

**À ILUSTRÍSSIMA SENHORA PREGOEIRA, LUISA AIRES OLIVEIRA, DO  
CONSELHO DA JUSTIÇA FEDERAL.**

**Ref.:** Pregão Eletrônico Nº 90.003/2024

**BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA**, empresa regularmente qualificada no procedimento licitatório identificado em epígrafe, vem, respeitosamente, à presença desta ilustríssima Autoridade Administrativa apresentar, tempestivamente,

**CONTRARRAZÕES**

ao recurso administrativo apresentado pela empresa ALLTECH – SOLUÇÕES EM TECNOLOGIA LTDA, que questiona a respeitável Decisão Administrativa que houve por bem habilitar a Recorrida, declarando-a vencedora do certame, aduzindo para tanto as razões de defesa abaixo delineadas.

**I – SÍNTESE FÁTICA**

Trata-se de certame licitatório realizado pelo CONSELHO DA JUSTIÇA FEDERAL, na modalidade Pregão, na forma Eletrônica, do tipo menor preço global, cujo objeto é a 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.

A abertura do certame ocorreu no dia 15.02.2024, tendo a empresa ora Recorrida sido a 1ª colocada no certame, tendo ofertado o lance de R\$ 2.764.082,75 (dois milhões, setecentos e sessenta e quatro mil, oitenta e dois reais e setenta e cinco centavos).

No dia 21.02.2024, a Ilma. Pregoeira solicitou a promoção de diligência que fossem prestados esclarecimentos adicionais sobre a conformidade de sua proposta

com os itens 4.52, 4.53.6, 4.53.7, 5.4.2, 5.4.3, 6.1, 6.38, 9.1, 9.18, 9.19, 9.22, 9.24, 9.34, 9.44, 9.65, 9.92.1, 9.98, 9.99, 9.119, 10.5, 10.9, 10.21, 11.4.1, 11.4.3, 11.6, 11.7, 11.8, 11.9, 11.18, 12.2, 12.2.1, 12.2.3, 12.2.5, 12.2.6, 12.14.16, 14.1, 14.3, 14.7.1, 14.8.1, 14.8.2, 14.8.3, 14.8.4 referentes às especificações técnicas, descritas no ANEXO I do Termo de Referência.

A empresa BLUE EYE apresentou a resposta da diligência promovida no mesmo dia 21.02.2024, tendo a proposta da empresa sido classificada no dia 23.02.2024.

Com a comprovação de que a empresa ora Recorrida cumpriu com todos os requisitos do Edital, no dia 26.02.2024, a empresa foi habilitada, pois, após diligências e análise dos documentos, a Ilma. Pregoeira e sua equipe de apoio entenderam que a empresa cumpriu com todas as exigências estabelecidas no Edital.

Irresignada com a decisão que declarou a BLUE EYE como empresa vencedora do certame, a empresa ALLTECH SOLUÇÕES EM TECNOLOGIA LTDA, empresa que prestava os serviços licitados anteriormente ao CONSELHO DA JUSTIÇA FEDERAL, interpôs o Recurso Administrativo contra a habilitação da BLUE EYE SOLUÇÕES, alegando, de forma indevida, que a solução ofertada pela Recorrida não atende aos requisitos do Edital.

Todavia, conforme se verá, não subsiste qualquer um dos pontos levantados pela Recorrente, uma vez que a habilitação da Recorrida se deu de forma ilibada, escoimada e livre de qualquer vício, dentro dos princípios da legalidade, da vinculação ao edital e, sobretudo, do julgamento objetivo que deve permear toda a atuação administrativa.

É a síntese dos fatos.

## **II – DOS ELEMENTOS QUE CONDUZEM À MANUTENÇÃO DA DECISÃO ORA RECORRIDA.**

Mister rebater, aqui, os argumentos levantados pela Empresa Recorrente, de forma a demonstrar, patentemente, a completa insubsistência do que foi aduzido pela ALLTECH, refletindo tão somente a ação de recorrer por puro inconformismo.

## III – DA ALEGAÇÃO DE NÃO ATENDIMENTO ÀS EXIGÊNCIAS DE QUALIFICAÇÃO TÉCNICA DO EDITAL.

Inicialmente, é importante registrar que a BLUE EYE é uma empresa que possui anos de experiência, possuindo um vasto acervo técnico compatível com o objeto do certame em questão.

Pois bem, o recurso da empresa ALLTECH se repousa, energeticamente, em uma interpretação completamente desvirtuada da solução ofertada pela BLUE EYE, tendo a Recorrente agido com notória má-fé no caso em tela.

Em resposta aos apontamentos técnicos realizados pela empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA, nota-se claramente que a mesma possui explícito dolo nas suas alegações, objetivando nada menos que o prejuízo ao processo licitatório, causando o retardamento de seu curso natural, uma vez que a decisão aplicada de habilitar a empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA se faz correta, pois além de todos os requisitos editalícios terem sido devidamente cumpridos e atendidos, seguindo todo o processo instruído no edital e seus anexos, a proposta da vencedora ainda é mais viável do ponto de vista econômico para a administração pública.

A empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA inicia sua fala contando os fatos ocorridos durante a sessão pública, porém questiona, de forma 100% equivocada, a decisão da Sra Pregoeira em realizar diligência em referência a comprovação dos atendimentos técnicos, vide a íntegra abaixo:

*“De uma maneira um tanto quanto confusa, sem explicar o que seria necessário comprovar em sede de diligência, o sistema registrou o seguinte comunicado:*

*Sistema para o participante 26.025.401/0001-90 21/02/2024 14:01:26 Senhor licitante, com base ao disposto no subitem 19.2.1 do edital, solicita-se que sejam prestados os esclarecimentos adicionais, por meio de documentos ou declarações, sobre a conformidade da proposta com os itens:*

*Sistema para o participante 26.025.401/0001-90 21/02/2024 14:01:46 4.52, 4.53.6, 4.53.7, 5.4.2, 5.4.3, 6.1, 6.38, 9.1, 9.18, 9.19, 9.22, 9.24, 9.34, 9.44, 9.65, 9.92.1, 9.98, 9.99, 9.119, 10.5, 10.9, 10.21, 11.4.1, 11.4.3, 11.6, 11.7, 11.8, 11.9, 11.18, 12.2, 12.2.1, 12.2.3, 12.2.5, 12.2.6, 12.14.16, 14.1, 14.3, 14.7.1, 14.8.1, 14.8.2, 14.8.3, 14.8.4 referentes às especificações técnicas, descritas no ANEXO I do Termo de Referência.”*

Seguindo a fala da empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA, não foi possível compreender o que há de confuso na fala da Sra Pregoeira, uma vez que diligências e pedidos de esclarecimento adicionais são previstos em edital e é prática extremamente comum em processos licitatórios. Nessa ocasião, a

empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA respondeu devidamente a diligência e conforme observada na correta decisão da Sra Pregoeira, a proposta foi devidamente aceita, uma vez que todas as dúvidas foram devidamente sanadas.

Não parando por aí, a empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA de forma a tentar reverter a correta decisão já adotada durante a sessão pública, alega que não houve o cumprimento de diversos itens técnicos por parte da proposta apresentada pela empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA, vide abaixo a íntegra das alegações apresentadas em fase recursal:

*“Identificamos junto ao processo, lista de **supostos itens não atendidos na solução ofertada**: 5.56, 5.81, 5.87, 5.103, 5.122, 5.130, 7.33, 7.49, 8.36, 8.37, 8.38, 8.39, 8.42, 8.46, 8.47, 8.48, 8.50, 8.67, 8.68.9, 8.80 (e seus subitens), 9.2, 9.48, 9.98, 9.99, 9.119, 10.10, 12.2.1. A seguir, de forma didática e buscando uma fácil compreensão, estruturamos nossas considerações itemizando cada elemento acima.”*

Claramente tais alegações se provam 100% infundadas, representando apenas o descontentamento da empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA em não vencer o certame e, provavelmente, uma tentativa desesperada de tentar reverter a situação em benefício próprio. Por mais que toda a documentação já enviada no sistema seja suficiente para compreender todos os requerimentos editalícios, será apresentado abaixo uma resposta para cada alegação realizada, por mais inverídicas que tais alegações sejam, vamos a elas:

## **1. Razão técnica número 1 apresentada.**

### **Íntegra da alegação:**

**“5.81 Deve possuir configuração de classificação de spam com, no mínimo, três níveis: Alto, Médio e Baixo ou escala equivalente.**

*Resta claro o não atendimento do item 5.81 com a comprovação apresentada através do documento anexado “es\_admin\_guide.pdf - Threat Type” - Página 199, citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) que não atende aos requisitos e não demonstram que possuem a possibilidade de configuração de classificação de spam com, no mínimo, três níveis: Alto, Médio e Baixo ou escala equivalente*

*A comprovação evidencia como é classificado o spam, apenas menciona que existe uma classificação única. A classificação em vários níveis permite uma avaliação mais precisa da natureza do conteúdo. Além do simples “spam” ou “não spam”, é possível distinguir entre ameaças mais sutis e, potencialmente, perigosa.*

*Desta forma, proporciona precisão para os administradores, permitindo que compreendam melhor por que uma mensagem foi classificada de uma determinada maneira e tomem ações apropriadas.*

*Ou seja, com uma escala mais ampla, a solução pode ser ajustada para se adaptar dinamicamente às ameaças emergentes. A capacidade de adicionar novos níveis ou ajustar as configurações conforme necessário permite uma resposta mais eficaz a padrões de spam em constante evolução. A falta de níveis adicionais dificulta a personalização das configurações de segurança com base nas necessidades específicas da organização. Uma abordagem mais granular permite ajustar a sensibilidade do filtro para atender aos requisitos únicos de cada ambiente.*

*Por isso, o não atendimento ao item especificado, traz instabilidade para categorização de mensagens além de dificultar a implantação da política de segurança que atualmente o C/JF realiza e, claramente, a oferta da LICITANTE não atende ao requisito.”*

### **Resposta da recorrida:**

Claramente a recorrente tenta depreciar a solução entregue pela recorrida, que possui capacidades de proteção inclusive superiores ao que foi especificado no edital e seus anexos.

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 payloads 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 antivírus.

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.

Os relatos acima não compreendem 100% das capacidades da ferramenta, porém nos apresentam uma boa amostragem da capacidade da plataforma e principalmente, sua capacidade de identificar e classificar mensagens em diversos tipos diferentes, permitindo ao administrador do ambiente o contexto necessário para combater ameaças por este canal e não apenas visualizar níveis simplórios como Baixo, Médio ou Alto.

Desta forma, resta demonstrado que a alegação da Recorrente não passa de mera irresignação, não havendo qualquer embasamento técnico para que seja reconhecido. Assim, faz-se necessária o improvimento do recurso apresentado pela ALLTECH - SOLUCOES EM TECNOLOGIA LTDA, mantendo incólume a r. decisão administrativa que declarou vencedora a empresa BLUE EYE.

## **2. Razão técnica número 2 apresentada.**

### **Íntegra da alegação:**

#### **“5.56 Deve possuir capacidade de identificar e proteger o MTA contra ataques de Negação de Serviços (DoS).”**

*Fica evidente o não atendimento do item 5.56 com a comprovação apresentada através do documento anexo “es\_admin\_guide.pdf” página 237, citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) que não atende aos requisitos e não demonstram a capacidade de identificar e proteger o MTA contra-ataques de Negação de Serviços (DoS).*

### Spam and attack codes

Codes starting with 200 are related to spam and attack protection services and indicates that the sending MTA is untrusted.

Code	Message	Type	Rejection reason
ETP200	Invalid recipient	Reject	Directory Harvest Attack Protection. Too many failed recipient checks causes Directory Harvest Attack Protection to kick in and ban a sending MTA.
ETP202	Your IP (\${_ipsrc}) is listed by Spamhaus. Please see <a href="http://www.spamhaus.org/query/ip/\${_ipsrc}">http://www.spamhaus.org/query/ip/\${_ipsrc}</a> if you feel this is in error.	Reject	Spamhaus Zen RBL Protection. The sending MTA IP address was listed on the Spamhaus Zen RBL.
ETP203	SPF Failure for domain (<domain>).	Reject	SPF failure for sending domain.
ETP204	DKIM Failure for domain (<domain>).	Reject	DKIM failure for sending domain.
ETP205	DMARC Failure for domain (<domain>).	Reject	DMARC failure for sending domain.
ETP206	Unknown sender reputation	Defer	Unknown sender profile, temporarily deferring incoming injection.
ETP207	Your IP %s is listed by Invalvement. Please see <a href="http://">http://</a>	Reject	The sending MTA IP address was listed on Invalvement Sip RBL.

*O documento anexado como evidência da funcionalidade novamente se revela ineficaz, pois em nenhum ponto oferece demonstração da capacidade de proteção contra-ataques do tipo DoS (Denial of Service).*

*O objetivo principal de um ataque DoS é negar ou prejudicar o acesso legítimo a um serviço, sistema ou recurso.*

*Durante um ataque DoS, as operações cotidianas são prejudicadas, podendo levar a interrupções nos serviços internos, como o e-mail corporativo, afetando a eficiência operacional e a capacidade de responder às demandas.*

*Portanto, seria um prejuízo ao CJF habilitar uma solução que claramente sequer lista a proteção a este tipo de ataque e, na prática, não sustentaria o serviço de e-mail ativo. Fica o questionamento: O que aconteceria caso o serviço de e-mail ficasse indisponível por 2, 5, 10 horas ou até mesmo 1 dia? Os danos são evidentes e, mais uma vez, deixa explícito que a solução oferecida é ineficiente a demanda do CFJ.”*

### Resposta da recorrida:

Neste tópico a empresa recorrente ALLTECH - SOLUCOES EM TECNOLOGIA LTDA demonstra mais uma vez seu desejo em distorcer fatos ou seu completo desconhecimento de como plataformas SaaS (Software as a service) funcionam, onde o próprio fabricante cuida da segurança de diversos aspectos da plataforma disponibilizada como serviço, inclusive de algo tão básico como ataques do tipo DoS.

Ao analisar o documento <https://www.trellix.com/assets/data-sheets/trellix-email-security-cloud-datasheet.pdf>, presente nas documentações já enviadas, podemos observar na página 7 o seguinte trecho:

## Authorization and compliance certifications

### ISO 27001

Trellix Email Security – Cloud meets the ISO 27001 information security standard that ensures data centers are securely managed.

### FedRAMP

Email Security – Cloud with AVAS protection meets the FedRAMP security requirements for cloud services operated by government and public education entities.

### SOC 2 Type 2

Email Security – Cloud also complies with the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC 2) Type 2 Certification for Security and Confidentiality.

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.

Mais uma vez, resta demonstrado a falta de embasamento do recurso apresentado pela Recorrente, merecendo se manter na íntegra a r. decisão que declarou a empresa BLUE EYE habilitada no certame em tela.

### **3. Razão técnica número 3 apresentada.**

#### **Íntegra da alegação:**

**“5.87 Deve possuir capacidade para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados.**

Fica evidente o não atendimento do item 5.87 com a comprovação apresentada através do link (<https://www.trellix.com/assets/data-sheets/trellix-email-security-cloud-datasheet.pdf>) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram a capacidade de análise e proteção de ameaças de dia zero, conforme trecho retirado do documento:



*Trellix Email Security – Cloud offers industry-leading detection to identify, isolate, and immediately stop ransomware, business email compromise, spear phishing, impersonation, and attachment-based attacks before they enter your environment. Email Security – Cloud also scans outgoing email traffic for advanced threats, spam, and viruses.*

*Tradução livre:*

*Trellix Email Security – Cloud oferece detecção líder do setor para identificar, isolar e interromper imediatamente ransomware, comprometimento de e-mail comercial, spear phishing, falsificação de identidade e ataques baseados em anexos antes que eles entrem em seu ambiente. Segurança de e-mail – A nuvem também verifica o tráfego de e-mail de saída em busca de ameaças avançadas, spam e vírus.*

*As ameaças de dia zero geralmente exploram vulnerabilidades desconhecidas, tornando padrões de ataque únicos. Uma análise detalhada permite identificar comportamentos específicos que podem indicar uma ameaça de dia zero em desenvolvimento, contribuindo para a detecção precoce.*

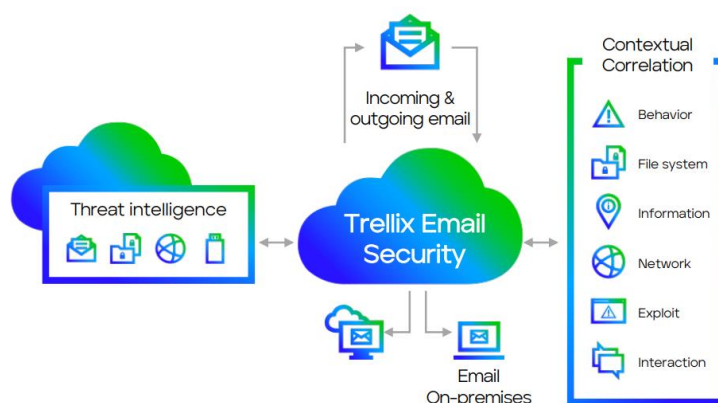
*Por isso, ao visualizar detalhes sobre o comportamento da ameaça, os administradores podem responder rapidamente e implementar medidas de mitigação específicas para conter ou neutralizar a ameaça. A capacidade de resposta ágil é crucial para minimizar danos em ataques de dia zero. Desta forma, é vital, pois os cibercriminosos frequentemente ajustam suas abordagens para contornar as soluções de segurança existentes.*

*Portanto, torna-se vital que as soluções de proteção possuam motores capazes de analisar ameaças novas e desconhecidas utilizando técnicas de Machine Learning e Análise de Comportamento, por exemplo.”*

## **Resposta da recorrida:**

Novamente a empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA busca distorcer a interpretação dos fatos, numa evidente tentativa de desfigurar inclusive dados técnicos e conceitos sobre ameaças cibernéticas, de forma errônea, buscando cada vez mais claramente o benefício próprio e nunca a exposição da veracidade dos fatos.

Utilizando o mesmo link citado pela recorrente, <https://www.trellix.com/assets/data-sheets/trellix-email-security-cloud-datasheet.pdf>, na página 7 temos o seguinte diagrama:



Em tal informação, claramente encontramos todos os recursos citados no item, incluindo detecção de exploits, sandbox e ameaças de dia zero. Apenas de forma a

complementar, trazemos novamente a informação abaixo para reafirmar algumas funcionalidades presentes na plataforma:

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 payloads maliciosos, roubo de credenciais por meio de phishing e variantes, etc.
- Configure recipient validation settings - Permite 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 antivírus.

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-programadas 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.

