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.15.5. A solução deve ser capaz de gerar script de instalação do agente;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.15.6. Monitoração de Status - Visualização do status dos hosts gerenciados, incluindo a realização de healthcheks.	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.15.7. A solução deverá permitir a entrega de agentes por pelo menos uma dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet.	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?

3.2.16.10. Deverá habilitar e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (caso a área monitorada não seja mais importante, a regra deverá ser removida automaticamente; e vice-versa);	O agente da solução proposta já possui tecnologia embarcada para identificar alterações em arquivos e configurações críticos do Sistema Operacional, utilizando Machine Learning e inteligência artificial para identificar quaiquer contextos de alteração maliciosa. Todas as ações são correlacionadas em uma única detecção, trazendo agilidade para resposta a incidentes a atividades em caráter forense. Com base no breve contexto, concluimos que o item é superado. Está correto o nosso entendimento?
3.2.16.11. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;	O agente da solução proposta já possui tecnologia embarcada para identificar alterações em arquivos e configurações críticos do Sistema Operacional, utilizando Machine Learning e inteligência artificial para identificar quaiquer contextos de alteração maliciosa. Todas as ações são correlacionadas em uma única detecção, trazendo agilidade para resposta a incidentes a atividades em caráter forense. Com base no breve contexto, concluimos que o item é superado. Está correto o nosso entendimento?
3.2.16.17. Deverá classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;	O agente da solução proposta já possui tecnologia embarcada para identificar alterações em arquivos e configurações críticos do Sistema Operacional, utilizando Machine Learning e inteligência artificial para identificar quaiquer contextos de alteração maliciosa. Todas as ações são correlacionadas em uma única detecção, trazendo agilidade para resposta a incidentes a atividades em caráter forense. Com base no breve contexto, concluimos que o item é superado. Está correto o nosso entendimento?
3.2.17.3. Deverá habilitar e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (caso a área monitorada não seja mais importante, a regra deverá ser removida automaticamente; e vice-versa);	Nosso entendimento para o referido item é que devem possuir mecanismos para identificar todos os dados de interesse relacionados a uma detecção. A solução proposta possui recursos de coletar a telemetria dos dispositivos mesmo que estes não tenham gerado nenhuma detecção. Os dados da telemetria contidos são muito mais abrangentes do que o pacote de rede. Tais dados incluem: Informações do host Mapeamento de conexões de rede, portas, origem, destino, executável, processo, linha de comando Conexões externas, por país, incluindo portas e número de conexões List of external network connections (by country, including the port and the # of connections) Endereços IP externos e internos Atividades de logon de usuário Quaiquer valores ou modificações relacionadas a inicialização do dispositivo (Registro do Windows, tarefas, pastas de inicialização) Executáveis escritos e executados DLL injections Execuções a partir de navegadores Web Histórico de comandos Execução de processos Histórico de comandos executados, parâmetros, usuário, data e hora Uso de ferramentas administrativas Scripts executados Atividades de DNS, resolução de nomes, processos Informações de rede de portas abertas (Network Listening) Arquivos e scripts escritos Uso de mídia removível Portanto, de acordo com a ampla coleta de dados de telemetria descritos, concluimos que o item é atendido de forma superior ao requisito. Está correto o nosso entendimento?
3.2.17.4. Deverá permitir customização de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;	Nosso entendimento para o referido item é que devem possuir mecanismos para identificar todos os dados de interesse relacionados a uma detecção. A solução proposta possui recursos de coletar a telemetria dos dispositivos mesmo que estes não tenham gerado nenhuma detecção. Os dados da telemetria contidos são muito mais abrangentes do que o pacote de rede. Tais dados incluem: Informações do host Mapeamento de conexões de rede, portas, origem, destino, executável, processo, linha de comando Conexões externas, por país, incluindo portas e número de conexões List of external network connections (by country, including the port and the # of connections) Endereços IP externos e internos Atividades de logon de usuário Quaiquer valores ou modificações relacionadas a inicialização do dispositivo (Registro do Windows, tarefas, pastas de inicialização) Executáveis escritos e executados DLL injections Execuções a partir de navegadores Web Histórico de comandos Execução de processos Histórico de comandos executados, parâmetros, usuário, data e hora Uso de ferramentas administrativas Scripts executados Atividades de DNS, resolução de nomes, processos Informações de rede de portas abertas (Network Listening) Arquivos e scripts escritos Uso de mídia removível

