



MATRIZ DE COMPATIBILIDADE

1.1. DOS REQUISITOS TÉCNICOS

1.1.1. DOS REQUISITOS TÉCNICOS PARA O ITEM 1 E O ITEM 2:

1.1.1.1. **Características gerais da solução de segurança:**

1.1.1.1.1. Proteção em tempo real contra vírus, *trojans*, *worms*, *cavalos-de-troia*, *spywares*, *ransomwares*, *adwares* e outros tipos de códigos maliciosos;

https://help.eset.com/ees/8/pt-BR/?idh_config_scanner.html

https://help.eset.com/glossary/pt-BR/?trojan_horses.html

<https://help.eset.com/glossary/pt-BR/?spyware.html>

https://help.eset.com/glossary/pt-BR/unsafe_application.html?zoom_highlightsub=keyloggers

https://help.eset.com/glossary/pt-BR/?technology_ams.html

https://help.eset.com/glossary/pt-BR/?worm_attacks.html

<https://help.eset.com/glossary/en-US/email.html?adware.html>

<https://help.eset.com/glossary/en-US/email.html?rootkits.html>

<https://help.eset.com/glossary/en-US/email.html?ransomware.html>

<https://help.eset.com/glossary/en-US/email.html?spyware.html>

<https://help.eset.com/glossary/en-US/email.html?viruses.html>

<https://help.eset.com/glossary/en-US/email.html?phishing.html>

1.1.1.1.2. Proteção *anti-spyware* nativa do antivírus, não dependente de plugin ou módulo adicional;

https://help.eset.com/ees/8/pt-BR/index.html?zoom_highlightsub=spyware

1.1.1.1.3. Permitir a configuração de diferentes ações executadas automaticamente para cada ameaça, com as opções de, no mínimo: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;

https://help.eset.com/ees/8/pt-BR/idh_config_threat_sense.html?idh_scan_target.html

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_quarantine_management.html

https://help.eset.com/ees/8/pt-BR/idh_config_threat_sense.html?idh_config_scan.html

https://help.eset.com/ees/8/pt-BR/idh_config_threat_sense.html?idh_profile_target.html

1.1.1.1.4. Permitir verificação das ameaças da maneira manual, agendada e em tempo real, detectando ameaças no nível do kernel do sistema operacional, fornecendo a possibilidade de detecção de *rootkits*;

<https://help.eset.com/glossary/en-US/email.html?rootkits.html>

https://help.eset.com/ees/8/pt-BR/index.html?idh_scan_clean.html

https://help.eset.com/ees/8/pt-BR/index.html?idh_scan_target.html

- 1.1.1.1.5. Capacidade de identificação da origem da infecção, para *malwares* que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou IP da origem com opção de bloqueio da comunicação via rede;

https://help.eset.com/ees/8/pt-BR/index.html?idh_scan_clean.html

https://help.eset.com/protect_admin/81/pt-BR/?threats.html

- 1.1.1.1.6. Antivírus de Web (módulo para verificação de sites e *downloads* contra vírus).

https://help.eset.com/ees/8/pt-BR/idh_page_settings_antivirus.html?idh_config_web.html

- 1.1.1.1.7. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

https://help.eset.com/ees/8/pt-BR/idh_config_epfw_advanced_settings.html?zoom_highlightsub=vulnerabilidades

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?zoom_highlightsub=exploit

- 1.1.1.1.8. Na verificação de tráfego *web*, caso encontrado código malicioso o programa deve:

- 1.1.1.1.8.1. Perguntar o que fazer, ou;
- 1.1.1.1.8.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- 1.1.1.1.8.3. Permitir acesso ao objeto.

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_config_web.html

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_config_web_basic.html

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_config_epfw_scan_http_address_list.html

- 1.1.1.1.9. O antivírus de *web* deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

- 1.1.1.1.9.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo real, ou;

1.1.1.1.9.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação.

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_config_web.html

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_config_shared_cache.html

1.1.1.1.10. Possibilidade de adicionar *sites* da *web* em uma lista de exclusão, onde não serão verificados pelo antivírus de *web*.

