PROCESSAMENTO DE DADOS AMAZONAS S.A

RESPOSTA AO RECURSO ADMINISTRATIVO

Referência : Pregão Eletrônico SRP **nº 14/2022**

Assunto : RECURSO ADMINISTRATIVO

Objeto : Contratação de solução de cibersegurança, auditoria e prevenção de ameaças à base de dados não estruturados em endpoint, na modalidade de subscrição, incluindo garantia, serviço de instalação e treinamento, visando ampliar a capacidade de atendimento ao ambiente de desktops e servidores da Prodam e seus clientes em relação ao combate às ameaças cibernéticas, conforme especificações detalhadas no Termo de Referência, constante do Anexo I, do edital.

1 CONSIDERAÇÕES GERAIS

1.1 Trata-se de Recurso interposto pela empresa **DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA**., por meio de seu representante legal, com espeque no art. 4º, XVIII, da Lei n.º 10.520/02, subsidiada pela Lei n.º 13.303/16 em face de ato administrativo praticado pelo Pregoeiro no Edital de Licitação de **Pregão Eletrônico SRP n.º 014/2022**.

1.2 Razões e contrarrazões encontram-se disponíveis para consulta, **na íntegra**, no portal de compras do Governo Federal, site: www.gov.br/compras/pt-br e transparência da PRODAM, site https://www.prodam.am.gov.br/licitacoes/pregoes/

2 DA TEMPESTIVIDADE

2.1 No Pregão Eletrônico, a manifestação da intenção de recorrer deve ser apresentada em campo específico no sistema Comprasnet, sítio de compras do governo, que se oportuniza a partir da habilitação da última proposta ou o cancelamento dos itens, logo após se abrir o prazo para interposição de intenção recursos.

2.2 Desta feita, havendo registrada prévia e motivada intenção de recorrer, e, sendo-lhe aceita, inicia-se a contagem do prazo legal para apresentação das razões recursais, que são de 3 (três) dias úteis, sendo igual o prazo para apresentação das contrarrazões.

2.3 A intenção de recurso da empresa DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA foi aceita e esta apresentou TEMPESTIVAMENTE as razões recursais.

3 DO RECURSO

3.1 No mérito, a empresa **DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA** apresentou as seguintes alegações, **sucintamente** transcritos, visto que **a íntegra** está disponível no portal de compras do Governo Federal, site: www.gov.br/compras/pt-br e transparência da PRODAM, site https://www.prodam.am.gov.br/licitacoes/pregoes/

3.1.1 A exclusão da proposta da DFTI se deu por suposto não atendimento aos itens 13.2.7.23; 13.3.11.9; 13.3.11.15; 13.3.12.6.4; 13.3.12.6.5; 13.3.12.6.6; 13.3.12.6.7 e 13.3.12.6.10, referentes às exigências do Anexo 1-A – Tabela de Demonstração. Igualmente, em termos de habilitação, a sua documentação não estaria aderente à exigência constante no item 1.10.1 do ANEXO 2 - DOCUMENTOS PARA HABILITAÇÃO do edital, este abaixo transcrito: 1.10.1. Apresentar atestado (s) ou certidão (ões) de capacidade técnica-operacional emitidas por entidades públicas e/ou privadas indicando que a empresa já prestou serviço semelhante por um período mínimo de 12 (doze) meses e que forneceu no mínimo 10% das quantidades descritas para o item 1, da tabela do anexo1-B (modelo de proposta de preços).

3.1.2 Como restará demonstrado, tanto a solução ofertada quanto a capacidade técnico-operacional da DFTI atendem integralmente ao exigido, com a existência, no que tange aos elementos técnicos, inclusive de recursos adicionais aos requisitos mínimos obrigatórios.

3.1.3 Em complemento, para que reste transparente e indubitável a integralidade do atendimento dos itens que geraram EM PRINCÍPIO, a desclassificação da DFTI após análise da documentação enviada pela equipe técnica da PRODAM, corrobora-se além do detalhamento explícito na console e documentação já enviada, Declaração do Fabricante da solução ofertada SOPHOS, atestando em sua íntegra a conformidade ao exigido.

3.2 DO PEDIDO

3.2.1 Requer-se a revisão da decisão que excluiu a recorrente da disputa e a consequente aceitação da sua proposta, convocando-a para a realização da Prova de Conceito, conforme preconizado no Edital e seus anexos.

4 DA ANÁLISE

4.1 Imperioso ressaltar que todos os julgados da Administração Pública estão embasados nos princípios insculpidos no art. 31 da Lei 13.303/16, conforme segue:

> Art. 31. As licitações realizadas e os contratos celebrados por empresas públicas e sociedades de economia mista destinam-se a assegurar a seleção da proposta mais vantajosa, inclusive no que se refere ao ciclo de vida do objeto, e a evitar operações em que se caracterize sobrepreço ou superfaturamento, devendo observar **os princípios da impessoalidade, da moralidade, da igualdade, da publicidade, da eficiência, da probidade administrativa, da economicidade, do desenvolvimento nacional sustentável, da vinculação ao instrumento convocatório, da obtenção de competitividade e do julgamento objetivo.**

4.2 Ressalta-se que tal disposição é corroborada pelo disposto no Decreto n.º 10.024/2019:

> Art. 2º O pregão, na forma eletrônica, é condicionado aos **princípios da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da eficiência, da probidade administrativa, do desenvolvimento sustentável, da vinculação ao instrumento convocatório, do julgamento objetivo, da razoabilidade, da competitividade, da proporcionalidade e aos que lhes são correlatos.**

4.3 Dito isto, após apreciação dos fundamentos elencados no recurso interposto pela recorrente **DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA**., passamos a análise do mérito:

4.4 Os questionamentos levantados pela recorrente **DFTI** foram analisados pela equipe técnica da PRODAM quanto ao atendimento dos itens exigidos no edital e anexos, em conformidade ao **parágrafo único do item 8 do Edital** que trata da solicitação de manifestação técnica.

4.5 Considerando este contexto, a equipe técnica da PRODAM analisou minuciosamente a peça recursal e a comprovação documentais adicionais apresentada pela recorrente **DFTI** conforme parecer técnico anexo a este relatório e devidamente publicado no Portal de Transparência através do link: **https://www.prodam.am.gov.br/transparencia/**

4.6 Assim sendo, verificou-se que a recorrente **DFTI** não atende às exigências editalícias, visto que foram identificados **08 (oito) itens do edital** que permanecem sem evidências documentais suficientes para comprovar que a solução ofertada pela empresa atende a tais requisitos exigidos no instrumento convocatório.

5 DA DECISÃO

Isto posto, sem mais nada a considerar, respeitados os princípios constitucionais do contraditório, da ampla defesa e do devido processo legal, CONHEÇO das razões ao recurso por tempestivo, para, NO MÉRITO**, NEGAR-LHE PROVIMENTO**, mantendo assim inalterada a decisão anterior que desclassificou a empresa DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA.

Mantendo a decisão, encaminho a presente manifestação à autoridade competente para deliberação, nos termos da legislação de regência.

Manaus AM, 27 de fevereiro de 2023.

Atenciosamente,

CLEANE VIDAL TEIXEIRA
Assinado de forma digital por CLEANE VIDAL TEIXEIRA
Dados: 2023.02.28 08:29:04 -04'00'

Cleane Vidal Teixeira
Pregoeira

DE ACORDO:

LINCOLN NUNES DA SILVA
Diretor-Presidente

Nível de Classificação	Grupo de acesso
Público	**Público**

PARECER TÉCNICO

Após conclusão da sessão pública realizada no dia 17/01/2023 que tratou do **Pregão Eletrônico de Nº 14/2022** cujo objeto é a contratação de solução de cibersegurança, auditoria e prevenção de ameaças à base de dados não estruturados em endpoint, na modalidade de subscrição, incluindo garantia, serviço de instalação e treinamento, foi solicitado ao GINFS (Gerência de Infraestrutura e Serviços de TI) e GESIQ (Gerência de Segurança da Informação e Qualidade) que realizasse análise de conformidade da documentação entregue pela LICITANTE DFT INFORMAÇÃO, primeira classificada do certame.

Considerando a interposição de recurso apresentado pela empresa DFTI COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA, este departamento realizou a análise minuciosa nas fontes de comprovação documentais, adicionais, apresentadas pela LICITANTE.

Abaixo seguem as **análises dos recursos apresentados para cada item avaliado**:

ITEM 13.2.7.23. do Edital	Identificar, por meio de varreduras automatizadas, a superfície de ataque (vulnerabilidades, falhas, configurações inseguras, portas abertas).
COMPROVAÇÃO INICIALMENTE APRESENTADA	

Nível de Classificação **Público**	Grupo de acesso **Público**

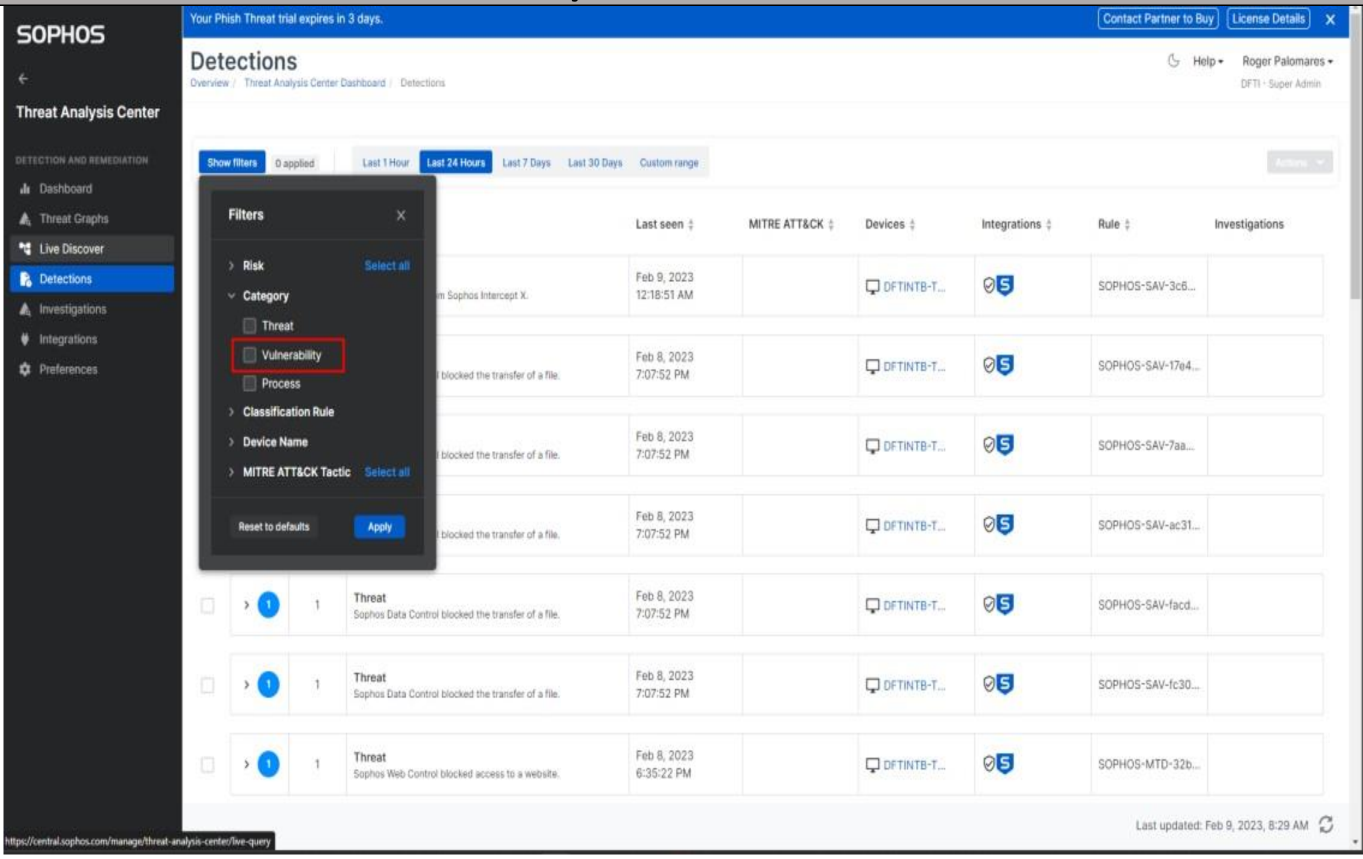
Ep **Intercept X Endpoint** — Features | Tech Specs | How to Buy | Get Pricing | Free Trial

Features	Intercept X Advanced	Intercept X Advanced with XDR	Intercept X Advanced with MDR	Intercept X Advanced with MDR Complete
ATTACK SURFACE				
Web Security	✓	✓	✓	✓
Download Reputation	✓	✓	✓	✓
Web Control / Category-based URL Blocking	✓	✓	✓	✓
Peripheral Control	✓	✓	✓	✓
Application Control	✓	✓	✓	✓
BEFORE IT RUNS ON DEVICE				
Deep Learning Malware Detection	✓	✓	✓	✓
Anti-Malware File Scanning	✓	✓	✓	✓
Live Protection	✓	✓	✓	✓
Pre-execution Behavior Analysis (HIPS)	✓	✓	✓	✓
Potentially Unwanted Application (PUA) Blocking	✓	✓	✓	✓
Intrusion Prevention System	✓	✓	✓	✓
STOP RUNNING THREAT				
Data Loss Prevention	✓	✓	✓	✓
Runtime Behavior Analysis (HIPS)	✓	✓	✓	✓
Antimalware Scan Interface (AMSI)	✓	✓	✓	✓
Malicious Traffic Detection (MTD)	✓	✓	✓	✓
Exploit Prevention	✓	✓	✓	✓

