JUSTIÇA FEDERAL
CONSELHO DA JUSTIÇA FEDERAL

DECISÃO

RELATÓRIO DE RECURSO - PREGOEIRA

ASSUNTO: Recurso contra decisão da pregoeira apresentado pela Empresa ALLTECH - SOLUÇÕES EM TECNOLOGIA LTDA.

REFERENTE: Pregão Eletrônico nº. 90.003/2024. - PROCESSO SEI n. 0001703-88.2023.4.90.8000

OBJETO: Contratação de solução de segurança para proteção de estações de trabalho, Data Center, e-mail corporativo e aplicativos Microsoft 365, contemplando instalação e configuração, transferência de conhecimento e, suporte técnico com garantia do fabricante do Conselho da Justiça Federal, pelo prazo de 36 meses, conforme as especificações e os quantitativos constantes do edital.

RECORRENTE: ALLTECH - SOLUÇÕES EM TECNOLOGIA LTDA.

RECORRIDA: BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA.

1. RELATÓRIO

Trata-se de resposta ao recurso interposto (id. 0556306) em contraposição à decisão da pregoeira que classificou a proposta da empresa BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA., no certame licitatório, conforme o relato que se segue abaixo.

A sessão do Pregão nº. 90.003/2024, teve início no dia 15/02/2024, às 10h. Após a fase da disputa de lances, constatou-se que a empresa BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA., apresentou a proposta de menor valor. Dessa forma, foi a primeira proposta a ser analisada. Em seguida, teve sua proposta classificada no dia 26/02/2024, por atender aos requisitos do edital, (id 0545788), a empresa não apresentou nenhuma restrição em contratar com o serviço público, conforme documentos apresentados pela empresa e certidões de "nada consta" acostadas aos autos (id. 0554644).

2. TEMPESTIVIDADE

Após a habilitação da empresa BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA., no Portal de Compras (www.gov.br/compras), foram abertos prazos para registro de intenção recursal, ficando delimitado da seguinte forma (id. 0554870):

Data limite para registro das razões: 29/02/2024;

Data limite para registro das contrarrazões: 05/03/2024; e

Data limite para registro de decisão da pregoeira: 19/03/2024.

As razões e as contrarrazões recursais foram registradas via Portal de Compras dentro do prazo, sem qualquer intercorrência sistêmica.

3. DAS RAZÕES DA RECORRENTE ALLTECH - SOLUÇÕES EM TECNOLOGIA LTDA (id. 0556306)

Em apertada síntese, assevera a recorrente que o ato que classificou a empresa BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA., foi equivocado quanto ao aceite da proposta da aludida empresa, *"...a RECORRIDA não tomou conhecimento prévio do edital e seus requisitos, resultando na oferta de uma solução com padrões de qualidade abaixo do mínimo definido no edital, ou seja, proposta que claramente NÃO ATENDE AO EDITAL, portanto, deveria ter sido inabilitada." (id. 0556306, fl. 4).*

Aduz, ainda, a recorrente, que a recorrida não está ofertando uma solução capaz de atender os requisitos mínimos exigidos, resultando em uma oferta de solução de qualidade muito inferior ao descrito no termo de referência, resultando em uma PROPOSTA que não atende ao EDITAL.

Na conclusão de sua petição, a recorrente pugna pelo "*PROVIMENTO total das presentes razões e justificativas, a fim de provocar uma revisão dos atos praticados, promovendo a desclassificação da empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA e convocação das demais licitantes*".

4. DAS CONTRARRAZÕES DA RECORRIDA - (id. 0557942)

A empresa recorrida sustenta, em resumo, que:

> a) diante das razões apresentadas em sua peça não há qualquer outra conclusão lógica que não a manutenção da r. Decisão Administrativa no tocante à classificação/ habilitação da Recorrida, por atender plenamente os requisitos previstos no Edital;
>
> b) NÃO SEJA ACOLHIDO O RECURSO ADMINISTRATIVO apresentado pela Recorrente, por total falta de veracidade dos pontos alegados e de fundamento técnico-jurídico, afastando-se quaisquer das razões ali elencadas, MANTENDO-SE A JUSTA DECLARAÇÃO DE VENCEDORA DA EMPRESA BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA.

5. DA ANÁLISE DA UNIDADE DEMANDANTE

Instada a manifestar-se a unidade demandante da Subsecretaria de Segurança da Tecnologia da Informação - SUSTI (id. 0559738), que os argumentos apresentados pela recorrente são descabidos, entendendo que:

> 1. Do Atendimento ao Item 5.81 – Sobre o item, esta EPC concorda com a contrarrazão, indicando o documento "es_admin_guide.pdf" páginas 97, 32, 115-118 e 66, com destaque as transcrições abaixo apresentadas pela recorrida.
>
> "Utilizando o mesmo documento citado pela recorrente em sua fala (es_admin_guide.pdf), podemos ir até a página 97 e constatar as seguintes capacidades de proteção presentes em apenas um, dos diversos módulos integrantes da solução ofertada, sendo o módulo de AntiSpam capaz de:
>
> • Enable advanced URL defense - Responsável pela análise de todos os links recebidos pelo por email, aplicando toda a inteligência do fabricante no combate a domínio e urls maliciosas.
>
> • Enable URL rewrite - Permite quando detectada uma url suspeita, reencaminhar o link para uma página do fabricante, de forma a impedir 100% dos casos de download de paylods maliciosos, roubo de credenciais por meio de phishing e variantes, etc.
>
> • Configure recipient validation settings - Pemite a validação de usuários na ferramenta de usuários do cliente e a recusa de mensagens para usuários inexistentes antes que as mesmas sejam entregues.
>
> • Configure settings for verifying sender authenticity - Controles de DNS comuns como SPF, DKIM e DMARC.
>
> • Configure the maximum message size accepted - Configuração de tamanho de mensagens.
>
> • Enable automatic release settings related to spam and viruses - Configuração do primeiro nível de classificação de mensagens, como spam e malware.
>
> • Enable quarantine and header tags for newsletters, mail magazines, and marketing emails - Configuração do segundo nível de mensagens SPAM, porém classificadas de acordo com o seu conteúdo, para que a empresa possa aplicar as ações necessárias.
>
> • Enable AS/AV scanning - Configuração da engine de antivirus.
>
> Já na página 32, do mesmo documento, obtemos do modo de configuração "Inline with Hygiene mode" que além de todas features já listadas, traz ainda toda a inteligência de reputação do fabricante para bloqueio de diversas ações maliciosas antes mesmo da comunicação SMTP ser iniciada, incluindo também o MVX que provê o recurso de sandbox avançada do fabricante que abrange tanto o teste de arquivos quanto URLs, protegendo inclusive contra ameaças de dia zero (0-day).
>
> Caminhando um pouco mais adiante, podemos ir até a página 115, mais precisamente no tópico "Managing riskware policies" que se estende até a página 119, trazendo apenas alguns exemplos de Técnicas, Táticas e Procedimentos de ataque que
>
> podem ser cobertos por políticas pré-programados e pré-alimentadas pelo fabricante, o que eleva e muito o nível de proteção, principalmente quando falamos de ataques do tipo "Living-off-the-land" que estão cada vez mais comuns.
>
> Por último, porém não menos importante, na página 66 temos o tópico "Managing custom rule policies" que prossegue algumas páginas a frente, proporcionando ao administrador da plataforma a criação de políticas que interagem com qualquer propriedade ou header da mensagem, de forma que praticamente qualquer controle desejado pela organização possa ser devidamente implementado, inclusive para possíveis ataques novos e não mapeados."
>
> 2. Do Atendimento ao Item 5.56 – Sobre o item, esta EPC concorda com a contrarrazão, visto a conformidade com a SOC2 que prevê entre seus elementos a disponibilidade de serviços, com destaque a transcrição abaixo apresentada pela recorrida.
>
> "Tais dados representam algumas certificações existentes para o ambiente SaaS que sustenta essa solução e por mais que o dado fale por si só, podemos ainda recorrer a uma fonte pública que descreve um pouco sobre os controles aplicados na certificação SOC 2 Type 2, vide a referência: https://secureframe.com/blog/soc-2-type-ii.
>
> Irrefutavelmente demonstrando-se um ambiente que possui porte computacional auto escalonável e controles avançados, a ponto de possuir tal certificação, ficam evidenciados inegavelmente a garantia sobre a disponibilidade da plataforma, bem como de seus dados e de seus clientes, e por conseguinte prevenindo ameaças do tipo DoS, que não retrata uma ameaça nova e nem mesmo avançada."
>
> 3. Do Atendimento ao Item 5.87 – Sobre o item, esta EPC concorda com a contrarrazão, conforme documento "es_admin_guide.pdf" páginas 97, 32, 115-118 e 66, com destaques as transcrições abaixo apresentadas pela

recorrida.