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_config_epfw_url_set_manager.html

1.1.1.1.11. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

<https://help.eset.com/eei/1.6/en-US/?alarms.html>

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_page_update.html

1.1.1.1.12. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

<https://support.eset.com/pt/melhores-praticas-para-se-proteger-contr-o-malware-filecoder-ransomware>

https://help.eset.com/ees/7/en-US/idh_config_dmon.html

1.1.1.1.13. Deve possuir módulo de bloqueio de *phishing*, com atualizações incluídas nas vacinas;

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_config_antiphish.html

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?idh_page_settings_antivirus.html

1.1.1.1.14. Deve possuir proteção contra vulnerabilidades desconhecidas, tais como estouro de *buffer* (*buffer overflow*);

https://help.eset.com/glossary/pt-BR/technology_ams.html

1.1.1.1.15. Capacidade de implementar varreduras otimizadas em máquinas

físicas e virtuais, onde o arquivo verificado pela varredura uma vez não será verificado novamente, até que ocorra alguma alteração nesse;

https://help.eset.com/ees/8/pt-BR/idth_hips_main.html?work_avas_ondemand_profiles.html

1.1.1.1.16. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados;

https://help.eset.com/efsw/6.2/en-US/index.html?idh_config_threat_sense.htm

1.1.1.1.17. Capacidade de remoção dos danos causados por *spyware*, *adwares* e *worms*, como limpeza do registro e pontos de carregamento;

https://help.eset.com/eea/7/pt-BR/?idh_scan_clean.html

https://help.eset.com/ees/7/en-US/idth_config_interactive_alert.html

1.1.1.1.18. Capacidade de executar varreduras em tempo real contra-ataques dirigidos a vulnerabilidades do navegador

https://help.eset.com/ees/8/pt-BR/idth_config_threat_sense.html?idh_config_amon.html

https://help.eset.com/ees/8/pt-BR/idth_config_threat_sense.html?idh_config_scanner.html

https://help.eset.com/ees/8/pt-BR/idth_config_web_basic.html

https://help.eset.com/eei/1.6/en-US/process_scripts.html

1.1.1.1.19. Reputação de arquivos – verificar a reputação de arquivo através de pesquisa em base de dados do fabricante em nuvem;

https://help.eset.com/ees/8/pt-BR/idth_config_charon.html?zoom_highlightsub=live+grid

1.1.1.1.20. Reputação *WEB* – rastrear a credibilidade de domínios, atribuindo uma classificação com base em fatores de reputação, como o tempo de existência do *site* etc;

https://help.eset.com/ees/8/pt-BR/?idh_config_web.html

https://help.eset.com/ees/8/pt-BR/?idh_config_web_basic.html

1.1.1.1.21. Bloqueio de URLs de má reputação;

1.1.1.1.22. tempo de existência do *site* etc;

https://help.eset.com/ees/8/pt-BR/?idh_config_web.html

https://help.eset.com/ees/8/pt-BR/?idh_config_web_basic.html

1.1.1.1.23. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em base local ou na nuvem da reputação das URLs acessadas;

https://help.eset.com/ees/8/pt-BR/?idh_config_epfw_url_set_manager.html

1.1.1.1.24. Deve permitir a criação de listas de exclusão, permitindo que os *hots* acessem determinadas *URLs* especificadas pelo administrador do sistema;

https://help.eset.com/ees/8/pt-BR/?idh_config_epfw_url_set_manager.html

1.1.1.1.25. Proteção de navegadores (*Browser Protection*);

https://help.eset.com/ees/8/pt-BR/idh_config_sb.html?zoom_highlightsub=navegador

1.1.1.1.26. Controle de Aplicações em ambiente Windows (*Application Control*);

https://help.eset.com/ees/8/pt-BR/idh_config_epfw_ssl_app.html

1.1.1.1.27. Proteção avançada contra *ransomware*, com capacidade de reverter o incidente;

https://help.eset.com/glossary/pt-BR/technology_ransomware_protection.html

https://help.eset.com/protect_admin/81/pt-BR/?ransomware_shield.html

1.1.1.1.28. Solução que simule o ambiente real do Tribunal, criando armadilhas para permitir que o malware execute ações em um ambiente totalmente isolado e seja bloqueado antes de atingir qualquer computador;

