ILUSTRÍSSIMA SENHORA PREGOEIRA OFICIAL DO CONSELHO DA JUSTIÇA FEDERAL - LUISA AIRES OLIVEIRA

Pregão Eletrônico n. 90.003/2024

Processo SEI n. 0001703-88.2023.4.90.8000

Recurso Administrativo

ALLTECH - SOLUCOES EM TECNOLOGIA LTDA, com sede no SCN Quadra 01 Bloco F – Salas 802 a 810 – Ed. América Office Tower Asa Norte – Brasília - DF, CEP. n. 70.711-905, inscrita no CNPJ sob o nº 21.547.011/0001-66, **VEM**, de forma tempestiva e respeitosa, conforme previsto na cláusula XII – DOS RECURSOS, do edital e fundamentada no art. 165 da Lei n. 14.133/2021, por intermédio de seu representante legal, apresentar

RECURSO

pelas razões de fato e de direito adiante expostas, que têm por objetivo fornecer subsídios para que a MD. Decisão Proferida pela Ilma. Pregoeira seja revista em todos os seus termos, reconsiderando posicionamento de aceitar proposta que não atende o edital. O processo de análise da solução ofertada não considerou certos elementos e condicionantes adiante expostos, que podem colocar em risco não somente o certame, mas atendimento às necessidades que deram origem ao presente processo.

Assim, diante do equivocado aceite da proposta da licitante BLUE EYE SOLUCOES EM TECNOLOGIA LTDA, requeremos imediato afastamento da licitante do bojo do presente processo, a fim de preservar esse CJF, a Ilma. Pregoeira e os servidores envolvidos no presente processo frente aos riscos que correm ao aceitar oferta de solução com qualidade abaixo dos padrões mínimos definidos, ocasionando suposto dano erário.

I. MANIFESTAÇÃO PRELIMINAR QUE RESGUARDA O DIREITO

Após comunicação junto ao portal de Compras, manifestando a intenção de aceitar e habilitar a RECORRIDA, a MD. Pregoeira possibilitou a manifestação prévia de intenção de recorrer contra a fase de julgamento e a habilitação, em campo próprio do sistema Compras.

Vejamos:

"23/02/2024 15:25:14 Fornecedor ALLTECH - SOLUCOES EM TECNOLOGIA LTDA, CNPJ 21.547.011/0001-66 registra a intenção de recurso na fase julgamento."

e

"26/02/2024 16:14:30 Fornecedor ALLTECH - SOLUCOES EM TECNOLOGIA LTDA, CNPJ 21.547.011/0001-66 registra a intenção de recurso na fase habilitação."

Após encerramento, o sistema divulgou junto ao histórico de recursos, a data limite para a apresentação do recurso, sendo 29/02/2024.

A possibilidade de ingressar contra a decisão se apresenta como sendo uma atitude diligente e imparcial, a qual se mostra totalmente alinhada e suficientemente garantidora do direito, tendo por base os pressupostos recursais, que são: sucumbência, tempestividade, legitimidade, interesse e motivação, os quais se mostrarão ao longo desta petição.

II. TEMPESTIVIDADE

Nos termos da Ata da Sessão Pública realizada, nosso prazo de apresentar alegações e razões encerra-se nesta data (29/02/2024). Tendo por base a presente inserção no sistema Compras nesta data, resta comprovada a tempestividade, nos sendo assistido o direito ao aceite e sua apreciação em todos os seus termos.

Ademais, se o caráter suspensivo do recurso não for convalidado pela administração, esvaziaremos o sentido constitucional do art. 5°, inciso LV, da CF/88, pois tornará o recurso em questão imprestável, extirpando o comando segundo o qual os litigantes em processo judicial ou administrativos têm prerrogativas asseguradas de ampla defesa e contraditório

III. BREVE INTROITO DOS FATOS

Esse CONSELHO DA JUSTIÇA FEDERAL – CJF deflagrou em 15/02/2024 às 10:00 horas, o Pregão Eletrônico n. 90.003/2024 visando a contratação de empresa para **CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO DE ESTAÇÕES DE TRABALHO, DATA CENTER, E-MAIL CORPORATIVO E APLICATIVOS MICROSOFT 365, CONTEMPLANDO INSTALAÇÃO E CONFIGURAÇÃO, TRANSFERÊNCIA DE CONHECIMENTO E, SUPORTE TÉCNICO COM GARANTIA DO FABRICANTE DO CONSELHO DA JUSTIÇA FEDERAL, PELO PRAZO DE 36 MESES, CONFORME AS ESPECIFICAÇÕES E OS QUANTITATIVOS CONSTANTES DO TERMO DE REFERÊNCIA E ANEXOS – MÓDULO I DO EDITAL E SEUS ANEXOS**.

Encerrada a etapa de lances, restou como ofertante do melhor preço a licitante BLUE EYE SOLUCOES EM TECNOLOGIA LTDA, oportunizando a esse CJF realizar a pretendida contratação pelo valor de R$ 2.792.002,78, um valor bastante

considerável para soluções desse segmento, o que exige maior poder de cautela na condução do presente certame.