Anti-Malware File Scanning

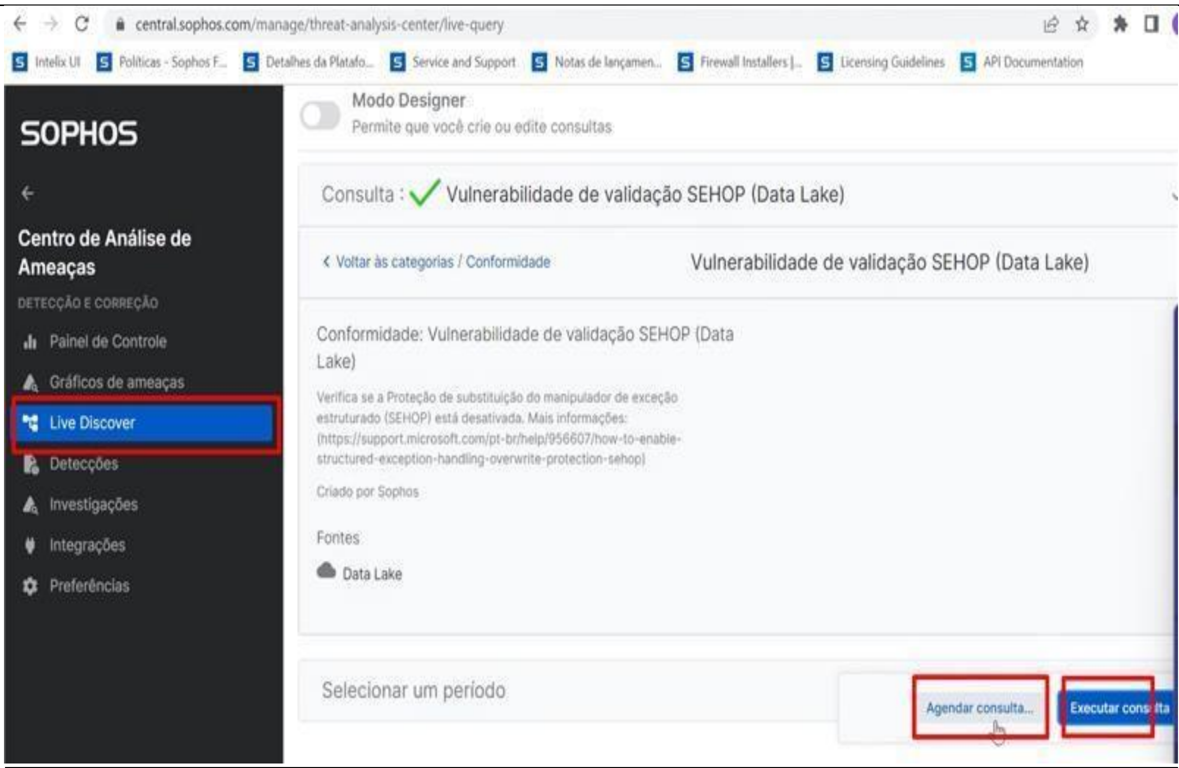
Pela imagem comprobatória do datasheet de recursos para identificação de vulnerabilidades da solução ofertada, não há evidências de que são identificadas vulnerabilidades, falhas, configurações inseguras e portas abertas. Apenas controle de malwares, acesso Web, downloads, controle de aplicações instaladas e controle de periféricos.

COMPROVAÇÃO ADICIONAL APRESENTADA



A imagem nova enviada mostra que a ferramenta permite a identificação das ameaças bloqueadas em um endpoint, a partir de política previamente definidas (Rule). A imagem mostra ainda a possibilidade de identificar qual comportamento, técnica e etapa fazem parte o ataque (segundo o framework MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge – Táticas, Técnicas e Conhecimento Comum de Adversários), apesar de na tela apresentada não identificar, coluna Mitre, a referência do ataque/vulnerabilidade identificado. O framework Mitre é uma representação abrangente dos comportamentos que os invasores utilizam quando comprometem as redes, sendo um framework útil para diversas medidas ofensivas e defensivas e outros mecanismos. É uma ferramenta consistente para identificação de ameaças e vulnerabilidades.

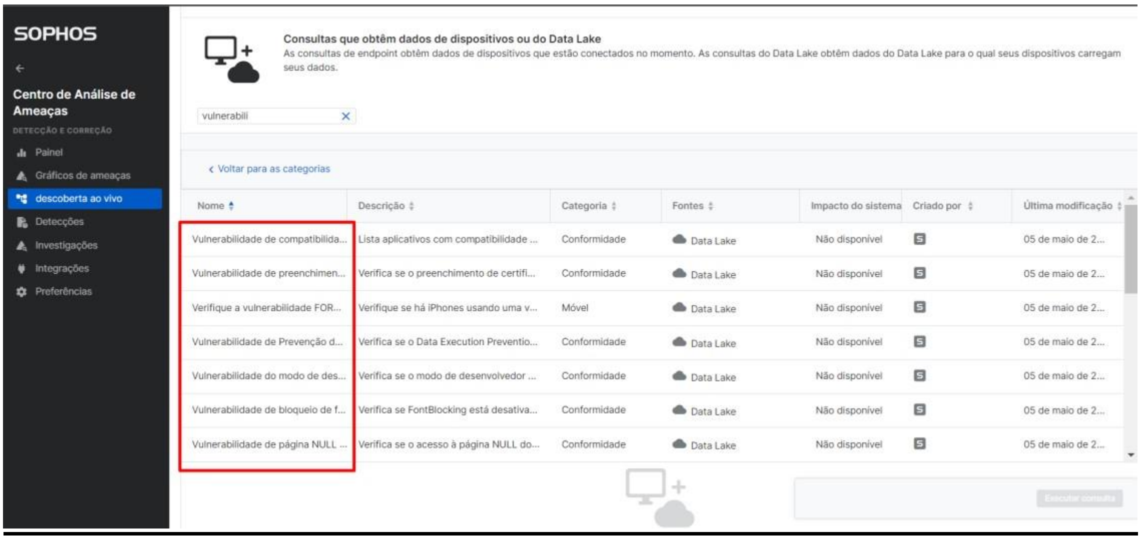
Nível de Classificação	Grupo de acesso
Público	**Público**

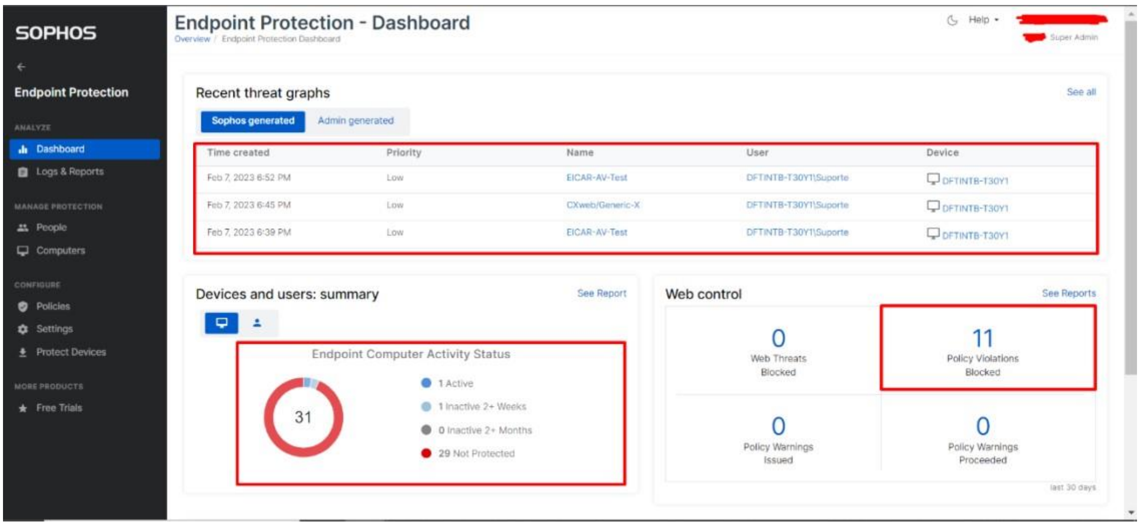


A imagem mostra que é permitido ativar a opção de criação ou edição de consultas de vulnerabilidades, através da “Proteção de substituição do manipulador de exceção estruturado" (SEHOP).

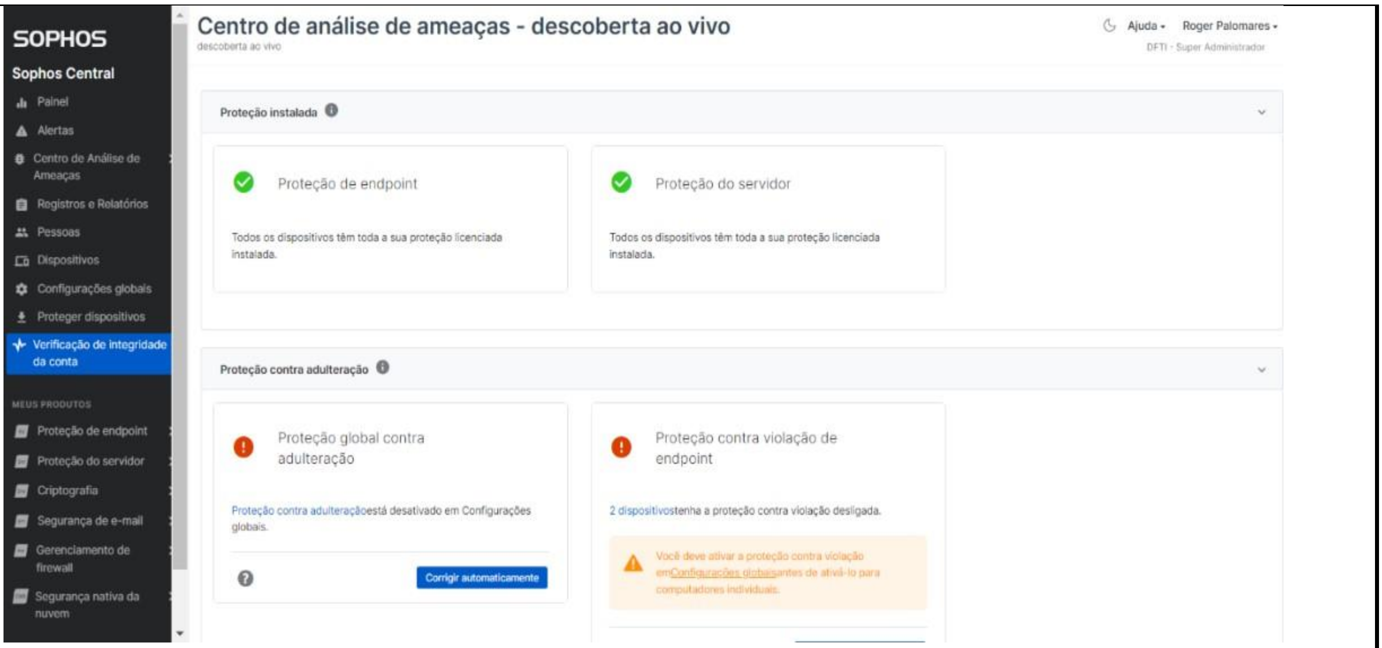
Nível de Classificação	Grupo de acesso
Público	**Público**

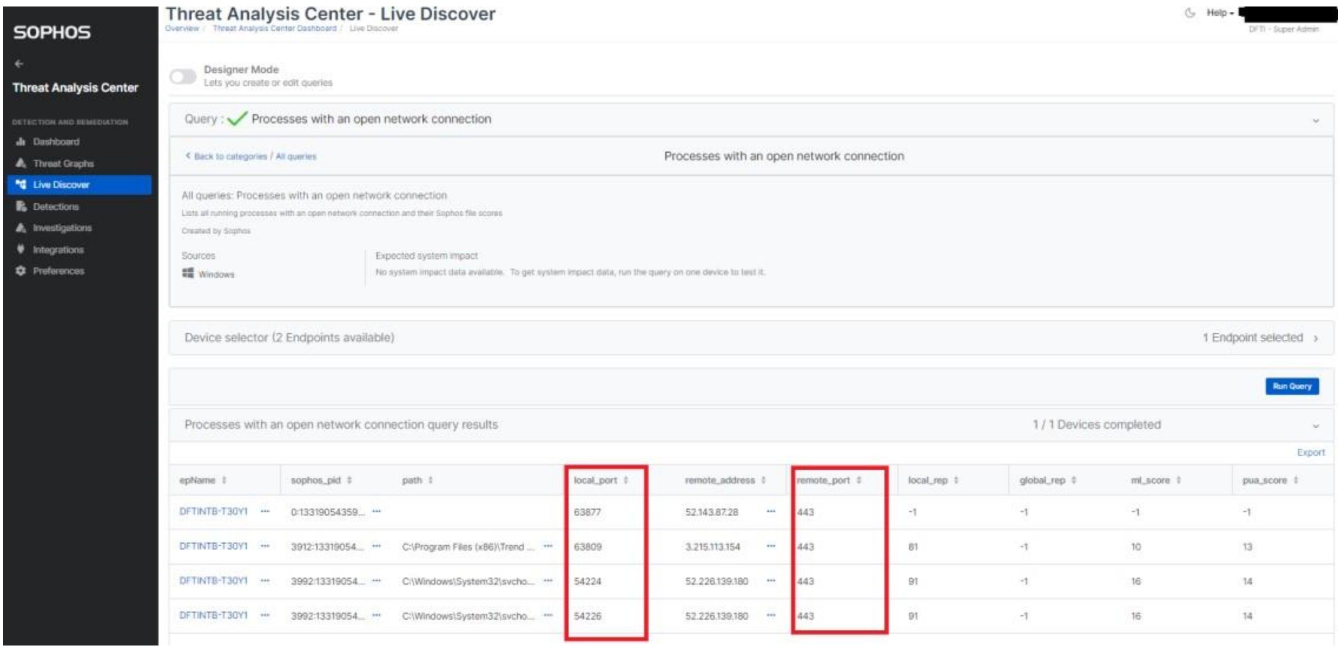
A descoberta ao vivo permite a listagem on line de compatibilidade definida com um executável específico. A tela exemplifica ainda a possibilidade de identificar 18 categorias e 438 consultas de vulnerabilidade. Através de pesquisa na Internet pôde-se identificar um Datasheet Internet sobre o SOPHOS MTR (sophos-workload-protection-licensing-guide-ptbr.pdf) que especifica as consultas de vulnerabilidades disponíveis - "De informações patrimoniais sobre versões de SO, aplicativos e vulnerabilidades à identificação de patrimônios gerenciados e não gerenciados, fornecemos valiosos insights durante avaliações de impacto, captura de ameaças e como parte das recomendações proativas de melhoria da postura de segurança", conforme documentação do fabricante.