<https://help.eset.com/eei/1.6/en-US/?incidents.html>

https://help.eset.com/eei/1.6/en-US/?computer_details.html

1.1.1.1.29. Mitigação de exploração de vulnerabilidades em aplicações conhecidas;

https://help.eset.com/ees/8/pt-BR/idh_config_epfw_advanced_settings.html?zoom_highlightsub=vulnerabilidades

https://help.eset.com/ees/8/pt-BR/idh_hips_main.html?zoom_highlightsub=exploit

1.1.1.1.30. Bloqueio de ameaças polimorficas;

<https://help.eset.com/edtd/pt-BR/?overview.html>

<https://help.eset.com/eei/1.6/en-US/?index.html>

1.1.1.1.31. Bloqueio de ataques “zero-day”;

<https://help.eset.com/edtd/pt-BR/?overview.html>

1.1.1.1.32. Impedir técnicas de manipulação de memória (*Memory Exploit Mitigation*);

https://help.eset.com/ees/8/pt-BR/idh_config_threat_sense.html?zoom_highlightsub=memoria

<https://help.eset.com/eei/1.6/en-US/?index.html>

1.1.1.1.33. Impedir ataques direcionados, mesmo que utilizando vulnerabilidades de dia zero;

<https://help.eset.com/edtd/pt-BR/?overview.html>

<https://help.eset.com/eei/1.6/en-US/?index.html>

1.1.1.1.34. O *software* de proteção do *endpoint* deve ter a capacidade de bloquear *exploits* que trabalham com “shellcode”;

https://help.eset.com/eei/1.6/en-US/process_scripts.html

1.1.1.1.35. Deve ter administração centralizada por console único de gerenciamento (tanto para estações de trabalho quanto para os servidores);

https://help.eset.com/protect_admin/81/pt-BR/

1.1.1.1.36. Deve ter acesso a console de gerenciamento via HTTP e HTTPS;

https://help.eset.com/protect_install/81/pt-BR/?arch_webconsole.html

1.1.1.1.37. Deve executar, na instalação do cliente, varredura em relação à existência de outros antivírus;

https://help.eset.com/ees/8/pt-BR/idh_config_shellex.html?idh_config_startup_scan.html

1.1.1.1.38. Deve desinstalar soluções de antivírus de outros fabricantes, na instalação do cliente;

https://help.eset.com/ees/7/pt-BR/idh_bts_installer.html?idh_bts_avremover.html

1.1.1.1.39. Deve avisar aos administradores, via e-mail, sobre infecções por *malwares*;

https://help.eset.com/protect_admin/81/pt-BR/?admin_ntf_notifications.html

1.1.1.1.40. Permitir a criação de relatórios, sob demanda, ou agendados;

https://help.eset.com/protect_admin/81/pt-BR/?create_a_new_report_template.html

https://help.eset.com/protect_admin/81/pt-BR/?schedule_a_report.html

1.1.1.1.41. Permitir mecanismos para minimizar impacto na rede durante o processo de instalação em clientes;

https://help.eset.com/protect_admin/81/pt-BR/?fs_agent_deploy_remote.html

https://help.eset.com/protect_admin/81/pt-BR/?fs_local_deployment.html

1.1.1.1.42. A solução deverá possuir indicadores para medir a eficácia da solução, como, por exemplo, a quantidade de ameaças bloqueadas com sucesso, computadores e/ou usuários envolvidos etc;

https://help.eset.com/protect_admin/81/pt-BR/?threats.html

1.1.1.1.43. As configurações de todos os módulos da solução deverão ser realizadas através da mesma console, exceto as configurações e própria operação do EDR, que poderá ser feita por console específica;

<https://help.eset.com/eei/1.6/en-US/>

https://help.eset.com/eei/1.6/en-US/?working_with_eei.html

1.1.1.1.44. Mecanismo de comunicação em tempo real entre servidor e clientes, para entregar configurações e assinaturas;

https://help.eset.com/protect_install/81/pt-BR/?arch_agent.html

1.1.1.1.45. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, criar grupos de forma manual e grupos do *active directory* com administração individualizada por máquina ou grupo.