A MD. Pregoeira provocou aquela RECORRIDA quanto a negociação de melhores condições, momento em que a licitante informou não ser possível. Assim, a convocou para proceder com ajustes na proposta.

Deixando claro que a convocação seria apenas para envio da proposta ajustada ao lance vencedor, a RECORRIDA solicitou dilação do prazo inicial de 02 (duas) horas, sendo prontamente aceito pela MD. Pregoeira.

Esse primeiro envio tratou exclusivamente da proposta ajustada e **suposta comprovação do atendimento dos requisitos técnicos**, enviados como anexo da proposta em arquivo Excel, contendo catálogos e/ou prospectos do fabricante em arquivos compactados.

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."*

O prazo inicialmente concedido foi prorrogado, sendo enviado anexo pela RECORRIDA dentro do prazo estipulado.

EM 23/02/2024 a MD. Pregoeira informou a decisão de aceitar a proposta, sendo convocado para envio dos documentos habilitatórios.

Neste mesmo momento, houve a possibilidade de manifestar intenção de recorrer contra a proposta.

EM 26/02/2024, encontra-se registrada no sistema, mensagem de aceite e habilitação da documentação, concedendo prazo para intenção de recurso contra a habilitação.

Assim, surge o nosso interesse e direito de representar contra a MD. Decisão.

IV. FUNDAMENTOS DO RECURSO

Os fundamentos ora trazidos são prova inequívoca de que a **RECORRIDA não tomou conhecimento prévio do edital e seus requisitos**, resultando na oferta de uma solução com padrões de qualidade abaixo do mínimo definido no edital, ou seja, proposta que claramente NÃO ATENDE AO EDITAL, portanto, deveria ter sido inabilitada.

a) Previsões editalícias

Nada obstante o princípio da vinculação ao instrumento convocatório, destacamos preliminarmente algumas previsões que se mostrarão indispensáveis ao perfeito entendimento dos pontos que iremos abordar ao longo desta peça:

> *"5.1 Poderão participar deste pregão eletrônico as empresas que:*
>
> *5.1.1 **Atendam a todas as exigências, inclusive quanto à documentação, constantes deste edital**." (edital)*
>
> *"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.*
>
> *6.13.1 O CJF poderá diligenciar a licitante, caso a proposta esteja não integralmente o disposto nos itens 6.12 e 6.13, nos termos ora exigidos, sem que isso implique a desclassificação imediata da proposta apresentada."*
>
> *"11.9 O descumprimento das exigências contidas nesta cláusula determinará a inabilitação da licitante." (edital) (grifo nosso)*

Da leitura do texto editalício acima, temos claramente que em relação a participação, o ingresso está condicionado ao **atendimento dos requisitos e apresentação completa da documentação** requeridas no edital.

b) Princípio da vinculação ao instrumento convocatório

O princípio da vinculação ao instrumento convocatório é uma regra aplicada em licitações e contratações públicas que determina que todos os participantes devem se submeter estritamente às cláusulas, condições e exigências estabelecidas no edital ou convocação, incluindo tanto o órgão licitante quanto às proponentes. Isso significa que as propostas, lances apresentados pelos licitantes e regras a serem observadas o decurso do processo, devem estar em conformidade com as especificações e requisitos previamente definidos no documento oficial da licitação, garantindo a igualdade de oportunidades e a transparência no processo de seleção. Qualquer proposta que viole as regras do instrumento convocatório pode ser desclassificada ou considerada inabilitada, assim como a criação posterior de regras.

Pelo princípio do vínculo ao instrumento convocatório, **todos os licitantes devem cumprir rigorosamente as regras previstas no edital, de forma que não há discricionariedade da MD. Pregoeira em admitir a sua não observância**.

O TCU tem entendimento pacífico e manso acerca dessa questão:

> ***Acórdão 2630/2011 – Plenário | Relator: AUGUSTO SHERMAN CAVALCANTI***
>
> ***configura restrição à competitividade*** *da licitação a* ***utilização de critérios inadequados de habilitação****, a exemplo do ocorrido na Concorrência 2/2008-DA/L,* ***na qual foram utilizados*** *quantitativos mínimos,* ***não previstos em edital****, cuja execução os licitantes deveriam comprovar em suas propostas, o que afronta o art. 3º da Lei 8.666/1993 e a jurisprudência deste Tribunal".*

O edital é regra inafastável e suas diretrizes devem ser observadas por ambas as partes envolvidas (órgão e proponentes). Destacamos que existe a previsão quanto a interpretação das normas que disciplinam o pregão ser no sentido da ampliação da disputa, entretanto, desde que não comprometam o interesse da Administração e a segurança da contratação e nem transgridam direitos, legalidades ou imponham condições não previstas inicialmente.