Com base nas informações acima, resta demonstrado que a solução ofertada pela Recorrida atende a todas as especificações do Edital, estando correta a r. decisão da Ilma. Pregoeira que declarou a empresa ora Recorrida habilitada e vencedora da licitação em tela.

#### **4. Razão técnica número 4 apresentada.**

##### **Íntegra da alegação:**

**“ITENS 5.103, 5.103.1, 5.103.2, 5.103.3**

**5.103 Deve ser possível criar políticas de malwares, spam e filtragem de conteúdo com:**

**5.103.1 Definição do destinatário, possibilitando selecionar domínios cadastrados, domínios específicos e grupos de usuários;**

**5.103.2 Especificação de endereços de remetente;**

**5.103.3 Exceções.**

*Na planilha “Atendimento dos requisitos técnicosv2.xlsx” de comprovação técnica (ponto a ponto) anexada é mencionado o documento “5.103.pdf”, porém o arquivo não foi anexado, inviabilizando a comprovação detalhada do item e seus subitens.*

*Nunca é demais lembrar que a empresa já foi diligenciada e lhe foi oportunizada a possibilidade de demonstrar atendimento do item. Ademais, essa previsão era uma obrigação de comprovação prévia do edital, que por sua vez reza:*

**“19.2.1 Promover, em qualquer fase da licitação, diligência destinada a esclarecer ou a complementar a instrução do processo, fixando as licitantes, prazos para atendimento, vedada a inclusão posterior de informação que deveria constar originalmente da proposta.”**

*Assim, não lhe cabe mais o direito de inserir documentos novos, uma vez que era obrigação inserir originalmente na proposta e em sede de diligência, ela já falhou na comprovação:*

**“6.1 Após a divulgação deste edital no sítio www.gov.br/compras, as licitantes deverão encaminhar, exclusivamente por meio do sistema eletrônico, proposta com a descrição do objeto ofertado e do preço, com as características mínimas e quantidades estipuladas no termo de referência, até a data e hora marcadas para abertura da sessão quando, então, se encerrará a fase de recebimento de propostas.**

*(...)*

**6.13 A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item.”**

*Assim, não lhe assiste mais o direito de incluir documentos novos.”*

## **Resposta da recorrida:**

Por mais repetitiva que tal informação possa ser, não restam dúvidas que a empresa recorrente busca apenas benefício próprio e nunca a contribuição correta para a disputa pública.

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.

Mais uma vez, resta demonstrado que a solução atende ao exigido no Edital, não merecendo prosperar a alegação da Recorrente.

## **5. Razão técnica número 5 apresentada.**

### **Íntegra da alegação:**

#### **“5.122 - Deve ser possível encaminhar os logs para syslog.**

*Na planilha “Atendimento dos requisitos técnicosv2.xlsx” de comprovação técnica (ponto a ponto) anexada é mencionado o documento “5.122.pdf”, porém o arquivo não foi anexado, inviabilizando a comprovação detalhada do item e seus subitens.*

*Nunca é demais lembrar que a empresa já foi diligenciada e lhe foi oportunizada a possibilidade de demonstrar atendimento do item. Ademais, essa previsão era uma obrigação de comprovação prévia do edital, que por sua vez reza:*

*“19.2.1 Promover, em qualquer fase da licitação, diligência destinada a esclarecer ou a complementar a instrução do processo, fixando as licitantes, prazos para atendimento, **vedada a inclusão posterior de informação que deveria constar originalmente da proposta.**”*

*Assim, não lhe cabe mais o direito de inserir documentos novos, uma vez que era obrigação inserir originalmente na proposta e em sede de diligência, ela já falhou na comprovação:*

*“6.1 **Após a divulgação deste edital** no sítio [www.gov.br/compras](http://www.gov.br/compras), as licitantes deverão encaminhar, exclusivamente por meio do sistema eletrônico, proposta com a descrição do objeto ofertado e do preço, com as características mínimas e quantidades estipuladas no termo de referência, **até a data e hora marcadas para abertura da sessão quando, então, se encerrará a fase de recebimento de propostas.**”*

(...)

6.13 A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item.”

*Assim, não lhe assiste mais o direito de incluir documentos novos.”*

### **Resposta da recorrida:**

Novamente a empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA procede com seu modus operandi, tentando distorcer a realidade dos fatos.

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.

Assim, resta demonstrado que a solução atende ao exigido no Edital, não merecendo prosperar a alegação da Recorrente.

## **6. Razão técnica número 6 apresentada.**

### **Íntegra da alegação:**

“5.130 Deve permitir visualizar as mensagens quarentenadas por data, remetente, destinatários e conteúdo.

*Na planilha “Atendimento dos requisitos técnicosv2.xlsx” de comprovação técnica (ponto a ponto) anexada é mencionado o documento “5.122.pdf”, porém o arquivo não foi anexado, inviabilizando a comprovação detalhada do item e seus subitens.*

*Nunca é demais lembrar que a empresa já foi diligenciada e lhe foi oportunizada a possibilidade de demonstrar atendimento do item. Ademais, essa previsão era uma obrigação de comprovação prévia do edital, que por sua vez reza:*

“19.2.1 Promover, em qualquer fase da licitação, diligência destinada a esclarecer ou a complementar a instrução do processo, fixando as licitantes, prazos para atendimento, **vedada a inclusão posterior de informação que deveria constar originalmente da proposta.**”

*Assim, não lhe cabe mais o direito de inserir documentos novos, uma vez que era obrigação inserir originalmente na proposta e em sede de diligência, ela já falhou na comprovação:*

“6.1 Após a divulgação deste edital no sítio www.gov.br/compras, as licitantes deverão encaminhar, exclusivamente por meio do sistema eletrônico, proposta com a descrição do objeto ofertado e do preço, com as características mínimas e quantidades estipuladas no termo de referência, **até a data e hora marcadas para abertura da sessão quando, então, se encerrará a fase de recebimento de propostas.**”

(...)

6.13 A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item.”

*Assim, não lhe assiste mais o direito de incluir documentos novos.”*

### **Resposta da 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. Razão técnica número 7 apresentada.**

#### **Íntegra da alegação:**

**“7.33 A verificação Antimalware deve permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.”**

*Fica evidente o não atendimento do item 7.33 com a comprovação apresentada através do link Support Site [https://success.skyhighsecurity.com/Skyhigh\\_CASB/Skyhigh\\_CASB\\_Incidents/Policy\\_Incidents/Quarantined\\_Files](https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Incidents/Policy_Incidents/Quarantined_Files) do documento apresentado no ponto a ponto não atende aos requisitos e não demonstram as possibilidades de customizações de ações, , por exemplo:*

*quarentenar, deletar*

*e passar.*

*A comprovação anexada pela LICITANTE, não demonstra o atendimento às ações que podem ser configuradas em uma política de proteção e, na diferente disso, mostra os tipos de pesquisa e filtros que podem ser aplicados para encontrar um log entre mensagens quarentenadas, retirando o contexto solicitado no item.*

*This page provides the ability to search for a specific user, or filter quarantined files. You can also preview or download a file in Quarantine to make a decision on whether to Delete or Restore it. When you select one or more files from this list, Restore or Delete buttons are enabled. The Quarantined Files page is located at Incidents > Policy Incidents > Quarantined Files.*

*Tradução livre:*

*Esta página oferece a capacidade de procurar um usuário específico ou filtrar arquivos em quarentena. Você também pode visualizar ou baixar um arquivo na Quarentena para decidir se deseja excluí-lo ou restaurá-lo. Quando você seleciona um ou mais arquivos desta lista, os botões Restaurar ou Excluir são ativados. A página Arquivos em quarentena está localizada em Incidentes > Incidentes de política > Arquivos em quarentena*

*É evidente que o item descreve obrigatoriedade de customização de tipos de ação para uma política: Quarentenar, deletar ou passar.*

*Ressalta-se que a customização de ações em um antimalware é crucial para garantir que o CJF possa adaptar a proteção contra ameaças de acordo com suas políticas, requisitos regulatórios e características específicas do ambiente, proporcionando maior eficácia e flexibilidade na resposta a incidentes de segurança.*

*Na imagem abaixo pode-se observar que o conteúdo de comprovação fala apenas sobre mensagens que já foram quarentenadas.*

Home / Skyhigh CASB / Skyhigh CASB Incidents / Policy Incidents / Quarantined Files

Review files quarantined by Skyhigh based on your DLP policies. Then choose to delete or release the files from quarantine.

### QUARANTINED FILES

File Name	Application	Instance	User	File	Response	QUARANTINE DATE	Policy
Test Email	Microsoft Exchange Online	Default	frances@france.com	Sent Items	Quarantined	24-Jul-2018 14:53:04	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	andrew@paga.com	Mailbox	Quarantined	07-Jul-2018 17:53:32	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	andrew@paga.com	Mailbox	Quarantined	08-Jul-2018 17:53:32	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	andrew@paga.com	Mailbox	Quarantined	08-Jul-2018 17:53:32	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	frances@france.com	Sent Items	Quarantined	24-Jul-2018 14:53:04	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	andrew@paga.com	Mailbox	Quarantined	05-Jul-2018 17:53:32	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	andrew@paga.com	Mailbox	Quarantined	05-Jul-2018 17:53:32	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	andrew@paga.com	Mailbox	Quarantined	05-Jul-2018 17:53:32	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	andrew@paga.com	Mailbox	Quarantined	05-Jul-2018 17:53:32	Social Security Numbers, PCI, Government
Test Email	Microsoft Exchange Online	Default	frances@france.com	Sent Items	Quarantined	05-Jul-2018 17:53:42	Social Security Numbers, PCI, Government

On the Quarantined Files page, the following information and actions are available:

- Search.** Enter a username to search.
- Filter.** Select filters for Status, Application, Instance, Policy, or Response.
- CSV.** Click the button to generate a CSV file including the information from the table.
- Edit Table Columns.** Click to show or hide table columns.
- Download File.** Click the link in the File Name column to download the quarantined file from the hosting cloud service. (Skyhigh CASB never stores customer documents in our cloud.)
- Restore.** Select the checkbox for one or more files to enable the Restore button. When a file is restored, it is returned to its original location in the cloud service. This removes the warning message and sends an e-mail to the uploading user, informing them that their file has been removed from quarantine.
- Delete.** Select the checkbox for one or more files to enable the Delete button. This permanently deletes the file from the cloud service.

Adicionalmente, fica claro que a solução não traz a possibilidade de configuração de políticas de bloqueio e, muito menos, oferece visibilidade de ameaças (virus, malware, zero day, entre outros) considerando a camada de proteção para Microsoft 365. Vale destacar a imagem abaixo que traz a descrição da própria SkyHigh e, visivelmente, não atende ao item 7.33, o qual exige a configuração de ações em caso de detecção de artefatos.

Home / Skyhigh CASB / Skyhigh CASB Reports / Report Examples

This section provides descriptions of preconfigured reports that you can use as examples to create your own reports.

### Topics

- Map Classic Report Templates to new Reports
- Report - Add the D-U-N-S Number to the Services Report
- Report - CSP Data Between Dates
- Report - Data Exfiltration
- Report - New Services
- Report - Number of Services by Category
- Report - Services by Access Count
- Report - Services by Allowed Percentage
- Report - Services by Denied Percentage
- Report - Services by Inbound Data Traffic
- Report - Services by Outbound Data Traffic
- Report - Services by Risk Score
- Report - Services by Total Traffic Volume
- Report - Services by Upload Data
- Report - Services with Breaches in the Last Year
- Report - Top Users by Access Count
- Report - Top Users by Total Data Traffic Volume
- Report - Users Exposed to Vulnerable Services
- Report - Vulnerability

“A primary purpose of a Cloud Access Security Broker (CASB) is to provide a unified set of controls and policies that apply to multiple, dissimilar cloud services. While the abstracted toolset is similar to what many IT Security experts expect in terms of DLP, remote access, and event monitoring, they are implemented differently with the CASB, smoothing out the differences between one cloud service provider (CSP) and another.”

Tradução livre:

“O objetivo principal de um Cloud Access Security Broker (CASB) é fornecer um conjunto unificado de controles e políticas que se aplicam a vários serviços de nuvem diferentes. Embora o conjunto de ferramentas abstrato seja semelhante ao que muitos especialistas em segurança de TI esperam em termos de DLP, acesso remoto e monitoramento de eventos, eles são implementados de forma diferente com o CASB, suavizando as diferenças entre um provedor de serviços em nuvem (CSP) e outro.”

The screenshot shows the Skyhigh Security website. The header includes the Skyhigh Security logo, navigation links for Support, Status, Website, and Partners, a language selection dropdown, and a Sign In button. Below the header is a search bar with the text "How can we help you?". The main navigation breadcrumb is: Home / Skyhigh CASB / Skyhigh CASB Architecture / Skyhigh CASB / About Skyhigh CASB. The page title is "About Skyhigh CASB", last updated on Jun 16, 2020. A table of contents is visible. The main content area discusses the challenges of securing cloud applications and the role of a CASB. A sidebar on the left lists various Skyhigh CASB features and settings.

[https://success.skyhighsecurity.com/Skyhigh\\_CASB/Skyhigh\\_CASB\\_Architecture/Skyhigh\\_CASB/About\\_Skyhigh\\_CASB](https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Architecture/Skyhigh_CASB/About_Skyhigh_CASB)”

## Resposta da recorrida:

As pesquisas apresentadas pela recorrida, se não demonstram imperícia ou profundo desconhecimento, denotam deliberada intenção de apresentar dados desconexos de qualquer lógica. A comprovação utilizada no link: [https://success.skyhighsecurity.com/Skyhigh\\_CASB/Skyhigh\\_CASB\\_Incidents/Policy\\_Incidents/Quarantined\\_Files](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 recorrida 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.

Entretanto, para que não restem dúvidas quanto às capacidades da solução, quanto à definição de políticas de contenção, e sobrem apenas certezas quanto às dúbias intenções da recorrente, destaca-se em comprovação adicional detalhada abaixo, as formas de configuração oferecidas pela plataforma, evidenciadas no link: [https://success.skyhighsecurity.com/Skyhigh\\_Data\\_Loss\\_Prevention/Policy\\_Settings/Quarantine\\_Configuration/Quarantine\\_Configuration](https://success.skyhighsecurity.com/Skyhigh_Data_Loss_Prevention/Policy_Settings/Quarantine_Configuration/Quarantine_Configuration).

Ainda, visando total esclarecimento, embora redundante, mas pertinente, destacar através da tradução do conteúdo abaixo, as plenas capacidades de configuração das ações de contenção requeridas, como observa-se no trecho original, seguidamente do mesmo trecho traduzido:

- **Original:** The Quarantine Configuration tab allows you to enable the Auto-Remediation action for quarantined files: auto-delete, or auto-restore. Or you can choose to not perform any automatic remediation actions, which is the default. Also, you can configure the time limit in days for files to remain in quarantine before the Auto-Remediation action takes effect.
- **Traduzido:** *A guia Configuração de quarentena permite ativar a ação de correção automática para arquivos em quarentena: exclusão automática ou restauração automática. Ou você pode optar por não executar nenhuma ação de correção automática, que é o padrão. Além disso, você pode configurar o limite de tempo em dias para que os arquivos permaneçam em quarentena antes que a ação de correção automática entre em vigor.*

Visando ainda tornar mais claro, o que trecho acima já tornou evidente, destacamos detalhes das capacidades disponíveis de auto-remediação sobre os arquivos indesejáveis deflagrados:

### 3. Auto Remediation Action. Select an action:

- **None.** No files are automatically deleted or restored.
- **Auto-Delete.** Quarantined files are automatically deleted.
- **Auto-Restore.** Quarantined files are automatically restored.
- **Auto-Delete or Auto-Restore After X Days.** Enter the number of days. All quarantined files with the status of New will be deleted or restored after the specified number of days in quarantine.

Evidencia-se, portanto, e de maneira cabal, a reles tentativa da recorrente, de deturpar e desmerecer, com artifícios inúteis, buscar informações de maneira propositadamente errônea, visando apenas se contrapor sem nenhuma base técnica, à decisão da licitante, que reitera-se, já inclusive fora favorável à referida solução.

### 8. Razão técnica número 8 apresentada.

#### Íntegra da alegação:

**“7.49, Deve ser possível obter relatório sobre com resumo do tráfego de e-mail de todos os domínios e por domínio, detecções de ameaças, detecções de arquivos da sandbox, detecções de URL da sandbox e os principais destinatários comprometidos por e-mail (BEC).**

Fica evidente o não atendimento do item 7.49 com a comprovação apresentada através do link <https://www.trellix.com/assets/data-sheets/trellix-email-security-cloud-datasheet.pdf> citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram os tipos de relatórios solicitados no item conforme detalhado abaixo:

relatório sobre resumo do tráfego de e-mail de todos os domínios, relatório sobre resumo do tráfego de e-mail domínio, relatório sobre detecções de ameaças, relatório sobre detecções de arquivos da sandbox, relatório sobre detecções de URL da sandbox e relatório sobre os principais destinatários comprometidos por e-mail (BEC)

Considerando o item 7.49, o trecho anexado para comprovar não menciona a capacidade de geração de relatórios, apenas mostra as funcionalidades de proteção de forma rasa e não detalhada.

*"Trellix Email Security – Cloud offers industry-leading detection to identify,*

*isolate, and immediately stop ransomware, business email compromise, spear phishing, impersonation, and attachment-based attacks before they enter your environment." Tradução livre:*

*"O Trellix Email Security – Cloud oferece detecção líder do setor para identificar, isolar e interromper imediatamente ransomware, comprometimento de e-mail comercial, spear phishing, falsificação de identidade e ataques baseados em anexos antes que eles entrem em seu ambiente."*

A comprovação não menciona quais são os relatórios disponíveis na solução para obter resumo das informações citadas como domínio, detecções de ameaças, arquivos, sandbox e possíveis ameaças de fraude.

A visualização de relatórios detalhados oferece transparência sobre estatísticas e números de detecções relacionadas às mensagens trafegadas por domínio. Por isso, como forma de obter informações resumidas sobre

determinadas métricas torna-se importante para que os administradores da solução possam reportar sobre os seguintes pontos:

*E-mails trafegados por domínio:* permite entender o volume padrão esperado de tráfego no CJF. Além de possibilitar a detecção de possíveis campanhas maliciosas (representadas em picos de tráfego, por exemplo).

*Detecções de ameaças:* listar quais e quantos artefatos maliciosos trafegam via email;

*Artefatos analisados em sandbox:* permite entender quais e quantos artefatos foram considerados desconhecidos e necessitaram de análise aprofundada.

*Usuários comprometidos:* identificação de usuários alvo de fraude.”