https://help.eset.com/protect_admin/81/pt-BR/?fs_using_ad_sync.html

https://help.eset.com/protect_admin/81/pt-BR/?admin_groups.html

1.1.1.1.46. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais *Microsoft Windows Server 2012 R2* e superiores ou *Ubuntu Server 18.04* e superiores;

https://help.eset.com/protect_install/81/pt-BR/?windows.html

https://help.eset.com/protect_install/81/pt-BR/?linux.html

1.1.1.1.47. Caso o servidor de gerenciamento seja *appliance*, será aceita apenas a modalidade virtual e deverá ser instalado em:

1.1.1.1.47.1. PROXMOX/KVM;

1.1.1.1.47.2. Ambiente VMware, desde que a contratada implante todo o ambiente necessário para a execução, que deverá contemplar, no mínimo:

1.1.1.1.47.2.1. Servidor de, no máximo 2U, a ser instalado no rack do

TCDF, com especificações necessárias para a correta execução da aplicação;

1.1.1.1.47.2.2. Licenciamento completo para execução do VMware e do *appliance* de gerenciamento, incluindo sistema operacional e demais *softwares* ou *hardwares* necessários.

https://help.eset.com/protect_deploy_va/81/pt-BR/

https://help.eset.com/protect_deploy_va/81/pt-BR/?prerequisites.html

https://help.eset.com/protect_deploy_va/81/pt-BR/?supported_hypervisors.html

1.1.1.1.48. Será aceita console de gerenciamento na nuvem.

https://help.eset.com/protect_admin/81/pt-BR/

1.1.1.1.49. O servidor de gerenciamento deverá ser instalado em sistema operacional 64 bits;

https://help.eset.com/protect_install/81/pt-BR/?windows.html

https://help.eset.com/protect_install/81/pt-BR/?linux.html

1.1.1.1.50. Possuir integração com LDAP ou *Active Directory*, para importação das estruturas organizacionais e autenticação dos Administradores;

https://help.eset.com/protect_admin/81/pt-BR/?fs_using_ad_sync.html

1.1.1.1.51. Possibilidade de aplicar regras diferenciadas, baseado na estrutura lógica da rede;

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol_assign_policy_to_group.html

1.1.1.1.52. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol_assign_policy_to_group.html

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol_assign_policy_to_client.html

1.1.1.1.53. O servidor de gerenciamento deverá permitir o uso do banco de dados Microsoft SQL Server na versão 2014 ou superior;

https://help.eset.com/protect_install/81/pt-BR/?database_requirements.html

1.1.1.1.54. Possuir a funcionalidade e recursos para criação e agendamento periódicos de backups da base de dados ou fornecer ferramenta para tal finalidade;

https://help.eset.com/protect_install/81/pt-BR/?db_migration.html

1.1.1.1.55. Permitir a instalação de servidores de gerenciamento adicionais

https://help.eset.com/protect_install/81/pt-BR/?arch_proxy.html

https://help.eset.com/protect_install/81/pt-BR/?apache_http_proxy.html

1.1.1.1.56. Possibilidade de instalação dos clientes em estações de trabalho de forma remota, via console de gerenciamento, com opção de remoção de soluções previamente instaladas;

https://help.eset.com/protect_admin/81/pt-BR/?fs_agent_deploy_remote.html

https://help.eset.com/ees/7/pt-BR/idh_bts_installer.html?idh_bts_avremover.html

1.1.1.1.57. Permitir a instalação remota do *software* por *Group Policy* (GPO);

https://help.eset.com/protect_admin/81/pt-BR/?fs_agent_deploy_gpo_sccm.html

1.1.1.1.58. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;

https://help.eset.com/protect_admin/81/pt-BR/?fs_using_rd_sensor.html

1.1.1.1.59. Fornecer atualizações do produto e das definições de *malware*;

https://help.eset.com/protect_admin/81/pt-BR/client_tasks_virus_db_update.html

1.1.1.1.60. A console de gerenciamento deve permitir travar as configurações nos clientes, definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;

https://help.eset.com/protect_admin/81/pt-BR/client_tasks_virus_db_update.html?fs_agent_deploy_password_protection.html

1.1.1.1.61. Permitir a criação de múltiplos perfis de segurança vinculados aos diferentes tipos de servidores do ambiente;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html

1.1.1.1.62. Permitir o envio de notificações via SMTP;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?admin_ntf_notifications.html