Veja o que diz o brilhante texto do ilustríssimo MARÇAL JUSTEN FILHO:

> *"Além da lei, o instrumento convocatório da licitação determina as condições a serem observadas pelos envolvidos na licitação. A vinculação ao instrumento convocatório complementa a vinculação à lei. A autoridade administrativa dispõe da faculdade de escolha, ao editar o ato convocatório. Porém, nascido tal ato, a própria autoridade fica subordinada ao conteúdo dele. Editado o ato convocatório, o administrado e o interessado submetem-se a um modelo norteador de sua conduta.* ***Tornam-se previsíveis, com segurança, os atos e a serem praticados e as regras que o regerão****. Restará margem mínima de liberdade ao administrador, usualmente de extensão irrelevante. O instrumento convocatório (seja edital, seja convite), cristaliza a competência discricionária da administração, que se vincula a seus termos. Conjugando-se a regra do art. 41 com aquela do art. 4º, pode-se afirmar a estrita vinculação da administração ao Edital, seja quanto a regras de fundo quanto àquelas de procedimento." (Comentário a Lei de Licitações e Contratos Administrativos, Ed. Dialética, 8ª Edição, p. 65 e 417)*

c) **Desatendimento do edital - catálogos ou prospectos do fabricante ou da internet**

A empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA **não logrou êxito em sua tentativa de comprovar atendimento aos itens exigidos no edital**, nem mesmo quando lhe foi oportunizada a possibilidade de complementar os documentos em sede de diligenciamento.

A RECORRIDA não conseguiu e jamais iria conseguir tal feito, pois a solução por ela ofertada simplesmente **não possui uma série de recursos exigidos**, e, em muitos outros tendo qualidade abaixo do mínimo esperado por esse CJF.

Como veremos a seguir, resta comprovado o desatendimento da proposta, na fase de julgamento. **Ao ser instada a efetuar comprovações, induziu esse CJF ao entendimento equivocado de que a solução ofertada atende os itens, mesmo tendo ciência que ofertou solução com qualidade abaixo do mínimo definido junto ao edital, e em outros SEQUER ATENDE AO MINIMO EXIGIDO.**

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.

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 CJF realiza e, claramente, a oferta da LICITANTE não atende ao requisito.

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 anexado "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 ($(_ipsrc)) is listed by Spamhaus. Please see http://www.spamhaus.org/query/ip/$(_ipsrc) 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 Invaluement. Please see http://	Reject	The sending MTA IP address was listed on Invaluement 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.

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.

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.

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 aos 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.

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 aos 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.

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 Sitehttps://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.

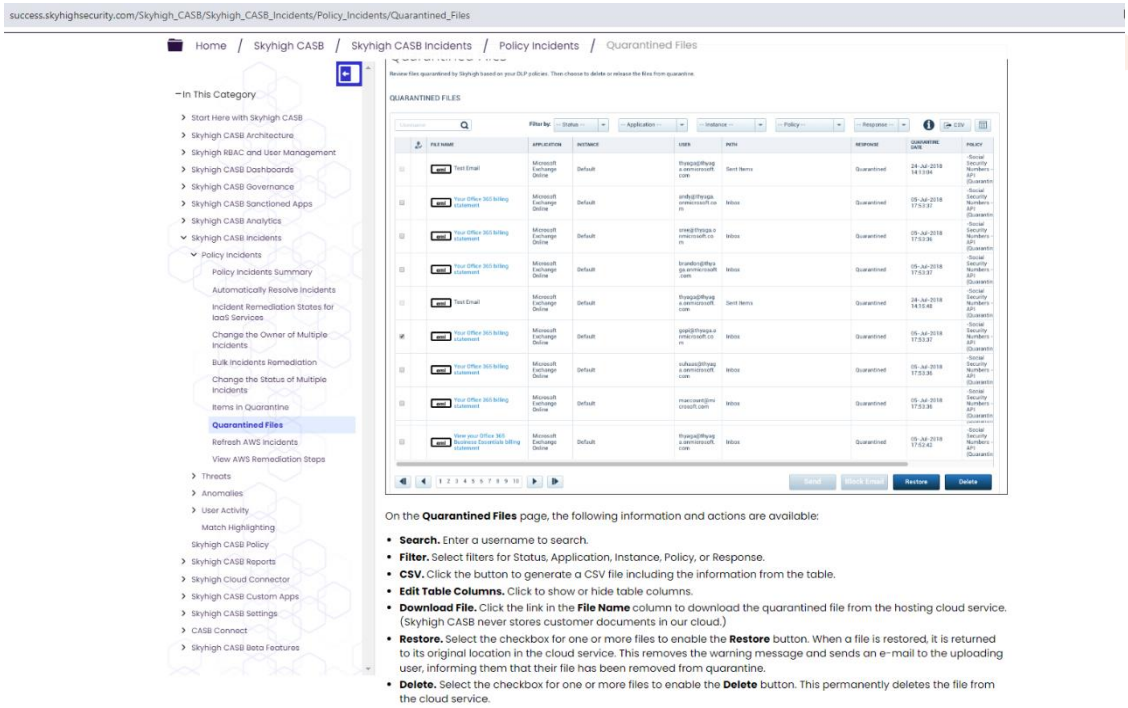
> This page provides the ability to search for a specific user, or filter quarantined files. You can also preview or download a file in Quarantine to make a decision on whether to Delete or Restore it. When you select one or more files from this list, Restore or Delete buttons are enabled. The Quarantined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