“Utilizando o mesmo documento citado pela recorrente em sua fala (es_admin_guide.pdf), podemos ir até a página 97 e avaliar as seguintes capacidades de proteção presentes apenas no módulo de antispam:

• Enable advanced URL defense - Responsável pela análise de todos os links recebidos pelo por email, aplicando toda a inteligência do fabricante no combate a domínio e urls maliciosas.

• Enable URL rewrite - Permite quando detectada uma url suspeita, reencaminhar o link para uma página do fabricante, de forma a impedir 100% dos casos de download de paylods maliciosos, roubo de credenciais por meio de phishing e variantes, etc.

• Configure recipient validation settings - Pemite a validação de usuários na ferramenta de usuários do cliente e a recusa de mensagens para usuários inexistentes antes que as mesmas sejam entregues.

• Configure settings for verifying sender authenticity - Controles de DNS comuns como SPF, DKIM e DMARC.

• Configure the maximum message size accepted - Configuração de tamanho de mensagens.

• Enable automatic release settings related to spam and viruses - Configuração do primeiro nível de classificação de mensagens, como spam e malware.

• Enable quarantine and header tags for newsletters, mail magazines, and marketing emails - Configuração do segundo nível de mensagens SPAM, porém classificadas de acordo com o seu conteúdo, para que a empresa possa aplicar as ações necessárias.

• Enable AS/AV scanning - Configuração da engine de antivirus.

Já na página 32, do mesmo documento, obtemos do modo de configuração “Inline with Hygiene mode” que além de todas features já listadas, traz ainda toda a inteligência de reputação do fabricante para bloqueio de diversas ações maliciosas antes mesmo da comunicação SMTP ser iniciada, incluindo também o MVX que é retrata o recurso de sandbox avançada do fabricante que abrange tanto o teste de arquivos quanto URLs, protegendo inclusive contra ameaças de dia zero (0-day).

Caminhando um pouco mais adiante, podemos ir até a página 115, mais precisamente no tópico “Managing riskware policies” que se estende até a página 119, trazendo apenas alguns exemplos de Técnicas, Táticas e Procedimentos de ataque que podem ser cobertos por políticas pré-programas e pré-alimentadas pelo fabricante, o que eleva e muito o nível de proteção, principalmente quando falamos de ataques do tipo “Living-off-the-land” que estão cada vez mais comuns.

Por último, porém não menos importante, na página 66 temos o tópico “Managing custom rule policies” que prossegue algumas páginas a frente, proporcionando ao administrador da plataforma a criação de políticas que interagem com qualquer propriedade ou header da mensagem, de forma que praticamente qualquer controle desejado pela organização possa ser devidamente implementado, inclusive para possíveis ataques novos e não mapeados”

4. Do Atendimento ao Item 5.103 e subitens 5.103.1, 5.103.2 e 5.103.3 – Sobre o item e subitens, esta EPC concorda com a contrarrazão conforme documento “es_admin_guide.pdf” páginas 66 e 130, com destaque a transcrição abaixo apresentada pela recorrida.

“Observando o documento (es_admin_guide.pdf), já enviando anteriormente na proposta, na página 66 temos o tópico “Managing custom rule policies” que prossegue algumas páginas a frente, proporcionando ao administrador da plataforma a criação de políticas que interagem com qualquer propriedade ou header da mensagem, de forma que praticamente qualquer controle desejado pela organização possa ser devidamente implementado, inclusive para possíveis ataques novos e não mapeados, tal recurso compreende todas as propriedades solicitadas no item, além de todas as demais informações citadas até então.

No mesmo documento, na página 130, temos ainda o tópico “Azure AD syncing” que representa a leitura/importação de todos os usuários/grupos para que os mesmos possam ser utilizados na plataforma”

5. Do Atendimento ao Item 5.122 – Sobre o item, esta EPC concorda com a contrarrazão conforme documento “es_admin_guide.pdf” página 146, com destaque a transcrição abaixo apresentada pela recorrida.

“Observando o documento (es_admin_guide.pdf), já enviado anteriormente na proposta, na página 146 temos a configuração de um servidor com Rsyslog para encaminhamento de logs para qualquer destino desejado.”

6. Do Atendimento ao Item 5.130 – Sobre o item, esta EPC concorda com a contrarrazão conforme documento “es_admin_guide.pdf” página 216, com destaque a transcrição abaixo apresentada pela recorrida.

“Observando o documento (es_admin_guide.pdf), já enviando anteriormente na proposta, na página 216 temos o tópico “Quarantine filtering and searching” que apresenta nas páginas seguintes todas as características solicitadas no item, não havendo que se falar em qualquer inconsistência entre a solução ofertada e o exigido no edital.”

7. Do Atendimento ao Item 7.33 – Sobre o item, esta EPC concorda com a contrarrazão contida no link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrida.

“A comprovação utilizada no link: https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Incidents/Policy_Incidents/Quarantined_Files, visava demonstrar, de forma objetiva, a possibilidade de quarentenar os arquivos, como forma de contenção, e status dos arquivos após a quarentena. A recorrente claramente ignora, ou o mais provável, desconhece propositadamente as informações registradas na página, pelos trechos em destaque abaixo:

• Deleted. The file has been permanently removed from the cloud service provider.

• Restored. The file has been restored to its original location, the tombstone has been removed, and an email was sent to the user.

• Auto Restored. The file has been restored automatically based on Auto Restore settings and an email was sent to

the user.

• Processing. The quarantine is still in process.

• Failed. Restore or delete operation failed due to a service disruption, connectivity issues, etc.

• Quarantine Unsuccessful. Skyhigh CASB could not quarantine a file even after multiple attempts. This could be caused by:

• A user is editing the document, so the file is locked and cannot be quarantined by Skyhigh Security.

• Data retention is enabled in Microsoft Office 365, and that is preventing Skyhigh Security from quarantining or deleting the data.

Ou seja, desta maneira evidencia-se, tanto pela imagem apresentada na URL, quanto pelas informações em destaque que é comum à plataforma, operar contenção, sobre arquivos detectados, de maneira a:

• Deleta-los

• Quarentena-los

• Restaura-los. ”

8. Do Atendimento ao Item 7.49 – Sobre o item, esta EPC concorda com a contrarrazão conforme documento “es_admin_guide.pdf” página 190, com destaque a transcrição abaixo apresentada pela recorrida.

“Observando o documento (es_admin_guide.pdf), já enviando anteriormente na proposta, na página 190 temos o tópico “Email executive summary” que apresenta nas páginas seguintes todas as características solicitadas no item, com sobra.”

9. Do Atendimento ao Item 8.36 – Sobre o item, esta EPC concorda com a contrarrazão contida no link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrida.

“Observando o documento citado https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-dbec0981-b6ddc9f3-367a-a8ccf9c84e23.html, evidenciam-se, dados que já permitem a classificação e indicação de diversos níveis diferentes. Ainda no mesmo documento, porém em uma sessão diferente, temos o seguinte link https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-32d28d65-5100-cc4c-edd5-5d35be4c87f4.html, onde já existe a clara correlação da plataforma e seus dados com o framework do MITRE, Framework este, aderente ao objetivos preconizados pelo NIST, mas ainda superior no quesito granularidade e expertise em táticas, técnicas e procedimentos de ataques cibernéticos, compreendendo não somente, todos os quesitos oferecidos pelo NIST, como ainda provendo melhor orientação quanto à compreensão das muitas e variadas formas de ameaça cibernética, onde todas as detecções terão associação automática com as Técnicas, Táticas e Procedimentos, presentes no framework citado, que pode ser lido no seguinte link https://attack.mitre.org/. Uma interpretação rápida dos dados já é capaz de esclarecer, que as informações mapeadas corroboram para apoio no atendimento de requisitos presentes no framework do NIST e também muitos outros existentes atualmente.”

10. Do Atendimento ao Item 8.37 – Sobre o item, esta EPC concorda com a contrarrazão contida no link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrida.