1.1.1.1.63. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html

1.1.1.1.64. A solução deverá possuir, no mínimo para ambiente Windows, gerenciamento de patches e vulnerabilidades:

1.1.1.1.64.1. *Scanning* automático de vulnerabilidades em sistemas operacionais e aplicações instaladas;

1.1.1.1.64.2. Remediação de vulnerabilidades aplicando patches, de forma remota, via console de gerenciamento.

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?client_tasks_system_update.html

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?client_tasks_software_install.html

1.1.1.1.65. Instalação e atualização do *software* sem a intervenção do usuário;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?client_tasks_software_install.html

1.1.1.1.66. Suportar redirecionamentos dos *logs* para um servidor de *log*;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?client_tasks_diagnostics.html

https://help.eset.com/eei/1.6/en-US/?computer_events.html

1.1.1.1.67. Utilizar comunicação segura entre cliente e servidor;

https://help.eset.com/protect_install/81/pt-BR/?arch_agent.html

https://help.eset.com/protect_install/81/pt-BR/arch_proxy.html#protocol

https://help.eset.com/protect_install/81/pt-BR/arch_proxy.html?network_requirements.html

https://help.eset.com/protect_install/81/pt-BR/arch_proxy.html?ports_used.html

1.1.1.1.68. Atualização incremental, remota e em tempo real das vacinas da solução;

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_virus_db_update.html

1.1.1.1.69. Permitir criar planos de distribuição das atualizações, via comunicação segura, entre cliente e servidor de gerenciamento;

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_virus_db_update.html

https://help.eset.com/protect_install/81/pt-BR/?arch_proxy.html

<https://support.eset.com/en/kb7854-configure-an-eset-endpoint-product-to-function-as-a-mirror-server-8x>

1.1.1.1.70. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das vacinas, podendo eleger mais de um cliente para esta função;

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_virus_db_update.html

https://help.eset.com/protect_install/81/pt-BR/?arch_proxy.html

<https://support.eset.com/en/kb7854-configure-an-eset-endpoint-product-to-function-as-a-mirror-server-8x>

1.1.1.1.71. As atualizações das configurações e das definições de vírus não poderão utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e deverá ser feito sem requerer reinicialização do computador ou serviço para aplicá-la;

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_virus_db_update.html

https://help.eset.com/protect_install/81/pt-BR/?arch_proxy.html

<https://support.eset.com/en/kb7854-configure-an-eset-endpoint-product-to-function-as-a-mirror-server-8x>

1.1.1.1.72. Capacidade de voltar, pelo menos, uma vacina e assinatura anteriormente armazenadas no servidor, utilizando opção e comando da console.

https://help.eset.com/ees/8/pt-BR/idh_config_update_rollback.html

1.1.1.1.73. Possuir funcionalidades que possibilitem, quando na detecção de um objeto potencialmente perigoso:

1.1.1.1.73.1. Perguntar o que fazer, ou.

1.1.1.1.73.2. Bloquear acesso ao objeto;

1.1.1.1.73.3. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador).

1.1.1.1.73.4. Caso positivo de desinfecção: restaurar o objeto para uso.

1.1.1.1.73.5. Caso negativo de desinfecção: mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

https://help.eset.com/ees/8/pt-BR/idh_config_update_rollback.html?idh_scan_clean.html

1.1.1.1.74. Recursos de relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?reports.html

1.1.1.1.75. Capacidade de Geração de relatórios estatísticos e gráficos;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?reports.html

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?dashboard.html

1.1.1.1.76. Possibilidade de exibir a lista de estações que possuam o antivírus instalado, contendo informações, como nome da estação de trabalho, versão do antivírus, data das vacinas, data da última verificação;

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?computer_details.html

1.1.1.1.77. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

https://help.eset.com/eei/1.6/en-US/?computer_alerts.html

1.1.1.1.78. A solução deverá suportar análise de comportamento para a detecção avançada de ameaças;

<https://help.eset.com/eei/1.6/en-US/rules.html>

1.1.1.1.79. A solução deverá incluir técnicas de inteligência artificial baseada em *machine learning* para análise preditiva de ameaças;

https://help.eset.com/ees/8/pt-BR/idh_config_update_rollback.html?idh_config_scanner.html

1.1.1.1.80. Deve exibir todos ou os principais detalhes do incidente em uma única página (EDR), contendo no mínimo:

- 1.1.1.1.80.1. Status do incidente;
- 1.1.1.1.80.2. Escopo impactado;
- 1.1.1.1.80.3. Quantidade de estações de trabalho impactadas;
- 1.1.1.1.80.4. Quantidade de servidores impactados;
- 1.1.1.1.80.5. Quantidade de usuários impactados;
- 1.1.1.1.80.6. Data e hora da detecção;
- 1.1.1.1.80.7. Modelo(s) de detecção acionado(s).