Nível de Classificação	Grupo de acesso
Público	**Público**





Já a tela enviada que indica há a possibilidade de fazer-se uma consulta "on line" das portas abertas pelos processos em execução no endpoint. Atenderia, desde que esta varredura possa ser realizada de forma automatizada, e não apenas através de uma consulta on line. Esta evidência da possibilidade da consulta ser automatizada não foi apresentada (em forma de um relatório periódico, por exemplo).

ANÁLISE DA COMPROVAÇÃO POSTERIORMENTE APRESENTADA

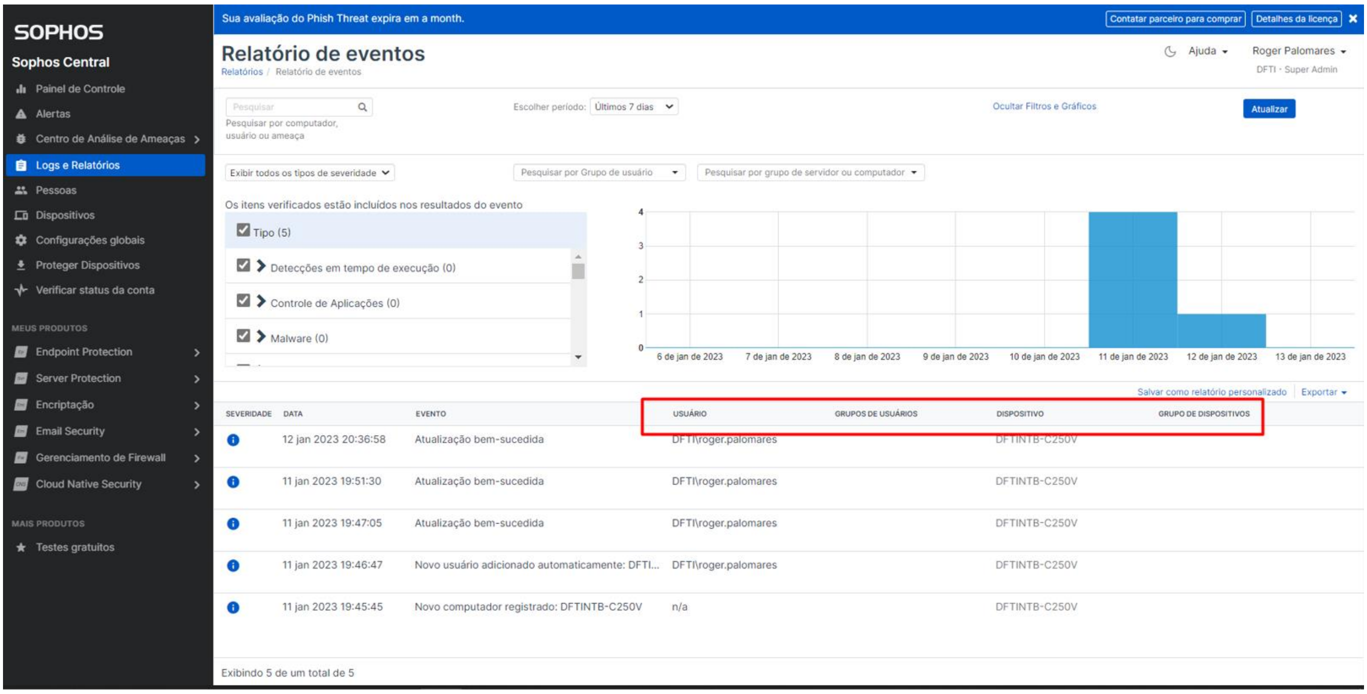
Conforme apresentado nas novas telas enviadas, a gestão de vulnerabilidades é um recurso disponível de forma consistente através do produto MTR. Apesar disto, em todas as telas comprobatórias enviadas há sempre referências a bloqueio de regras de políticas previamente definidas ou necessidade de realização consultas "on line", para se obter as informações das vulnerabilidades. Pelas informações comprobatórias enviadas, a automatização depende, necessariamente, de configuração prévia de políticas e não de buscas ativas automatizadas. Também não fica evidente, pelas comprovações emviadas, que a consulta de portas abertas no endpoint é realizada automaticamente, ou está apenas disponíveis em consultas "on line".

Desta forma, **não foi comprovado (1)** o atendimento a todos os requisitos deste item do Edital.

ITEM 13.3.11.9. do Edital	Informações por usuário (atividade web, uso de aplicativos e produtividade);

COMPROVAÇÃO INICIALMENTE APRESENTADA

A documentação apresentada indica a tela do Sophos Central para os itens do menu Logs e Relatórios:

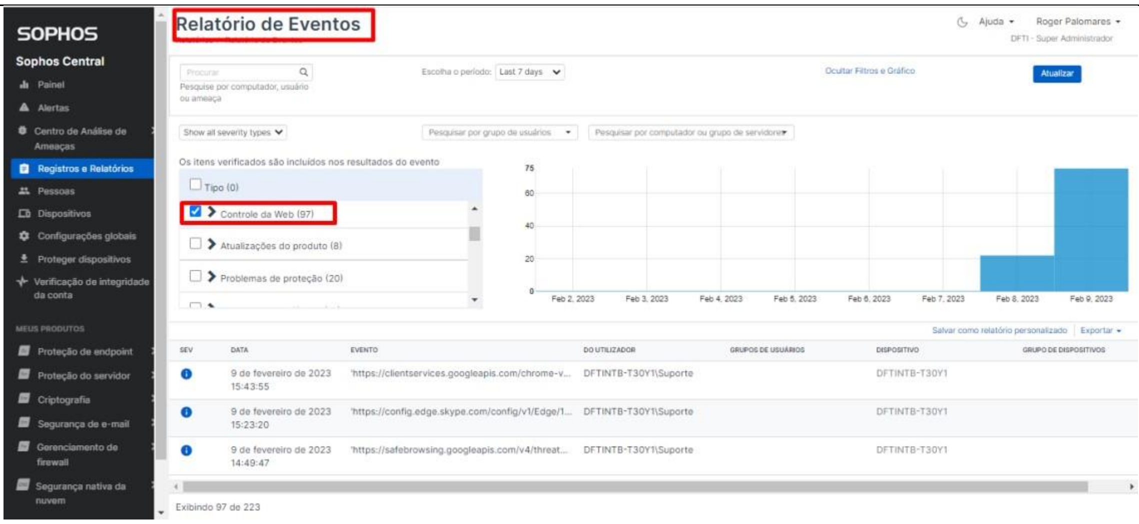


A imagem comprobatória do item não apresenta o relatório personalizado do usuário com informações da atividade Web, uso de aplicativos e sua produtividade diária). Mostra somente eventos do Windows, não exibe atividade web, como por exemplo, sites acessados, janelas acessadas, navegadores etc. Tampouco, informações sobre o uso de aplicativos, como por exemplo, acesso a planilhas, editores de texto, aplicativos de contabilidade etc. Em relação a produtividade, é necessário que sejam evidenciadas informações sobre tempo de uso de cada aplicativo, para que haja identificação de produtividade.

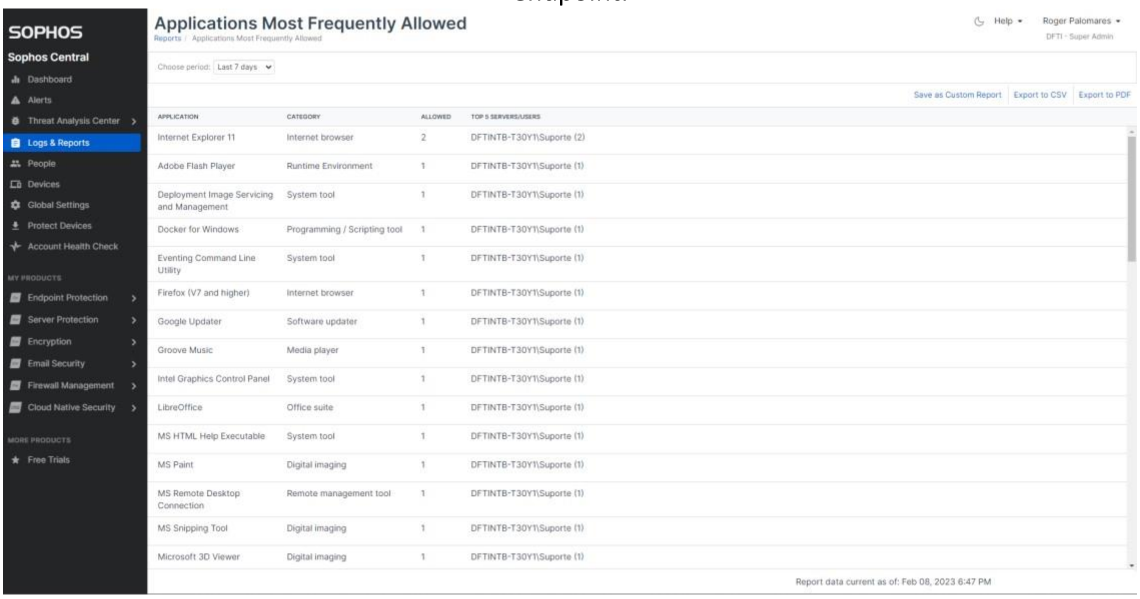
COMPROVAÇÃO ADICIONAL APRESENTADA

AMAZONAS
GOVERNO DO ESTADO

Nível de Classificação	Grupo de acesso
Público	**Público**



A imagem nova presenta a possibilidade de emissão de um relatório de atividades na web realizada por um endpoint.



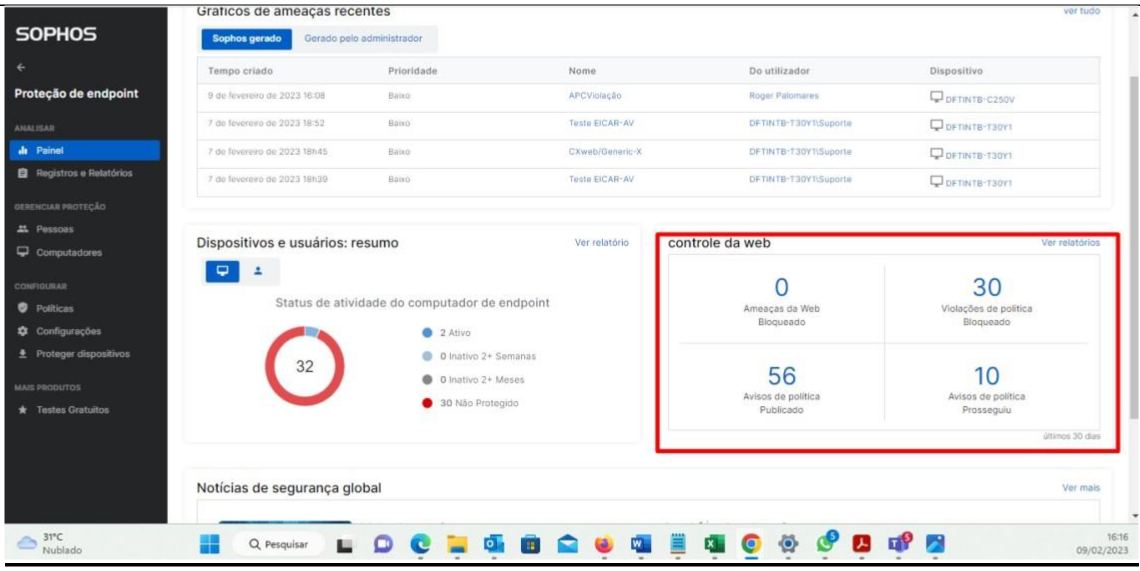
A tela enviada, adicionalmente, presenta um relatório dos aplicativos mais utilizados em um determinado período. Não fica evidenciado de que é possível presentar um relatório de TODOS os aplicativos utilizados por um endpoint.

Nível de Classificação	Grupo de acesso
Público	**Público**

A nova tela apresentada mostra que podem ser configurados os critérios de política web do endpoint.

A nova tela apresentada mostra que, a partir da política definida, pode ser emitido um relatório das violações do endpoint à política, em um determinado período. Registra se o acesso foi permitido ou bloqueado, a partir das regras definidas na política. Contudo, não foi possível identificar o quantitativo de tempo utilizado em cada tipo de aplicação na rotina diária ou outra forma que permita identificar a produtividade do usuário da estação.