“Dessa forma, e para dissuadir quaisquer possíveis dúbias intenções da recorrente, esclarecemos que no mesmo link referenciado na pesquisa apresentada – que aparenta ter sido realizada com intenção única e descabida de depreciar a oferta aceita pela licitante, portanto, vencedora deste certame, já é possível, constatar que há sim, um dashboard global de risco da organização, bastando-se buscar pela palavra “risk”, já se obteria a informação que comprova o item refutado.”

11. Do Atendimento ao Item 8.38 – Sobre o item, esta EPC concorda com a contrarrazão contida no link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrida.

“Contribuindo para a veracidade dos fatos, o link https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-885433ce-9217-cfac-e6eb-6afb15513d96.html e sub-páginas, encontradas no mesmo sítio web, permitem a observação de inúmeras evidências quanto a capacidade contestada. Partindo da seção “Investigation Tips” que proporcionam não apenas dicas de remediação, mas também um direcionamento claro e inequívoco (sugestões) quanto à investigação, para que o hunting de ameaças se torne de fato possível e o administrador/operador da plataforma, possa economizar horas de trabalho investigativo.

Estendemos ainda o esclarecimento, ao painel de risco por ameaça, através do link https://docs.trellix.com/bundle/helix_pg/page/UUID-84d8f696-4c40-1605-3145-b1c9c0292973.html, onde se pode notar, que cada incidente retratado, dispõe de uma nota de risco, que é fruto do motor de inteligência artificial da plataforma, motor este, capaz de atribuir risco ao incidente com base comportamento de cada ativo ou usuário da organização, e ainda na severidade de cada ocorrência suspeita ou maliciosa atrelada ao referido incidente. Ver link para referência no cálculo de risco https://docs.trellix.com/bundle/helix_pg/page/UUID-64524f51-71d6-6c7b-8683-173222bee874.html

Sendo assim, há de fato, orientação sobre a resposta a incidentes da organização, oportunamente guiada às entidades mais recorrentemente associadas a riscos, facilitando a priorização, já que estas, tendem a oferecer mais risco de comprometimento, por conseguinte, auxiliando a organização, a definir e priorizar as ações de mitigação dentro da urgência adequada, inclusive com suporte a identificação de ativos e usuários, de acordo com a relevância intrínseca à sua organização, (usuários e ativos VIPs), ver link para referência https://docs.trellix.com/bundle/helix_pg/page/UUID-b4366c71-9a71-d289-101c-848cbcc9bee6.html

Aprofundando mais ainda nas capacidades de suporte à tomada de decisão, a plataforma ainda oferece outros inúmeros métodos de orientação quanto à mitigação de riscos e incidentes, e para que não reste dúvidas, segue explicado em termos claros e objetivos, apenas alguns, desses recursos.

Descrição clara e objetiva sobre as características do ataque: Ver imagem 3, https://docs.trellix.com/bundle/helix_pg/page/UUID-32d28d65-5100-cc4c-edd5-5d35be4c87f4.html

Identificação imediata de indicadores globais de ameaça pela conjunção de feeds próprios (nativos) de Threat Intelligence:

https://docs.trellix.com/bundle/helix_pg/page/UUID-034abcc7-3022-d8c7-e91f-fce9d9badb9f.html é possível observar no item 2, todos os dados de um alerta, porém indicado em vermelho, a orientação quanto ao bloqueio de um indicador malicioso (hash), que fora apontado automaticamente pelo motor integrado de threat intelligence. Depreende-se portanto, que não somente são oferecidas medidas de mitigação, bem como são apontadas de forma imediata a recomendação do fabricante sobre quais indicadores são nocivos dentro do incidente de maneira facilitada.

Ainda é possível obter dentro da plataforma, no painel de investigação, referência direta quanto à mitigação de táticas, técnicas e procedimentos conforme a visão global do mitre framework: https://docs.trellix.com/bundle/helix_pg/page/UUID-bebe7bfe-f045-7791-8c3f-cda24e9929e8.html onde cada Tática, Técnica ou Procedimento é referenciado diretamente nesta visão global através de links diretos, que indicam de maneira objetiva todos os detalhes sobre os métodos de ataque, e formas de investigação e mitigação, conforme link: https://attack.mitre.org/techniques/T1090/ seção Mitigations.

Por fim, mas não menos importante, todos as métricas de risco, compõem ainda um dashboard que indica em gráfico de linha, o risco acumulado da organização (risco total), que pode ser exibido dentro de linhas de tempo especifica, como últimas 24 horas, últimos dias, últimos 30 dias e último ano, conforme evidenciado no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-dc833c8f-1e7b-5d54-e4fe-a14d9e6f8e7f.html ficando portanto esclarecido, de maneira irremediável e inequívoca as plenas capacidades de atendimento do item em questão da plataforma ofertada."

12. Do Atendimento ao Item 8.39 – Sobre o item, esta EPC concorda com a contrarrazão conforme documento "trellix_insights_product_guide.pdf" e link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrida.

"Ainda, diante de tamanho e inverossímil ataque, destacamos duas funcionalidades agregadas nativamente, que permitem atender de maneira inegável o item contestado, oferecendo ainda ampla granularidade sobre os pontos discorridos, a saber:

• Estendemos ainda o esclarecimento, ao painel de risco por ameaça, através do link https://docs.trellix.com/bundle/helix_pg/page/UUID-84d8f696-4c40-1605-3145-b1c9c0292973.html, onde se pode notar, que cada incidente retratado, dispõe de uma nota de risco, que é fruto do motor de inteligência artificial da plataforma, motor este, capaz de atribuir risco ao incidente com base comportamento de cada ativo ou usuário da organização, e ainda na severidade de cada ocorrência suspeita ou maliciosa atrelada ao referido incidente. Ver link para referência no cálculo de risco https://docs.trellix.com/bundle/helix_pg/page/UUID-64524f51-71d6-6c7b-8683-173222bee874.html. Sendo assim, há de fato, orientação sobre a resposta a incidentes da organização, oportunamente guiada às entidades mais recorrentemente associadas a riscos, facilitando a priorização, já que estas, tendem a oferecer mais risco de comprometimento, por conseguinte, auxiliando a organização, a definir e priorizar as ações de mitigação dentro da urgência adequada, inclusive com suporte a identificação de ativos e usuários, de acordo com a relevância intrínseca à sua organização, (usuários e ativos VIPs), ver link para referência https://docs.trellix.com/bundle/helix_pg/page/UUID-b4366c71-9a71-d289-101c-848cbcc9bee6.html

• A partir do motor integrado Trellix Insights, a plataforma Trellix XDR é capaz de monitorar campanhas, atores e indicadores maliciosos em todo o planeta, em meio à toda telemetria obtida de maneira agnóstica pela plataforma. Porém, as funções do Trellix Insights se estendem à essa capacidade, conferindo ainda à organização, um portal de pesquisa global, que provê as informações exemplificadas abaixo:

o Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.

o Ataques associados à uma ou mais indústrias e comparativos do cenário global de ameaças, com o perfil e postura de risco da organização.

o Validação automática de postura de segurança da organização, com base nos indicadores de threat intelligence fornecidos pela plataforma, conjugadas a oportunidades de melhorias em configurações nos motores de proteção da plataforma (Varreduras e proteções contra exploits, e comportamentos.)

o Medidas preditivas (proativas) de segurança, permitindo à organização, precaver-se contra uma ou mais campanhas, ataques, atores, ou indicadores pesquisáveis dentro da plataforma.

o Guias de recomendação em mitigação e prevenção contra a mera hipótese desses ataques ou campanhas serem desferidos contra o ambiente, oferecendo:

▪ Lista de dispositivos em risco, sejam os que requerem atualização da proteção ou aqueles com ações de mitigação pendentes.

▪ Listas de indicadores pertencentes a campanhas ou ataques, para pesquisa em tempo real no ambiente.