### **Resposta da 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.

Desta forma, não merece prosperar a alegação da Recorrente, merecendo seu recurso ser julgado improcedente, mantendo-se, incólume, a r. decisão que habilitou e declarou vencedora do certame a empresa BLUE EYE.

### **9. Razão técnica número 9 apresentada.**

#### **Íntegra da alegação:**

**“8.36 Deve fornecer mecanismos de gestão e governança que permitam a identificação e avaliação de riscos sobre os ativos da organização, em conformidade com as recomendações do NIST (National Institute of Standards and Technology).**

*Fica evidente o não atendimento do item 8.36 com a comprovação apresentada através dos links abaixo citados na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram o atendimento em conformidade com as recomendações do NIST (National Institute of Standards and Technology).*

[https://docs.trellix.com/pt-BR/bundle/helix\\_pg/page/UUID-d520f6cb-8bca-2072-a115-c0c697ea6fb9.html](https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-d520f6cb-8bca-2072-a115-c0c697ea6fb9.html)

[https://docs.trellix.com/pt-BR/bundle/helix\\_pg/page/UUID-dbec0981-b6dd-c9f3-367a-a8ccf9c84e23.html](https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-dbec0981-b6dd-c9f3-367a-a8ccf9c84e23.html)

*O NIST é conhecido por seu papel central no estabelecimento de padrões e diretrizes que são amplamente adotados não apenas nos Estados Unidos, mas também internacionalmente. As publicações do NIST são frequentemente referenciadas como fontes confiáveis para práticas e padrões de segurança, confiabilidade e eficiência em tecnologias e processos.*

*A agência é notável por suas diretrizes e padrões de segurança da informação. O Framework de Gerenciamento de Riscos de Cybersecurity do NIST (NIST Cybersecurity Framework) é uma referência amplamente adotada para organizações que buscam melhorar sua postura de segurança cibernética, por isso é de extrema importância o atendimento ao item 8.36. Seguir padrões definidos traz maior ASSERTIVIDADE e ROBUSTEZ à solução adquirida.*

*A solução fornecida claramente não fornece um índice global de risco, conforme item 8.37, onde o cálculo de risco utiliza as diretrizes do NIST.*

*Para uma melhor compreensão, o NIST é um dos frameworks de segurança da informação mais utilizados no mundo. Ele fornece uma estrutura e ajuda as empresas a entenderem, comunicarem e gerenciarem os riscos cibernéticos.*

*O NIST oferece diretrizes valiosas para as organizações fortalecerem sua postura de segurança cibernética. Ao abordar as funções de Identificar, Proteger, Detectar, Responder e Recuperar, as empresas podem desenvolver uma estratégia abrangente de cibersegurança.*

*O NIST também permite priorizar as atividades de segurança cibernética. Ele fornece um guia passo a passo sobre como estabelecer ou melhorar seu programa de gerenciamento de riscos de segurança de informações.*

The top screenshot displays the 'Asset-based alert correlation table' page. It features a table with the following columns and descriptions:

Column	Description
Risk	The alert risk is represented by a series of colored dots. <ul style="list-style-type: none"><li>Four red dots indicate that the alert is a critical alert.</li><li>Three orange dots indicate that the alert is an alert with high risk.</li><li>Two yellow dots indicate that the alert is an alert with medium risk.</li><li>One blue dot indicates that the alert is an alert with low risk.</li></ul> You can filter the alerts table by selecting the risk ( <b>Critical</b> , <b>High</b> , <b>Medium</b> , or <b>Low</b> ) in the column title. More than one risk can be selected.
Risk Score	The risk score assigned to the asset. You can sort in ascending or descending numeric order.
Asset Name	The name of the asset. You can enter filter based on the name. Enter all or part of an asset name in the column heading.
Alerts	The number of alerts related to this asset. Closed alerts are not included in this number. Click the number to view the alerts table in the asset details page.
Asset Type	The type of asset. You can filter by asset type ( <b>Host</b> , <b>User</b> , or <b>All</b> ).

The bottom screenshot displays the 'Using asset-based alert correlation' page. It explains that Helix analyzes organizational-level assets (or entities) to identify potential insider threats. It lists several key features and pages:

- Asset-Based Alert Correlation page**—A 30-day view of user and host entities that Helix automatically analyzed to identify potential threats. See [Entity-based alert correlations](#).
- Entities page**—Users and hosts with detections tracked by Helix over the last 30 days. See [Entities](#).
- Asset details page**—Information about individual hosts or users, and related assets (if any). See [Asset details](#).
- Summary Dashboard**—Widgets on the dashboard quantify the potential threats within your organization and the assets that post the biggest potential security threats. See [Summary Dashboard](#).
- Index Searches**—Index search has keys that allow you to build a search query based on assets. Index Search Results allows you to search based on asset attributes. See [Asset-based searches](#).
- Risk Assessments**—Detections are captured for each type of asset. The risk score of a detection is based on the severity of the rule and the alert that was triggered. If you close an alert after assigning it to a case and investigating it, the risk score for the entity is reduced by the risk score of that detection.

*Além disso, o documento de configuração não faz menção a qualquer regulamentação para a análise de risco da organização e utiliza análise própria para categorização de risco que traz, consequentemente, menor credibilidade.*

*Portanto, torna-se vital que as soluções ofertadas possuem mecanismos de gestão e governança que permitam a identificação e avaliação de riscos sobre os ativos da organização, em conformidade com as recomendações do NIST.*

*O NIST é planejado para ser um documento vivo que é refinado, aprimorado e evolui com o tempo. Essas atualizações ajudam o Framework a acompanhar as tendências de tecnologia e ameaças, integrar as lições aprendidas e transformar as melhores práticas em práticas comuns.*

*Consequentemente, as soluções que não possuem mecanismos de gestão e governança que permitam a identificação e avaliação de riscos sobre os ativos da organização, em conformidade com as recomendações do NIST, são soluções obsoletas, ultrapassadas e que colocaram em risco o ambiente de tecnologia do CJF.*

*Desta forma, restou comprovado que a solução ofertada NÃO ATENDE AO EDITAL.”*

### **Resposta da recorrida:**

Neste item, mais uma vez a recorrente tenta interpretar dados de forma a direcionar o edital para o atendimento da plataforma comercializada por ela própria. Sabemos da importância do NIST e do seu papel em indicar a direção em muitos aspectos de segurança a nível global, porém a adesão ao framework do NIST não é uma ferramenta ou processo isolado, mas sim um conjunto de ações de governança, que quando coordenados em conjunto vão possibilitar alcançar diferentes objetivos de gestão sobre a cibersegurança.

Observando o documento citado [https://docs.trellix.com/pt-BR/bundle/helix\\_pg/page/UUID-dbec0981-b6ddc9f3-367a-a8ccf9c84e23.html](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](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.

Apenas de forma cabal e complementar, temos a referência <https://www.trellix.com/about/public-policy/partnerships/> que demonstra a participação da Trellix com influência em tais institutos, o que assegura a aderência a padrões globais de referência em cibersegurança.

### **10. Razão técnica número 10 apresentada.**

#### **Íntegra da alegação:**

##### **8.37 Deve fornecer um índice global de risco.**

*“Fica evidente o não atendimento do item 8.37 com a comprovação apresentada através do link [https://docs.trellix.com/pt-BR/bundle/helix\\_pg/page/UUID-64524f51-71d6-6c7b-8683-173222bee874.html](https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-64524f51-71d6-6c7b-8683-173222bee874.html) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstra que existe uma pontuação da organização, ou seja, não apresenta o índice global de risco.*

No documento da Trellix, mencionam três tipos de pontuação de risco que são calculados de forma SEPARADA: por ALERTA, por CORRELAÇÃO (conjunto de alerta) ou por ASSET.

O gerenciamento de riscos em uma organização refere-se ao processo de identificar, avaliar, controlar e monitorar os riscos que podem afetar seus objetivos e operações. O objetivo é tomar decisões informadas para mitigar ou controlar os riscos, equilibrando oportunidades e ameaças de forma eficiente. Um índice global de risco, representado por um índice geral, é usado para fornecer uma visão consolidada do ambiente de risco da organização.

O índice global de risco é usado para avaliar a resiliência da organização. Portanto, a importância de consumir esta informação como forma de comunicação na própria equipe do CJF, facilitando de gestão e definição de próximos passos.

Conforme documentação do fabricante, as métricas de cálculo são analisadas de forma separada, a pontuação de risco indica a gravidade de uma ameaça e não a gravidade global de risco da organização

É importante deixar claro que a pontuação de risco indica a gravidade de uma ameaça não irá apresentar o quão exposta está a organização para sofrer um ataque cibernético, ou seja, se o CJF solicita essa funcionalidade é porque demonstra preocupação global da organização e não somente sobre a pontuação de risco de uma ameaça isoladamente.

Observem no texto abaixo retirado da documentação fornecida que não existe qualquer relação para atendimento ao item, como reproduzido abaixo:

*“In Helix, the risk score indicates the severity of a threat. The higher the risk score, the more severe the threat. Separate risk scores are calculated for alerts, correlations, and assets.*

**Alert risk score**

*An alert risk score is calculated from the severity and confidence of an alert.*

**Correlation risk score**

*A correlated threat is a collection of multiple alerts. The correlation risk score is calculated by multiplying the sum of the individual alert risk scores by the unique number of rules, and then dividing by the total number of alerts in the correlation group.*

*If a VIP asset is affected by a threat, the risk score is automatically set to 100, irrespective of the risk score derived from the formula. If you tag or untag an asset as a VIP asset, the risk score is automatically recalculated.*

**Asset risk score**

*You can view the asset risk score on the Assets page. The table displays VIP assets first, sorted by risk score, followed by all other assets sorted by risk score. The asset risk score is calculated by multiplying the sum of the risk scores of all open and reopened alerts on the asset by the unique number of rules across all open and reopened alerts on the asset, and then dividing by the total number of open and reopened alerts on the asset.*

*The following table displays the risk score and the corresponding severity of the threat.”*

Tradução livre:

*“No Helix, a pontuação de risco indica a gravidade de uma ameaça. Quanto maior a pontuação de risco, mais grave é a ameaça. Pontuações de risco separadas são calculadas para alertas, correlações e ativos.*

**Pontuação de risco de alerta**

*Uma pontuação de risco de alerta é calculada a partir da gravidade e da confiança de um alerta.*

**Pontuação de risco de correlação**

*Uma ameaça correlacionada é uma coleção de vários alertas. A pontuação de risco de correlação é calculada multiplicando a soma das pontuações de risco de alerta individuais pelo número exclusivo de regras e, em seguida, dividindo pelo número total de alertas no grupo de correlação.*

*Se um ativo VIP for afetado por uma ameaça, a pontuação de risco será automaticamente definida como 100, independentemente da pontuação de risco derivada da fórmula. Se você marcar ou desmarcar um ativo como VIP, a pontuação de risco será recalculada automaticamente.*

### **Pontuação de risco de ativos**

*Você pode visualizar a pontuação de risco do ativo na página Ativos. A tabela exibe primeiro os ativos VIP, classificados por pontuação de risco, seguidos por todos os outros ativos classificados por pontuação de risco. A pontuação de risco do ativo é calculada multiplicando a soma das pontuações de risco de todos os alertas abertos e reabertos no ativo pelo número exclusivo de regras em todos os alertas abertos e reabertos no ativo e, em seguida, dividindo pelo número total de alertas abertos e reabertos. alertas sobre o ativo.*

A tabela a seguir exibe a **pontuação de risco e a gravidade correspondente da ameaça.**”

*Observem que a pontuação de risco está sempre atrelada a uma **ameaça e não de forma global**, ou seja, o CJF terá apenas uma visão do índice de risco de um determinado ativo conforme detalhado no texto mencionado acima do fabricante.*

*O próprio texto deixa claro que ameaça correlacionada é uma coleção de vários alertas. A pontuação de risco de correlação é calculada multiplicando a soma das pontuações de risco de alerta individuais pelo número exclusivo de regras e, em seguida, dividindo pelo número total de alertas no grupo de correlação. Para não restar dúvidas, um ativo (endpoints ou servidor ou usuário etc) podem ter várias ameaças e a documentação apresentada deixa claro que será feito um cálculo para um determinado ativo e não um índice global considerando todos os ativos existentes no ambiente do CJF.*

*Um índice global de risco cibernético ajudará a identificar a tendência global de um ataque dentro da organização, ou seja, apresentará o quanto (índice global) a organização está exposta para sofrer um ataque cibernético, quanto maior o índice global, mais exposta a sofrer um ataque cibernético. Os ataques cibernéticos podem afetar a reputação, a capacidade financeira, as operações comerciais e a confiança do cliente de uma empresa.*

*A quantificação de riscos cibernéticos é uma área emergente onde a automação e a análise de dados podem agregar insights e ajudar na priorização de riscos.*

*Claramente a solução ofertada não possui uma métrica global de risco para a organização, ou seja, será fornecido apenas a pontuação de risco para uma ameaça, consequentemente a solução ofertada não atende aos requisitos do edital e não é suficiente para a adoção do processo de gerenciamento de risco.*

*Se o CJF não tiver conhecimento do seu risco cibernético global, como ter certeza de que estão protegidos contra ataques cibernéticos.*

*Desconsiderar o atendimento ao item, é aceitar soluções obsoletas colocando o ambiente do CJF em risco, uma vez que o CJF não terá conhecimento do quão exposto está seu ambiente tecnológico.*

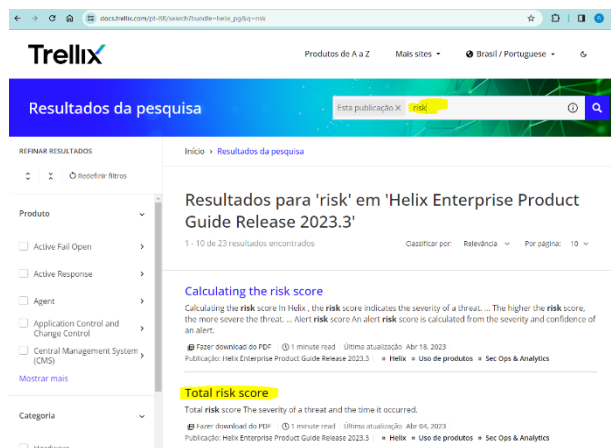
*O Índice Global de Risco Cibernético é uma ferramenta valiosa para compreender e gerenciar os riscos cibernéticos em todo o mundo. É importante que as empresas estejam cientes dos riscos e tomem medidas para se protegerem.”*

### **Resposta da recorrida:**

Não obstante às vexatórias tentativas de deturpar as funcionalidades apresentadas, e uma vez mais reitera-se, já aceitas pela licitante, a recorrente demonstra extremo esforço em pesquisar na documentação, deliberadamente somente aquilo que a interessa. Ora, se tal pesquisa os fez até localizar as métricas de cálculo de risco do motor de UEBA (User and Entities Behavior Analytics), função essa, que eles mesmos alegaram não estar presente na solução ofertada na razão técnica contestada de número 14.

Dessa forma, e para dissuadir quaisquer possíveis dúvidas intencionalmente 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. Vide exemplo na imagem abaixo, realizado na própria URL utilizada pela recorrente em sua alegação. Onde vê-se, que o primeiro link é o link apresentado pela recorrente, e o segundo, o item que desmentiria as suas vis alegações.



- Ainda que não sejam suficientes as comprovações acima, destacamos o referido link que demonstra irrefutavelmente a capacidade de exibir de maneira global um panorama geral sobre todas as métricas de risco, em um dashboard que indica em gráfico de linha, o risco acumulado da organização (risco total), que pode ser exibido dentro de linhas de tempo específica, 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](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.
- Em aprofundamento, embora os alegados descumprimentos já tenham sido dirimidos pelas informações acima, destacamos funcionalidade agregada à plataforma Trellix XDR, que fornece integração de Threat Intelligence ao XDR, mas também um panorama geral de risco à dentro do contexto da organização, 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:
  - Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.
  - 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.)



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

Com base nas informações técnica acima dispostas, resta demonstrado, mais uma vez, que a solução da empresa Recorrida atende ao exigido no Edital, devendo manter na íntegra a r. decisão administrativa.

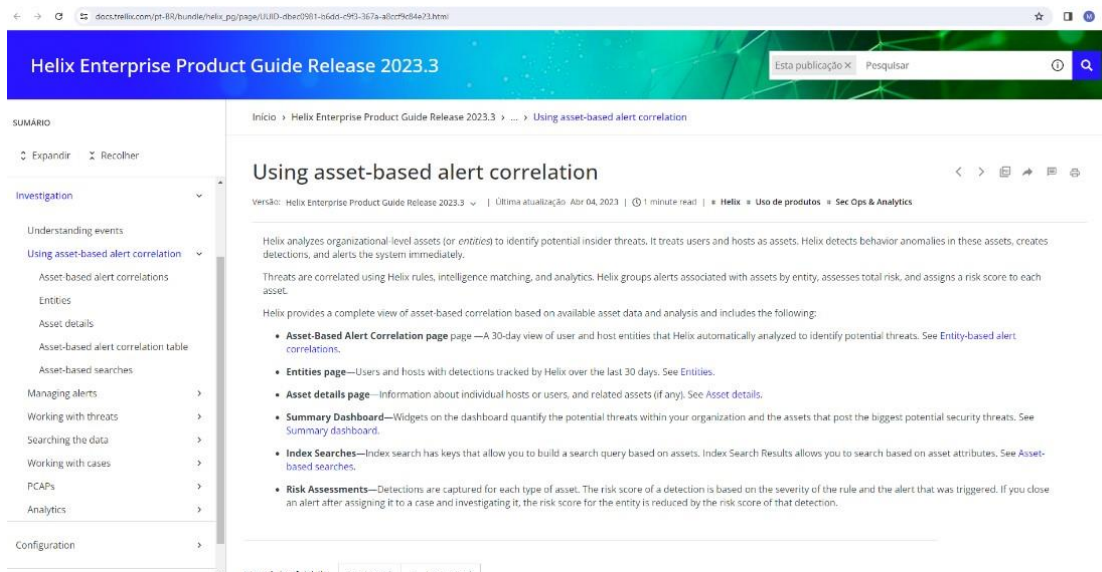
## **11. Razão técnica número 11 apresentada.**

### **Íntegra da alegação:**

**“8.38 Deve fornecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.**

*Fica evidente o não atendimento do item 8.38 com a comprovação apresentada através do [https://docs.trellix.com/pt-BR/bundle/helix\\_pg/page/UUID-dbec0981b6dd-c9f3-367a-a8ccf9c84e23.html](https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-dbec0981b6dd-c9f3-367a-a8ccf9c84e23.html) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram as sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.*

*Claramente, não existe na documentação as recomendações para mitigação dos riscos detectados e listados pela solução, ou seja, não é possível ter as sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.*



*Isto é, a equipe técnica do CJF não obteria o direcionamento do fabricante para melhorar a postura de segurança baseada nos riscos observados no ambiente. Uma vez que os riscos são avaliados, o CJF pode desenvolver estratégias para controlar, mitigar ou tratar esses riscos. Isso envolve a implementação de medidas preventivas e de resposta para minimizar o impacto dos eventos adversos. Destaca-se que estas sugestões facilitam o dia a dia para implementação de gerenciamento de risco adequado e assertivo.*

*Conforme já explicado no item anterior (8.37), a solução ofertada não apresenta o risco geral da organização tão pouco será capaz de oferecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.*

*O CJF entende que ao solicitar que a solução seja capaz de oferecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral é para:*

- *Detectar rapidamente qualquer problema antes de um ataque causar um grande impacto na organização o.*
- *Responder rapidamente para gerir os riscos durante um incidente ciberne tico.*
- *Implementar medidas para mitigar os riscos advindos de falhas de segurança ciberne tica, e que possam ter acesso aos sistemas da empresa ou a seus dados.*
- *Elaborar um plano de açã o para lidar com incidentes ciberne ticos.*

*Diante do exposto, existem evidências que a solução ofertada pela LICITANTE não é capaz de fornecer as sugestões para melhorar a postura de segurança do CJF, baseado nos alertas de risco, o que inviabiliza a definição das ações da equipe técnica do CJF e dificulta o processo de gerenciamento de riscos.”*

## **Resposta da recorrida:**

Em atenção às comprovações necessárias, esclarecemos que os índices e evidências anexos na comprovação técnica, objetivam demonstrar o atendimento do item de maneira clara, porém concisa, mas diante de tentativas desqualificadas e infundadas de desmerecer, distorcer ou desmentir as comprovações, já inclusive aceitas pelo licitante, faz-se necessário elaborar comprovações mais detalhadas, para que nem mesmo o desconhecimento ou imperícia daqueles que atentam contra as evidências apresentadas e aceitas, as possam desqualificar, sendo necessário portanto, seguirmos ao extenso, mas, minucioso esclarecimento das funções da plataforma ofertada, que permitem a gestão de fim-a-fim do risco incidente à organização.