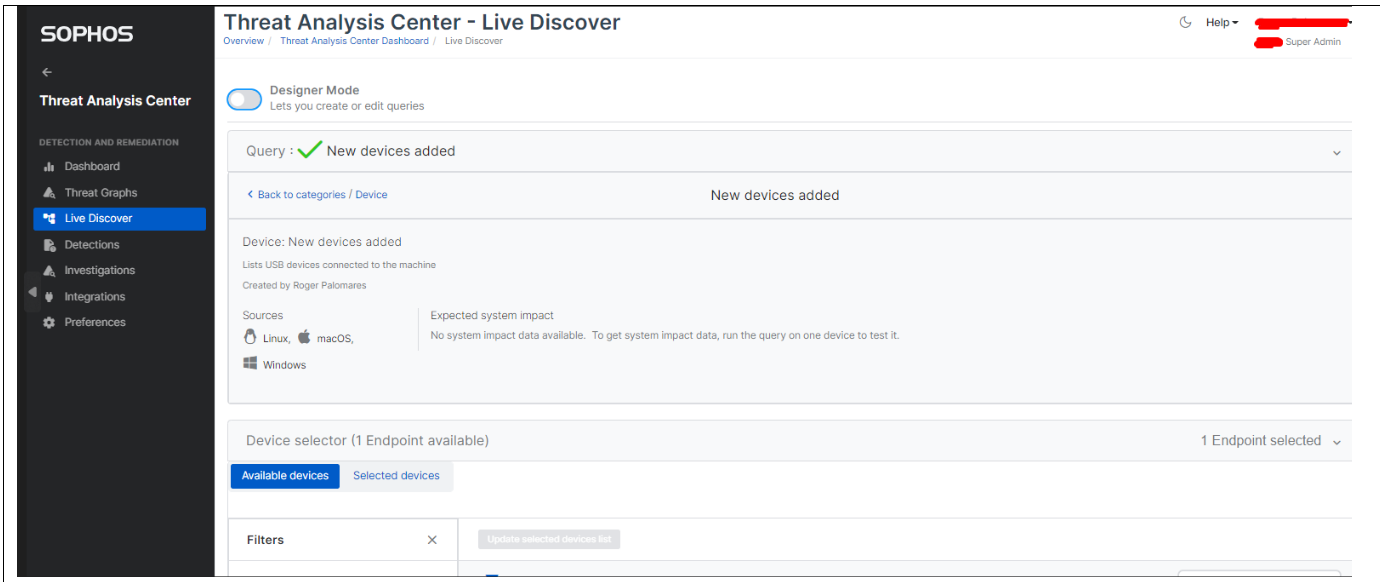
Nível de Classificação **Público**	Grupo de acesso **Público**



ANÁLISE DA COMPROVAÇÃO POSTERIORMENTE APRESENTADA
Apesar das novas imagens, ainda não foi possível evidenciar que será possível configurar uma política satisfatória de monitoramento, continuado, automático e contínuo, de produtividade de usuários utilizando a ferramenta. Desta forma, **não foi comprovado (2)** o atendimento a este item do Edital.

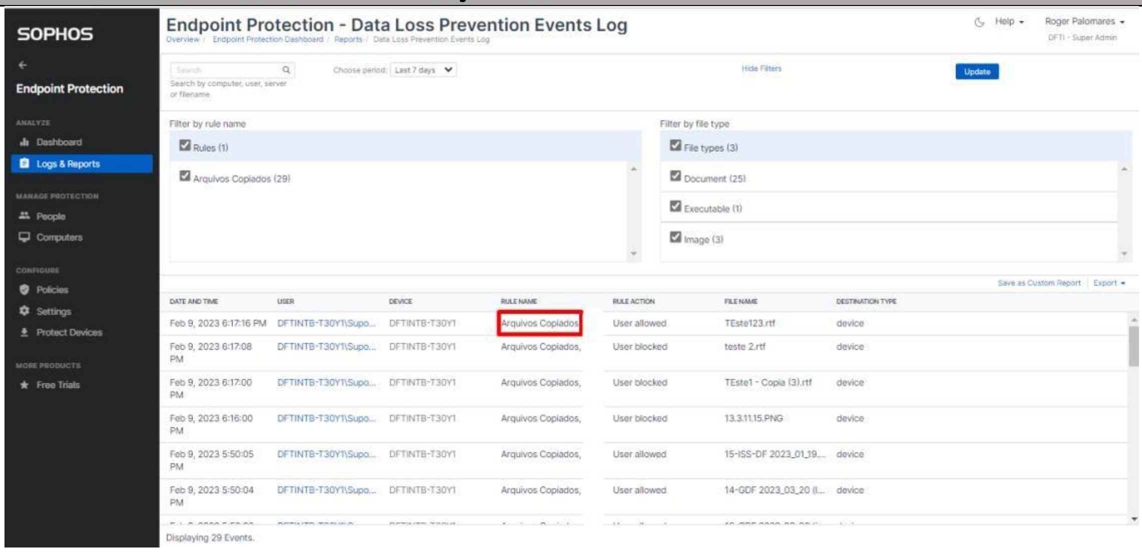
ITEM 13.3.11.15. do Edital	Informações de arquivos copiados dos discos locais dos endpoints para dispositivos de armazenamento externo e vice- versa;
ANÁLISE DA COMPROVAÇÃO INICIALMENTE APRESENTADA	
A documentação da comprovação apresenta a seguinte tela do Threat Analysis Center:	

Nível de Classificação	Grupo de acesso
Público	**Público**



Na imagem comprobatória indica que registra-se novos dispositivos USB conectados ao endpoint. Contudo, não há comprovação de que é possível evidenciar quais arquivos foram copiados dos discos locais dos endpoints para dispositivos de armazenamento externo e vice- versa. Não há evidências de que todos os tipos de arquivos, como por exemplo planihas excel, arquivos de mídia, arquivos de configuração, documentos, maliciosos são ou não, monitorados pelo produto ofertado.

COMPROVAÇÃO ADICIONAL APRESENTADA

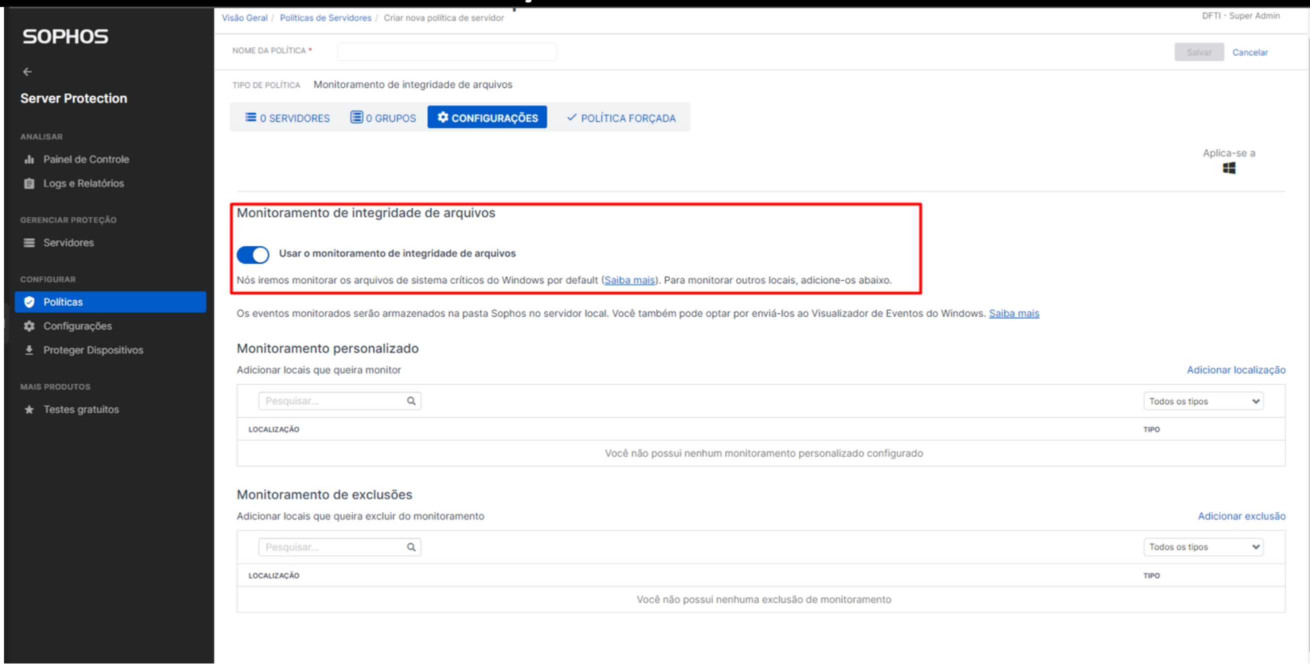


A nova imagem apresentada mostra uma listagem de arquivos copiados para fora, uma vez que o recurso utilizado é de monitorar o vazamento de informação.

Nível de Classificação **Público**	Grupo de acesso **Público**

ANÁLISE DO RECURSO APRESENTADO	
Evidenciou-se o monitoramento de arquivos copiados dos discos locais dos endpoints para dispositivos de armazenamento externo. Não ficou evidenciado, no entanto, que também é possível obter uma listagem dos arquivos recebidos pelo dispositivo (o “vice-versa”). Desta forma, **não foi comprovado (3)** o atendimento a este item do Edital.	
ITEM 13.3.12.6.4. do Edital	**Notificações e Alertas** - Arquivos acessados;

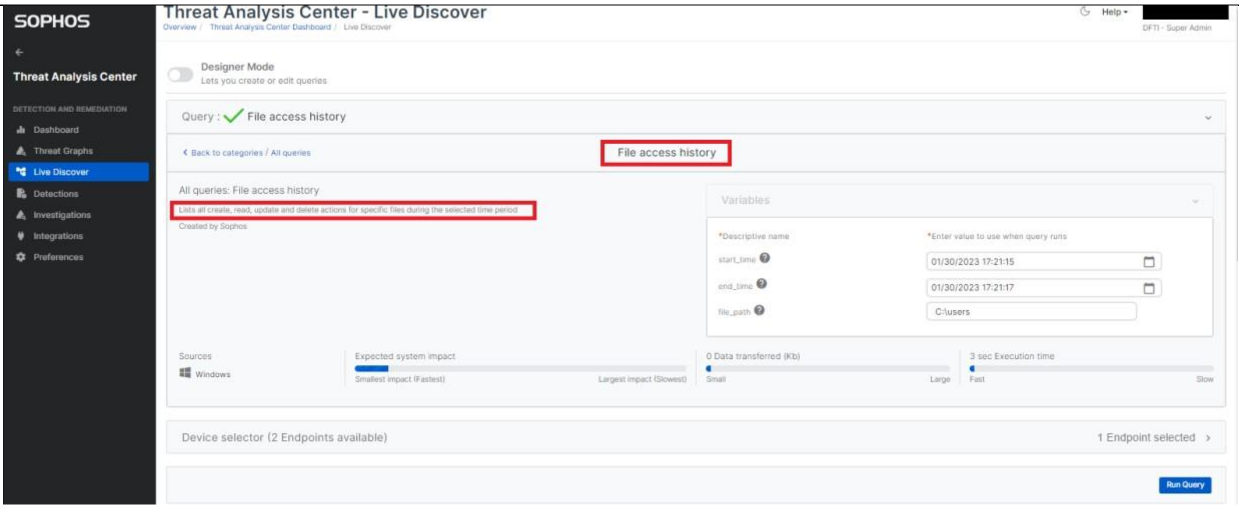
COMPROVAÇÃO INICIALMENTE APRESENTADA



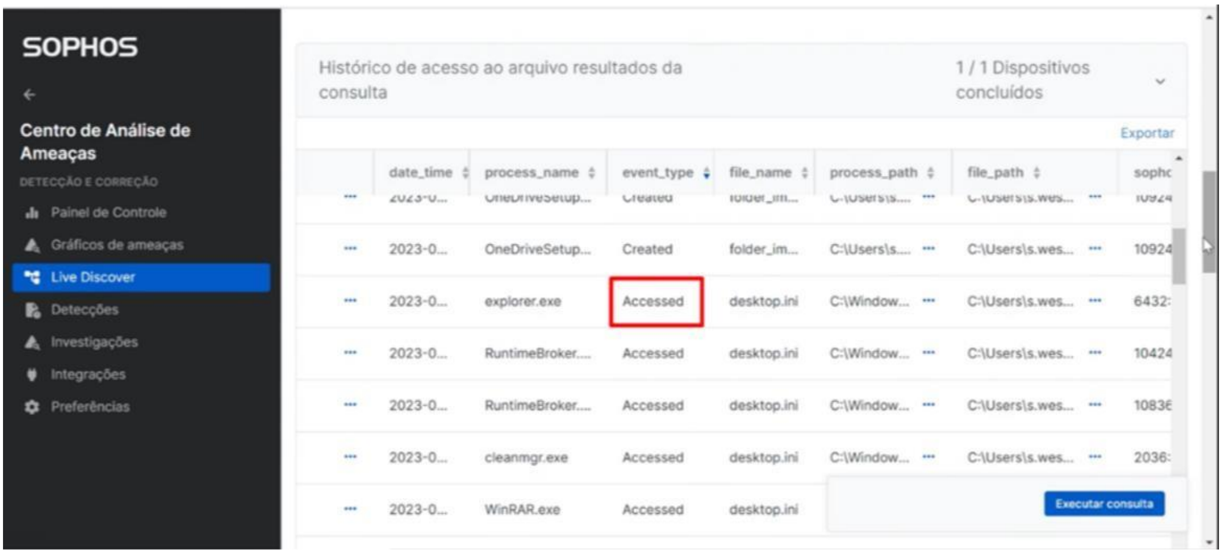
Na imagem comprobatória indica que é possível configurar o monitoramento da integridade dos arquivos críticos do Windows ou definir uma política que permita monitorar arquivos armazenados em um determinado drive. Contudo, não comprova que é possível receber alertas e notificações para **TODOS** os arquivos acessados a partir de um determinado endpoint, sejam eles em drives físicos ou lógicos.