▪ Recomendação de ações de defesa (playbooks de defesa, contra ataques ou campanhas em específico. Ver detalhes em: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-f0364034-02a4-ec8d-c787-88fea1a22490.html

Referência: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-142f8922-bb9d-45c6-cab5-09a26c50d235.html e https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-1ee12346-846f-1a91-c0f1-3f3cea77c65c.html"

13. Do Atendimento ao Item 8.42 – Sobre o item, esta EPC concorda com a contrarrazão conforme link internet fornecido com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

"A partir do motor integrado Trellix Insights, a plataforma Trellix XDR é capaz de monitorar campanhas, atores e indicadores maliciosos em todo o planeta, em meio à toda telemetria obtida de maneira agnóstica pela plataforma. Porém, as funções do Trellix Insights se estendem à essa capacidade, conferindo ainda à organização, um portal de pesquisa global, que provê as informações exemplificadas abaixo:

o Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.

o Ataques associados à uma ou mais indústrias e comparativos (benchmarking) do cenário global de ameaças, com o perfil e postura de risco da organização.

o Validação automática de postura de segurança da organização, com base nos indicadores de threat intelligence fornecidos pela plataforma, conjugadas a oportunidades de melhorias em configurações nos motores de proteção da plataforma (Varreduras e proteções contra exploits, e comportamentos.)

o Medidas preditivas (proativas) de segurança, permitindo à organização, precaver-se contra uma ou mais campanhas, ataques, atores, ou indicadores pesquisáveis dentro da plataforma.

o Guias de recomendação em mitigação e prevenção contra a mera hipótese desses ataques ou campanhas serem desferidos contra o ambiente, oferecendo:

▪ Lista de dispositivos em risco, sejam os que requerem atualização da proteção ou aqueles com ações de mitigação pendentes.

▪ Listas de indicadores pertencentes a campanhas ou ataques, para pesquisa em tempo real no ambiente.

▪ Recomendação de ações de defesa (playboos de defesa, contra ataques ou campanhas em específico. Ver detalhes em: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-f0364034-02a4-ec8d-c787-88fea1a22490.html

Referência: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-142f8922-bb9d-45c6-cab5-09a26c50d235.html e https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-1ee12346-846f-1a91-c0f1-3f3cea77c65c.html"

14. Do Atendimento ao Item 8.46 – Sobre o item, esta EPC concorda com a contrarrazão com a documentação e link internet fornecido com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

"No link https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-885433ce-9217-cfac-e6eb-6afb15513d96.html e suas sub-páginas, encontradas no mesmo sítio web, é possível a observação de inúmeras evidências quanto a capacidade contestada. Partindo da seção "Investigation Tips" que proporcionam não apenas dicas de remediação, mas também um direcionamento claro e inequívoco (sugestões) quanto à investigação, para que o hunting de ameaças se torne de fato possível e o administrador/operador da plataforma, possa economizar horas de trabalho investigativo.

Estendemos ainda o esclarecimento, ao painel de risco por ameaça, através do link https://docs.trellix.com/bundle/helix_pg/page/UUID-84d8f696-4c40-1605-3145-b1c9c0292973.html, onde se pode notar, que cada incidente retratado, dispõe de uma nota de risco, que é fruto do motor de inteligência artificial da plataforma, motor este, capaz de atribuir risco ao incidente com base comportamento de cada ativo ou usuário da organização, e ainda na severidade de cada ocorrência suspeita ou maliciosa atrelada ao referido incidente. Ver link para referência no cálculo de risco https://docs.trellix.com/bundle/helix_pg/page/UUID-64524f51-71d6-6c7b-8683-173222bee874.html

Sendo assim, há de fato, orientação sobre a resposta a incidentes da organização, oportunamente guiada às entidades mais recorrentemente associadas a riscos, facilitando a priorização, já que estas, tendem a oferecer mais risco de comprometimento, por conseguinte, auxiliando a organização, a definir e priorizar as ações de mitigação dentro da urgência adequada, inclusive com suporte a identificação de ativos e usuários, de acordo com a relevância intrínseca à sua organização, (usuários e ativos VIPs), ver link para referência https://docs.trellix.com/bundle/helix_pg/page/UUID-b4366c71-9a71-d289-101c-848cbcc9bee6.html

Aprofundando mais ainda nas capacidades de suporte à tomada de decisão, a plataforma ainda oferece outros inúmeros métodos de orientação quanto à mitigação de riscos e incidentes, e para que não reste dúvidas, segue explicado em termos claros e objetivos, apenas alguns, desses recursos.

Descrição clara e objetiva sobre as características do ataque: Ver imagem 3, https://docs.trellix.com/bundle/helix_pg/page/UUID-32d28d65-5100-cc4c-edd5-5d35be4c87f4.html

• Identificação imediata de indicadores globais de ameaça pela conjunção de feeds próprios (nativos) de Threat Intelligence: https://docs.trellix.com/bundle/helix_pg/page/UUID-034abcc7-3022-d8c7-e91f-fce9d9badb9f.html é possível observar no item 2, todos os dados de um alerta, porém indicado em vermelho, a orientação quanto ao bloqueio de um indicador malicioso (hash), que fora apontado automaticamente pelo motor integrado de threat intelligence. Depreende-se, portanto, que não somente são oferecidas medidas de mitigação, bem como são apontadas de forma imediata a recomendação do fabricante sobre quais indicadores são nocivos dentro do incidente de maneira facilitada.

• Ainda é possível obter dentro da plataforma, no painel de investigação, referência direta quanto à mitigação de táticas, técnicas e procedimentos conforme a visão global do mitre framework: https://docs.trellix.com/bundle/helix_pg/page/UUID-bebe7bfe-f045-7791-8c3f-cda24e9929e8.html onde cada Tática, Técnica ou Procedimento é referenciado diretamente nesta visão global através de links diretos, que indicam de maneira objetiva todos os detalhes sobre os métodos de ataque, e formas de investigação e mitigação, conforme link: https://attack.mitre.org/techniques/T1090/ seção Mitigations.

• Por fim, mas não menos importante, todos as métricas de risco, compõem ainda um dashboard que indica em gráfico de linha, o risco acumulado da organização (risco total), que pode ser exibido dentro de linhas de tempo especifica, como últimas 24 horas, últimos dias, últimos 30 dias e último ano, conforme evidenciado no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-dc833c8f-1e7b-5d54-e4fe-a14d9e6f8e7f.html ficando portanto esclarecido, de maneira irremediável e inequívoca as plenas capacidades de atendimento do item em questão da plataforma ofertada.

Ainda, quanto a recomendações com base na postura de segurança, destacamos uma das funcionalidades agregadas nativamente, que permitem atender de maneira inegável o item contestado, oferecendo ainda ampla granularidade sobre os pontos discorridos, a saber:

• A partir do motor integrado Trellix Insights, a plataforma Trellix XDR é capaz de monitorar campanhas, atores e indicadores maliciosos em todo o planeta, em meio à toda telemetria obtida de maneira agnóstica pela plataforma.

Porém, as funções do Trellix Insights se estendem à essa capacidade, conferindo ainda à organização, um portal de pesquisa global, que provê as informações exemplificadas abaixo:

o Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.

o Ataques associados à uma ou mais indústrias e comparativos do cenário global de ameaças, com o perfil e postura de risco da organização.

Validação automática de postura de segurança da organização, com base nos indicadores de threat intelligence fornecidos pela plataforma, conjugadas a oportunidades de melhorias em configurações nos motores de proteção da plataforma (Varreduras e proteções contra exploits, e comportamentos.)

o Medidas preditivas (proativas) de segurança, permitindo à organização, precaver-se contra uma ou mais campanhas, ataques, atores, ou indicadores pesquisáveis dentro da plataforma.

o Guias de recomendação em mitigação e prevenção contra a mera hipótese desses ataques ou campanhas serem desferidos contra o ambiente, oferecendo:

▪ Lista de dispositivos em risco, sejam os que requerem atualização da proteção ou aqueles com ações de mitigação pendentes.

▪ Listas de indicadores pertencentes a campanhas ou ataques, para pesquisa em tempo real no ambiente.