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](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](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](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](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](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-](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](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 específica, 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](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. Razão técnica número 12 apresentada.**

### **Íntegra da alegação:**

**“8.39 Deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.**

Fica evidente o não atendimento do item 8.39 com a comprovação apresentada através do [https://docs.trellix.com/pt-BR/bundle/helix\\_pg/page/UUID-64524f5171d6-6c7b-8683-173222bee874.html](https://docs.trellix.com/pt-BR/bundle/helix_pg/page/UUID-64524f5171d6-6c7b-8683-173222bee874.html) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.

A documentação não comprova como é atendida a necessidade de um guia para redução de risco da organização. Novamente é demonstrado o não atendimento aos itens relativos ao gerenciamento de risco solicitado pelo CJF.

Ao não fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor, a organização fica vulnerável a uma série de riscos decorrentes de erros humanos não identificados e corrigidos. Isso pode resultar em exposição a ameaças cibernéticas e vulnerabilidades de segurança que permanecem não detectadas, aumentando a probabilidade de incidentes de segurança e comprometendo a integridade, confidencialidade e disponibilidade dos dados e sistemas da organização. Além disso, a ausência de um índice de risco preciso dificulta a priorização e implementação de medidas de segurança proativas para mitigar os riscos identificados.

Assim, o índice de risco pode ajudar as empresas a garantir que suas configurações de produtos estejam em conformidade com os requisitos regulatórios e de segurança. Ao identificar as configurações de produtos que apresentam maior risco, o índice de risco pode ajudar a evitar erros que podem levar a custos significativos.

O índice de risco fornece uma avaliação quantitativa do nível de risco associado a diferentes configurações de produtos.

*É evidente que a solução ofertada não possui um posicionamento robusto para aplicação de conceitos, métricas e processos para que o CJF possa implementar de forma eficaz no ambiente e no cotidiano. Não existe índice global de risco, sugestões de mitigação e não utilizam padrão reconhecido pelo mercado, NIST, exigido pelo CJF.”*

### **Resposta da recorrida:**

Mais uma vez temos a empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA buscando confabular fatos infundados, demonstrando sua falta de compromisso com a veracidade das informações e também falta de conhecimento técnico para julgar as comprovações apresentadas.

A plataforma Helix, da Trellix é de fato uma plataforma de XDR, pois a mesma possui uma característica especial que é ser agnóstica, ou seja, ela trabalha integrada com todo o ambiente da CONTRATADA, independentemente de quais fabricantes de tecnologias estejam sendo utilizadas. Portanto, quando avaliamos as notas de risco apresentadas no documento referenciado, elas sempre estarão apontando para as plataformas integradas, ou seja, todos os alertas e notas de risco atribuídos serão alimentados e regidos pela integração com as outras plataformas já existentes no ambiente.

Portanto a afirmação da recorrente, mais uma vez se mostra infundada e até mesmo incoerente do ponto de vista técnico.

Vale ressaltar ainda a capacidade da plataforma Helix em interagir com as ferramentas integradas, de forma a mitigar os alertas deflagrados, ou seja, se existe um alerta a partir de um evento do Firewall, o próprio produto irá interagir, de forma automática, com o firewall, independentemente de seu fabricante, para corrigir o problema de segurança, ou seja, o objetivo da ferramenta não é apenas gerar uma nota de risco, mas sim além de emitir a nota de risco, cobrir de fim-a-fim todo o ciclo de vida do incidente, desde sua detecção, até as suas tratativas de investigação, resposta e mitigação, impedindo assim de forma automática, que comportamentos indesejados ou maliciosos possam retornar a ocorrer ou mesmo se alastrar no ambiente.

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](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](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](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:
  - Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.
  - 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.)
  - Medidas preditivas (proativas) de segurança, permitindo à organização, precaver-se contra uma ou mais campanhas, ataques, atores, ou indicadores pesquisáveis dentro da plataforma.
  - 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. Razão técnica número 13 apresentada.**

#### **Íntegra da alegação:**

**“8.42 Deve ser possível realizar benchmarking em tempo real com comparação de nível de risco.**

Fica evidente o não atendimento do item 8.42 com a comprovação apresentada através do link [https://docs.trellix.com/bundle/helix\\_pg/page/UUID-367f0730bcdd-8bf1-e384-70f790b85e1d.html](https://docs.trellix.com/bundle/helix_pg/page/UUID-367f0730bcdd-8bf1-e384-70f790b85e1d.html) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram ser possível realizar benchmarking em tempo real com comparação de nível de risco.

Observem no texto abaixo retirado da documentação fornecida que não existe qualquer relação para atendimento ao item, como reproduzido abaixo:

*Click the Timeline tab on an alert's details page to view and explore a timeline of events associated with this alert. Hover over an associated alert to display the name of the alert, the time the alert was detected, the alert ID, and its related value. Click View Alert to open the alert details page for that alert. The timeline also displays any correlated alerts.*

Tradução livre:

*Clique na guia Linha do tempo na página de detalhes de um alerta para visualizar e explorar uma linha do tempo de eventos associados a esse alerta. Passe o mouse sobre um alerta associado para exibir o nome do alerta, a hora em que o alerta foi detectado, o ID do alerta e seu valor relacionado. Clique em Exibir alerta para abrir a página de detalhes desse alerta. A linha do tempo também exibe alertas correlacionados.*

*Benchmarking é um método utilizado para comparar as práticas de segurança cibernética com organizações do mesmo segmento e pode revelar melhores práticas que podem ser incorporadas para fortalecer a postura cibernética. Inclui configurações, procedimentos, tecnologias e abordagens de resposta a incidentes.*

*O benchmarking é uma forma de observar como outras organizações respondem às ameaças emergentes e pode ajudar na preparação para desafios futuros. Combinado com as recomendações de mitigação de riscos, o benchmarking auxiliará o CJF no direcionamento para construção de configuração, tecnologia, processos robustos, como objetivo de aumentar a resiliência cibernética.*

*O benchmarking em tempo real com comparação de nível de risco cibernético é uma prática crucial para auxiliar empresas e organizações a fortalecerem sua postura de segurança diante das crescentes ameaças digitais. Através da comparação contínua de suas medidas de segurança com as de outras empresas do mesmo setor ou porte, é possível identificar áreas de risco, avaliar a efetividade das medidas existentes e implementar ações proativas para mitigar vulnerabilidades e por exemplo alguns benefícios:*

*Monitoramento constante da postura de segurança da organização em comparação com seus pares do setor.*

*Identificação de lacunas de segurança e implementação de medidas corretivas para fortalecer a postura de segurança da organização.*

*Aprimoramento contínuo das medidas de segurança, acompanhando a evolução das ameaças cibernéticas.*

*Base de dados com informações atualizadas sobre o nível de risco cibernético de diferentes empresas do setor.*

*Suporte para a tomada de decisões estratégicas sobre investimentos em segurança cibernética.*

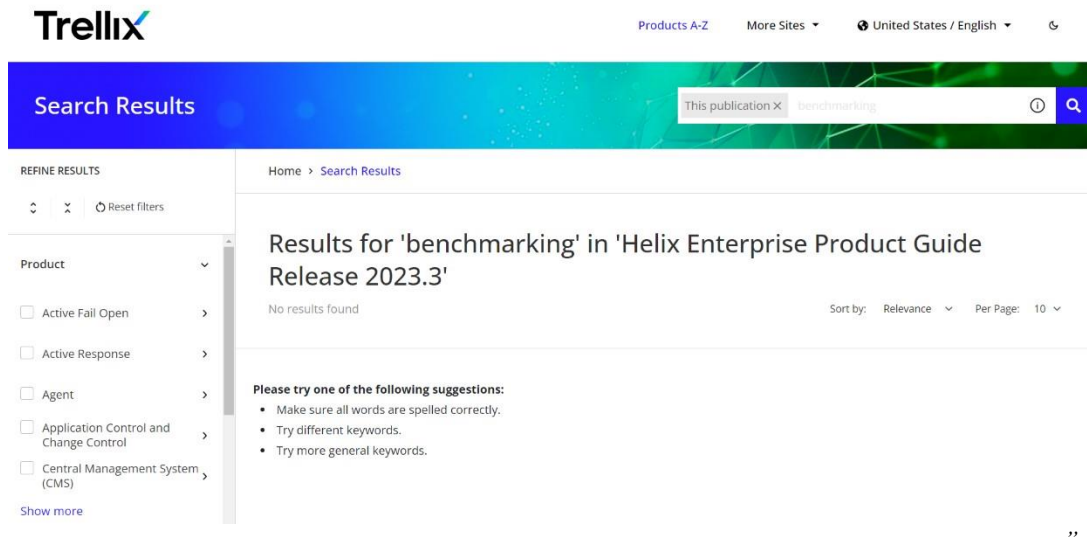
*Alocação eficiente de recursos para as áreas de maior risco, otimizando o orçamento de segurança da organização.*

*Diferenciaça o por meio de uma postura de segurança robusta e proativa.*

*Sendo mais objetivo, o benchmarking irá apresentar se a organização está no caminho certo quando se comparado com empresas do mesmo setor ou tamanho.*

*É evidente o não cumprimento da necessidade de benchmarking, ferramenta de comparação em tempo real capaz de oferecer uma referência de índice de risco praticado em organizações públicas.*

*O documento anexado ao ponto a ponto não cita funcionalidade correspondente, pelo contrário, traz um contexto que não condiz com o solicitado no item referido, ressaltando, inclusive, o não cumprimento da funcionalidade. Destaca-se que em nenhuma página da documentação pública da fabricante é mencionado quaisquer formas de benchmarking conforme demonstrado abaixo.*



### **Resposta da recorrida:**

Mais uma vez temos a empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA buscando confabular fatos infundados, demonstrando sua falta de compromisso com a veracidade das informações e também falta de conhecimento técnico para julgar as comprovações apresentadas.

O recurso indicado no link referenciado, visava de maneira concisa, apresentar, uma das muitas funcionalidades de análise e comparação de risco disponível na plataforma, que se utiliza da correlação global de dados de ameaças, integrada por um dos motores de Threat Intelligence presentes na plataforma, que busca junto das linhas de tempo e dicas de investigação “Investigation Tips”, fornecer contexto externo de inteligência em pesquisa de ameaças ou Threat Hunting, a partir da expertise do fabricante.

Contudo, diante de tamanho e inverossímil ataque da recorrente, destacamos em minuciosos detalhes as funcionalidades agregadas nativamente por esta capacidade, 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:
  - Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.
  - Ataques associados à uma ou mais indústrias e comparativos (benchmarking) 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.)
  - Medidas preditivas (proativas) de segurança, permitindo à organização, precaver-se contra uma ou mais campanhas, ataques, atores, ou indicadores pesquisáveis dentro da plataforma.
  - 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>

Ficando, assim, de maneira irrefutável, comprovado e irrevogável o atendimento sobre a capacidade exigida, dentro das qualidades mínimas exigidas para a funcionalidade, demonstrando-se ainda, todas aquelas ainda, que superam a expectativa expressa pelo item.

#### **14. Razão técnica número 14 apresentada.**

## Íntegra da alegação:

### “8.46 Deve fornecer um guia para reduzir fatores de risco detectados

Fica evidente o não atendimento do item 8.46 com a comprovação apresentada através do link <https://www.trellix.com/assets/data-sheets/trellix-helix-enterprise-datasheet.pdf> citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não fornecem um guia para reduzir fatores de risco detectados.

Diante de mais um item sobre gerenciamento de riscos, a LICITANTE comprova de forma duvidosa, anexando apenas um datasheet. O item claramente solicita um guia para mitigação de riscos identificados na solução a ser adquirida pelo CJF. Fica claro o não atendimento às funcionalidades descritas no Termo de Referência. Ressaltase que o único trecho que menciona riscos (risk) a seguir:

*User and entity behavior analytics (UEBA)*

*Correlate alerts with machine learning to identify activities that suggest a high risk of insider threats, lateral movement, or final-stage attacks ✓Traduça o Livre:*

*Ana lise de comportamento de usuarios e entidades (UEBA)*

*Correlacione alertas com aprendizado de maquina para identificar atividades que sugerem alto risco de ameaças internas, movimentos laterais ou ataques em esta gio final*

Da mesma forma que o item 8.38 não é cumprido pela fabricante, o item 8.46 também não é. Não restam dúvidas quanto aos benefícios gerados a partir do direcionamento/guia e de recomendações para melhoria da postura de segurança do CJF. Novamente, não foram encontradas evidências que a TRELIX atende ao item e, destaca-se inclusive, a tentativa de incluir trechos de comprovação que não dizem respeito ao assunto do item.

Conforme documentação apresentada pela LICITANTE, correlacionar alertas não significa **fornecer um guia** para reduzir fatores de risco detectados.

Ao implementar as medidas recomendadas em um guia adequado, as organizações podem aumentar significativamente sua segurança cibernética e proteger seus ativos contra diversas ameaças e trazendo alguns benefícios:

*Um guia ajuda as organizaço es a priorizar seus esforços de segurança ciberne tica, concentrando-se nos riscos mais relevantes e com maior impacto potencial. Isso otimiza o uso de recursos e garante que as medidas de segurança sejam mais eficazes.*

*Fornecer um guia aumenta a consciencializaça o dos membros da organizaça o sobre os riscos ciberne ticos e as melhores pra ticas para mitiga -los. Isso pode levar a uma cultura de segurança mais forte e a um comportamento mais seguro por parte dos usuarios.*

*Diversas leis e normas exigem que as organizaço es implementem medidas de segurança para proteger dados e sistemas. Um guia pode ajudar as organizaço es a demonstrar conformidade com essas regulamentação es.*

*A implementaçã o das medidas de um guia pode fortalecer significativamente a postura de segurança geral de uma organizaça o, tornando-a mais resiliente a ataques ciberne ticos.*

*O guia de recomendação para mitigação capacita a equipe a tomar ações proativas para reduzir ou eliminar os riscos identificados. Auxilia a evitar a ocorrência de incidentes indesejados. A plataforma que fornece recomendações criando um ciclo de melhoria contínua e à medida que as recomendações são implementadas e os resultados são avaliados, o CJF pode ajustar suas práticas de mitigação com base nas lições aprendidas, criando um processo contínuo de melhoria.”*

## Resposta da recorrida:

De maneira incoerente, e já exaustiva, percebe-se ou, que a recorrente desferiu à esmo e sem qualquer critério, acusações e contestações de maneira desleixada, ou que, houve dolo motivado por litigância de má fé, pois refuta informações arduamente já comprovadas em itens anteriores, levantando-se questão sobre a seriedade de suas

manifestações ou mesmo demonstrando total imperícia no exame das evidências, que reitera-se, já foram aceitas pelo licitante.

Diante disso, e contribuindo de maneira séria e consciente, novamente dispomos abaixo comprovação minuciosa, sobre o irrefutável atendimento do item desta especificação técnica.

No link [https://docs.trellix.com/pt-BR/bundle/helix\\_pg/page/UUID-885433ce-9217-cfac-e6eb-6afb15513d96.html](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](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](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](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](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](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](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 específica, 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](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 inequívoca o item contestado, oferecendo ainda ampla granularidade sobre os pontos percorridos, 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:
  - Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.
  - 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.)
- Medidas preditivas (proativas) de segurança, permitindo à organização, precaver-se contra uma ou mais campanhas, ataques, atores, ou indicadores pesquisáveis dentro da plataforma.
- 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>

Diante das informações acima, resta demonstrado que a solução ofertada pela Recorrida, ao contrário do alegado pela empresa ALLTECH SOLUÇÕES, atende, na íntegra aos requisitos editalícios, não havendo qualquer embasamento fático, técnico ou jurídico que corrobore com as informações falsamente apresentadas no recurso ora combatido.