COMPROVAÇÃO ADICIONAL APRESENTADA

Nível de Classificação	Grupo de acesso
Público	**Público**



Indica ser possível listar todos os arquivos lidos, deletados, atualizados para arquivos “específicos” em uma consulta, para um determinado período de tempo, em um drive específico, em uma consulta “ao vivo”. Não fica claro se é possível configurar a emissão de notificações e alertas para todos os arquivos acessados.



Nesta nova imagem enviada, apresenta-se uma consulta de acesso aos arquivos do sistema Windows em um determinado período. Não fica claro se é possível configurar a emissão de notificações e alertas para todos os arquivos acessados.

ANÁLISE DO RECURSO APRESENTADO
Em todas as imagens enviadas evidencia-se que é possível configurar o monitoramento dos arquivos críticos do Windows ou definir uma política que permita monitorar arquivos enumerados ou que estejam em atividade em um determinado drive. Indica ser possível fazer consultas aos arquivos acessados, deletados, atualizados para arquivos,

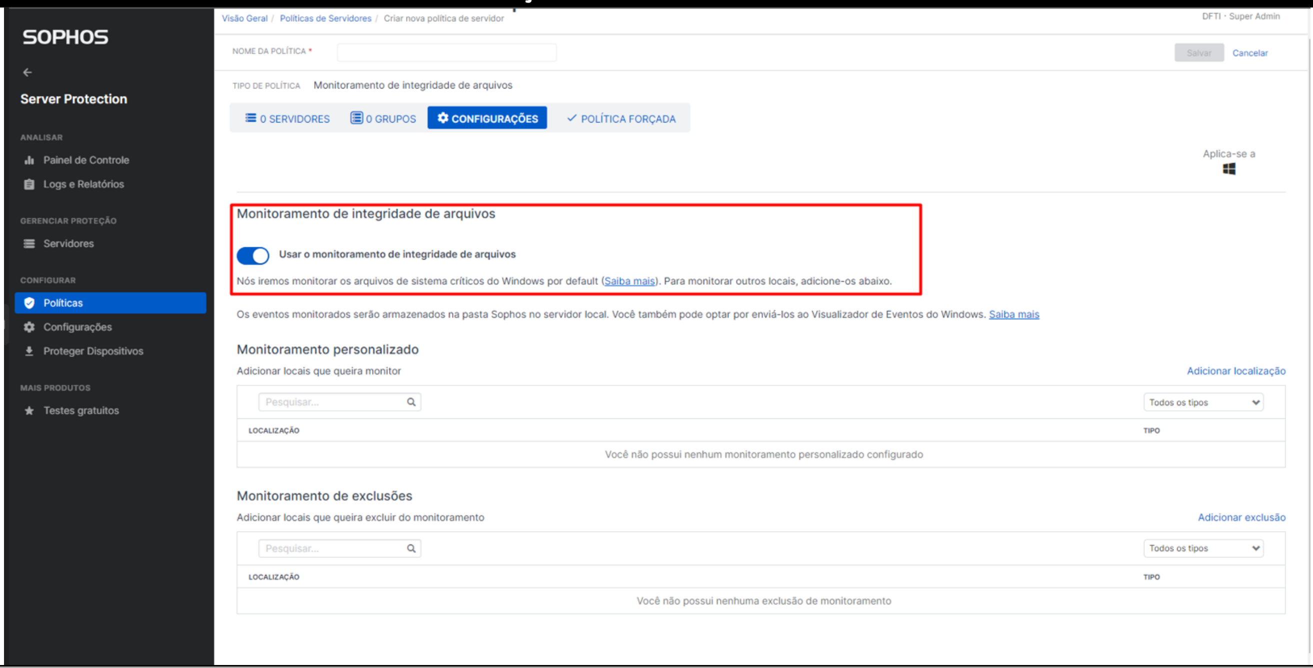
Nível de Classificação **Público**	Grupo de acesso **Público**

por um determinado período de tempo, em um drive específico, em uma consulta “on line”. Contudo, ainda não comprova que é possível configurar alertas e notificações de **todo acesso realizado em** arquivos, a partir de um determinado endpoint.

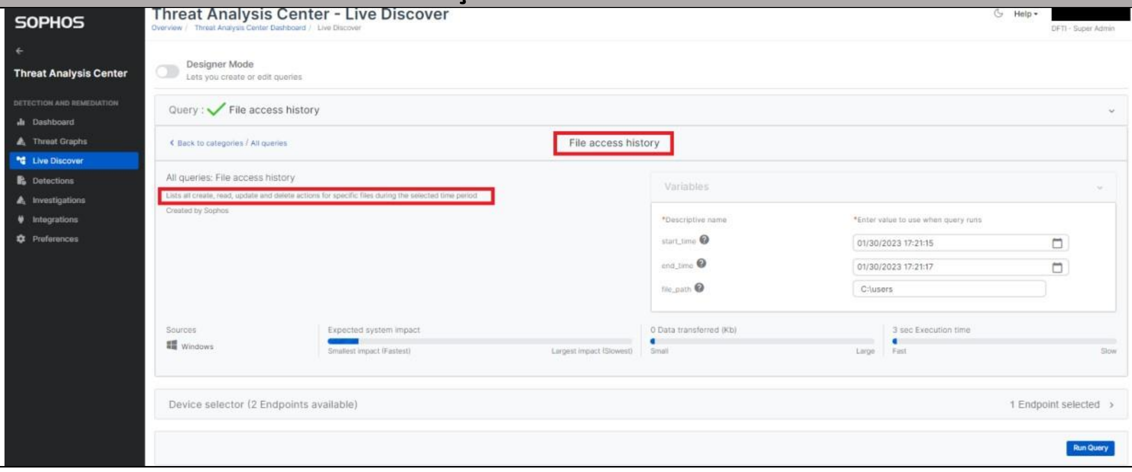
Desta forma, **não foi comprovado (4)** o atendimento a este item do Edital.

ITEM 13.3.12.6.5. do Edital	Arquivos copiados;

COMPROVAÇÃO INICIALMENTE APRESENTADA

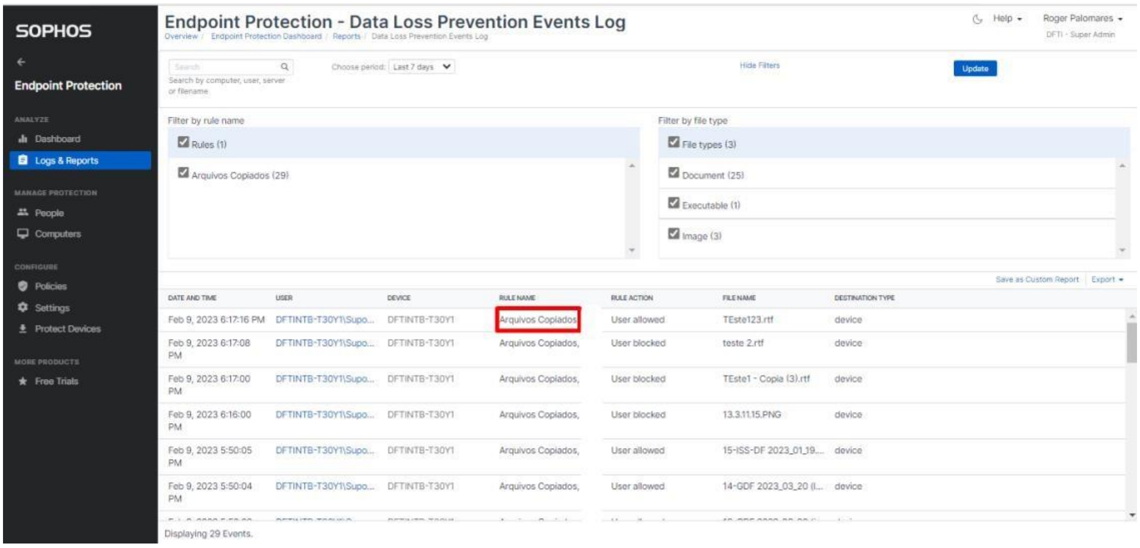


COMPROVAÇÃO ADICIONAL APRESENTADA



Nível de Classificação **Público**	Grupo de acesso **Público**

Na nova tela apresentada, a solução ofertada monitora todo o fluxo de arquivos, tanto do próprio Windows, quanto de qualquer outro drive que se defina, durante um determinado período de tempo.



A nova tela enviada no recurso evidencia uma visão dos arquivos copiados a partir do endpoint para ambiente externo.

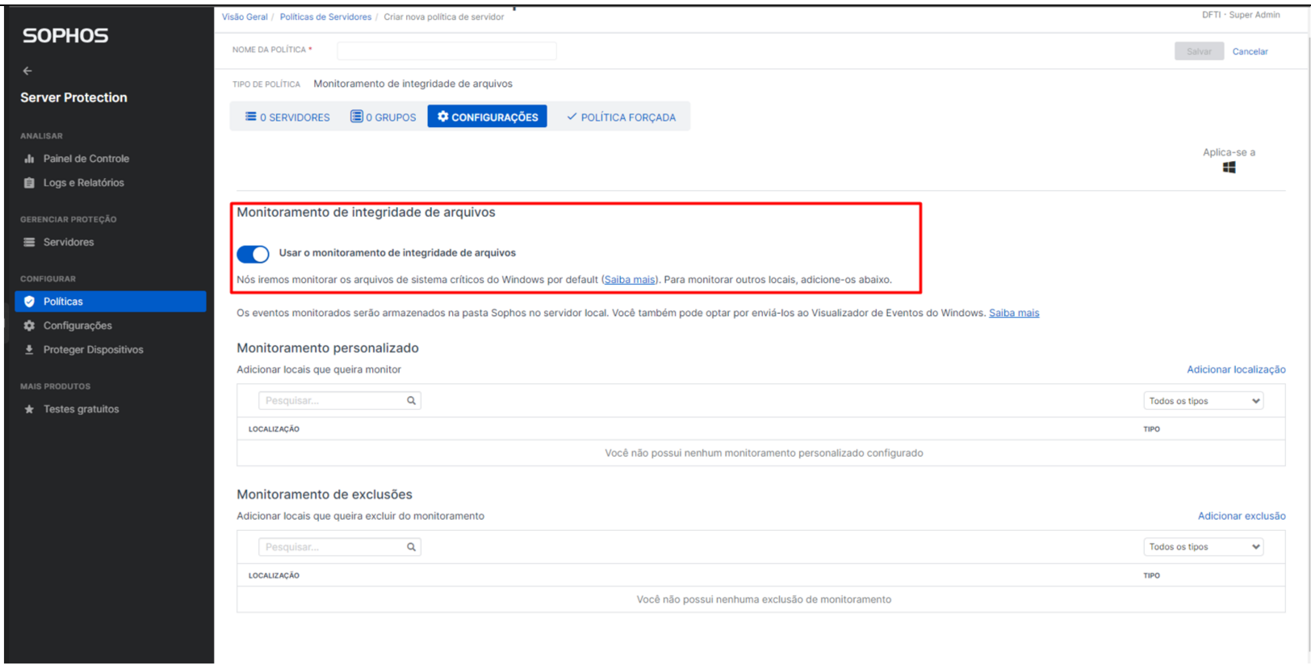
ANÁLISE DO RECURSO APRESENTADO

A imagem comprobatória indica que é possível configurar o monitoramento da cópia dos arquivos críticos do Windows ou definir uma política que permita o monitoramento de arquivos copiados a partir de drives especificados, em um determinado período de tempo. Contudo, não comprova que é possível configurar alertas e notificações de todos os arquivos foram copiados a partir de um determinado endpoint.

Desta forma, **não foi comprovado (5)** o atendimento a este item do Edital.