	Portanto, de acordo com a ampla coleta de dados de telemetria descritos, concluimos que o item é atendido de forma superior ao requisito. Está correto o nosso entendimento?
3.2.17.5. Deverá permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;	Nosso entendimento para o referido item é que devem possuir mecanismos para identificar todos os dados de interesse relacionados a uma detecção. A solução proposta possui recursos de coletar a telemetria dos dispositivos mesmo que estes não tenham gerado nenhuma detecção. Os dados da telemetria contidos são muito mais abrangentes do que o pacote de rede. Tais dados incluem: Informações do host Mapeamento de conexões de rede, portas, origem, destino, executável, processo, linha de comando Conexões externas, por país, incluindo portas e número de conexões List of external network connections (by country, including the port and the # of connections) Endereços IP externos e internos Atividades de logon de usuário Quaiquer valores ou modificações relacionadas a inicialização do dispositivo (Registro do Windows, tarefas, pastas de inicialização) Executáveis escritos e executados DLL injections Execuções a partir de navegadores Web Histórico de comandos Execução de processos Histórico de comandos executados, parâmetros, usuário, data e hora Uso de ferramentas administrativas Scripts executados Atividades de DNS, resolução de nomes, processos Informações de rede de portas abertas (Network Listening) Arquivos e scripts escritos Uso de mídia removível Portanto, de acordo com a ampla coleta de dados de telemetria descritos, concluimos que o item é atendido de forma superior ao requisito. Está correto o nosso entendimento?
3.2.17.7. Deverá permitir modificar as regras por severidade de ocorrência de eventos;	Nosso entendimento para o referido item é que devem possuir mecanismos para identificar todos os dados de interesse relacionados a uma detecção. A solução proposta possui recursos de coletar a telemetria dos dispositivos mesmo que estes não tenham gerado nenhuma detecção. Os dados da telemetria contidos são muito mais abrangentes do que o pacote de rede. Tais dados incluem: Informações do host Mapeamento de conexões de rede, portas, origem, destino, executável, processo, linha de comando Conexões externas, por país, incluindo portas e número de conexões List of external network connections (by country, including the port and the # of connections) Endereços IP externos e internos Atividades de logon de usuário Quaiquer valores ou modificações relacionadas a inicialização do dispositivo (Registro do Windows, tarefas, pastas de inicialização) Executáveis escritos e executados DLL injections Execuções a partir de navegadores Web Histórico de comandos Execução de processos Histórico de comandos executados, parâmetros, usuário, data e hora Uso de ferramentas administrativas Scripts executados Atividades de DNS, resolução de nomes, processos Informações de rede de portas abertas (Network Listening) Arquivos e scripts escritos Uso de mídia removível Portanto, de acordo com a ampla coleta de dados de telemetria descritos, concluimos que o item é atendido de forma superior ao requisito. Está correto o nosso entendimento?
3.2.17.8. Deverá suportar sintaxe OSSEC padrão aberto;	Nosso entendimento para o referido item é que devem possuir mecanismos para identificar todos os dados de interesse relacionados a uma detecção. A solução proposta possui recursos de coletar a telemetria dos dispositivos mesmo que estes não tenham gerado nenhuma detecção. Os dados da telemetria contidos são muito mais abrangentes do que o pacote de rede. Tais dados incluem: Informações do host Mapeamento de conexões de rede, portas, origem, destino, executável, processo, linha de comando Conexões externas, por país, incluindo portas e número de conexões List of external network connections (by country, including the port and the # of connections) Endereços IP externos e internos Atividades de logon de usuário

	Quaiquer valores ou modificações relacionadas a inicialização do dispositivo (Registro do Windows, tarefas, pastas de inicialização) Executáveis escritos e executados DLL injections Execuções a partir de navegadores Web Histórico de comandos Execução de processos Histórico de comandos executados, parâmetros, usuário, data e hora Uso de ferramentas administrativas Scripts executados Atividades de DNS, resolução de nomes, processos Informações de rede de portas abertas (Network Listening) Arquivos e scripts escritos Uso de mídia removível Portanto, de acordo com a ampla coleta de dados de telemetria descritos, concluimos que o item é atendido de forma superior ao requisito. Está correto o nosso entendimento?
3.2.18.2.1. Bloqueio: possibilitando o bloqueio de aplicações, impedindo a execução de todos os softwares novos ou alterados, a menos que sejam expressamente permitidos;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.3. Deverá possuir lista de permissões de inventário, ou seja, ao ativar o controle de aplicações, todos os softwares atualmente instalados devem ser adicionados à lista de permissões do inventário do servidor e pode ser executado;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?