### **15. Razão técnica número 15 apresentada.**

#### **Íntegra da alegação:**

**“8.47 Deve permitir definir um objetivo de redução de risco.**

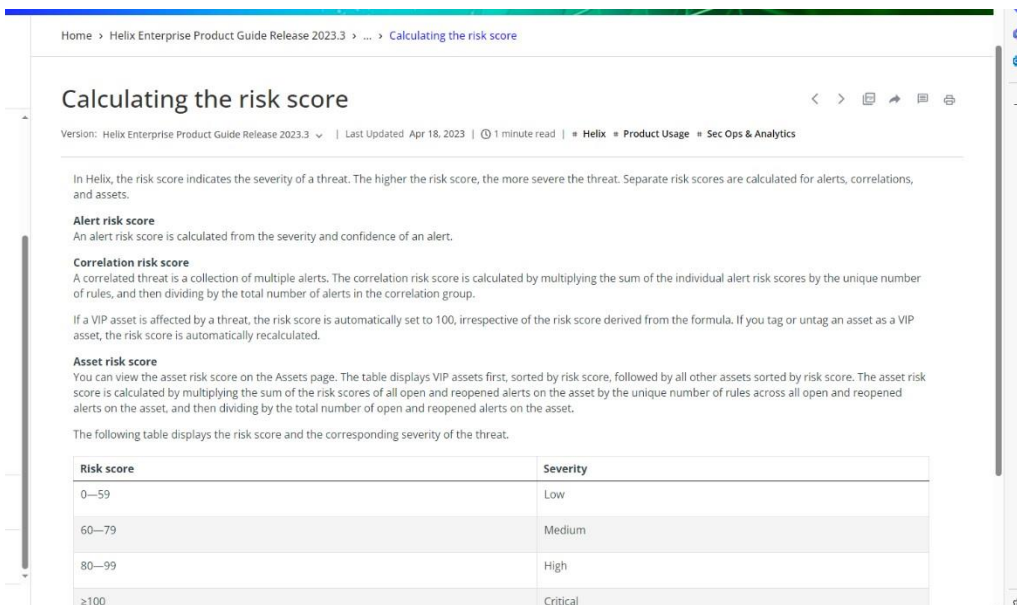
**e**

**8.48 Visualizar um resumo dos eventos de risco que você deve remediar para alcançar o objetivo selecionado e alterar o status dos eventos de risco.**

Fica evidente o não atendimento dos itens 8.47 e 8.48 com a comprovação apresentada através do link [https://docs.trellix.com/bundle/helix\\_pg/page/UUIDhttps://docs.trellix.com/bundle/helix\\_pg/page/UUID-D-64524f51-71d6-6c7b-8683-173222bee874.html](https://docs.trellix.com/bundle/helix_pg/page/UUIDhttps://docs.trellix.com/bundle/helix_pg/page/UUID-D-64524f51-71d6-6c7b-8683-173222bee874.html) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende

aos requisitos e não permitem definir um objetivo de redução de risco e não é possível visualizar um resumo dos eventos de risco que você deve remediar para alcançar o objetivo selecionado e alterar o status dos eventos de risco.

A comprovação utilizada não menciona uma meta/objetivo para o índice de risco da organização e muito menos um resumo dos eventos de riscos que devem ser mitigados conforme tela abaixo.



Home > Helix Enterprise Product Guide Release 2023.3 > ... > Calculating the risk score

## Calculating the risk score

Version: Helix Enterprise Product Guide Release 2023.3 | Last Updated Apr 18, 2023 | 1 minute read | Helix # Product Usage # Sec Ops & Analytics

In Helix, the risk score indicates the severity of a threat. The higher the risk score, the more severe the threat. Separate risk scores are calculated for alerts, correlations, and assets.

**Alert risk score**  
An alert risk score is calculated from the severity and confidence of an alert.

**Correlation risk score**  
A correlated threat is a collection of multiple alerts. The correlation risk score is calculated by multiplying the sum of the individual alert risk scores by the unique number of rules, and then dividing by the total number of alerts in the correlation group.

If a VIP asset is affected by a threat, the risk score is automatically set to 100, irrespective of the risk score derived from the formula. If you tag or untag an asset as a VIP asset, the risk score is automatically recalculated.

**Asset risk score**  
You can view the asset risk score on the Assets page. The table displays VIP assets first, sorted by risk score, followed by all other assets sorted by risk score. The asset risk score is calculated by multiplying the sum of the risk scores of all open and reopened alerts on the asset by the unique number of rules across all open and reopened alerts on the asset, and then dividing by the total number of open and reopened alerts on the asset.

The following table displays the risk score and the corresponding severity of the threat.

Risk score	Severity
0—59	Low
60—79	Medium
80—99	High
≥100	Critical

Vale ressaltar que a solução não dispõe de índice global, conforme comprovado neste documento. Portanto, tampouco seria possível definir uma meta a ser atingida por este índice. Resta claro o não atendimento do item. Pode-se concluir, novamente, a falta de funcionalidades importantes para a gestão de riscos como: guia de recomendações, dicas para mitigação de riscos, uso de padrão (NIST) para cálculo de risco e definição de um objetivo de índice para o CJF.

A definição de objetivo ajuda na criação de métricas e indicadores de desempenho específicos relacionados à mitigação de riscos. Isto é, facilita o monitoramento eficaz do progresso na gestão de riscos no cotidiano da equipe técnica do CJF.

Adicionalmente, a gestão de risco cibernético é essencial para proteger ativos, preservar a reputação, cumprir regulamentações, minimizar impactos financeiros, manter a continuidade operacional e promover uma cultura organizacional voltada para a segurança cibernética. Essa abordagem é crucial para enfrentar os desafios de segurança em um ambiente digital cada vez mais complexo.

Portanto, o não cumprimento de funcionalidades importantes para o gerenciamento de riscos, deixa claro que a solução ofertada está aquém do que foi especificado pela equipe técnica diante das necessidades atuais, e das especificações do EDITAL.”

### Resposta da recorrida:

As inúmeras e repetitivas tentativas de deturpar os itens do edital, demonstra inclusive que a solução ofertada pela recorrente não deverá ter capacidades de detecção e resposta estendidas, por isso a forma como são interpretados os requerimentos técnicos do edital recaem tanto à dashboards informativos e muito pouco ou quase nada à inteligência cibernética, expertise em técnicas de detecção e capacidades estendidas de investigação e resposta, como se desejaria que uma solução dita XDR (eXtended Detection & Response) deveria ser.

Para erradicar as infundadas alegações da recorrente, iremos em meticolosos detalhes explicar como a solução Trellix é composta, e oferece total visão de riscos sobre:

- As entidades (usuários e ativos)
  - 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](https://docs.trellix.com/bundle/helix_pg/page/UUID-64524f51-71d6-6c7b-8683-173222bee874.html)
- Os alertas e incidentes
  - Os alertas são eventos suspeitos ou maliciosos (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](https://docs.trellix.com/bundle/helix_pg/page/UUID-36ec00cd-21a3-2652-eebe-9860800f8e0b.html)
- A organização
  - 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 painéis, o painel total de riscos visto no link: [https://docs.trellix.com/bundle/helix\\_pg/page/UUID-dc833c8f-1e7b-5d54-e4fe-a14d9e6f8e7f.html](https://docs.trellix.com/bundle/helix_pg/page/UUID-dc833c8f-1e7b-5d54-e4fe-a14d9e6f8e7f.html)
- Os setores e a indústria da sociedade
  - 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:

- Verificação de campanhas, atores e indicadores globais, quer estes estejam ativos ou mesmo suscetíveis no ambiente.
- 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.)
- Medidas preditivas (proativas) de segurança, permitindo à organização, precaver-se contra uma ou mais campanhas, ataques, atores, ou indicadores pesquisáveis dentro da plataforma.
- 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>

Observe, Ilma. Pregoeira, que o recurso ora combatido não passa de uma tentativa da Recorrente de tumultuar o certame em questão, trazendo informações que não possuem a mínima veracidade, possuindo como intuito prejudicar não só a empresa vencedora, mas, também, o órgão licitante, o que não se pode permitir.

## **16. Razão técnica número 16 apresentada.**

### **Íntegra da alegação:**

**“8.50 Deve permitir as seguintes ações para responder a riscos: Desativar/Ativar conta do usuário - Forçar logout - Redefinir senha - Isolar/Restaurar Endpoint - Monitorar tentativas de login - Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno - Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.**



Fica evidente o não atendimento do item 8.50 com a comprovação apresentada através do link [https://docs.trellix.com/bundle/so\\_sag\\_6-6-0\\_pdf/resource/SO\\_SAG\\_6.6.0\\_pdf.pdf](https://docs.trellix.com/bundle/so_sag_6-6-0_pdf/resource/SO_SAG_6.6.0_pdf.pdf) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram os tipos de ações para responder a risco conforme detalhado abaixo:

*Desativar/Ativar conta do usuário*  
*Forçar logout*  
*Redefinir senha*  
*Isolar/Restaurar Endpoint*  
*Monitorar tentativas de login*  
*Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno*  
*Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.*

Além disso, sequer detalha qual trecho ou página poderia ser considerado para leitura. Sendo evidente que a LICITANTE trouxe documentos de comprovação fora do contexto do item e, portanto, demonstra o não atendimento. As ações listadas são necessárias para uma plataforma de RESPOSTA à incidentes.

As respostas à incidentes são procedimentos e ações planejadas para lidar com eventos adversos que afetam a segurança. Uma resposta eficaz a incidentes é essencial para minimizar danos, preservar evidências e restaurar a normalidade operacional, consequentemente garantir resiliência cibernética do CJF.

As seguintes ações são (e devem) ser consideradas para uma plataforma de XDR, o qual é capaz de agir em eventos suspeitos de forma automatizada ou gerenciada pelo administrador, são eles: Desativar/Ativar conta do usuário, Forçar logout, Redefinir senha, Isolar/Restaurar Endpoint, Monitorar tentativas de login, Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno e Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem. Todas estas são formas esperadas de resposta para uma plataforma robusta de segurança.

É importante ressaltar a necessidade explícita no Termo de Referência, sobre a plataforma centralizada que permite descobrir, analisar e RESPONDER aos alertas e detecções. Portanto, sem a possibilidade de ações de mitigação, uma das principais funções de XDR é perdida.

Abaixo o porquê de tomar **ações para responder a riscos**, detalhado em cada item.

#### **Desativar/Ativar conta do usuário:**

##### **Motivos para desativação:**

*Limitar o acesso a dados confidenciais: Se a conta de um usuário for comprometida, um invasor pode obter acesso a informações e confidenciais da empresa. Desativar a conta impede que o invasor acesse esses dados.*

*Prevenir a propagação de malware: Se a conta de um usuário for infectada com malware, desativá-la pode evitar que o malware se espalhe para outras contas e sistemas.*

*Conter o dano: Desativar a conta de um usuário pode ajudar a conter o dano causado por um incidente cibernético, limitando a capacidade do invasor de realizar ações maliciosas.*

##### **Motivos para reativação:**

*Apois a investigação: Depois que a investigação do incidente cibernético for concluída e a conta for considerada segura, ela pode ser reativada.*

*Necessidade de acesso: Se o usuário precisar acessar dados ou sistemas da empresa para realizar seu trabalho, sua conta pode ser reativada.*

*Resolução do problema: Se o problema que levou a desativação da conta for resolvido, a conta pode ser reativada.*

#### **Forçar logout**

##### **Contenção de danos:**

*Limita o acesso de invasores: Ao forçar o logout de todos os usuários, você impede que hackers e outros invasores explorem vulnerabilidades ou credenciais comprometidas para acessar sistemas e dados confidenciais.*

*Interrompe atividades maliciosas: O forçar logout pode interromper atividades maliciosas em andamento, como a transferência de dados confidenciais ou a instalação de malware.*

#### **Prevenção de ataques em cascata:**

*Reduz a superfície de ataque: Ao desconectar dispositivos e usuários, você reduz o número de pontos de entrada que os invasores podem explorar para se infiltrar em sua rede.*

*Limita o movimento lateral: O forçar logout impede que os invasores se movam lateralmente entre diferentes sistemas e dispositivos dentro da sua rede.*

#### **Proteção de dados confidenciais:**

*Reduz o risco de exfiltração de dados: Ao negar o acesso de usuários não autorizados, você protege dados confidenciais contra roubo ou exfiltração.*

*Minimiza o impacto de uma violação: Se uma violação de dados ocorrer, o forçar logout pode ajudar a minimizar a quantidade de dados que são acessados e/ou roubados.*

#### **Investigação e recuperação:**

*Facilita a investigação: Ao registrar os detalhes de todos os logouts forçados, você pode obter informações valiosas sobre o escopo e o impacto de um ataque cibernético.*

*Acelera a recuperação: O forçar logout pode ajudar a acelerar o processo de recuperação ao limpar a rede de usuários e dispositivos não autorizados.*

#### **Redefinir senha**

***Mitigação de danos:** Se suas informações foram comprometidas, o hacker pode ter acesso à sua senha. Redefinir a senha impede que o hacker continue usando sua conta para causar mais danos, como roubar dados, realizar transações fraudulentas ou enviar spam.*

***Prevenção de ataques futuros:** Uma senha antiga e comprometida pode ser usada para acessar outras contas online, especialmente se você reutilizar a mesma senha em vários sites. Redefinir a senha para uma nova e única torna mais difícil para o hacker acessar outras contas.*

#### **Isolar/Restaurar Endpoint**

##### **Motivos para Isolar um Endpoint:**

*Conter a ameaça: O isolamento impede que a ameaça se espalhe para outros dispositivos na rede.*

*Limitar o dano: Reduz o impacto potencial da ameaça, protegendo dados e sistemas críticos.*

*Facilitar a investigação: Permite a análise forense do endpoint para determinar a origem e o escopo da ameaça.*

*Evitar a reinfecção: Impede que a ameaça retorne ao endpoint após a remoção.*

##### **Motivos para Restaurar um Endpoint:**

*Recuperar o acesso: Permite que os usuários acessem novamente o endpoint e seus dados.*

*Retornar a operação normal: Restaura a funcionalidade do endpoint e da rede.*

*Minimizar a interrupção: Reduz o tempo de inatividade e a perda de produtividade causados pelo incidente.*

### **Monitorar tentativas de login**

*Identificar atividades incomuns, como logins em horários ou locais inesperados, pode indicar um ataque em andamento.*

*Agir rapidamente pode minimizar o impacto do ataque e reduzir o tempo de inatividade.*

*Monitorar logins pode ajudar a identificar e bloquear tentativas de acesso não autorizado a contas e sistemas confidenciais.*

*Isso protege dados confidenciais contra roubo, perda ou uso indevido.*

*Monitorar logins pode ajudar a identificar e rastrear a origem de atividades maliciosas, como ataques de força bruta ou malware.*

*Isso pode ajudar a identificar e corrigir as vulnerabilidades que os invasores estão explorando.*

### **Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno**

*Conter a propagação de malware: Bloquear aplicativos internos infectados com malware pode ajudar a conter a propagação e da infecção para outros sistemas.*

*Prevenir o acesso a dados confidenciais: Bloquear aplicativos internos que não precisam acessar dados confidenciais pode ajudar a proteger esses dados de acesso não autorizado.*

*Limitar o impacto de um ataque: Bloquear aplicativos internos que estão sendo explorados por um ataque pode ajudar a limitar o impacto do ataque.*

### **Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.**

*Limitar o Ataque: Bloquear o acesso a aplicativos ou URLs em nuvem pode conter a propagação de um ataque cibernético, isolando o sistema comprometido e impedindo que o invasor acesse dados confidenciais ou cause mais danos.*

*Proteger Recursos: O bloqueio protege recursos críticos contra acesso não autorizado, evitando a exfiltração de dados confidenciais, a interrupção de serviços essenciais ou a sabotagem de sistemas.*

*Mitigar Riscos: Reduz a superfície de ataque, diminuindo as chances de um ataque ter sucesso.*

*Observem que são ações de respostas básicas e se a solução ofertada não é capaz de responder a um risco, o CJF estará vulnerável a sofrer ataques cibernéticos e não ter conhecimento do que foi comprometido e quais ações executar durante um risco cibernético.”*

### **Resposta da recorrida:**

Outra vez temos a empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA buscando confabular fatos infundados, demonstrando sua falta de compromisso com a veracidade das informações e principalmente falta de conhecimento técnico para julgar as comprovações apresentadas.

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.

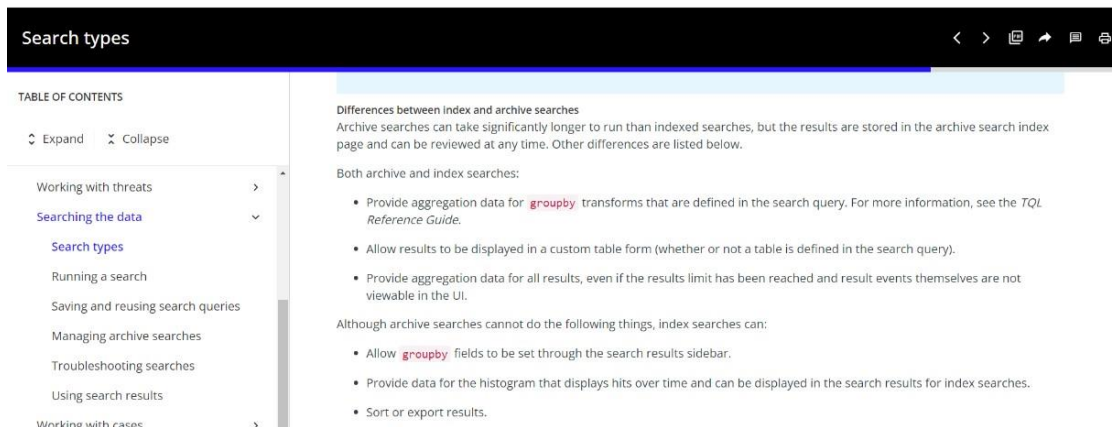
## **17. Razão técnica número 17 apresentada.**

**Íntegra da alegação:**

**“8.67 Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.”**

Fica evidente o não atendimento do item 8.67 com a comprovação apresentada através do link [https://docs.trellix.com/bundle/helix\\_pg/page/UUID-55ce8aa7https://docs.trellix.com/bundle/helix\\_pg/page/UUID-55ce8aa7-e429-204a-0c33-73d71d94e1b4.html](https://docs.trellix.com/bundle/helix_pg/page/UUID-55ce8aa7https://docs.trellix.com/bundle/helix_pg/page/UUID-55ce8aa7-e429-204a-0c33-73d71d94e1b4.html) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram a consolidação e correlacionamento diferentes modelos de ameaça relacionados a um único evento.

Em relação ao atendimento da solução ofertada pela LICITANTE, conforme a evidência anexada ao documento de ponto a ponto, a solução ofertada não é capaz de integrar diversas fontes de dados em um único alerta.



O XDR deve ser capaz de integrar dados de diversas fontes, como endpoints, servidores, redes, e-mails e serviços na nuvem. Isso fornece uma visão holística do ambiente de segurança e ajuda na detecção de ameaças que podem atravessar várias camadas de defesa, além de auxiliar na gestão de riscos do ambiente.

Para isso, é crucial que a plataforma seja capaz de receber dados de diferentes fontes e traduzir e correlacionar os alertas recebidos para que o administrador seja capaz de analisá-los em um único evento. A correlação de informações permite a análise de cadeia de ataques, onde diferentes eventos são conectados para formar um panorama mais completo de uma atividade maliciosa. Dessa forma, auxilia na compreensão do método de ataque e na identificação de possíveis pontos de entrada e movimentação lateral.