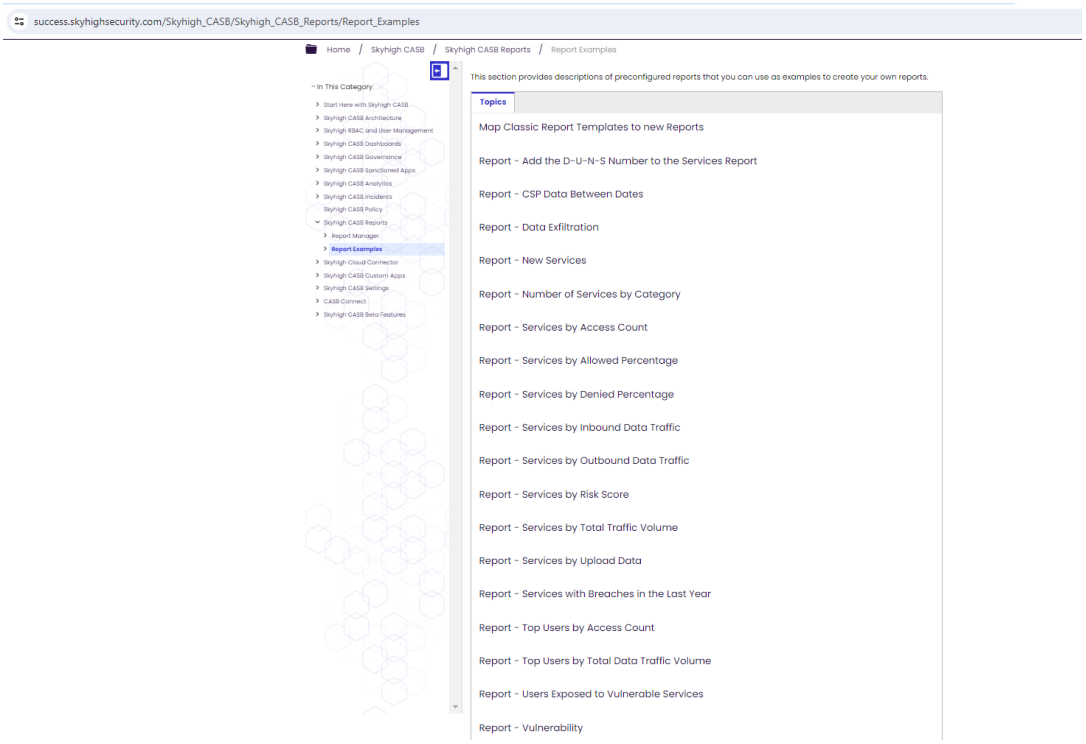
É evidente que o item descreve obrigatoriedade de customização de tipos de ação para uma política: Quarentenar, deletar ou passar.

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.



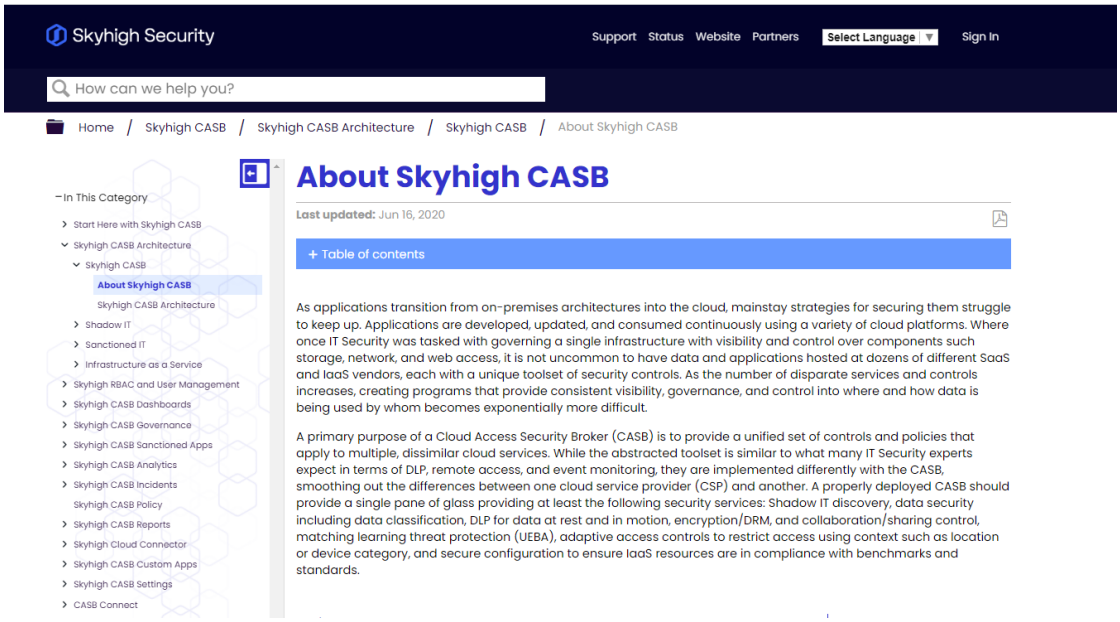
Adicionalmente, fica claro que a solução não traz a possibilidade de configuração de políticas de bloqueio e, muito menos, oferece visibilidade de ameaças (virus, malware, zero day, entre outros) considerando a camada de proteção para Microsoft 365. Vale destacar a imagem abaixo que traz a descrição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



“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.”



https://success.skyhighsecurity.com/Skyhigh_CASB/Skyhigh_CASB_Architecture/Skyhigh_CASB/About_Skyhigh_CASB

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 e-mail;

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.