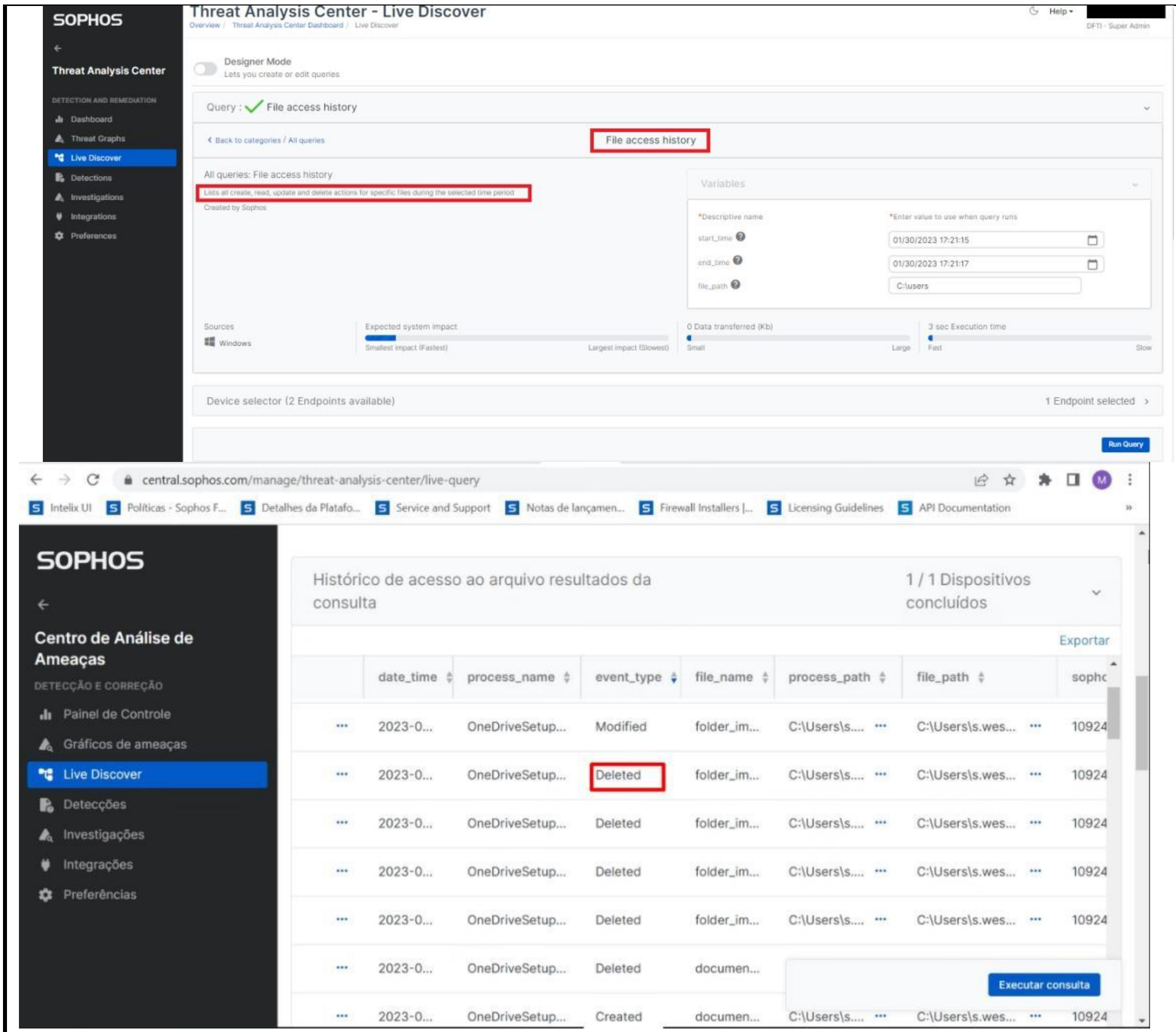
ITEM 13.3.12.6.6. do Edital	Arquivos apagados;

COMPROVAÇÃO INICIALMENTE APRESENTADA



Na imagem comprobatória indica que é possível configurar os arquivos críticos do Windows ou definir uma política que permita monitorar arquivos que estejam armazenados em determinado drive. Contudo, não ficou claro se é possível configurar a emissão de alertas e notificações de todos os arquivos foram apagados a partir de um determinado endpoint.

COMPROVAÇÃO ADICIONAL APRESENTADA



ANÁLISE DO RECURSO APRESENTADO

As imagens comprobatórias indicam que é possível configurar os arquivos críticos do Windows ou definir uma política que permita monitorar a remoção de arquivos que estejam em drives listados. Ou realizar consultas "on line" ou emitir relatório dos arquivos removidos por um endpoint, em um determinado período de tempo. Contudo, não comprova que é possível configurar notificações e alertas todas as exclusões de arquivos que foram realizados por um determinado endpoint.

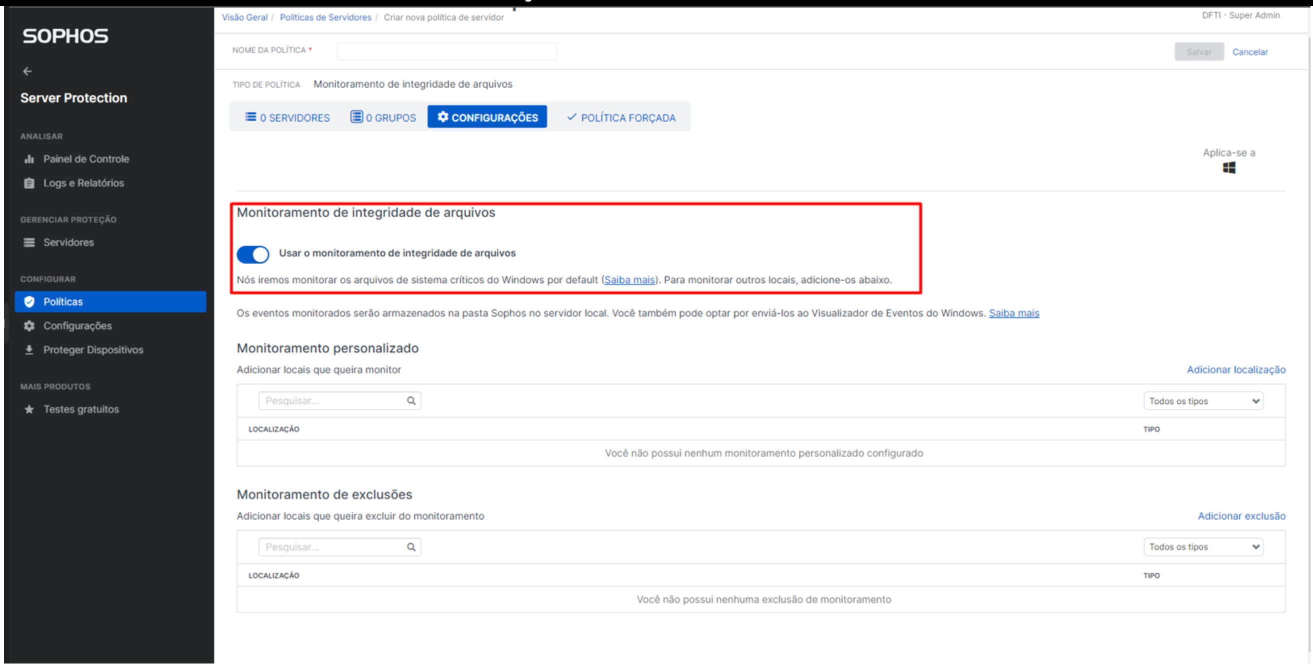
Desta forma, **não foi comprovado (6)** o atendimento a este item do Edital.

ITEM 13.3.12.6.7. do Edital	Arquivos alterados;

AMAZONAS
GOVERNO DO ESTADO

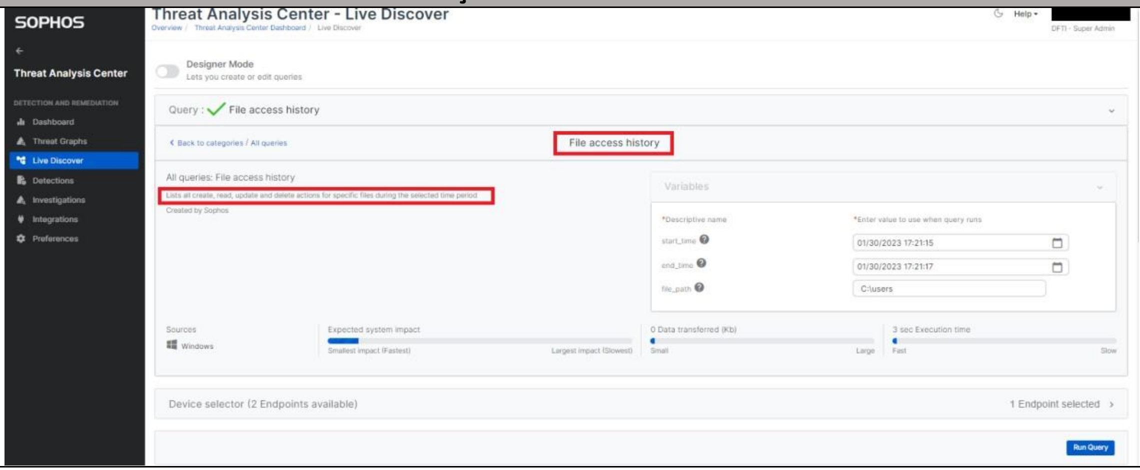
Nível de Classificação **Público**	Grupo de acesso **Público**

COMPROVAÇÃO INICIALMENTE APRESENTADA



Na imagem comprobatória indica que é possível configurar os arquivos críticos do Windows ou definir uma política que permita monitorar arquivos que sejam enumerados. Contudo, não ficou claro de que é possível evidenciar que são emitidos alertas e notificações, de todos os arquivos foram alterados a partir de um determinado endpoint.

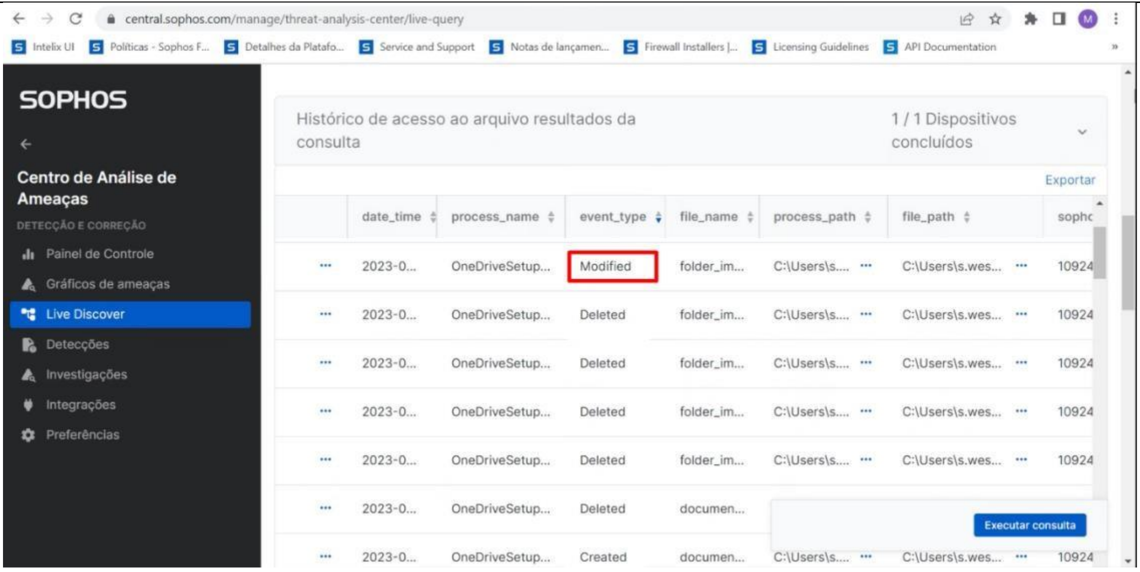
COMPROVAÇÃO ADICIONAL APRESENTADA



Rua Jonathas Pedrosa, nº 1937,
Pça. 14 de Janeiro, Manaus-AM
CEP 69020-110
SAC-PRODAM: (92) 2121-6500
WWW.PRODAM.AM.GOV.BR
@prodam_am

PRODAM
Processamento de Dados Amazonas

Nível de Classificação	Grupo de acesso
Público	**Público**



Na nova imagem apresentada verifica-se que é possível realizar uma consulta “on line” ou emitir um relatório das alterações de arquivos realizadas em drives previamente especificados, em um determinado período de tempo.

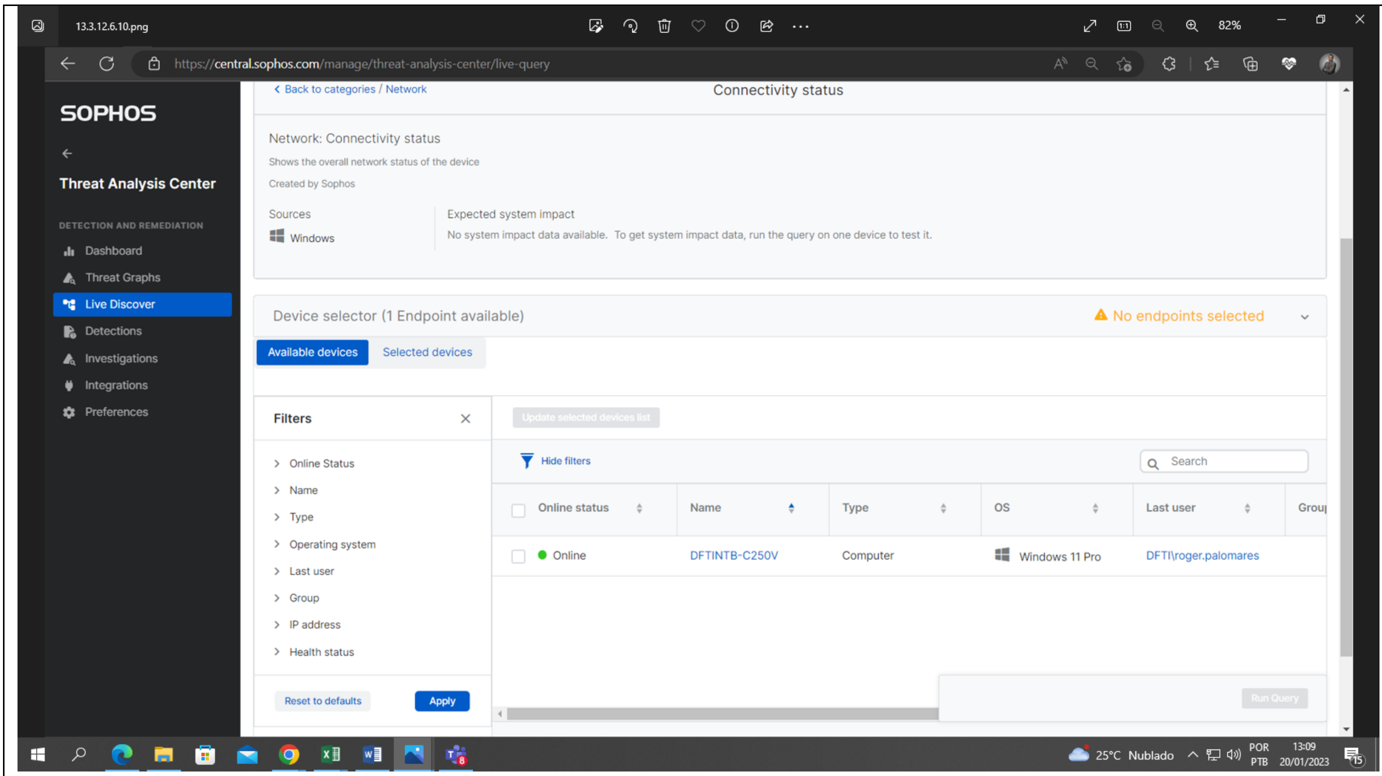
ANÁLISE DO RECURSO APRESENTADO

As novas imagens evidenciaram a emissão de relatórios dos arquivos alterados. Contudo, não comprova que é possível configurar a emissão de alertas e notificações de todas as alterações realizadas em todo tipo de arquivos, ou se a configuração do alerta está disponível apenas para os drivers especificados para monitoramento.