Portanto, ao apresentar informações correlacionadas de maneira organizada, o XDR facilita a investigação por parte das equipes de segurança. Assim, a equipe do CJF poderá acessar dados relevantes rapidamente, acelerando o processo de identificação e resposta.

O link em questão mostra apenas o AGRUPAMENTO de pesquisas que podem ser realizadas em um campo de busca. Notadamente, uma pesquisa simples não oferece detalhes sobre um alerta de natureza complexa. Da mesma forma, uma pesquisa com informações agrupadas difere de um alerta único e correlacionado, que agrega informações provenientes de distintas camadas de proteção.

Observem no texto abaixo retirado da documentação fornecida que não existe qualquer relação para atendimento ao item, como podemos observar abaixo:

*“About index searches*

*Helix index search capability lets you search events both as a starting point to find a potential compromise and to locate specific events associated with alerts. Helix index search can search billions of events in seconds.”*

*“About archive searches*

*After a contractually set time, data from your Helix instance is archived and no longer indexed. With an archive search, you can search events in your archived data. Although an archive search is slower than an index search, it provides access to a much larger set of data and allows a significantly longer retention period.*

Tradução livre:

*“Sobre pesquisas de índice*

*O recurso de pesquisa de índice Helix permite pesquisar eventos como ponto de partida para encontrar um comprometimento potencial e para localizar eventos específicos associados a alertas. A pesquisa de índice Helix pode pesquisar bilhões de eventos em segundos.”*

*“Sobre pesquisas de arquivo*

*Após um período definido contratualmente, os dados da sua instância Helix são arquivados e não são mais indexados. Com uma pesquisa de arquivo, você pode pesquisar eventos nos dados arquivados. Embora uma pesquisa de arquivo seja mais lenta que uma pesquisa de índice, ela fornece acesso a um conjunto muito maior de dados e permite um período de retenção significativamente mais longo.*

*Isto é, a solução não é capaz de prover a visibilidade de um alerta que envolve diferentes tipos de camadas do XDR, trazendo graves prejuízos ao que se espera da solução a ser adquirida através deste edital. Ou seja, a equipe técnica do CJF não teria implementado em seu ambiente uma solução que tem por objetivo facilitar a investigação e resposta aos eventos suspeitos.”*

### **Resposta da recorrida:**

Dessa vez a empresa ALLTECH - SOLUCOES EM TECNOLOGIA LTDA se superou em sua fábula e busca infundada, ignorando todas as demais comprovações realizadas durante o envio da proposta.

O link [https://docs.trellix.com/bundle/helix\\_dscg/page/UUID-3d04119d-b16b-7e2d-84e1-390d8ca86fec.html](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. Razão técnica número 18 apresentada.**

#### **Íntegra da alegação:**

**“8.68.9 Deve permitir alterar o status de cada evento, para no mínimo Novo, Em progresso/análise e Fechado ou escala equivalente.**

Fica evidente o não atendimento do item 8.68.9 com a comprovação apresentada através do link [https://docs.trellix.com/pt-BR/bundle/xdr\\_pg/page/UUIDhttps://docs.trellix.com/pt-BR/bundle/xdr\\_pg/page/UUID-78ee86d5-9bb6-3816-881b-0001572813c4.html](https://docs.trellix.com/pt-BR/bundle/xdr_pg/page/UUIDhttps://docs.trellix.com/pt-BR/bundle/xdr_pg/page/UUID-78ee86d5-9bb6-3816-881b-0001572813c4.html) citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram como alterar o status de cada evento, para no mínimo:

Novo,

*Em progresso/ana lise e  
Fechado ou escala equivalente..*

*Conforme tela abaixo, o link fornecido não está disponível para consulta, o que impossibilita a avaliação do cumprimento do item.*



Erro: 404

Isso é estranho.

Não foi possível encontrar o conteúdo que você está procurando.

Início

Ou encontre publicações e tópicos

Esta publicação X Pesquisar  

”

### **Resposta da recorrida:**

Resta à recorrente apelar para a incoerência em suas alegações. Uma vez que em itens anteriores já comprovados, aceitos pela licitante e não questionados pela própria recorrente o item aqui mencionado já fora irrefutavelmente evidenciado. 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](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](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 períodos
- 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](https://docs.trellix.com/bundle/helix_pg/page/UUID-3257cbf6-855e-3ecc-10b3-b2d1851c2195.html).

## **19. Razão técnica número 19 apresentada.**

### **Íntegra da alegação:**

#### **“ITEM 8.80 e seus subitens**

##### **8.80 Deve exibir os seguintes painéis de controle:**

##### **8.80.1 Índice de risco dar empresa;**

##### **8.80.2 MITRE ATT&CK® Mapping for Enterprise;**

##### **8.80.3 Visão geral de alertas;**

##### **8.80.4 Top 10 vulnerabilidades em risco;**

##### **8.80.5 Top 10 usuários em risco;**

##### **8.80.6 Top 10 dispositivos em risco;**

Fica evidente o não atendimento do item 8.80 e seus subitens com a comprovação apresentada através do documento “helix\_api\_doc.pdf” citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram os seguintes painéis de controle:

*Índice de risco dar empresa;*



*MITRE ATT&CK® Mapping for Enterprise;*

*Visão geral de alertas;*

*Top 10 vulnerabilidades em risco;*

*Top 10 usuários em risco;*

*Top 10 dispositivos em risco;*

*A solução ofertada revelou-se inadequada, pois não apresentava claramente a comprovação necessária, mesmo apresentando um extenso documento de 65 páginas não é possível identificar o atendimento aos itens e a falta de direcionamento para a evidência necessária reflete a incapacidade de entender o projeto e suas funcionalidades de maneira eficaz. Não comprovando diversos itens mencionados neste documento.*

*Índice de risco da empresa:*

- *O índice de risco de uma empresa é importante para identificar situações de perigo antes que se tornem ameaças reais. Isso permite que a empresa implemente medidas preventivas e elabore planos de contingência adequados.*

*MITRE ATT&CK® Mapping for Enterprise:*

- *O MITRE ATT&CK é um recurso interativo e constantemente atualizado que descreve as táticas, técnicas e procedimentos (TTPs) utilizados por cibercriminosos em seus ataques.*
- *As equipes de segurança podem usar as informações do MITRE ATT&CK para simular ataques cibernéticos do mundo real. Essas simulações podem testar a eficácia das políticas, práticas e soluções de segurança que elas têm em vigor e ajudar a identificar vulnerabilidades que precisam ser abordadas.*

*Visão geral de alertas:*

- *Visões gerais de alertas de segurança informam quando ocorrem eventos importantes no seu ambiente. Os detalhes do alerta e o nível de gravidade ajudam a decidir que plano de ação seguir.*

*Top 10 vulnerabilidades em risco:*

- *Lista as top 10 vulnerabilidades em risco*

*Top 10 usuários em risco:*

- *Lista os top 10 usuários em risco*

*Top 10 dispositivos em risco:*

- *Lista os top 10 dispositivos em risco”*

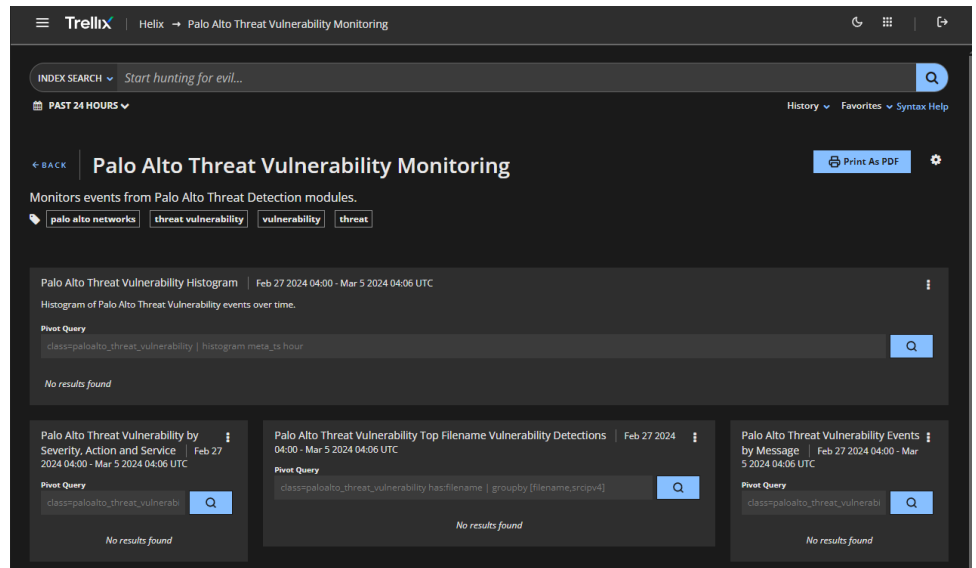
**Resposta da recorrida:**

As insistentes alegações denotam o único intuito de prejudicar o andamento do processo licitatório, uma vez que já foram, reiteradas vezes, comprovados em itens anteriores, as funções aqui apontadas. Portanto, para que não restem dúvidas, questionamentos ou alegações de quaisquer naturezas, as funções requeridas são alcançadas pelas funcionalidades descritas abaixo em detalhes:

- Quanto ao índice de risco da empresa:
  - O risco total da organização é uma métrica que resume todos os riscos associados dentro da severidade dos incidentes, somados aos riscos de cada entidade associada nesses incidentes. Este panorama geral é visto

em dois painéis, o painel total de riscos visto no link:  
[https://docs.trellix.com/bundle/helix\\_pg/page/UUID-dc833c8f-1e7b-5d54-e4fe-a14d9e6f8e7f.html](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:
  - 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](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:
  - Os alertas são eventos suspeitos ou maliciosos (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](https://docs.trellix.com/bundle/helix_pg/page/UUID-36ec00cd-21a3-2652-eebe-9860800f8e0b.html)
  
- Quanto ao Top 10 vulnerabilidades em Risco:
  - 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](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



Tela obtida em ambiente de testes

- 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 específicas 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](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](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](https://docs.trellix.com/bundle/helix_pg/page/UUID-d520f6cb-8bca-2072-a115-c0c697ea6fb9.html) (ver item ASSET TYPE: Host, USER, ALL).

## **20. Razão técnica número 20 apresentada.**

### **Íntegra da alegação:**

**“9.2 O módulo deve ser integrado a rede através de port mirror.**

**e**

**9.48 Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança.**

Fica evidente o não atendimento dos itens 9.2 e 9.48 com a comprovação apresentada através do documento “9.2.pdf” citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram que o módulo deve ser integrado a rede através de port mirror e permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança.

Abaixo o texto retirado da documentação fornecida:

*“This enables the Port Mirroring and SSL Decryption Mirroring features. (See the Network Security User Guide for information about these features.” - 9.7 e 9.10.pdf Tradução livre:*

*“Isso ativa os recursos Espelhamento de porta e Espelhamento de criptografia SSL. (Consulte o Guia do usuário de segurança de rede para obter informações sobre esses recursos.” - 9.7 e 9.10.pdf*

Nos itens 9.2 e 9.48, a comprovação de port mirroring não atende ao solicitado no item. A solução deve ser capaz de receber tráfego por meio do espelhamento de porta. Diferentemente de como foi comprovado, onde a direção do espelhamento é a partir da solução para soluções terceiras.

Observem no texto abaixo retirado da documentação fornecida que não existe qualquer relação para atendimento ao item, conforme podemos observar abaixo:

*“Port mirroring for all traffic The port mirroring for traffic feature allows the Network Security appliance to mirror the traffic that has been seen on the appliance to a third-party device through a TAP or SPAN port. You can configure the Network Security monitoring interface pair to forward a copy of the network traffic it processes to another port on the same appliance that is configured as a dedicated SPAN (or mirror) port. The mirror port is connected to another analysis device, which receives the traffic from the Network Security mirror port to perform further analysis. The feature is disabled by default and must be configured and enabled.” Tradução livre:*

*“Espelhamento de porta para todo o tráfego O recurso de espelhamento de porta para tráfego permite que o dispositivo Network Security espelhe o tráfego que foi visto no dispositivo para um*

*dispositivo de terceiros por meio de uma porta TAP ou SPAN. Você pode configurar o par de interfaces de monitoramento do Network Security para encaminhar uma cópia do tráfego de rede que ele processa para outra porta no mesmo dispositivo que está configurado como uma porta SPAN (ou espelho) dedicada. A porta espelho é conectada a outro dispositivo de análise, que recebe o tráfego da porta espelho do Network Security para realizar análises adicionais. O recurso está desabilitado por padrão e deve ser configurado e habilitado." O item 9.48 menciona que as portas espelhadas devem ser usadas para monitorar o tráfego e detectar riscos à segurança, porém, diferentemente da comprovação anexada, a solução Network Security somente encaminha uma cópia do tráfego espelhado às soluções terceiras para que estas o analisem. Portanto, o não atendimento está claro."*

### **Resposta da recorrida:**

Apresentando total desconhecimento sobre fundamentos de arquitetura de redes, a recorrente ignora completamente as capacidades comprovadas na solução ofertada e já inclusive aceita pela licitante, e ainda visa deturpar a compreensão descrita na documentação utilizada. Portanto, para fins de esclarecimento irrefutável, demonstra-se aqui, de maneira minuciosa todas as possibilidades de “posicionamento” da tecnologia, ou integração da solução ao ambiente:

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.

Portanto, quanto à capacidade de integração via PORT MIRROR, ou cópia de tráfego:

- Comprova-se de maneira muito clara o atendimento deste item, pelo singelo trecho descrito no datasheet da solução, encontrado em:  
<https://www.trellix.com/assets/docs/data-sheets/trellix-network-security-datasheet.pdf> à página, 4 - seção Imediata e resiliente proteção (Immediate and resilient protection), este trecho, segue reproduzido abaixo e traduzido logo em seguida:
  - **Original:** Network Security offers flexible deployment modes, including out-of-band monitoring via test access point (TAP)/switched port analyzer (SPAN), inline monitoring, or inline active blocking
  - **Traduzido:** O Network Security oferece modos de implantação flexíveis, incluindo monitoramento fora do tráfego (out-of-band), por meio de ponto de acesso de teste (TAP)/analisador de porta comutada (SPAN).

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.

Dessa maneira, faz-se necessário dissuadir a tentativa da recorrente de descontextualizar a comprovação fornecida, e com dúvidas intenções confundir a licitante. O modo inline da solução Trellix NDR Network Security, fornece, devido a características intrínsecas à arquitetura e fundamentos de redes, o espelhamento do tráfego por ele apurado, para fontes terceiras.

Cabe ressaltar, que essa funcionalidade, embora não seja requerida no edital é mais uma das features disponíveis na plataforma, o que confere à licitante ainda mais robustez e capacidades investigativas com a solução, reiterando, já inclusive aceita pela licitante.

## **21. Razão técnica número 21 apresentada.**

### **Íntegra da alegação:**

**“9.98 Deve permitir a integração com plataforma de detecção e resposta do próprio fabricante, com objetivo de correlacionar as detecções do NDR com as demais tecnologias de segurança implantadas nas camadas de endpoint, servidores e e-mail.**

**e**

**9.99 A integração com a solução de detecção e resposta deve permitir que as ameaças sejam rastreadas desde a entrada na rede até tentativas de roubo de dados, exibindo etapas gráficas da ação do atacante.**

*Fica evidente o não atendimento dos itens 9.98 e 9.99 com a comprovação apresentada através do documento “9.2.pdf” citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram a integração com plataforma de detecção e resposta do próprio fabricante, com objetivo de correlacionar as detecções do NDR com as demais tecnologias de segurança implantadas nas camadas de endpoint, servidores e e-mail e a integração com a solução de detecção e resposta deve permitir que as ameaças sejam rastreadas desde a entrada na rede até tentativas de roubo de dados, exibindo etapas gráficas da ação do atacante.*

***O arquivo 9.99.pdf mencionado não está disponível no arquivo zip anexado, porém, ressalta-se que publicamente é possível identificar o não atendimento aos itens mencionados:***

*Conforme imagens abaixo, pode-se concluir que a integração se trata apenas de um compartilhamento de informações e não de uma plataforma de RESPOSTA À INCIDENTES, capaz de correlacionar em um único evento diferentes tipos de informações de detecção e responder a partir de uma única plataforma.*

## NETWORK SECURITY:

“This server task can be scheduled for pulling in data to McAfee ePO from Network Security Platform.” Tradução livre:

## SEGURANÇA DE REDE:

“Esta tarefa do servidor pode ser agendada para extrair dados do McAfee ePO da Network Security Platform.”

Fica evidente o compartilhamento unidirecional de dados entre o Network Security e a plataforma ofertada pela licitante. Para que a plataforma receba as informações, uma atividade agendada precisa ser configurada e, mesmo assim, não existe retroalimentação de dados entre as soluções.

Em suma, caso um objeto suspeito seja identificado na camada de endpoint, esta informaria à plataforma de XDR, porém a solução de visibilidade de rede não conseguiria consumir determinada informação, pois o compartilhamento é unidirecional. Além disso, como consequência, as ações de resposta entre camadas são limitadas.

Outro ponto que chamamos a atenção de não atendimento, e referente a rastrear desde a entrada na rede até tentativas de roubo de dados, exibindo etapas gráficas da ação do atacante.

Ou seja, resta questionar: Se a plataforma de XDR é capaz APENAS de receber alertas da solução de visibilidade de rede, como esta será capaz de RESPONDER ativamente às detecções?

The screenshot shows a document page with a dark header containing the title "Configure a server task for Network Security Platform in McAfee ePO" and navigation icons. On the left, there is a "TABLE OF CONTENTS" sidebar with expand/collapse options and a list of sections including "Viewing McAfee ePO configuration details", "Configure a server task for Network Security Platform in McAfee ePO", "Create new Network Security Platform dashboards in McAfee ePO (optional)", "Define a permission set in McAfee ePO", "View and edit a permission set", and "Create McAfee ePO users with". The main content area has the same title and includes a version dropdown (McAfee Network Security Platform 10.1.9 Integration Guide), last updated date (Feb 16, 2023), and a 3-minute read indicator. The text explains that a default server task is created during extension file installation and can be scheduled for data pulling. It notes that the default task needs configuration for a user with the "ePO Dashboard Data Retriever" role. A "To configure" section follows. On the right, there are sections for "On This Topic" (Task) and "Related Links" (Configurations).