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-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.

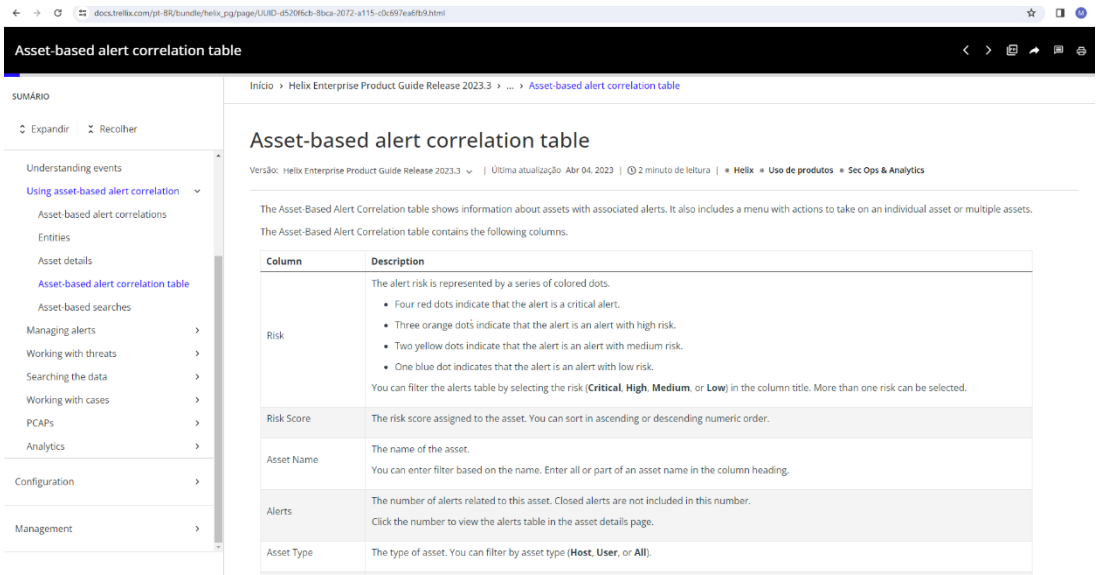
A agência é notável por suas diretrizes e padrões de segurança da informação. O Framework de Gerenciamento de Riscos de Cybersecurity do NIST (NIST Cybersecurity Framework) é uma referência amplamente adotada para organizações que buscam melhorar sua postura de segurança cibernética, por isso é de extrema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

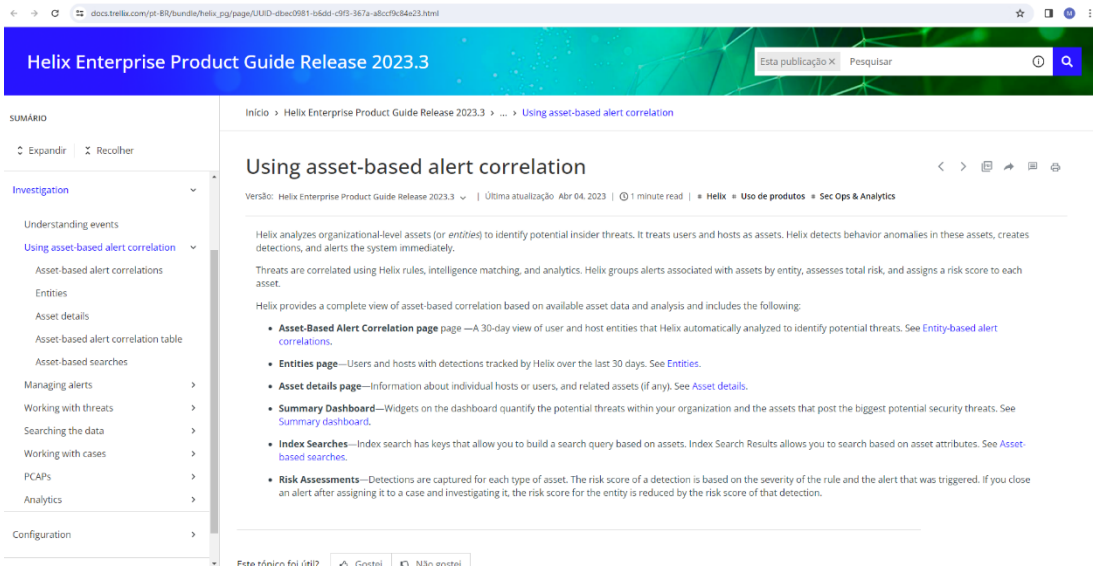
A solução fornecida claramente não fornece um índice global de risco, conforme item 8.37, onde o cálculo de risco utiliza as diretrizes do NIST.