3.2.18.4. Deve ser possível configurar modo de manutenção possibilitando instalar ou atualizar a lista de softwares permitidos na lista de inventário;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.5. Deverá monitorar continuamente o servidor quanto as alterações. Devendo ser integrado ao kernel e ao sistema de arquivos, monitorando todo o servidor, incluindo o software instalado pelas contas root e de administrador.	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.6. Deverá detectar novos softwares, comparando hash, tamanho do arquivo, nome do arquivo e pasta;	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais

	robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.7.1. Aplicações Windows (.exe, .com, .dll, .sys), bibliotecas Linux (.so) e outros binários e bibliotecas compilados	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.7.2. Arquivos Java .jar e .class e outro código de bytes compilado	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.7.3. Scripts PHP, Python e shell, além de outros aplicativos e scripts da web que são	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada:

interpretados ou compilados em tempo real	AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.7.4. Scripts do Windows PowerShell, batch (.bat) e outros scripts específicos do Windows (.wsf, .vbs, .js)	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.18.8. Deverá exibir todos os softwares não reconhecidos, ou seja, softwares que não estão na lista de permissões de inventário de um servidor e não possuem uma regra de controle de aplicação correspondente, possibilitando tomar a ação de "Permitir" ou "Bloquear".	O componente de controle de aplicação já está disponível no Sistema Operacional portanto, acaba sendo redundante. Ainda que torna a execução da solução endpoint detection response mais onerosa em termos de desempenho. Esse recurso pode ser encontrado por diferentes versões do Sistema Operacional Windows e pode ter diferentes nomes dependendo da versão instalada: AppLocker: Disponível nas versões empresariais do Windows, como o Windows 10 Enterprise e o Windows Server, o AppLocker permite que os administradores restrinjam quais aplicativos podem ser executados em um sistema com base em regras predefinidas. As regras podem ser definidas para permitir ou bloquear aplicativos com base em caminhos de arquivo, assinaturas digitais, editoras e outros critérios. Software Restriction Policies (SRP): Nas versões mais antigas do Windows, como o Windows 7 e o Windows Server 2008, o recurso de Políticas de Restrição de Software oferece funcionalidade semelhante ao AppLocker. Ele permite que os administradores criem políticas para controlar quais aplicativos podem ser executados com base em caminhos de arquivo, hashes (resumos criptográficos) e zonas da Internet. Windows Defender Application Control (WDAC):Essa é uma solução mais avançada e abrangente para controle de aplicativos. Ela oferece recursos de segurança mais robustos para empresas, permitindo a criação de políticas de restrição com base em informações sobre o aplicativo, como identificadores de pacote e níveis de integridade. O WDAC pode ser usado para implementar medidas de segurança ainda mais rigorosas para proteger contra ameaças avançadas. A solução proposta possui recursos para automatizar a ativação e configuração do recurso no Windows. Dessa forma entendemos que o recurso pode ser utilizado