<https://docs.trellix.com/bundle/network-security-platform-10.1.x-integrationguide-unmanaged/page/GUID-49A572C7-6564-4AA3-BOC8-286D0C877102.html>

The screenshot shows a document page with a dark header containing the title "Network Security Platform dashboard in McAfee ePO" and navigation icons. On the left, there is a "TABLE OF CONTENTS" sidebar with expand/collapse options and a list of sections including "Endpoint details query from the McAfee ePO server", "Network Security Platform dashboard in McAfee ePO", "Configurations", "Integration with McAfee Global Threat Intelligence", and "Integration with McAfee MVISION Insights". The main content area has the same title and includes a version dropdown (McAfee Network Security Platform 10.1.9 Integration Guide), last updated date (Feb 16, 2023), and a 2-minute read indicator. The text states that McAfee ePO provides an option to view Network Security Platform data on a dashboard. It lists monitors provided in the dashboard: Attack Severity Summary, Device Fault Summary, Manager Fault Summary, Top 10 Attack Destinations, Top 10 Attacks, and Top 10 Attack Sources. A note mentions that product data installation requires the Network Security Platform extension file. On the right, there are sections for "On This Topic" (Data retrieval when the McAfee® Network Security Manager is in Manager Disaster Recovery (MDR) mode) and "Related Links" (Configurations).

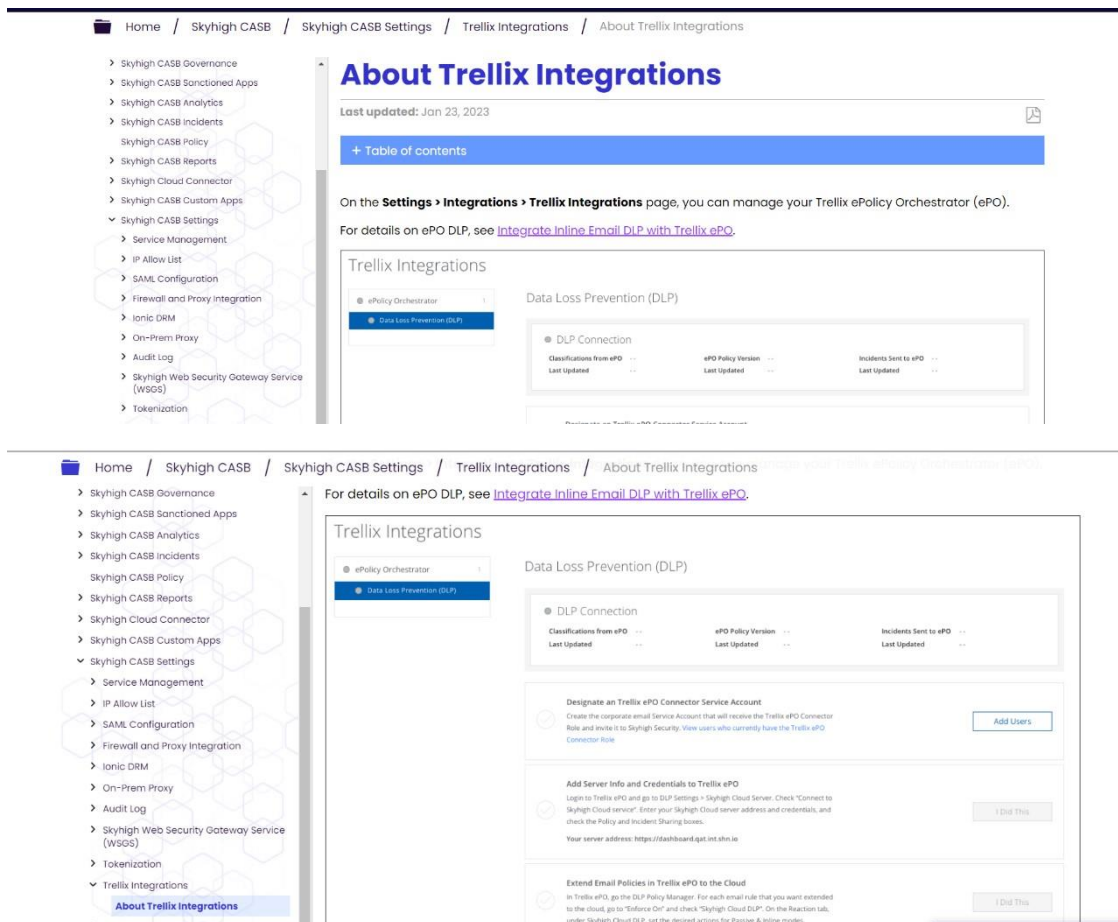
<https://docs.trellix.com/bundle/network-security-platform-10.1.x-integrationguide-unmanaged/page/GUID-78DE7E07-A490-49BA-A671-9FF9FF9ADB52.html>

## SKYHIGH CASB

A solução ofertada possui limitações, uma vez que o SKYHIGH CASB se restringe à integração apenas da funcionalidade de Prevenção de Perda de Dados (DLP) e não inclui alertas de detecção para correlacionar entre as diversas camadas de proteção diferentemente do conceito utilizado para XDR.

No link é possível identificar a integração disponível no SKYHIGH CASB e, claramente, está listado apenas DLP.

Ou seja, novamente, resta questionar: Se apenas as informações de DLP são integradas ao XDR, como a solução é capaz de RESPONDER às detecções realizadas sem ao menos recebê-las?



[https://success.skyhighsecurity.com/Skyhigh\\_CASB/Skyhigh\\_CASB\\_Settings/Trellix\\_Integrations/About\\_Trellix\\_Integrations](https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Settings/Trellix_Integrations/About_Trellix_Integrations)”

### Resposta da recorrida:

Em meio à tantos questionamentos feitos pela recorrente neste item, sobram confusões, imperícia, intenções dúbias e um tanto de dúvida quanto à capacidade cognitiva do elaborador de tal alegação, conjugar palavras que façam sentido. O item aqui alegado, nada tem a ver com a plataforma de proteção ao Office365, a menos que em sua própria solução, essa integração se dê desta forma.

Mas ao tomar como base, que todas as outras plataformas que não a que ela própria comercializa, a recorrente estaria de forma clara tentando direcionar o seu entendimento como verdade absoluta à equipe julgadora da licitante, o que não compete às práticas legais e fere inequivocamente os princípios básicos da ampla concorrência.



Portanto, iremos aqui detalhar o cumprimento dos itens 9.98 e 9.99, sem considerar a enorme trapalhada que faz a recorrente, ao associar pontos completamente distintos da comprovação. Restando a dúvida, quanto a tamanha imperícia ou a bisonha tentativa da recorrente, de confundir e desmerecer o sério trabalho de organizações de renome no território nacional e internacional.

### **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:

- 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.*
- 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;**

Em sua bizarra tentativa de desmerecer a plataforma vencedora e já aceita pela licitante, a recorrente realiza pesquisa, conforme seu próprio entendimento e vontade, e espera que isso seja tratado como verdade incontestável, resta entender se por dolo, ou incapacidade técnica. Há que se ressaltar que o item mencionado Skyhigh CASB, nada tem a ver com a plataforma NDR, não há sequer lógica em realizar essa associação. 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 dúvidas 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:
  - **Original:** The alerts provided by the Network Security appliance 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 an isolated and virtualized network, this traffic remains internal to the appliance.

- **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:
  - 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](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 (minimizadas) 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.
- 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 flagrar e impedir ataques característicos de roubo de dados (Data Theft). Temos na página 17, do manual Network\_Security\_User\_Guide.pdf, uma explicação sobre a classificação da infecção 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. Razão técnica número 22 apresentada.**

### **Íntegra da alegação:**

**“9.119 A partir da solução de detecção e resposta, os IOCs poderão ser compartilhados com outros sensores do fabricante e ferramentas de terceiros, sendo estas ao menos: MS Active Directory, Microsoft 365 e Fortinet.**

Fica evidente o não atendimento do item 9.119 com a comprovação apresentada através do documento “9.9.pdf” citado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram a partir da solução de detecção e resposta, os IOCs poderão ser compartilhados com outros sensores do fabricante e ferramentas de terceiros, sendo estas ao menos:

✓MS Active Directory, ✓  
Microsoft 365 e ✓Fortinet.

Não é apresentado a lista para integrações com a solução da fabricante Trellix, tampouco cita integração com solução da fabricante Fortinet.

*A não conformidade do item em questão pode acarretar diversas consequências negativas. Sem a capacidade de compartilhar IOCs (Indicadores de Comprometimento) com outros sensores e ferramentas, a eficácia na detecção de ameaças pode ser reduzida, levando a uma resposta inadequada ou atrasada a incidentes de segurança. Além disso, o compartilhamento de IOCs é fundamental para a colaboração entre diferentes sistemas de segurança e ferramentas de terceiros, facilitando a coordenação de esforços de segurança e a troca de informações sobre ameaças em tempo real. A falta desse recurso pode aumentar o risco de incidentes de segurança não detectados e não mitigados, comprometendo a eficácia global da postura de segurança cibernética da organização. Também pode haver implicações regulatórias e de conformidade, já que a falta de capacidade de compartilhamento de IOCs pode resultar em não conformidade com normas de segurança cibernética e regulamentações específicas, sujeitando o CJF a multas e penalidades. Em resumo, a não conformidade com este requisito pode comprometer seriamente a capacidade do CJF de detectar, responder e mitigar ameaças de segurança cibernética, aumentando seu risco geral de incidentes de segurança e possíveis repercussões regulatórias.”*

### **Resposta da recorrida:**

Diante de mais uma tentativa de deturpar o propósito da solução descrito pela licitante, faz-se necessário esclarecer itens óbvios, que geram inclusive redundância de informações, contudo, em vistas a erradicar de maneira irrefutável as infundadas alegações, cabem as seguintes explicações sobre o funcionamento e arquitetura da a plataforma vencedora e já aceita pela licitante, e incoerentemente contestada pela recorrente.

O item em questão requer que a solução de detecção e resposta possa ser capaz de difundir dados de seus sensores, para múltiplas soluções e elencam exemplos mínimos a serem garantidos, como: MS Active Directory, Microsoft 365 e Fortinet.

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](https://docs.trellix.com/bundle/so_sag_6-6-0_pdf/resource/SO_SAG_6.6.0_pdf.pdf) à página de número 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:

- **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.
- **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](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:
  - **Plugin Fortinet:** A integração com o ambiente Fortinet se dá pelo plugin: Fortinet Fortigate Plug-in, encontrado em: <https://fireeye.market/apps/xFg9Ptv5>
  - **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 possibilidade 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>.
  - **Plugin para Microsoft 365:** A Trellix oferece ainda, dentro dos mais de 10 plugins disponíveis para a plataforma Microsoft, plugins específicos para serviços específicos 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>.

Como é possível perceber, as capacidades de integração agnóstica, tomariam sozinhas, todas as páginas deste documento, entretanto, para que não restem dúvidas, ou fiquem suscetíveis à dúvidas intenções por parte da recorrente, quaisquer dos elementos de comprovação, iremos estender mais ainda a já óbvia e redundante explicação, sobre as possibilidades de integração e compartilhamento de indicadores via mecanismo de automatização de tarefas, ou as chamadas API.

- No documento: *trellix\_api\_reference.pdf*, à página 11, na seção Introdução (Introduction), é fornecida uma breve explicação sobre as capacidades da API disponível na solução Trellix NDR (Network Security). Um pequeno trecho desta capacidade está descrito abaixo e traduzida logo em seguida:
  - **Original:** The Web Services Application Programming Interface (API) allows Trellix partners to access Trellix product alert records and reports and to submit malware objects and URLs for evaluation. The Web Services API is a role-based access control (RBAC) compliant Representational State Transfer (REST) interface.
  - **Traduzido:** A Interface de Programação de Aplicativos de Serviços Web (API) permite que os parceiros da Trellix acessem registros e relatórios de alertas de produtos da Trellix e enviem objetos de malware e URLs para avaliação. A API de serviços da Web é uma interface Representational State Transfer (REST) compatível com controle de acesso baseado em função (RBAC).

Desta forma, fica determinantemente comprovada a capacidade de integração, não somente entre o componente Trellix NDR (Network Security), com a arquitetura de detecção e resposta do fabricante, cumprindo com o item que rege que: *“os IOCs poderão ser compartilhados com outros sensores do fabricante”*, bem como também fica inegavelmente comprovada a capacidade de compartilhamento desses indicadores, entre todos os vetores de proteção, que interligados pela plataforma central Trellix XDR, oferecem intercâmbio completo de dados de incidentes e indicadores entre plataformas Trellix e não-Trellix, sobretudo, mas não exaustivamente, aqueles conforme aqui destacado pelo trecho: *“e ferramentas de terceiros, sendo estas ao menos: MS Active Directory, Microsoft 365 e Fortinet”*.

### **23. Razão técnica número 23 apresentada.**

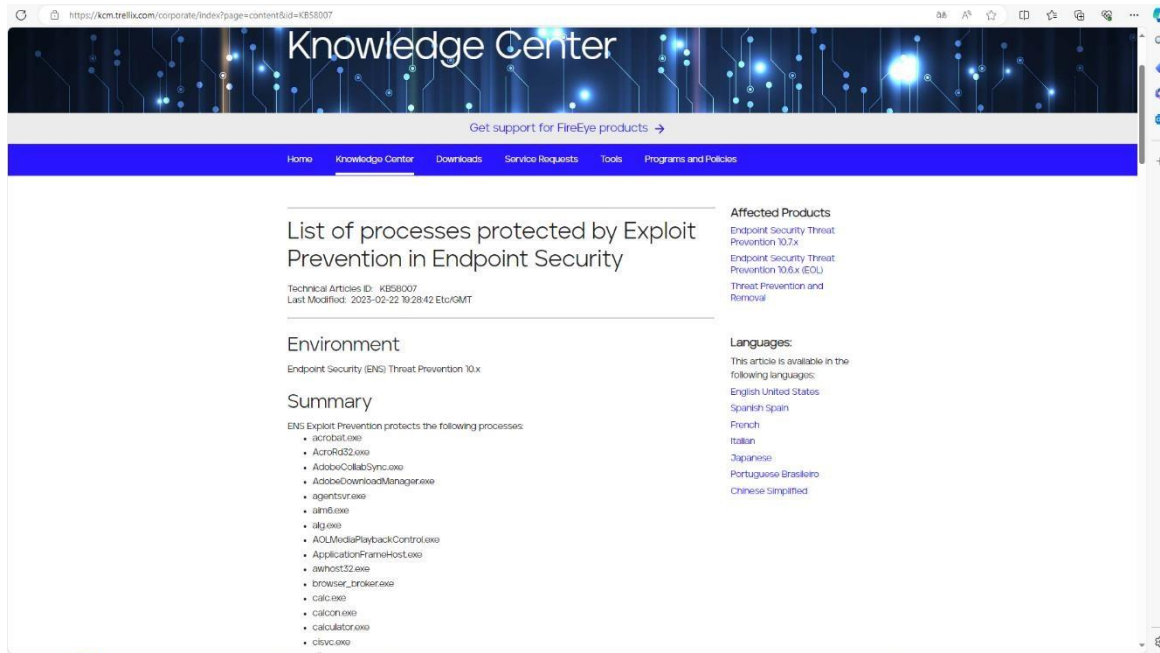
#### **Íntegra da alegação:**

**“10.10 Deve efetuar proteção automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host IPS para proteger o endpoint contra a possível exploração da vulnerabilidade.”**

Fica evidente o não atendimento do item 10.10 com a comprovação apresentada através do link *“<https://kcm.trellix.com/corporate/index?page=content&id=KB58007> List of processes protected by Exploit Prevention in Endpoint Security.*” citado na planilha de comprovação técnica “Atendimento dos requisitos

técnicosv2.xlsx” (ponto a ponto) não atende aos requisitos e não demonstram a possibilidade de apontar vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host IPS para proteger o endpoint contra a possível exploração da vulnerabilidade.

O link utilizado para comprovação não demonstra o atendimento ao item que, por sua vez, deixa clara a necessidade de proteção que aponte as vulnerabilidades dos sistemas operacionais e aplicações e, automaticamente, atribua a blindagem contra possíveis explorações. O documento apenas aponta vulnerabilidades listadas em site da Trellix, conforme abaixo:



O scan de vulnerabilidades automatizado proporciona uma avaliação de forma contínua para a postura de segurança do CJF. Permite que a equipe de segurança identifique e aborde rapidamente quaisquer pontos fracos que possam surgir. Por outro lado, a atribuição de regras de blindagem contra exploração é uma resposta rápida a ameaças emergentes e crucial neste processo de proteção.

Quando uma vulnerabilidade crítica é identificada, a regra correspondente deve ser implementada imediatamente, protegendo os sistemas e aplicações antes mesmo que uma correção definitiva esteja disponível.

O prejuízo de não possuir esta funcionalidade é incalculável, considerando que os atacantes exploram cada vez mais vulnerabilidades conhecidas, ou seja, a TRELIX, mais uma vez, demonstra a ineficácia de sua solução ofertada, trazendo brechas cruciais para o ambiente do CJF.”