<https://help.eset.com/eei/1.6/en-US/>

https://help.eset.com/eei/1.6/en-US/?dashboard_alarms.html

https://help.eset.com/eei/1.6/en-US/?dashboard_computers.html

1.1.1.1.81. A investigação deve permitir a análise do recebimento e execução de arquivos, processos e sessões de rede.

<https://help.eset.com/eei/1.6/en-US/?alarms.html>

1.1.1.1.82. A solução deve ter capacidade de apresentar a visibilidade completa do vetor de ataque, disseminação e extensão do impacto de ameaças avançadas;

<https://help.eset.com/eei/1.6/en-US/?alarms.html>

<https://help.eset.com/eei/1.6/en-US/?incidents.html>

1.1.1.1.83. Durante o processo de análise da cadeia de processos, deve ser possível verificar todos os objetos relacionados à esta análise, as atividades executadas pelos objetos e sua reputação conforme categorização do fabricante;

<https://help.eset.com/eei/1.6/en-US/?dashboard.html>

https://help.eset.com/eei/1.6/en-US/?dashboard_alarms.html

1.1.1.1.84. Após o vencimento das licenças, mesmo que sem atualizações, a solução deverá continuar funcionando.

https://help.eset.com/protect_admin/81/pt-BR/admin_access_rights.html?eula.html

1.1.2. DOS REQUISITOS TÉCNICOS PARA O ITEM 1

1.1.2.1. Características específicas para estações de trabalho:

1.1.2.1.1. Licenciamento para 1.032 (mil e trinta e duas) estações de trabalho;

https://help.eset.com/protect_install/81/pt-BR/?hw_requirements.html

1.1.2.1.2. Deverá ser compatível com as seguintes versões de sistemas operacionais (64 bits):

1.1.2.1.2.1. Windows 10 e superiores;

1.1.2.1.2.2. MacOS Big Sur e superiores.

<https://help.eset.com/ees/8/pt-BR/?sysreq.html>

https://help.eset.com/ees_mac/6.10/pt-BR/?ud_ena_intro_requirements.html

1.1.2.1.3. Possibilitar a criação de uma mídia (pendrive, CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;

https://help.eset.com/protect_install/81/pt-BR/iso_image.html?zoom_highlightsub=imagem

1.1.2.1.4. Possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo para ambiente Windows:

- 1.1.2.1.4.1. Discos de armazenamento locais.
- 1.1.2.1.4.2. Armazenamento removível;
- 1.1.2.1.4.3. CD/DVD;
- 1.1.2.1.4.4. Dispositivos multifuncionais;
- 1.1.2.1.4.5. Wi-Fi;
- 1.1.2.1.4.6. Adaptadores de rede;
- 1.1.2.1.4.7. Dispositivos MP3 ou smartphones;
- 1.1.2.1.4.8. Dispositivos *bluetooth*.

https://help.eset.com/ees/8/pt-BR/?idh_config_devmon.html

1.1.2.1.5. Limitar a escrita e leitura, no mínimo para ambiente Windows, em dispositivos de armazenamento externo por usuário ou dispositivo específico;

https://help.eset.com/ees/8/pt-BR/?idh_config_devmon_rule_dlg.html

1.1.2.1.6. Limitar a execução, no mínimo para ambiente Windows, de aplicativos por *hash*, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de *download*, jogos, aplicação de acesso remoto, etc);

https://help.eset.com/ees/8/pt-BR/idh_hips_editor_single_rule.html

1.1.2.1.7. Bloquear execução, no mínimo para ambiente Windows, de aplicativo que está em armazenamento externo;

https://help.eset.com/ees/8/pt-BR/idh_hips_editor_single_rule.html

https://help.eset.com/ees/8/pt-BR/idh_hips_editor_single_rule.html?idh_config_devmon_rule_edit_dlg.html

1.1.2.1.8. Limitar, no mínimo para ambiente Windows, o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

https://help.eset.com/ees/8/pt-BR/idh_hips_editor_single_rule.html

1.1.2.1.9. Possibilitar que, caso o computador cliente saia da rede corporativa, seja ativada política alternativa na qual a estação de trabalho possa ser atualizar diretamente no site do fabricante.