	para implementar controle de aplicação com um componente já presente no Sistema Operacional. Está correto o nosso entendimento?
3.2.19.7. Deverá suportar o envio ao menos nos seguintes formatos: Raw Syslog, CEF e LEEF;	Entendemos que o objetivo do item é garantir padronização e flexibilidade na gestão de informações e troca de dados no ambiente.A solução proposta funciona com o conceito de envio de logs de acordo com o padrão Syslog, amplamente difuldido entre as soluções de segurança. Sendo assim assegurando que os objetivos estejam atendidos. Está correto o nosso entendimento?
3.2.19.13. A console deverá ter a capacidade de se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução, com permissões customizadas pela própria solução;	Pela natureza da solução, são empregados conceitos de confiança zero (zero trust). Cerca de 80% dos ataques em 2023 utilizaram credenciais válidas e a maior superfície é liderada pelo Active Directory. Dessa forma a solução poderia ser comprometida facilmente nesses ataques utilizando credenciais válidas. A solução proposta possui capacidade de gerenciar os usuários em base própria, com recursos de de permissionamento granular baseados em RBAC (Role Based Access Control). A solução ainda conta com proteção extra, baseada em autenticação MFA. O que reduz em 99% o risco de acessos indevidos a console de administração. Adicionalmente a solução possui recursos de integração via SSO (Single SignOn) para as principais soluções avançadas de identidade em nuvem, como o Azure AD. Dessa forma acreditamos que o requisito é superado e atendido de forma superior. Está correto o nosso entendimento?
3.2.19.14.1. PostgreSQL	Nosso entendimento é que o requisito tem como objetivo garantir que os dados de políticas e logs estejam devidamente protegidos, atendendo aos princípios de Confidencialidade, Integridade e Disponibilidade. A solução proposta é toda baseada em nuvem, não sendo necessário nenhum componente on-premise. E garante que os princípios de segurança da informação são atendidos. Está correto o nosso entendimento?
3.2.19.14.2. Microsoft SQL Server	Nosso entendimento é que o requisito tem como objetivo garantir que os dados de políticas e logs estejam devidamente protegidos, atendendo aos princípios de Confidencialidade, Integridade e Disponibilidade. A solução proposta é toda baseada em nuvem, não sendo necessário nenhum componente on-premise. E garante que os princípios de segurança da informação são atendidos. Está correto o nosso entendimento?
3.2.19.14.3. Oracle database.	Nosso entendimento é que o requisito tem como objetivo garantir que os dados de políticas e logs estejam devidamente protegidos, atendendo aos princípios de Confidencialidade, Integridade e Disponibilidade. A solução proposta é toda baseada em nuvem, não sendo necessário nenhum componente on-premise. E garante que os princípios de segurança da informação são atendidos. Está correto o nosso entendimento?
3.2.19.20. Deverá permitir o envio de eventos da console via SNMP;	Entendemos que o requisito tem como objetivo garantir que os mecanismos de notificação sejam atendidos. Como a solução é toda baseada em nuvem e não possui requisitos de nenhum componente instalado no ambiente on-premise, a solução proposta possui mecanismos adicionais de notificação, como email, mensagem no Teams ou Slack ou até mesmo via Webhook. Com base no breve contexto e recursos de notificação e sem a necessidade de componentes no ambiente on-premise, acreditamos que o requisito é atendido de forma superior ao solicitado. Está correto o nosso entendimento?
3.6.13.9. A solução deve ser compatível com os sistemas operacionais Windows (versão 8.1 e superiores), Linux (Debian 6 e superiores, Fedora 12 e superiores) e MacOS (Mac OS X 10.13 e superiores);	O uso de sistemas operacionais legados trazem riscos extremamente críticos a operação, sendo um dos maiores vetores de ataque. O fabricante Microsoft não desenvolve ou mantém correções de vulnerabilidades críticas para estes sistemas operacionais, tornando-os alvos fáceis em ataques cibernéticos bastante simplificados. O risco de manter esses sistemas operacionais é bem crítico e soluções que alegam proteção para estes são questionáveis. Os fabricantes de solução de segurança que mantém soluções compatíveis com este legado são sempre baseadas em hashes e assinaturas. Atualmente 71% dos ataques não utilizam nenhum malware.

	Outro fator que a migração do Windows 8.1 para Windows 10 é relativamente simples e rápido. Portanto, a efetividade em proteger esses dispositivos legados dessas soluções é extremamente baixa. Nosso entendimento é que a solução deve proteger os dispositivos minimamente suportados pelos respectivos fabricantes. A solução proposta possui a suportabilidade alinhada com o suporte dos respectivos fabricantes. Está correto o nosso entendimento?
3.6.13.14. A solução deve utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;	O fabricante da solução proposta é líder em Inteligência contra ameaças, reconhecido pelo Gartner e Forrester, e possui seu próprio segmento no tema. Não depende de soluções de terceiros para gerar relatórios avançados e informações pertinentes. Entendemos que pela característica completa da solução no tema e não possuir quaisquer dependências para gerar relatórios de inteligência, o requisito é atendido. Está correto o nosso entendimento?
3.6.13.18. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;	A solução proposta possui sua própria linguagem e sintaxe de pesquisa para investigação e atividades de caça ameaças (Threat Hunting). Nosso entendimento que o requisito a linguagem Kibana (muito utilizado na solução de busca do fabricante Trend Micro) seja apenas uma referência para que a solução proposta possua capacidades de busca e pesquisa equivalentes. Está correto o nosso entedimento?
3.6.13.33. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;	Entendemos que tal requisito esteja relacionado para garantir rastreabilidade de logs e ações executadas por um administrador na solução.A solução proposta possui os mecanismos necessários para preservar a rastreabilidade de logs e ações mesmo que um usuário tenha sido excluído da console. Portanto, concluímos que a solução pode excluir os usuários ou resetar a senha para desativar o acesso do administrador, sem prejuízos ou perdas na administração. Está correto o nosso entendimento?

Sendo assim gostaríamos de saber se das formas descritas há o entendimento de que os itens seriam atendidos

Solicitamos que as respostas sejam fornecidas por escrito e, se possível, dentro do prazo estipulado no edital para questionamentos, a fim de garantir que possamos tomar as medidas
necessárias antes do prazo final de entrega de propostas, conforme estabelecido no cronograma do edital.

Agradecemos antecipadamente pela atenção dispensada a esta solicitação e pela colaboração na transparência e lisura deste processo licitatório.

Permanecemos à disposição para quaisquer esclarecimentos adicionais que possam se fazer necessários.

Atenciosamente,