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.





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.

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 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.

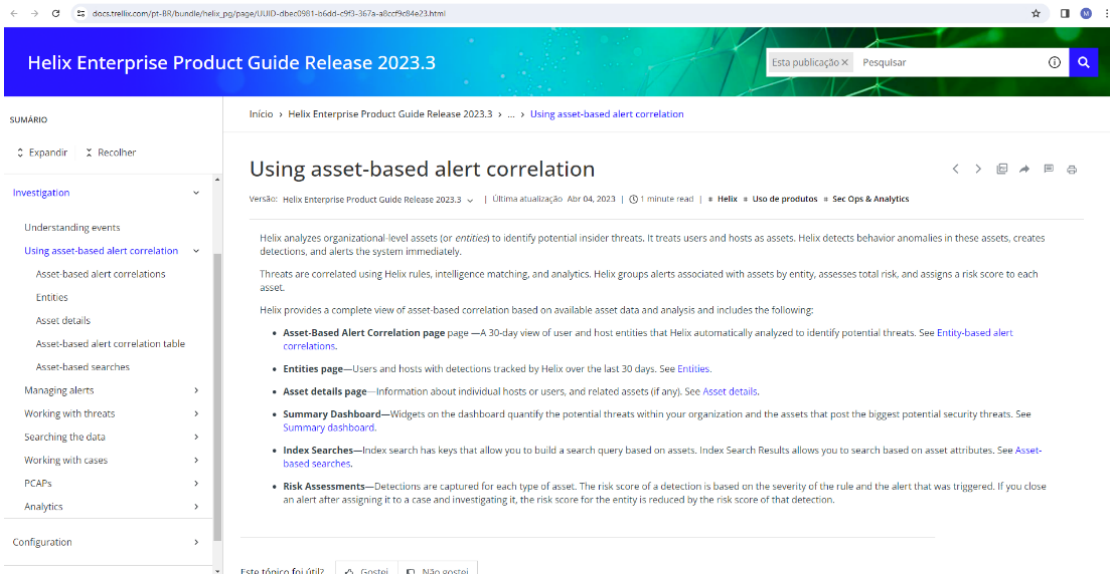
Desconsiderar o atendimento ao item, é aceitar soluções obsoletas colocando o ambiente do CJF em risco, uma vez que o CJF não terá conhecimento do quão exposto está seu ambiente tecnológico.

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.

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-dbec0981-b6dd-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.
- Responder rapidamente para gerir os riscos durante um incidente cibernético.
- Implementar medidas para mitigar os riscos advindos de falhas de segurança cibernética, e que possam ter acesso aos sistemas da empresa ou a seus dados.
- Elaborar um plano de ação para lidar com incidentes cibernéticos.

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.

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-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 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.

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-367f0730-bcdd-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:

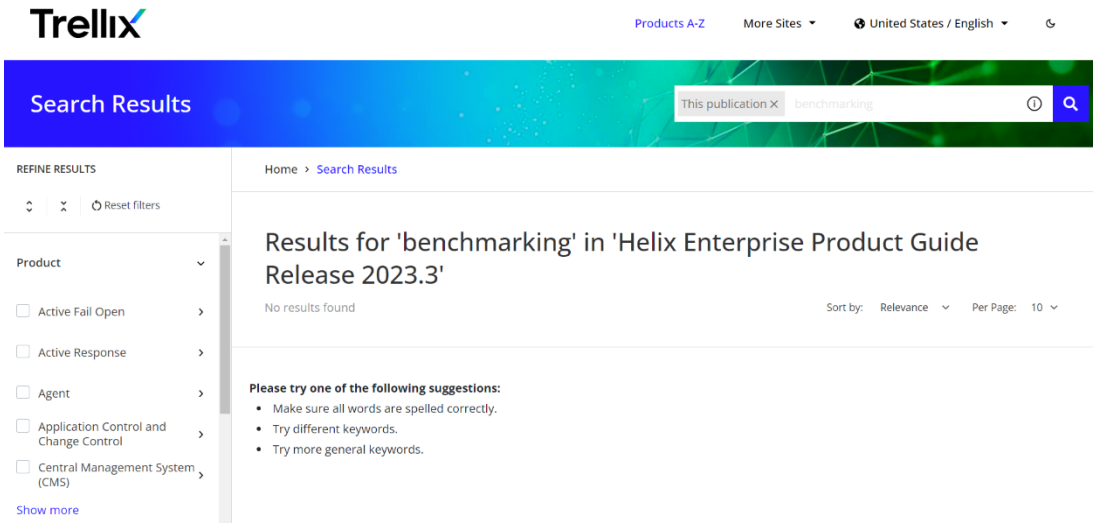
- ✓ Monitoramento constante da postura de segurança da organização em comparação com seus pares do setor.
- ✓ Identificação de lacunas de segurança e implementação de medidas corretivas para fortalecer a postura de segurança da organização.
- ✓ Aprimoramento contínuo das medidas de segurança, acompanhando 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.
- ✓ Diferenciação 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.