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_virus_db_update.html

https://help.eset.com/protect_install/81/pt-BR/?arch_proxy.html

<https://support.eset.com/en/kb7854-configure-an-eset-endpoint-product-to-function-as-a-mirror-server-8x>

1.1.3. DOS REQUISITOS TÉCNICOS PARA O ITEM 2

1.1.3.1. Características específicas para servidores:

1.1.3.1.1. Licenciamento para 173 (cento e setenta e três) servidores;

https://help.eset.com/protect_install/81/pt-BR/?hw_requirements.html

1.1.3.1.2. A solução deverá ser compatível e homologada, no mínimo, para os seguintes sistemas operacionais e versões (64 bits):

1.1.3.1.2.1. Ubuntu Server 14.04 e superiores;

1.1.3.1.2.2. Windows Server 2008 e superiores;

1.1.3.1.2.3. CentOS 6.6 e superiores.

https://help.eset.com/efs/8.1/en-US/?system_requirements.html

https://help.eset.com/efsw/8.0/pt-BR/system_requirements.html

1.1.3.1.3. A solução deve possuir funcionalidade de realizar verificações de **segurança** em ambientes virtualizados por KVM ou PROXMOX;

https://help.eset.com/efs/8.1/en-US/idh_config_shared_cache.html?system_requirements.html

1.1.3.1.4. A solução deverá ser compatível com máquinas físicas e virtuais.

https://help.eset.com/protect_install/81/pt-BR/?supported_desktop_provisioning_environments.html

https://help.eset.com/efs/8.1/en-US/?system_requirements.html

https://help.eset.com/efsw/8.0/pt-BR/system_requirements.html

1.1.3.1.5. A solução deve enviar, automaticamente, atualizações de vacinas, regras e políticas para todos os servidores;

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_virus_db_update.html

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol.html

1.1.3.1.6. Proteção de *hosts docker* e contêineres em ambiente Linux;

https://help.eset.com/efs/8.1/en-US/idh_config_shared_cache.html?system_requirements.html

1.1.3.1.7. A solução deverá permitir agrupar *hosts* gerenciados em pastas, possibilitando a aplicação de políticas diferenciadas para cada grupo;

https://help.eset.com/protect_admin/81/pt-BR/?admin_groups.html

1.1.3.1.8. A solução deverá efetuar a proteção contra códigos maliciosos por meio da instalação ou não de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

https://help.eset.com/efsw/8.0/pt-BR/idh_page_settings_antivirus.html

1.1.3.1.9. Deve ser capaz de executar rastreamento nos *hosts* e fornecer lista de recomendações de segurança para *softwares* que estiverem instalados, bem como para o sistema operacional;

https://help.eset.com/efsw/8.0/pt-BR/idh_page_scan.html

1.1.3.1.10. Permitir atuar no modo “em linha” para bloqueio de ataques ou modo “escuta” para monitoração e alertas;

https://help.eset.com/efsw/8.0/pt-BR/idh_page_settings_antivirus.html

<https://help.eset.com/eei/1.6/en-US/?hips.html>

<https://help.eset.com/eei/1.6/en-US/?antivirus.html>

1.1.3.1.11. Possuir a capacidade de varrer o servidor protegido, detectando o tipo e versão do sistema operacional e demais aplicações;

https://help.eset.com/efsw/8.0/pt-BR/idh_page_scan.html

https://help.eset.com/protect_admin/81/pt-BR/?hw_fingerprint.html

1.1.3.1.12. Possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

https://help.eset.com/efsw/8.0/pt-BR/idh_page_epfw_settings.html

1.1.3.1.13. Permitir que a opção de detecção e bloqueio seja implementada de forma global (todas as regras) ou apenas para uma regra ou grupos de regras;