▪ Recomendação de ações de defesa (playboos de defesa, contra ataques ou campanhas em específico. Ver detalhes em:https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-f0364034-02a4-ec8d-c787-88fea1a22490.html

Referência: https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-142f8922-bb9d-45c6-cab5-09a26c50d235.html e

https://docs.trellix.com/bundle/trellix-insights-product-guide/page/UUID-1ee12346-846f-1a91-c0f1-3f3cea77c65c.html"

15. Do Atendimento quanto aos Itens 8.47 e 8.48 – Sobre os itens, esta EPC concorda com a contrarrazão indicando o documento "trellix_insights_product_guide.pdf" página 7 e 37, link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

"... iremos em meticulosos detalhes explicar como a solução Trellix é composta, e oferece total visão de riscos sobre:

• As entidades (usuários e ativos)

o Cada usuário ou computador (entidades) é obtido pela plataforma, junto às integrações realizadas, com tecnologias terceiras de maneira agnóstica, como Active Directory, Office365, Firewalls, Proxies, Endpoint Protection dentre outras centenas de integrações. A partir disso, cada entidade é monitorada continuamente e essa monitoração é feita pela nota de risco atribuída e acumulada ao longo do tempo por cada evento suspeito ou malicioso oriundo dessa entidade. Essas entidades podem ainda receber o status de VIP, essa configuração é designada para elencar os usuários da alta gestão ou de alta relevância para a organização, se tornando assim entidades cuja prioridade no tratamento de incidentes será maior. Essa prioridade é apresentada por um valor nomeado Asset Risk Score (Pontuação de risco do ativo em tradução livre). Essa informação é apresentada de maneira objetiva no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-64524f51-71d6-6c7b-8683-173222bee874.html

• Os alertas e incidentes

o Os alertas são eventos suspeitos ou malicisos (Alerts), que podem compor um ou mais casos em tratamento (Cases), ou mesmo incidentes deflagrados pelo motor anti-ameaça (Threat). Toda essa mecanica permite à organização, não somente a visualização de eventos indesejados, dentro de uma correlação entre diferentes ativos e vetores de proteção, ou individualmente, podendo ainda agrupar esses eventos em investigações separadas. O risco pela visão dos incidentes em aberto e todos os detalhes apurados no painel de visualização dos alertas da plataforma podem ser vistos no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-36ec00cd-21a3-2652-eebe-9860800f8e0b.html

• A organização

o O risco total da organização é uma métrica que resume todos os riscos associados dentre a severidade dos incidentes, somados aos riscos de cada entidade associada nesses incidentes. Este panorama geral é visto em dois paineis, o painel total de riscos visto no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-dc833c8f-1e7b-5d54-e4fe-a14d9e6f8e7f.html

• Os setores e a indústria da sociedade

o A partir do motor integrado Trellix Insights, a plataforma Trellix XDR é capaz de monitorar campanhas, atores e indicadores maliciosos em todo o planeta, em meio à toda telemetria obtida de maneira agnóstica pela plataforma. Porém, as funções do Trellix Insights se estendem à essa capacidade, conferindo ainda à organização, um portal de pesquisa global, que provê as informações exemplificadas abaixo:"

16. Do Atendimento ao Item 8.50 – Sobre o item, esta EPC concorda com a contrarrazão indicando que a solução ofertada para atendimento é um SOAR conforme documento "fso.pdf" página 8, com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

"A documentação apresentada é suficiente para o atendimento do item, uma vez que a solução apresentada, dentro da plataforma de XDR da Trellix, representa um SOAR, ou seja, tais operações listadas são consideradas básicas frente a sua capacidade de execução de tarefas e integrações. Segue abaixo a íntegra do mesmo texto referenciado em proposta para contemplação:

"About Security Orchestrator

Security Orchestrator (SO) is an open playbook platform that integrates Security Orchestrator and third-party products and services to provide effective threat detection and event response for your system. Security

Orchestrator provides a playbook builder interface that allows you to model procedures, and a plug-in API architecture to integrate external systems into your playbooks.

Security Orchestrator initiates automated workflows called playbooks. These automated workflows can complete automated tasks and request human intervention to complete manual tasks. Playbooks can create cases and escalate important alerts or events. You can create playbooks and customize Security Orchestrator pre-configured playbooks to meet the needs of your organization using the Playbook Builder.

With the variety of Security Orchestrator plug-ins provided by FireEye, you can perform a diverse set of tasks using Playbooks and develop plug-ins to extend your Security

Orchestrator capabilities. Existing plug-ins can integrate created playbooks with many kinds of products and services, including:

- FireEye appliances and tools
- Threat intelligence services
- Malware analysis tools
- Security information and event management (SIEM) tools
- Cloud-based storage
- Ticketing and issue tracking systems
- Endpoints
- Firewalls
- Switches
- Sandbox tools
- Email servers
- Chat tools
- Mobile devices”

Claramente as capacidades de integração e automação de tarefas por este recurso é praticamente infinito, superando em muito, não somente todos os itens requeridos pela especificação técnica, mas que também estarão garantidos à organização, abrangência até mesmo de futuras plataformas a serem por ela adquiridas, uma vez que não há a cobrança de créditos por tipo de tecnologia ou função a ser orquestrada, sendo portanto, livre de qualquer custo adicional, toda e qualquer tecnologia alcançável por este componente universal.”

17. Do Atendimento ao Item 8.67 – Sobre o item, esta EPC concorda com a contrarrazão indicando os documentos “trellix_insights_product_guide.pdf.” página 83-84, “trellix_endpoint_detection_and_response_product_guide.pdf” página 63-70, com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

“O link https://docs.trellix.com/bundle/helix_dscg/page/UUID-3d04119d-b16b-7e2d-84e1-390d8ca86fec.html foi apresentado em comprovações pertinentes ao mesmo, o que comprova a capacidade da ferramenta de interação com praticamente qualquer tipo de plataforma que consiga enviar syslog.

Não restam dúvidas quanto à capacidade da plataforma de agir de forma integrada no ambiente correlacionando eventos e orquestrando a resposta de forma automatizada, implementando o real conceito de XDR.”

18. Do Atendimento ao Item 8.68.9 – Sobre o item, esta EPC concorda com a contrarrazão, com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

“A comprovação deste item tão básico já fora atestada em outros itens, mas para fins de comprovação contra infundadas alegações, reiteramos que o atendimento pode ser facilmente observado no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-bad6c927-dd95-ea6e-d9ca-0bee5f0df212.html já utilizado anteriormente, onde todos os status do alerta podem ser consultados.

Adicionalmente, para que não restem dúvidas, questionamentos ou alegações de quaisquer naturezas, as funções requeridas são alcançadas pelas opções descritas em detalhes abaixo:

• Assign: Com esta função, é possível designar um operador da plataforma que fará a investigação/tratamento do aleta/incidente em questão, tornando o alerta em status de em análise. Ver link: https://docs.trellix.com/bundle/helix_pg/page/UUID-bbf26257-4ebe-2a15-6140-e92d6768422d.html

• Closing and reopening an alert: Obviamente que um novo alerta estará automaticamente considerado com o status de NOVO, no entanto, uma das funções na gestão dos alertas é poder fechar ou até mesmo reabrir um alerta já fechado.

• Suppressing alerts: Funcionalidade adicional, a função suprimir pode ser desejada quando um alerta deve ter sua exibição interrompida, por qualquer motivo desejado pela organização. Essa supressão pode ser automaticamente interrompida em diversas opções de periodos

• Também é possível qualificar a detecção como um positivo verdadeiro ou falso negativo, sendo cada opção, utilizada automaticamente pela plataforma para apurar o motor de detecção.

Extensivamente, ainda destacamos que a plataforma possui mecanismo adicional de gerenciamento para ameaças, que podem ser um conjunto de alertas ou uma única ocorrência. A funcionalidade desse mecanismo é fornecer a experiência gráfica que permite a compreensão imediata dos variados eventos dentre todos os vetores correlacionados. Este mecanismo permite da mesma forma que o gerenciamento de alertas, a definição de status durante o progresso da investigação/mitigação da ameaça. Como pode ser visto no link a seguir, item STATUS: https://docs.trellix.com/bundle/helix_pg/page/UUID-3257cbf6-855e-3ecc-10b3-b2d1851c2195.html.”

19. Do Atendimento ao Item 8.80 e subitens (8.80.1 a 8.80.6) – Sobre o item e subitens, esta EPC concorda com a contrarrazão com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

“• Quanto ao índice de risco da empresa:

o O risco total da organização é uma métrica que resume todos os riscos associados dentre a severidade dos incidentes, somados aos riscos de cada entidade associada nesses incidentes. Este panorama geral é visto em dois paineis, o painel total de riscos visto no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-dc833c8f-1e7b-5d54-e4fe-a14d9e6f8e7f.html

• Quanto ao mapeamento das Táticas, Técnicas e Procedimentos conforme o Mitre ATT&CK:

o É possível obter dentro da plataforma, no painel de investigação, referência direta quanto à mitigação de táticas, técnicas e procedimentos conforme a visão global do mitre framework: https://docs.trellix.com/bundle/helix_pg/page/UUID-bebe7bfe-f045-7791-8c3f-cda24e9929e8.html onde cada Tática, Técnica ou Procedimento é referenciado diretamente nesta visão global através de links diretos, que indicam de maneira objetiva todos os detalhes sobre os métodos de ataque, e formas de investigação e mitigação, conforme link: https://attack.mitre.org/techniques/T1090/ seção Mitigations.