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. Ressalta-se 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
- ✓ Tradução Livre:
- ✓ Análise de comportamento de usuários e entidades (UEBA)
- ✓ Correlacione alertas com aprendizado de máquina para identificar atividades que sugerem alto risco de ameaças internas, movimentos laterais ou ataques em estágio 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 TRELLIX 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 organizações a priorizar seus esforços de segurança cibernética, 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 conscientização dos membros da organização sobre os riscos cibernéticos e as melhores práticas para mitigá-los. Isso pode levar a uma cultura de segurança mais forte e a um comportamento mais seguro por parte dos usuários.
- ✓ Diversas leis e normas exigem que as organizações implementem medidas de segurança para proteger dados e sistemas. Um guia pode ajudar as organizações a demonstrar conformidade com essas regulamentações.

- ✓ A implementação das medidas de um guia pode fortalecer significativamente a postura de segurança geral de uma organização, tornando-a mais resiliente a ataques cibernéticos.

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.

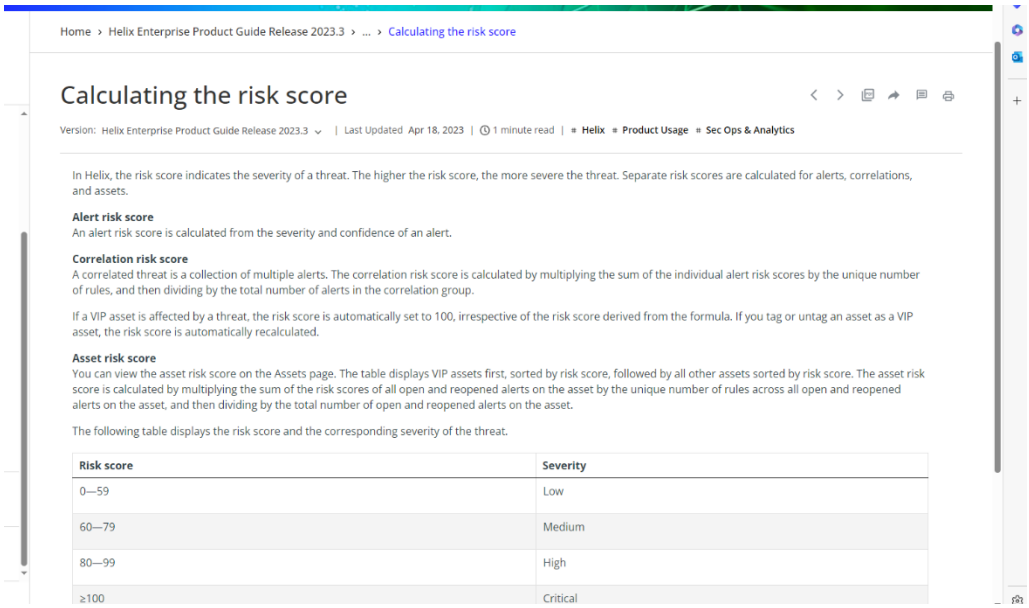
8.47 Deve permitir definir um objetivo de redução de risco.

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/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 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.



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.

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 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 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:

- ✓ Após 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 poderá ser reativada.
- ✓ Resolução do problema: Se o problema que levou à desativação da conta for resolvido, a conta poderá 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 à operação normal: Restaura a funcionalidade do endpoint e da rede.
- ✓ Minimizar a disrupção: 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 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.

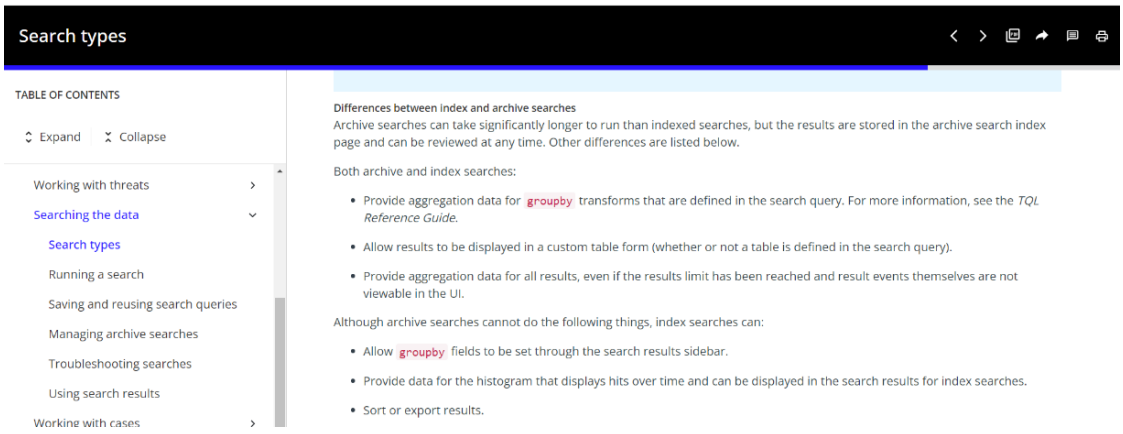
- ✓ Limitar o Ataque: Bloquear o acesso a aplicativos ou URLs em nuvem pode conter a propagação de um ataque cibernético, isolando o sistema comprometido e impedindo que o invasor acesse dados confidenciais ou cause mais danos.
- ✓ Proteger Recursos: O bloqueio protege recursos críticos contra acesso 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.