Desta forma, **não foi comprovado (7)** o atendimento a este item do Edital.

ITEM 13.3.12.6.10. do Edital	Utilização simultânea de redes sem fio e cabeadas;

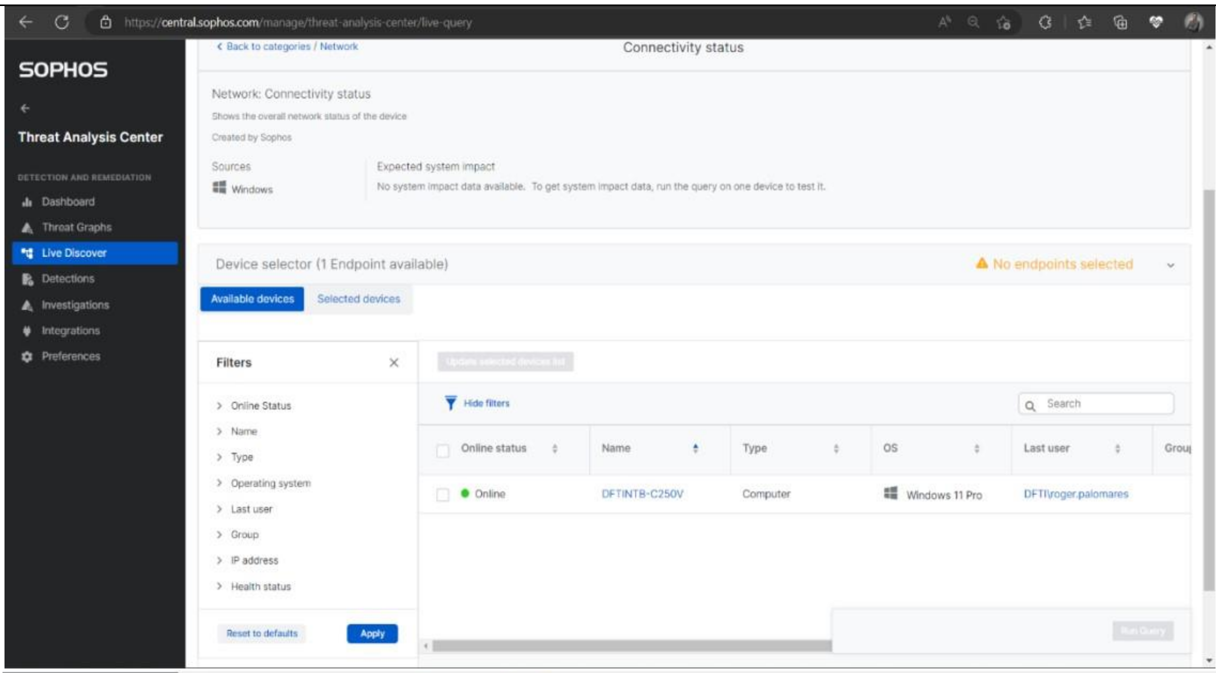
COMPROVAÇÃO INICIALMENTE APRESENTADA

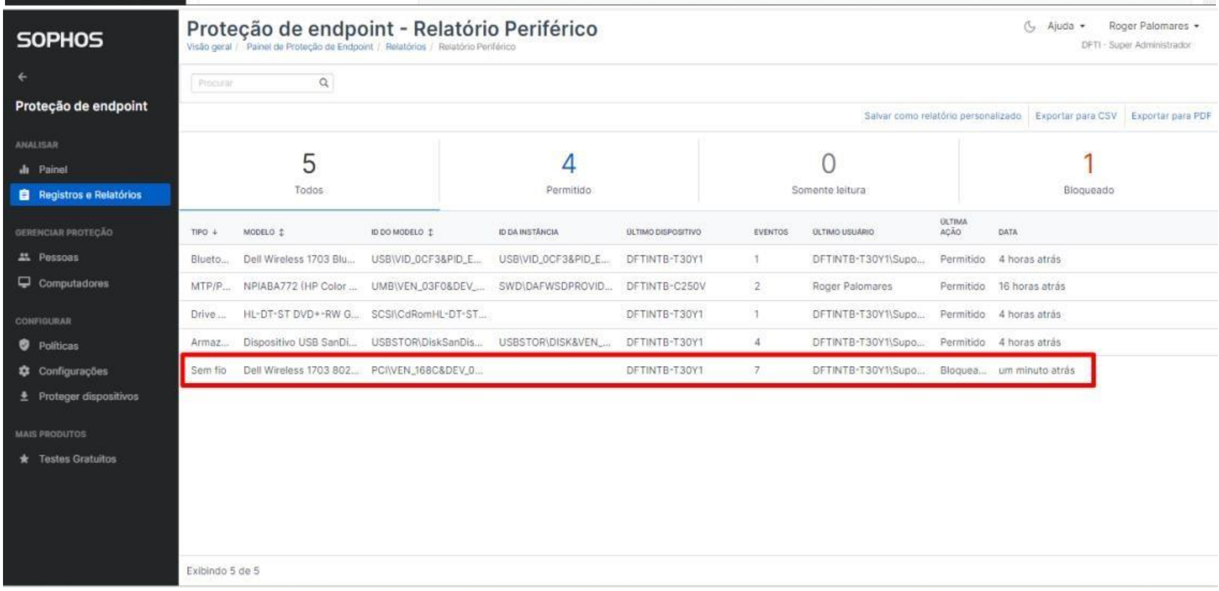


Na imagem comprobatória indica que é possível monitorar estações de trabalho ativas. Contudo, não há comprovação de que é possível notificar ou alertar que um endpoint está fazendo uso de mais de uma conexão em redes sem fio ou cabeadas.

COMPROVAÇÃO ADICIONAL APRESENTADA

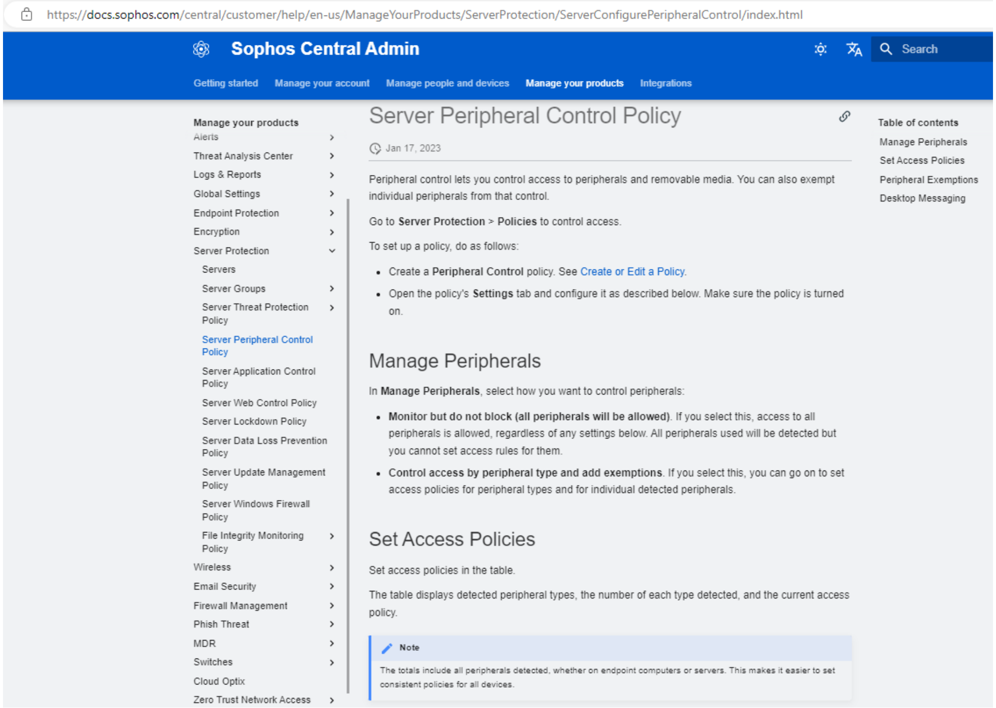
Nível de Classificação	Grupo de acesso
Público	**Público**





No recurso apresentado a licitante ressaltou que a solução monitora o uso das placas de rede, permitindo-se a configuração de políticas e geração de consultas e relatórios. Contudo, não foi apresentada tela onde consta a opção de configuração de notificação de notificações e alertas, quando identificar uso simultâneo de rede sem fio e cabeada. Segundo a licitante, pelo fato de ser uma política, a solução não seria alertar, mas impedir o uso simultâneo de placas de rede por política. Conforme telas a seguir:

Nível de Classificação	Grupo de acesso
Público	**Público**



https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/ServerProtection/ServerConfigurePeripheralControl/index.html

Sophos Central Admin

Getting started | Manage your account | Manage people and devices | Manage your products | Integrations

Manage your products: Alerts, Threat Analysis Center, Logs & Reports, Global Settings, Endpoint Protection, Encryption, Server Protection (Servers, Server Groups, Server Threat Protection Policy, Server Peripheral Control Policy, Server Application Control Policy, Server Web Control Policy, Server Lockdown Policy, Server Data Loss Prevention Policy, Server Update Management Policy, Server Windows Firewall Policy, File Integrity Monitoring Policy), Wireless, Email Security, Firewall Management, Phish Threat, MDR, Switches, Cloud Optix, Zero Trust Network Access

Server Peripheral Control Policy

Jan 17, 2023

Peripheral control lets you control access to peripherals and removable media. You can also exempt individual peripherals from that control.

Go to **Server Protection** > **Policies** to control access.

To set up a policy, do as follows:

- Create a **Peripheral Control** policy. See Create or Edit a Policy.
- Open the policy's **Settings** tab and configure it as described below. Make sure the policy is turned on.

Manage Peripherals

In **Manage Peripherals**, select how you want to control peripherals:

- **Monitor but do not block (all peripherals will be allowed)**. If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you cannot set access rules for them.
- **Control access by peripheral type and add exemptions**. If you select this, you can go on to set access policies for peripheral types and for individual detected peripherals.

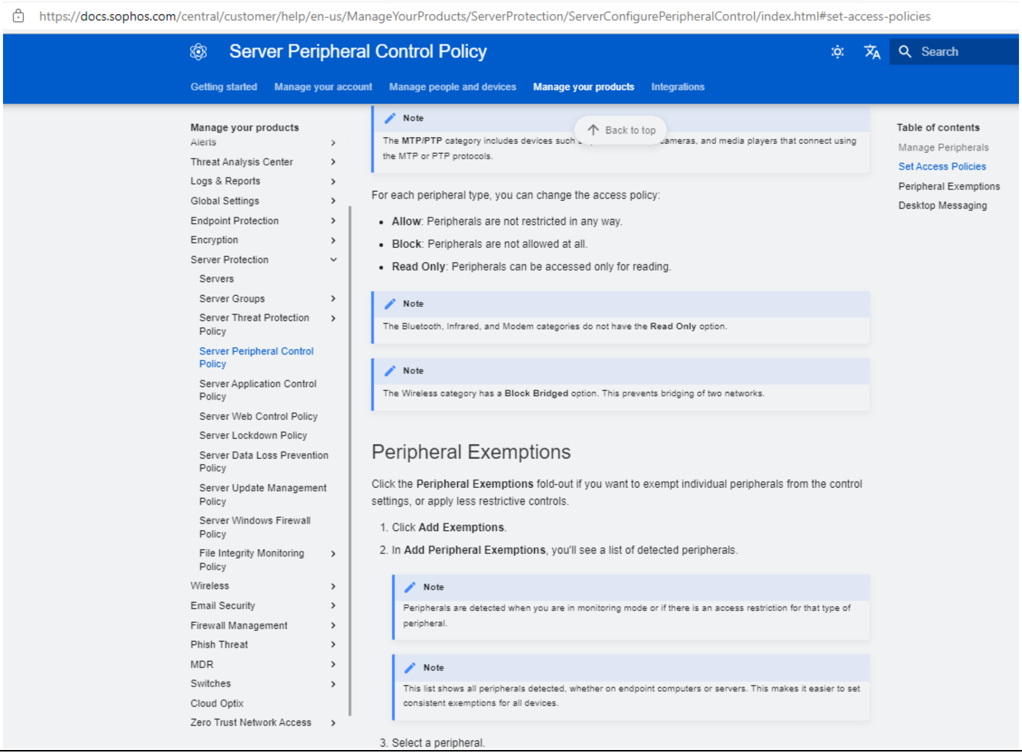
Set Access Policies

Set access policies in the table.

The table displays detected peripheral types, the number of each type detected, and the current access policy.

Note: The totals include all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent policies for all devices.

Table of contents: Manage Peripherals, Set Access Policies, Peripheral Exemptions, Desktop Messaging



https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/ServerProtection/ServerConfigurePeripheralControl/index.html#set-access-policies

Server Peripheral Control Policy

Note: The **MTP/PTP** category includes devices such ... cameras, and media players that connect using the MTP or PTP protocols.

For each peripheral type, you can change the access policy:

- **Allow**: Peripherals are not restricted in any way.
- **Block**: Peripherals are not allowed at all.
- **Read Only**: Peripherals can be accessed only for reading.