• Quanto à visão geral de alertas:

o Os alertas são eventos suspeitos ou malicisos (Alerts), que podem compor um ou mais casos em tratamento (Cases), ou mesmo incidentes deflagrados pelo motor anti-ameaça (Threat). Toda essa mecânica permite à organização, não somente a visualização de eventos indesejados, dentro de uma correlação entre diferentes ativos e vetores de proteção, ou individualmente, podendo ainda agrupar esses eventos em investigações separadas. O risco pela visão dos incidentes em aberto e todos os detalhes apurados no painel de visualização dos alertas da plataforma podem ser vistos no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-36ec00cd-21a3-2652-eebe-9860800f8e0b.html

• Quanto ao Top 10 vulnerabilidades em Risco:

o Por se tratar de um grande "data lake" agnóstico, capaz de se conectar a produtos Trellix e não-Trellix, como Rapid7, tenable, Qualys, Palo Alto, dentre outros, ver link https://docs.trellix.com/bundle/helix_dscg/page/UUID-869ff55d-4310-22a3-77d0-43ebea1028ff.html , as vulnerabilidades podem ser listadas em dashboards específicos na plataforma, dentro de uma tecnologia em específico, ou até mesmo pesquisadas dentre todos os vetores globais de proteção correlacionados. Como exemplo:

"▪ Em plataforma específica: Palo Alto Threat Vulnerability Monitoring"

▪ Dados globais: Em meio à todos os vetores integrados à plataforma, mesmo diferentes fontes de dados, são exibidas de uma maneira unificada, sendo portanto, normalizado automaticamente todos os eventos recebidos em uma mecânica de exibição única, sejam eles de soluções proteção a endpoint, como o da própria Trellix, ou mesmo outros, como soluções especificas de levantamento e gerenciamento de vulnerabilidades. Dessa maneira, a plataforma reserva em sua taxonomia de dados, um campo (metaclass) para identificar os chamados CVEID pelo seu identificador (Common vulnerabilities) ou nível de exposição (Exposures Identifier), conforme comprovado em: https://docs.trellix.com/bundle/xdr_tql/page/UUID-66c27d75-a198-113e-babd-75d86346a69d.html

Portanto a visão de Vulnerabilidades da ferramenta não é meramente identificada a partir da falta de patches em estações e servidores, mas sim em todo o conjunto de ingestão de eventos e integrações realizadas no ambiente, trazendo a visão específica e especializada de cada tecnologia de proteção, o que permite a extração de uma informação mais assertiva, confiável e certamente mais relevante.

• Quanto aos itens Top 10 usuários em Risco ao Top 10 dispositivos em Risco:

Esta comprovação, para fins de celeridade e bom uso do tempo, será respondida em evidência única, já que na plataforma ofertada estes itens são vistos em painel único, possuindo filtro adequado para isolar somente o grupo desejado (se usuários ou dispositivos, ou ambos).

Cada usuário ou computador (entidades) é obtido pela plataforma, junto às integrações realizadas, com tecnologias terceiras de maneira agnóstica, como Active Directory, Office365, Firewalls, Proxies, Endpoint Protection dentre outras centenas de integrações. A partir disso, cada entidade é monitorada continuamente e essa monitoração é feita pela nota de risco atribuída e acumulada ao longo do tempo por cada evento suspeito ou malicioso oriundo dessa entidade. Essas entidades podem ainda receber o status de VIP, essa configuração é designada para elencar os usuários da alta gestão ou de alta relevância para a organização, se tornando assim entidades cuja prioridade no tratamento de incidentes será maior. Essa prioridade é apresentada por um valor nomeado Asset Risk Score (Pontuação de risco do ativo em tradução livre). Essa informação é apresentada de maneira objetiva no link: https://docs.trellix.com/bundle/helix_pg/page/UUID-5d17a86c-de83-5bfa-775f-e067da3a92db.html e https://docs.trellix.com/bundle/helix_pg/page/UUID-d520f6cb-8bca-2072-a115-c0c697ea6fb9.html (ver item ASSET TYPE: Host, USER, ALL)."

20. Do Atendimento quanto aos Itens 9.2 e 9.48 – Sobre os itens, esta EPC concorda com a contrarrazão de acordo com o documento "9.7 e 9.10.pdf", com destaque a transcrição abaixo apresentada pela recorrida.

"No item de número 9.2 é solicitado que haja a possibilidade de implementação, através de port mirror, também conhecido como PORT-SPAN ou TAP,que são modos diferentes (ambos suportados pela solução Trellix NDR Network Security), mas que se utilizam da cópia de tráfego da rede.

(...)

Fica evidenciado portanto que a solução em questão, oferece o suporte requerido para o modo de integração via cópia de tráfego, que também é chamado de Port Mirror ou Port SPAN, sendo ainda possível, dada a tamanha flexibilidade da plataforma ofertada e já inclusive aceita pela licitante, que outros modos por vias de cópia sejam utilizados, como o TAP

Entretanto, destaca-se ainda que a solução também é capaz de oferecer, dentro da mesma plataforma, modalidade de integração mais efetiva, partindo-se da arquitetura de "posicionamento", inline ou em linha, o que confere além de todo mais, a capacidade preventiva e proativa de combate a ameaças, o que está em acordo com o item 9.7 da especificação técnica: "9.7. Deve permitir que seja implantada em linha com o tráfego de rede, e deve ser capaz de ser instalada em modo de espelhamento de rede.", que requer exatamente esta capacidade"

21. Do Atendimento quanto aos Itens 9.98 e 9.99 – Sobre os itens esta EPC concorda com a contrarrazão indicando o documento "network_security_user_guide.pdf" páginas 15, 17 e 233-235, link internet fornecido, com destaque

a transcrição abaixo apresentada pela recorrida.

“Quanto ao item 9.98;

• A Trellix considera mera obrigatoriedade que seus produtos falem entre si, o termo integração é empregado quando permitimos a capacidade de agregar múltiplas fontes de dados através plataformas terceiras, e nesse quesito a Trellix é referência mundial, possuindo centenas de integrações agnósticas. Contudo, o item exige que a plataforma NDR seja integrável com sua própria solução de NDR, portanto, vamos a tal comprovação:

o Nas páginas 233 a 235, do manual Network_Security_User_Guide.pdf, é possível ver nas seções:

▪ Helix Integration: As capacidades de integração nativa da plataforma Trellix NDR com o Trellix XDR, também conhecido como Helix. Um pequeno trecho desta capacidade está descrito abaixo e traduzida logo em seguida:

▪ Original: When you enable integration between Helix and the Network Security appliance, the Evidence Collector module on the Network Security appliance sends the network event logs to Helix for further analysis. The Evidence Collector module is a log aggregator that collects logs generated by the Network Security appliance. You also can configure your own custom filter rules or reset the rules to the default rules that Trellix provides to filter out each event type (HTTP, SMTP, DNS, TLS, and so forth) based on the JSON value and the corresponding event field on the Network Security appliance.

▪ Traduzido: Quando você habilita a integração entre o Helix e a plataforma Network Security, o módulo Evidence Collector no dispositivo Network Security envia os logs de eventos de rede para o Helix para análise adicional. O módulo Evidence Collector é um agregador de logs que coleta logs gerados pelo dispositivo Network Security. Você também pode configurar suas próprias regras de filtro personalizadas ou redefinir as regras para as regras padrão fornecidas pelo Trellix para filtrar cada tipo de evento (HTTP, SMTP, DNS, TLS e assim por diante) com base no valor JSON e no campo de evento correspondente em o dispositivo de segurança de rede.

o Ainda é possível, observar a facilidade dessa integração na seção Configuring HelixConnect:

▪ Original: The HelixConnect client connects your Trellix Network Security appliance directly to the Helix cloud using a secure VPN connection. This allows Helix to collect alert artifacts from the appliances

▪ Traduzido: O cliente HelixConnect conecta sua plataforma Trellix Network Security diretamente à nuvem Helix usando uma conexão VPN segura. Isso permite que o Helix colete artefatos de alerta desses dispositivos.

Quanto ao item 9.99

(...)

O item em questão expressa uma funcionalidade que é dividida entre as capacidades da solução de Extended Detection & Response e de Network Detection & Response, portanto, iremos de maneira detalhada, comprovar o inequívoco atendimento de ambas as capacidades, para que não restem dúvidas, ou fiquem suscetíveis à dúbias intenções por parte da recorrente, quaisquer dos elementos de comprovação.