### Resposta da recorrida:

Uma vez mais a recorrente denota acreditar que o item técnico só pode ser atendido por solução que ela designe. Cabe entender a que se deve tal presunção. O item é expressamente claro ao especificar que a funcionalidade deve ser entregue pelo módulo de prevenções contra intrusão ao host. Sendo, portanto, absolutamente irrelevante a alegação realizada. No entanto, iremos esclarecer como funciona tal capacidade na plataforma ofertada:

- 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 dúvidas 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 específicas, 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](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. Razão técnica número 24 apresentada.**

##### **Íntegra da alegação:**

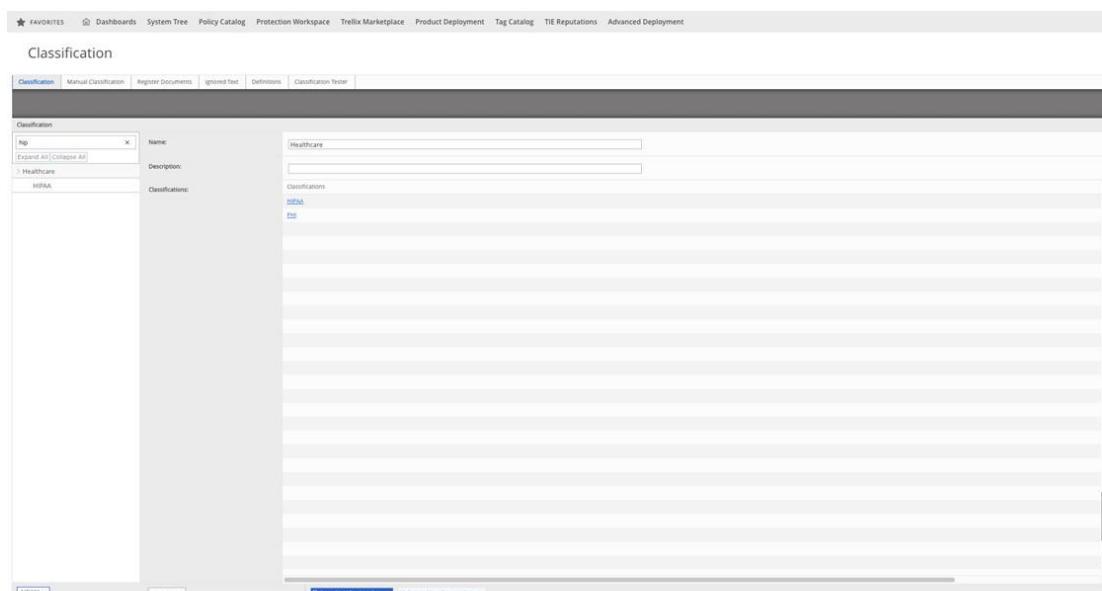
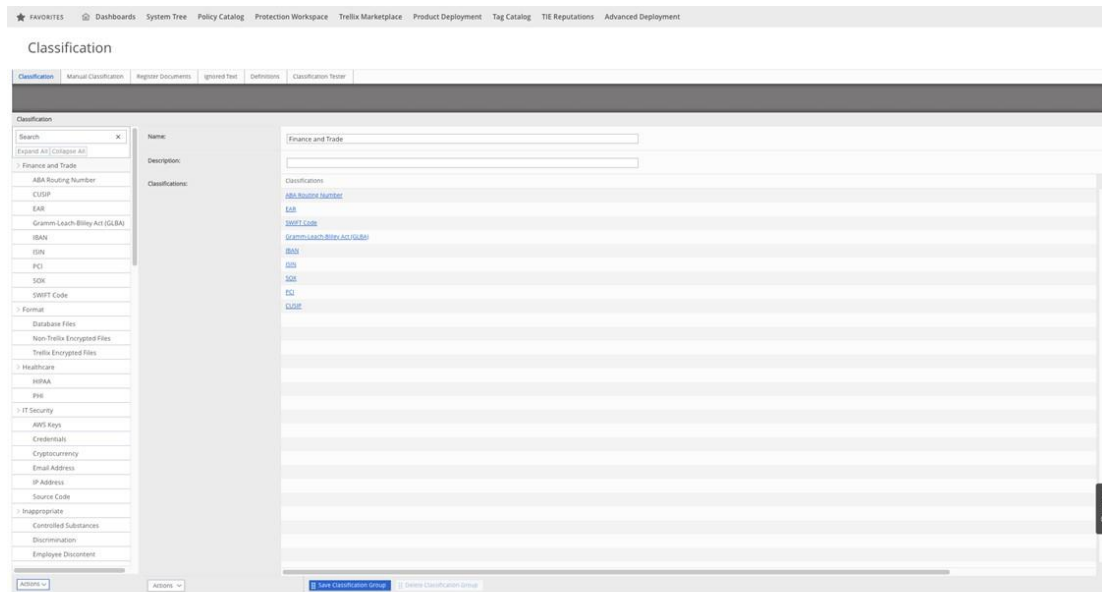
**“12.2.1 Deve possuir nativamente templates para atender as seguintes regulamentações: PCI/DSS, HIPA, Glba, SB-1386 e US PII.**

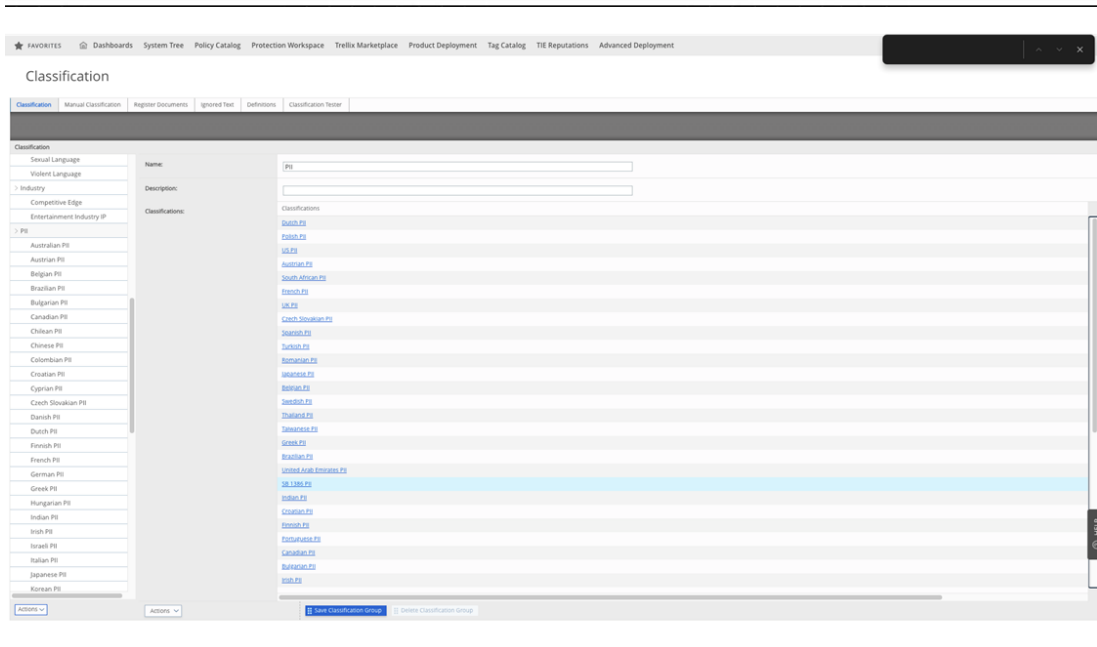
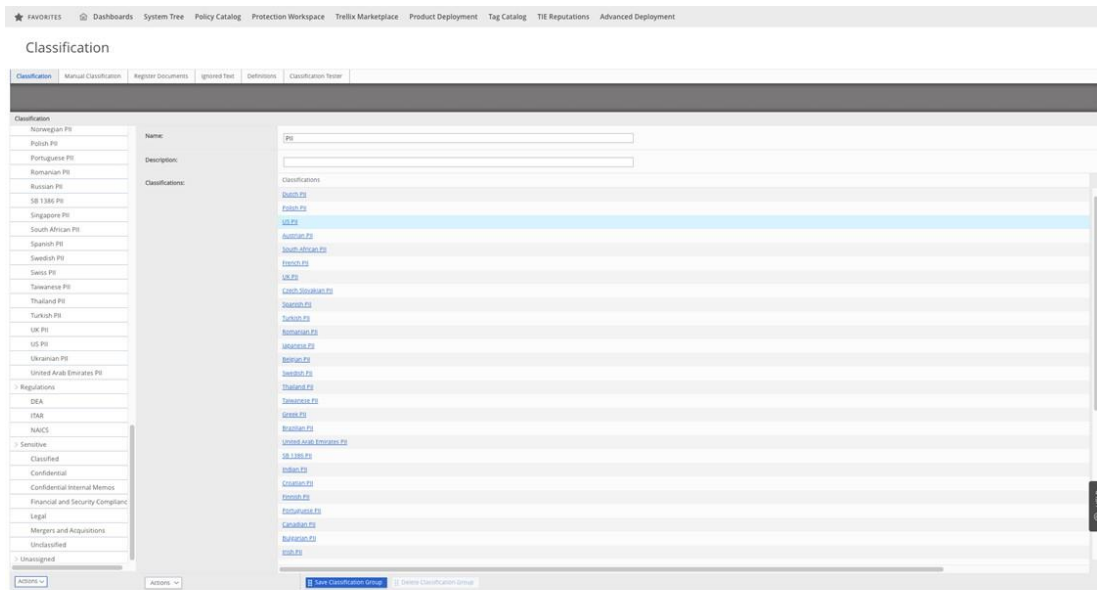
*Fica evidente o não atendimento do item 12.2.1, pois não foi comprovado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) e, após diligência, a LICITANTE disponibilizou algumas capturas de tela as quais não permitem identificar que tipo de solução se trata, se é um link de pesquisa ou*

alguma biblioteca interna. A comprovaç o do item n o atende aos requisitos e n o demonstram que possuem nativamente templates para atender as seguintes regulamentaç es:

PCI/DSS,  
HIPA,  
Glba,  
SB-1386 e ✓US PII.

O n o cumprimento do requisito de possuir nativamente templates para atender regulamentaç es espec ficas pode acarretar diversos riscos ao CJF. A falta de conformidade com regulamentaç es importantes, como o PCI/DSS, HIPAA, GLBA, SB-1386 e US PII, pode resultar em penalidades financeiras, multas e lit gios. Al m disso, aumenta a probabilidade de violaç es de dados e incidentes de seguran a cibern tica, expondo informaç es e danificando a reputa o do CJF. Em resumo, o n o cumprimento desse requisito representa um risco significativo, com potenciais impactos financeiros, legais, de reputa o e operacionais.





## Resposta da recorrida:

A tentativa da ALLTECH de questionar a capacidade da solução de DLP da Trellix não apenas subestima nossa tecnologia avançada, mas também revela um claro desinteresse em reconhecer a evidência técnica apresentada. Contra as alegações infundadas da ALLTECH, a Trellix demonstra, inequivocamente, o atendimento do item, através de:

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>

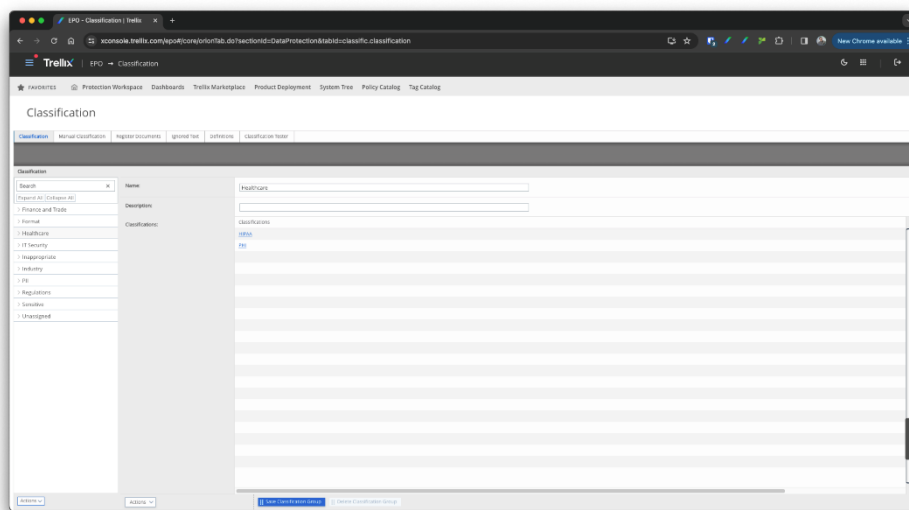
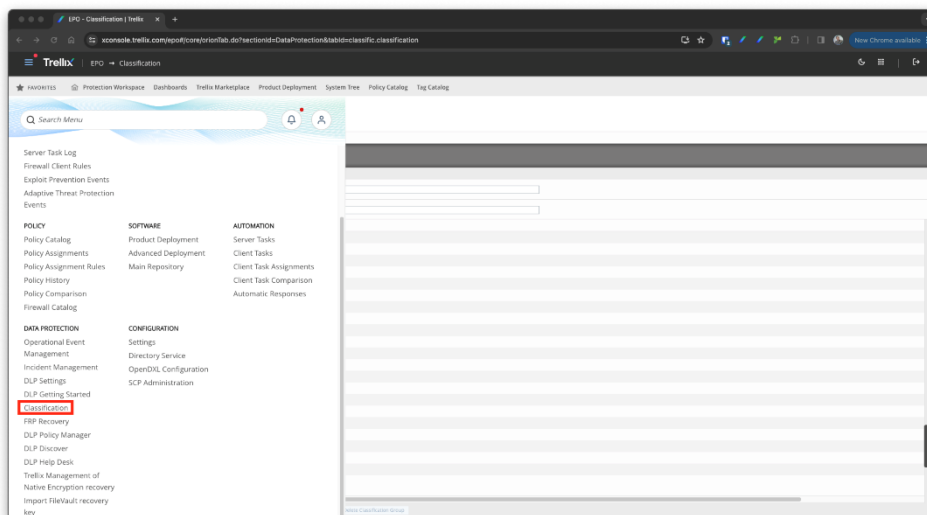
- HIPAA: <https://docs.trellix.com/bundle/data-loss-prevention-11.10.x-product-guide/page/GUID-2D8266D9-373C-433D-B9EB-BBF038FE49AA.html>

- 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.



Por fim, rejeita-se veementemente, qualquer tentativa da ALLTECH em desacreditar, deturpar e distorcer, as evidências ou qualquer dos itens utilizados na comprovação, ignorando inclusive a validação já realizada pela licitante, estando límpido o deliberado esforço em causar constrangimento e provocar atraso ao devido andamento do certame, priorizando disputas infundadas em detrimento da segurança e integridade do CJF.

A desatenção ou mesmo a insipiência técnica da Recorrente chega a beirar o inexplicável, uma vez que, a empresa Recorrente é a atual prestadora dos serviços ora licitados, tendo demonstrado sua irresignação por não ter ofertado o melhor lance e não ter sido declarada vencedora do certame, tentando, agora, direcionar a licitação para seu próprio benefícios, tentando ir de encontro com os princípios da isonomia, da

vantajosidade, da ampla concorrência, da vinculação ao instrumento convocatório, do julgamento objetivo, da legalidade, dentre outros, o que não se pode permitir.

### **III – DO DIREITO**

Verifica-se que a Ilma. Pregoeira, ao habilitar a empresa BLUE EYE, agiu com inteiro amparo do Edital, dado que a empresa Recorrida, conforme informado, logrou êxito em comprovar que cumpre todas as exigências questionadas pela Recorrente, procedendo de forma escoimada de vícios, sem qualquer irregularidade em sua decisão, tendo, inclusive, através de diligência, a Ilma. Pregoeira e sua equipe de apoio atestado que a solução da Recorrida atendia ao disposto no Edital.

Todas as participantes deveriam cumprir com todos os requisitos do Edital e, aquela que além de cumpri-los, apresentasse a proposta mais vantajosa, seria a vencedora, como assim aconteceu no presente caso.

Quando a Administração contrata determinada empresa com capacidades técnico operacional, profissional e econômico-financeira frágeis, o prejuízo social, econômico e administrativo é certo e enorme. E é justamente desses prejuízos que a Administração deseja esquivar-se mediante a aplicação, dentre outras regras, das exigências editalícias aqui debatidas.

**O QUE OCORREU NO CASO EM TELA FOI UMA ANÁLISE OBJETIVA DIANTE DE TODOS OS CRITÉRIOS DO EDITAL, NÃO HAVENDO SE FALAR EM REVISÃO DOS ATOS PRATICADOS, UMA VEZ QUE A EMPRESA RECORRIDA CUMPRIU COM OS REQUISITOS OBRIGATÓRIOS PREVISTOS NO INSTRUMENTO CONVOCATÓRIO.**

Vale lembrar que, o entendimento corrente tanto na doutrina, como na jurisprudência, é de que o edital, no procedimento licitatório, constitui Lei entre as partes e é o instrumento de validade dos atos praticados no curso da licitação, sendo certo que **“ao descumprir normas editalícias, a Administração frustra a própria razão de ser da licitação e viola os princípios que direcionam a atividade administrativa, tais como: o da legalidade, da moralidade e da isonomia”**, bem como os contidos no Art. 5º. da Nova Lei das Licitações (Lei nº 14.133/2021), in verbis:

“Art. 5º Na aplicação desta Lei, serão observados os princípios **da legalidade**, da impessoalidade, da

moralidade, da publicidade, da eficiência, **do interesse público**, da probidade administrativa, **da igualdade**, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da **vinculação ao edital, do julgamento objetivo**, da segurança jurídica, da razoabilidade, **da competitividade**, da proporcionalidade, da celeridade, **da economicidade** e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942”.

Com base nas informações acima, não é preciso qualquer esforço cognitivo para perceber que a proposta apresentada pela Recorrida não deixou de contemplar qualquer obrigação instituída no edital.

A Ilma. Pregoeira está restrita às normas editalícias, tendo em vista que sua atividade é vinculada. O princípio da vinculação é primordial na interpretação dos fatos ocorridos nas fases externas da licitação, não há espaço para aplicação de exigências não previstas.

Por tais razões, 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.

Assim, a conduta da Ilma. Pregoeira e da equipe de apoio estão totalmente válidas e encontram inteiro fundamento nas normas que regem as licitações públicas, o que sustenta a manutenção da decisão.

#### **IV – DA NECESSIDADE DE INVESTIGAÇÃO E EVENTUAL PUNIÇÃO DA RECORRENTE**

Diante de todo o contexto apresentado acima, onde é facilmente possível extrair o intuito protelatório da empresa Recorrente, necessário relembrar o disposto no artigo 337-I, da Lei nº 8.14.133/2021. *In verbis*:

Perturbação de processo licitatório

Art. 337-I. Impedir, **perturbar** ou fraudar a realização de qualquer ato de processo licitatório:

Pena - detenção, de 6 (seis) meses a 3 (três) anos, e multa.

O artigo mencionado trata de crime comum, em que o sujeito ativo pode ser qualquer pessoa. O tipo objetivo reside nas condutas de “impedir” – isto é obstar que o ato se realize –, “**perturbar**” – **termo que se refere a comportamentos que embora não impeçam o ato, dificultam-no** – ou “fraudar”, utilizar ardil ou artifício para se esquivar do cumprimento de requisitos legais do ato ou ocultar o descumprimento de exigências legais a ele inerentes.

A Recorrente atingiu todos os elementos citados, criando artifícios, desvirtuando os termos do Edital, para tentar a qualquer custo a inabilitação da Recorrida. A conduta passível de investigação e requer uma ação enérgica do administrador.

Ressalta-se que a pena de inidoneidade também pode ser aplicada em casos como tais. O interesse da Recorrente foi de atrapalhar o procedimento, causar o retardamento do mesmo e impedir a contratação da proposta muito mais vantajosa para a Administração, o que não se pode permitir.

Diante da comprovação dos elementos subjetivos e objetivos que consubstanciam a conduta da empresa, pleiteia-se pela apuração da conduta da Recorrente.

## **V – DO PEDIDO**

Ante ao exposto, **REQUER 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.**

Requer, ainda, seja instaurado processo administrativo para apurar a conduta da empresa **ALLTECH – SOLUÇÕES EM TECNOLOGIA LTDA**, que tenta perturbar o bom andamento do certame.

Termos em que  
Pede deferimento.



Brasília/DF, 05 de março de 2024.

**BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA.**

CNPJ nº. 26.025.401/0001-90

Rinaldo Araújo da Silva  
Representante Legal  
RG nº. 165512088 SSP SP  
CPF nº. 087.467.438-71