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol_assign_policy_to_group.html

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol_assign_policy_to_client.html

1.1.3.1.14. Possuir a capacidade de criação de regras customizadas para proteger aplicações desenvolvidas pelo cliente;

<https://help.eset.com/eei/1.6/en-US/?exclusions.html>

1.1.3.1.15. Implementar a customização avançada e criação de novas regras de proteção de aplicações *web*, permitindo proteger contra vulnerabilidades específicas de sistemas *web* legados e/ou proprietários;

<https://help.eset.com/eei/1.6/en-US/?rule.html>

https://help.eset.com/efs/8.1/en-US/idh_config_shared_cache.html?idh_config_threat_sense.html

1.1.3.1.16. Apresentar informações detalhadas das regras de blindagem contra vulnerabilidades, contendo, quando possível, *links* com referências externas, explicando a vulnerabilidade;

<https://help.eset.com/eei/1.6/en-US/?alarms.html>

https://help.eset.com/efs/8.1/en-US/idh_config_shared_cache.html?idh_config_threat_sense.html

1.1.3.1.17. Bloquear tráfego por aplicação independentemente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede;

https://help.eset.com/eei/1.6/en-US/?blocked_executable.html

1.1.3.1.18. Permitir habilitar modo *debug* na coleta de pacotes de forma a capturar o tráfego para análise;

<https://help.eset.com/eei/1.6/en-US/?incidents.html>

https://help.eset.com/eei/1.6/en-US/?server_settings.html

1.1.3.1.19. Permitir que o administrador do sistema tenha a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo um grupo ou host;

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol_assign_policy_to_group.html

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol_assign_policy_to_client.html

1.1.3.1.20. Possuir a capacidade de detectar mudanças de integridade em arquivos e diretórios do sistema operacional;

https://help.eset.com/efsw/8.0/pt-BR/idh_config_amon.html

https://help.eset.com/efs/8.1/en-US/idh_config_shared_cache.html?idh_config_amon.html

1.1.3.1.21. Permitir a customização de regras existentes, adicionando, removendo ou modificando regras;

https://help.eset.com/protect_admin/81/pt-BR/?admin_pol.html

1.1.3.1.22. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

https://help.eset.com/protect_admin/81/pt-BR/?client_tasks_on_demand_scan.html

1.1.3.1.23. Possuir a capacidade de detectar mudanças no estado de portas em sistemas operacionais;

https://help.eset.com/efsw/8.0/pt-BR/idh_hips_main.html

<https://help.eset.com/eei/1.6/en-US/?hips.html>

1.1.3.1.24. Possuir a capacidade de monitorar o status de serviços e processos do sistema operacional;

<https://help.eset.com/eei/1.6/en-US/?executables.html>

1.1.3.1.25. Classificar regras de acordo com a severidade, para melhor verificação nos logs e alertas;

https://help.eset.com/eei/1.6/en-US/rules_sets.html?zoom_highlightsub=severity

1.1.3.1.26. Possibilitar a criação de listas de exclusão para processos, diretórios ou arquivos do sistema operacional;

<https://help.eset.com/eei/1.6/en-US/exclusions.html>

https://help.eset.com/efs/8.1/en-US/?idh_config_exclude.html

1.1.3.1.27. O controle de aplicações deverá ser realizado através de *hash*;

https://help.eset.com/efs/8.1/en-US/idh_config_processes_exclude.html

https://help.eset.com/efs/8.1/en-US/idh_config_processes_exclude.html?idh_config_charon.html

https://help.eset.com/efsw/8.0/pt-BR/idh_config_server_scanner.html

1.1.3.1.28. A solução deverá possuir funcionalidade de bloquear tudo o que não for permitido explicitamente e permitir tudo o que não for bloqueado explicitamente;



Av. Professor Mário Werneck, 280 – lj01, 30455-610 – Belo Horizonte/MG

licitacoes@brinfor.com.br

www.brinfor.com.br

(31) 3324 - 2900

https://help.eset.com/efsw/8.0/pt-BR/idh_config_server_autoexclude.html

<https://help.eset.com/eei/1.6/en-US/exclusions.html>