Quanto às funcionalidades de rastreamento das ameaças:

• Estas são capacidades intrínsecas, à solução Network Detection & Response. Na página 15, do manual Network_Security_User_Guide.pdf, é possível alcançar a compreensão sobre como é feita a detecção e observar toda a cobertura oferecida pela funcionalidade. Um pequeno trecho desta capacidade está descrito abaixo e traduzida logo em seguida:

o Original: The alerts provided by the Network Security appliances identify incidents correlated with phases of the malware infection life cycle. For example, when a browser renders all the content on a legitimate Web page, the full page view often contains advertisements from third-party carriers. Attackers can post a fake advertisement with a zero-day exploit on the legitimate safe site. When exploit content is delivered by the browser, the first-stage analysis component of the Network Security MVX engine identifies the content as either suspicious or malicious. The Network Security sends the full page view of the Web page, including the exploit, to the MVX engines for detonation and second-stage analysis. The Network Security virtual environment is exploited as the content is rendered. This exploit may cause the browser to download a second-stage malware binary, known as dropper code. This binary is usually fetched from another website that is completely independent from the advertisement infrastructure, but that blends in to appear as though it is delivering ad content. The browser, as instructed by the initial exploit, unpacks the malware binary and executes it in order to load the attacker’s full malware toolkit into the Network Security MVX analysis engine. After the malware binary is loaded into the virtual victim machine, the binary instructs the MVX to transmit network callback traffic to the attacker, signaling that it is ready to be controlled remotely by the attacker. However, because the MVX operates in na isolated and virtualized network, this traffic remains internal to the appliance.

o Traduzido: Os alertas fornecidos pela plataforma Network Security identificam incidentes correlacionados de acordo com as fases do ciclo de vida da infecção por malware. Por exemplo, quando um navegador renderiza todo o conteúdo de uma página da Web legítima, a visualização completa da página geralmente contém anúncios de operadoras terceirizadas. Os invasores podem postar um anúncio falso com uma exploração de dia zero (0-day) no site legítimo e seguro. Quando o conteúdo de exploração é entregue pelo navegador, o componente de análise de primeiro estágio do mecanismo Network Security MVX identifica o conteúdo como suspeito ou malicioso. O Network Security envia a visualização completa da página da Web, incluindo a exploração, para os mecanismos MVX para detonação e análise de segundo estágio. O ambiente virtual do Network Security é explorado à medida que o conteúdo é renderizado. Essa exploração pode fazer com que o navegador baixe um binário de malware de segundo estágio, conhecido como código dropper. Esse binário geralmente é obtido de outro site que é completamente independente da infraestrutura de publicidade, mas que se mistura para parecer que está entregando conteúdo de anúncio. O navegador, conforme instruído pela exploração inicial, descompacta o binário do malware e o executa para carregar o arquivo do invasor kit de ferramentas de malware completo no mecanismo de análise Network Security MVX. Depois que o binário do malware for carregado na vítima virtual máquina, o binário instrui o MVX a transmitir o tráfego de retorno de chamada da rede para o invasor, sinalizando que está pronto para ser controlado remotamente pelo invasor. Porém, como o MVX opera em uma rede isolada e virtualizada, esse tráfego permanece interno ao aparelho

Quanto a demonstração gráfica, desde a entrada na rede até tentativas de roubo de dados:

• Como o item especifica um caso de uso muito particular, iremos detalhar as capacidades em duas etapas:

o Quanto a demonstração gráfica na plataforma de Detecção e Resposta Estendida:

▪ Nas figuras 5 e 6 do link: https://docs.trellix.com/bundle/helix_pg/page/UUID-32d28d65-5100-cc4c-edd5-5d35be4c87f4.html é possível observar um diagrama de fluxo, do incidente.

• Na figura 5 são exibidos (minimizados) que múltiplas ferramentas realizaram a detecção (2), também são exibidos que múltiplas fontes (4) foram relatadas no painel de ameaças, são também exibidos que múltiplos alertas (11) foram deflagrados, entre múltiplos ativos (8), onde múltiplos artefatos (11) foram relacionados.

• Na figura 6 são exibidos (maximizados), quais são os alertas deflagrados, bem como há diversas linhas que detalham o fluxo de dispersão e comunicação entre os elementos origem e alerta. Esses objetos no painel são interativos, e para cada elemento é exibido seu fluxo de comunicação, desde os equipamentos que relataram os incidentes, até as origens flagradas, bem como os alertas, seus destinos e indicadores.

o Quanto a capacidade de detecção de ataques de roubos de dados:

▪ Embora tenha sido um caso de uso esporádico, usado como referência na requisição do item, a solução Trellix Network Detection & Response, é capaz de flagar e impedir ataques caracteristicos de roubo de dados (Data Theft). Temos na página 17, do manual Network_Security_User_Guide.pdf, uma explicação sobre a classificação da infeção em dois tipos, ou fases. Um pequeno trecho desta capacidade está descrito abaixo e traduzida logo em seguida:

• Original: Each alert type may contain many events. The Network Security appliance classifies the infection life cycle in two phases. The exploitation and dropping of malicious code is the Infection Phase. The callback and extraction or theft of sensitive data and documents is the Callback Phase.

• Traduzido: Cada tipo de alerta pode conter muitos eventos. A plataforma Network Security classifica o ciclo de vida da infecção em duas fases. A exploração e dispersão de código malicioso é a Fase de Infecção. O retorno de chamada e extração ou roubo de dados e documentos confidenciais é a Fase de Retorno de Chamada (callback).”

22. Do Atendimento ao Item 9.119 – Sobre o item, esta EPC concorda com a contrarrazão, indicando o documento “network_security_user_guide.pdf” página 160, link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

“O item é expressamente claro, quando determina que estas funções devem ser entregues pela plataforma de detecção e resposta do fabricante entregue na proposta, o que justamente é garantido ao serem providas capacidades de integrações agnósticas, e orquestração de atividades de resposta por meio da automatização de processos e procedimentos, como visto na documentação detalhada abaixo:

Quanto à capacidade de compartilhamento de indicadores, pela automação de atividades:

• No link: https://docs.trellix.com/bundle/so_sag_6-6-0_pdf/resource/SO_SAG_6.6.0_pdf.pdf à página de numero 9, é possível ver singela descrição, que descreve a capacidade da plataforma em conectar-se abertamente a plataformas e serviços terceiros, visando a construção e modelagem de processos automatizados, bem como a integração de sistemas externos com esses processos automatizados, também chamados de playbooks.

Sendo ainda possível que tais integrações não nativas, isto é, aquelas não oferecidas por predefinição, possam ser criadas livremente. Um pequeno trecho desta capacidade está descrito abaixo e traduzida logo em seguida:

o Original: Security Orchestrator (SO) is an open playbook platform that integrates Security Orchestrator and third-party products and services to provide effective threat detection and event response for your system. Security Orchestrator provides a playbook builder interface that allows you to model procedures, and a plug-in API architecture to integrate external systems into your playbooks.

o Traduzido: O Security Orchestrator (SO) é uma plataforma aberta que integra o Security Orchestrator e produtos e serviços de terceiros para fornecer detecção eficaz de ameaças e resposta a eventos para o seu sistema. O Security Orchestrator fornece uma interface de criação de playbook que permite modelar procedimentos e uma arquitetura de API de plug-in para integrar sistemas externos em seus playbooks.