Note: The Bluetooth, Infrared, and Modem categories do not have the **Read Only** option.

Note: The Wireless category has a **Block Bridged** option. This prevents bridging of two networks.

Peripheral Exemptions

Click the **Peripheral Exemptions** fold-out if you want to exempt individual peripherals from the control settings, or apply less restrictive controls.

1. Click **Add Exemptions**.
2. In **Add Peripheral Exemptions**, you'll see a list of detected peripherals.

Note: Peripherals are detected when you are in monitoring mode or if there is an access restriction for that type of peripheral.

Note: This list shows all peripherals detected, whether on endpoint computers or servers. This makes it easier to set consistent exemptions for all devices.

3. Select a peripheral.

Nível de Classificação **Público**	Grupo de acesso **Público**

https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/ServerProtection/ServerConfigurePeripheralControl/index.html#peripheral-exemptions

Server Peripheral Control Policy

Search

Getting started | Manage your account | Manage people and devices | Manage your products | Integrations

Manage your products
- Alerts
- Threat Analysis Center
- Logs & Reports
- Global Settings
- Endpoint Protection
- Encryption
- Server Protection
  - Servers
  - Server Groups
  - Server Threat Protection Policy
  - Server Peripheral Control Policy
  - Server Application Control Policy
  - Server Web Control Policy
  - Server Lockdown Policy
  - Server Data Loss Prevention Policy
  - Server Update Management Policy
  - Server Windows Firewall Policy
  - File Integrity Monitoring Policy
- Wireless
- Email Security
- Firewall Management
- Phish Threat

3. Select a peripheral.
4. In the **Policy** column, you can optionally use the drop-down list to assign a specific access policy to an exempt peripheral.

> **Note**
> Do not set a stricter access policy for an individual peripheral than for its peripheral type. If you do, the setting for the individual policy is ignored and a warning icon is displayed beside it.

5. In the **Enforce By** column, you can optionally use the drop-down menu to apply the policy to all peripherals of that model or to ones with the same ID (the list shows you the model and ID).
6. Click **Add Exemption(s)**.

Desktop Messaging

You can add a message to the end of the standard notification. If you leave the message box empty only the standard message is shown.

Desktop Messaging is on by default.

> **Note**
> If you switch off **Desktop Messaging** you will not see any notification messages related to Peripheral Control.

Click in the message box and enter the text you want to add.

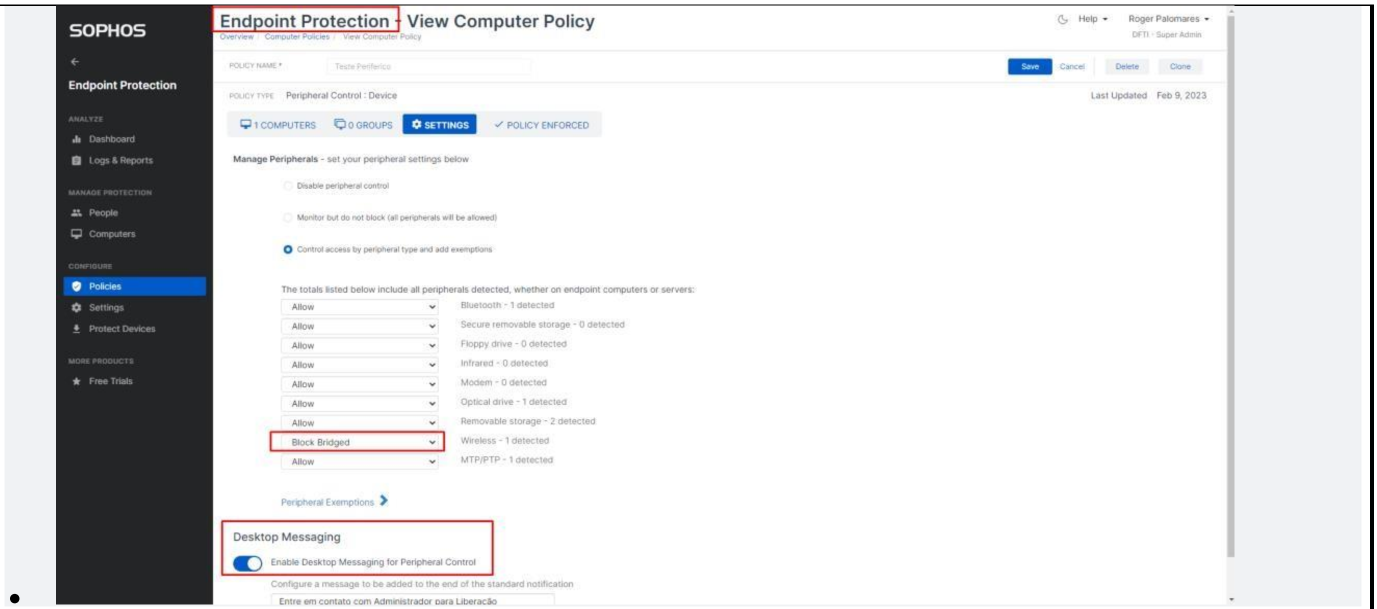
Was this page helpful?

Manage Peripherals

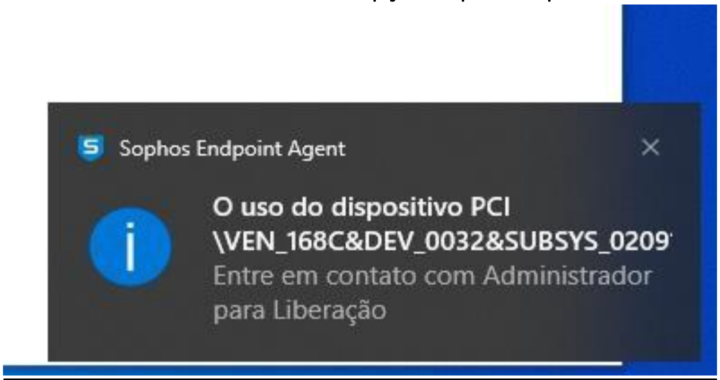
In **Manage Peripherals**, select how you want to control peripherals:

- **Monitor but do not block (all peripherals will be allowed)**. If you select this, access to all peripherals is allowed, regardless of any settings below. All peripherals used will be detected but you cannot set access rules for them.
- **Control access by peripheral type and add exemptions**. If you select this, you can go on to set access policies for peripheral types and for individual detected peripherals.

Nível de Classificação **Público**	Grupo de acesso **Público**



- No caso específico a tela mostra ser possível bloquear um dispositivo específico. Para este item, bloquear a interface de WI-FI não é uma opção. Apenas quando conflitar no uso da rede cabeada...



No caso, a imagem comprova a emissão de alerta e notificação para o usuário do endpoint, para apenas para o USO do dispositivo, e não para o conflito de uso de 2 interfaces de rede de forma simultânea.

ANÁLISE DO RECURSO APRESENTADO

Mesmo considerando as imagens comprobatórias adicionais enviadas, ainda não evidencia a possibilidade de se configurar notificações ou alertas, de forma automática, sempre que um endpoint estiver fazendo uso simultâneo de uma conexão em redes sem fio e cabeada. Para cada dispositivo pode-se definir uma política de: monitoramento e não bloqueio *OU* Controle de acesso por tipo ou isenção. No caso específico, bloquear a interface de WI-FI não é uma opção. Caso se opte pelo monitoramento, não está evidenciado onde configura-se a notificação ou emitido o alerta, no caso de uso simultâneo dos 2 periféricos.

Desta forma, **não foi comprovado (8)** o atendimento a este item do Edital.

Nível de Classificação	Grupo de acesso
Público	**Público**

ITEM. 8 do Edital	Qualificação técnica exigida;

COMPROVAÇÃO INICIALMENTE APRESENTADA

ESTADO DE SANTA CATARINA
SECRETARIA DE ESTADO DA FAZENDA
GABINETE DA SECRETÁRIA ADJUNTA
DIRETORIA DE ADMINISTRAÇÃO E FINANÇAS
GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos que a empresa **DFTI – COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA**, inscrita no CNPJ (MF) nº **09.650.283/0001-91**, inscrição estadual/distrital nº **07.505.692/001-81**, estabelecida no (a) **SCN Quadra 2, Bloco D, Torre A, No 810, Liberty Mall – Brasília/DF**, forneceu à **SECRETARIA DE ESTADO DA FAZENDA DO ESTADO DE SANTA CATARINA**, através do contrato Nº **002/2021**, decorrente do Edital de Pregão Eletrônico n°**0024/2020**, autorizado pelo Processo **SEF 17276/2019**, fornecimento de solução de segurança integrada para ambientes críticos, incluindo serviços de implantação da solução, repasse de conhecimento, garantia e suporte, pelo período de 36 (trinta e seis) meses e prorrogáveis até 48 (quarenta e oito) meses, conforme detalhamento abaixo:

Grupo	Item	Características Especificações Mínimas	Marca/Modelo
1	1	Proteção avançada de anti-malware para estação de trabalho	MARCA - SOPHOS MODELO - Sophos Intercept X Advanced with EDR.
	2	Proteção avançada de anti-malware para servidores	MARCA - SOPHOS MODELO - Sophos Intercept X Advanced for Server with EDR.
	3	Gerenciamento e administração centralizada	MARCA - SOPHOS MODELO - Sophos Central Admin.
	4	Manutenção e Suporte para 36 meses	Serviços especializados DFTI.
	1	Gestão de usuários privilegiados para estações de trabalho	MARCA - BEYONDTRUST MODELO - BeyondTrust BeyondInsight, Password Safe e BeyondTrust Privilege Management.
			MARCA - BEYONDTRUST

Dos atestados de capacidade técnica apresentados, apenas 01 (hum) é semelhante ao tipo de produto ofertado pelo licitante para o certame. Mesmo assim, o atestado enviado não especifica o quantitativo de licenças fornecidas. Assim não comprova que as licenças fornecidas pelo atestado em questão equivalem a 10% do quantitativo solicitado no certame.

COMPROVAÇÃO ADICIONAL APRESENTADA

No documento complementar enviado no recurso, está evidenciado os quantitativos fornecidos pelo contrato do atestado de capacitação técnica citado que, de fato, evidencia 10% do quantitativo solicitado semelhante ao produto solicitado:

Item	GRUPO	Especificações da Solução (requisitos mínimos)	Quant.	Unidade
01	1	Proteção avançada de contra malware para estação de trabalho (subitem 4.1 do Anexo II do Edital).	1500	un
02		Proteção avançada de contra malware para servidores (subitem 4.2 do Anexo II do Edital)	250	un
03		Gerenciamento e administração centralizada (subitem 4.3 do Anexo II do Edital).	01	un
04		Serviço de Suporte e Atualização (item 7 do Anexo II do Edital) referente a proteção avançada de contra malware para estação de trabalho, proteção avançada de contra malware para servidores e gerenciamento e administração centralizada.	36	mês

Conforme demonstrado no quantitativo solicitado pela Prodam:

PREGÃO ELETRÔNICO SRP 14/2022

Anexo 1-B – Modelo de Proposta de Preços

1. O preço deverá ser composto de acordo com a tabela abaixo:

Item	ESPECIFICAÇÃO	Referência	QTDE.	Valor Unitário (R$)	Valor Total (R$)
01	Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, em endpoint	Licença de uso para 12 meses	15.000		
02	Serviço de instalação para solução de segurança, auditoria e prevenção de ameaça à base de dados não estruturados em endpoint	Serviço	2		
03	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados em endpoint	Turma	4		
Valor total da Proposta (R$):					

Os preços para sessão pública do Pregão deverá ser a soma de valores da última coluna, indicado como "Valor Total" de CADA ITEM.

2. A Licitante deverá apresentar, juntamente com sua proposta comercial, documentação técnica (datasheets, manuais, cópia de documentos técnicos disponíveis publicamente no site do fabricante dos produtos etc.) dos produtos ofertados de modo a comprovar o atendimento de todos os requisitos técnicos da solução especificados neste Termo de Referência, além de permitir identificar de maneira inequívoca o modelo de produto proposto;

3. Será obrigatória demonstração de atendimento, na proposta comercial, de todos os requisitos exigidos por meio da indicação do número de páginas da documentação fornecido para cada Item/ Subitem das especificações técnicas descritas no Termo de Referência, conforme tabela do anexo 1-

ANÁLISE DO RECURSO APRESENTADO

Dos atestados de capacidade técnica apresentados, apenas 01 (hum) é semelhante ao tipo de produto ofertado pelo licitante para o certame. Com a nova página adicionando os quantitativos referentes a licitação do atestado em questão, o atestado evidencia o fornecimento em quantitativo equivalente a 10% do quantitativo solicitado.

Nível de Classificação	Grupo de acesso
Público	**Público**

Desta forma, **foi comprovado** o atendimento a este item do Edital.

Nível de Classificação	Grupo de acesso
Público	**Público**

CONCLUSÃO

Os documentos enviados adicionalmente pelo fornecedor foram analisados minuciosamente pela equipe técnica e constatou que não há evidências documentais suficientes para comprovar que a Solução ofertada pela empresa LICITANTE atende, **8 (oito) itens** dos itens do Edital.

Assim sendo, no nosso entendimento, a partir da documentação comprobatória apresentada no processo de licitação, a empresa ainda foi incapaz de evidenciar o atendimento a todos os requisitos técnicos do certame e, portanto, a partir dela, a equipe técnica não constatou que a mesma está apta a atender totalmente o objeto solicitado no certame.

Manaus, 17 de fevereiro de 2023

Lílian Gibson Santos

Gerente de Gerência de Segurança da Informação e Qualidade

Salim da Silva David

Gerência de Infraestrutura e Serviços de TI