• Observa-se ainda que o repositório de plugins, embora não esteja presente na documentação específica, é facilmente acessado na URL: https://fireeye.market/apps?types=orchestration_add-ons e lá são encontrados mais de 2 centenas de plugins pré-definidos. Para facilitar a comprovação, destacaremos aqui, de maneira objetiva, os 3 plugins mencionados, uma vez que na página em questão, há tantos plugins já disponíveis que poderá levar algum tempo para se ler a lista completa. São eles:

o Plugin Fortinet: A integração com o ambiente Fortinet se dá pelo plugin: Fortinet Fortigate Plug-in, encontrado em: https://fireeye.market/apps/xFg9Ptv5

o Plugin para MS Active Directory: A Trellix oferece mais de 1 dezena de plugins para ambientes Microsoft, contudo, vamos listar aqui 2, dos quais podem ser utilizados para emitir comandos orquestrados ao MS Active Directory: Microsoft Active Directory Plug-in, encontrado em: https://fireeye.market/apps/219716 onde é possível realizar atividades junto ao MS AD, através de LDAP e LDAP seguro. Ainda é possível realizar atividades no ambiente Windows de diferentes formas, sendo mais uma delas a possíbilidade de interagir com o ambiente de scripts, registros e outras funções do SO, através de comunicação remota via WMI, com o plugin: Microsoft Windows Commands Plug-in, encontrado em: https://fireeye.market/apps/219780.

o Plugin para Microsoft 365: A Trellix oferece ainda, dentro dos mais de 10 plugins disponíveis para a plataforma Microsoft, plugins especificos para serviços especificos da Microsoft, a exemplificar alguns exemplos, como: Microsoft Graph Security API Plug-in, encontrado em: https://fireeye.market/apps/226297 ou ainda, o plugin Microsoft Teams Plug-in, encontrado em: https://fireeye.market/apps/v3OurZUX ou também, Microsoft Exchange Graph Plug-in, encontrado em: https://fireeye.market/apps/eQTsoj1J ou também o Microsoft SharePoint Plug-in, encontrado em: https://fireeye.market/apps/219764.”

23. Do Atendimento ao Item 10.10 – Sobre o item, esta EPC concorda com a contrarrazão pelo link internet fornecido, com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

“A funcionalidade de prevenção automática é habilitada, através de regras de prevenção contra intrusão, partindo

de vulnerabilidades conhecidas. Este mecanismo é provido por um módulo permanente e constantemente atualizado diante de novas vulnerabilidades. Na URL utilizada para comprovação https://kcm.trellix.com/corporate/index?page=content&id=KB58007 , são detalhados inúmeros processos atualmente cobertos por esta capacidade. Observa-se no link utilizado na comprovação que além de aplicativos terceiros, contemplados, como: winword.exe, winzip32.exe, java.exe, acrobat.exe entre outros, também existem processos chave na estrutura de sistemas operacionais, como: cmd.exe, cscript.exe, crsss.exe, dns.exe, dllhost.exe, explorer.exe, powershell.exe, regsvc.exe, svchost.exe, dentre tantos outros ali listados.

Estendendo ainda a comprovação, para que não restem dúvidas ou questionamentos de dúbias intenções por parte da recorrente, evidencia-se ainda as capacidades de proteção deste módulo na URL, que atua de maneira proativa, isto é, automaticamente, visando oferecer proteção contra explorações do tipo estouro de memória (buffer overflow), uso ilegal ou indevido de APIs, e ataques de exploração via rede (network exploits). Na URL https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-interface-reference-guide-windows/page/GUID-3D9AB771-0415- 45C5-B62A-1EC74738BAB8.html são obtidas as informações quanto as características dessa capacidade. Este módulo, permite ainda a sua total customização pela criação de regras especificas, as chamadas Expert Rules. No link https://docs.trellix.com/bundle/endpoint-security-10.7.x-common-interface-reference-guide-windows/page/GUID-2EC3A246-8FE9-4D60-8E17-28B39C5AE2D0.html podem ser observadas as características para customização dessas regras.

Visando ainda dirimir quaisquer eventuais questionamentos quanto ao meticuloso atendimento de todas as funcionalidades exigidas, destacamos mais uma, na já extensa lista de capacidades da plataforma ofertada, e sobretudo, já aceita pela licitante, a possibilidade de varrer contra vulnerabilidades, evidenciando: patches pendentes (missing patches), patches instalados (installed patches), vulnerabilidades exploráveis (exploitable vulnerabilities). Ver seção Assess the vulnerabilities in the endpoint na URL:https://docs.trellix.com/bundle/mvision-endpoint-detection-and-response-product-guide/page/UUID-c33e6651-94a4-1bc9-fcd2-9301e26ddc60.html#assess_the_vulnerabilities_in_the_endpoint.”

24. Do Atendimento ao Item 12.2.1 – Sobre o item, esta EPC concorda com a contrarrazão, com destaque a transcrição abaixo apresentada pela recorrente/recorrida.

“1. Existência de templates nativos para, mas não limitado a, as regulamentações do requisito, acessíveis diretamente no caminho MENU -> Data Protection -> Classification, conforme verificado no Guia de Interface acessível através do link

https://docs.trellix.com/bundle/data-loss-prevention-11.10.x-interface-reference-guide/page/GUID-9C4B1B9A-A952-4960-964C-9ABD5B7D3CB1.html

2. Links específicos que refutam diretamente as alegações da ALLTECH, demonstrando algumas, mas não limitadas a, das capacidades de nossa solução:

- PCI: https://docs.trellix.com/bundle/data-loss-prevention-11.10.x-product-guide/page/GUID-FD23BE89-C7F4-4B6A-BADD-9EAF9F87788A.html

- HIPAA: https://docs.trellix.com/bundle/data-loss-prevention-11.10.x-product-guide/page/GUID-2D8266D9-373C-433D-B9EB-BBF038FE49AA.html

- GDPR (Esse não solicitado, mas utilizado como exemplo): https://docs.trellix.com/bundle/data-loss-prevention-11.10.x-product-guide/page/GUID-41003CDD-16B9-4F3B-9C75-3F9BE5561F7A.html

3. Datasheet da solução, que explicitamente afirma o suporte a regulamentações, mas não limitado a, como PCI, PII, GDPR, HIPAA e SOX, acessível através do link https://www.trellix.com/assets/docs/data-sheets/trellix-data-loss-prevention-dlp-datasheet-endpoint.pdf, reforçando nossa posição de liderança na conformidade regulatória.

Importante esclarecer que as imagens apresentadas como evidência são demonstrações diretas da solução Trellix Data Loss Prevention, capturadas diretamente da console unificada de gerência ePO.

Especificamente, essas imagens são da seção MENU -> Data Protection -> Classification, invalidando qualquer suposição de que as evidências fornecidas são ambíguas ou de fontes externas. A Trellix utiliza sua própria plataforma avançada para assegurar a conformidade com regulamentações críticas.... ”

DA ANÁLISE FINAL DOS PEDIDOS

Diante dos argumentos técnicos de contrarrazões expostos pela recorrida, a equipe técnica deste conselho concorda com a mesma de que as alegações interpostas pela empresa recorrente são descabidas e não são suficientes para a desclassificação da empresa recorrida. Por conclusão, a equipe técnica deste conselho decide por deferir tecnicamente a favor da recorrida, prosseguindo assim então com os ritos normais inerentes ao processo licitatório.

6. DA ANÁLISE DA PREGOEIRA

Primeiramente, cumpre esclarecer que o procedimento realizado pela pregoeira acerca da diligência foi um ato permissivo no procedimento licitatório, com a finalidade de esclarecimentos adicionais referentes aos aspectos técnicos, logo não há que se falar que foi uma ação confusa.

Quanto à classificação da empresa BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA., a decisão foi tomada em total consonância com o instrumento convocatório e com o apoio da equipe de contratação.

Após o recebimento da proposta da recorrente (ids. 0551229, 0551230, 0551231 e 0551233), foi solicitado à unidade demandante (id. 0551236), analisar o cumprimento dos requisitos técnicos do edital, especialmente os consignados no Anexo I do edital.

Em resposta, a unidade demandante (id. 0554183), informou que na "*...análise identificou que a Proposta Comercial atende* aos requisitos previstos no Edital do PE n. 90.003/2024 (0545788), sobretudo às especificações técnicas

consignadas no Anexo I do Termo de Referência (0545789)."

Portanto, a decisão de classificação da recorrida foi acertada, tendo em vista que, conforme atestado e confirmado pela unidade demandante, os requisitos técnicos da proposta da recorrida foram atendidos, não merecendo a pretensão recursal prosperar.

7 - CONCLUSÃO

Por todo exposto, e no uso das atribuições previstas no art. 165, § 2º, da Lei nº. 14.133/2021, diante das alegações da empresa recorrente, esta pregoeira NÃO RECONSIDERA a decisão que classificou a licitante BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA. Portanto, sugiro o envio dos autos à autoridade superior para proferir sua decisão, nos termos do referido dispositivo legal.

À SUCOP,

Com vistas à remessa dos autos à ASJUR, para prosseguimento da análise da peça recursal, nos termos do § 2º, do art. 165 da Lei nº. 14.133/2021.

Autenticado eletronicamente por **Luisa Aires Oliveira**, **Pregoeiro(a)**, em 11/03/2024, às 17:31, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0557384** e o código CRC **5F213F96**.