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-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.

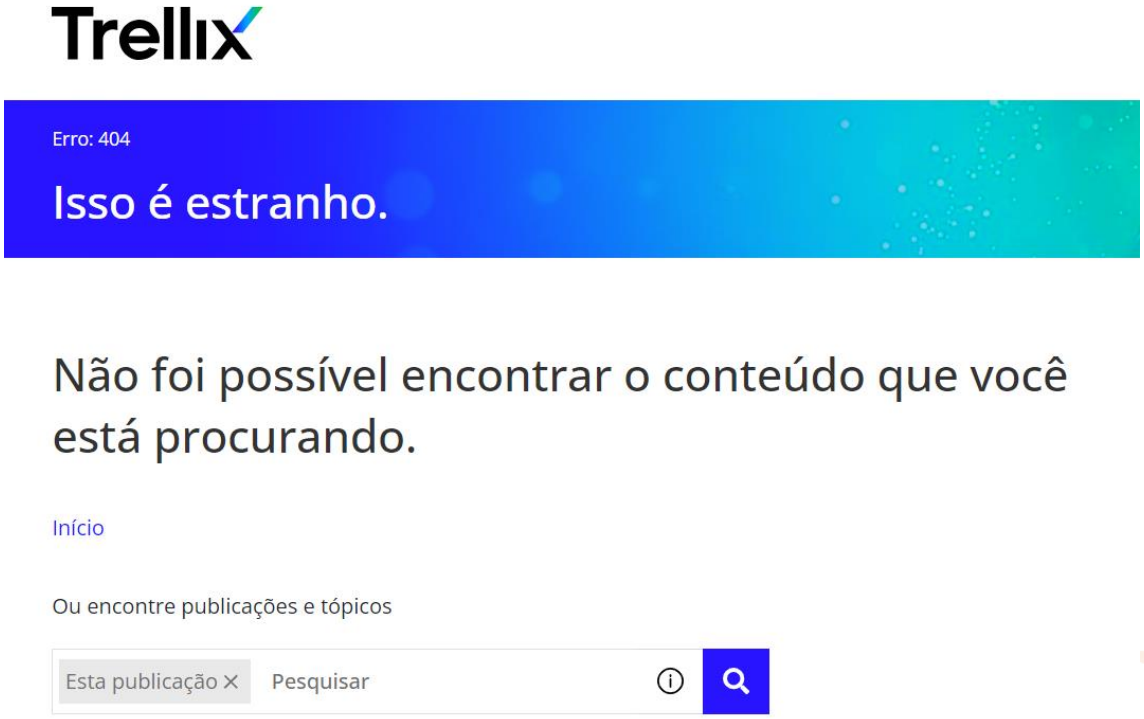
Isto é, a solução não é capaz de prover a visibilidade de um alerta que envolve diferentes tipos de camadas do XDR, trazendo graves prejuízos ao que se espera da solução a ser adquirida através deste edital. Ou seja, a equipe técnica do CJF não teria implementado em seu ambiente uma solução que tem por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

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/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/análise 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.



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 dar 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;

- Visão geral 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

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 descriptografia 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.

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:

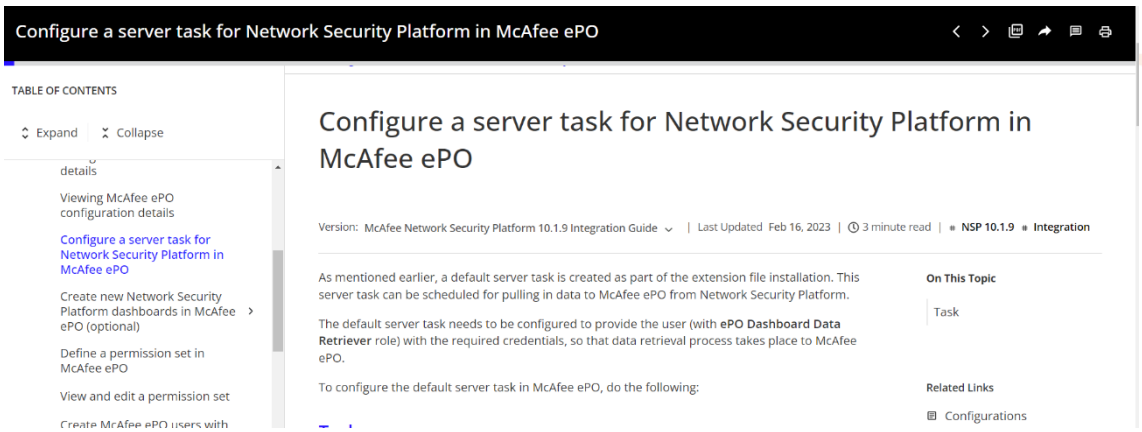
"Esta tarefa do servidor pode ser agendada para extrair dados do McAfee ePO da Network Security Platform."

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.

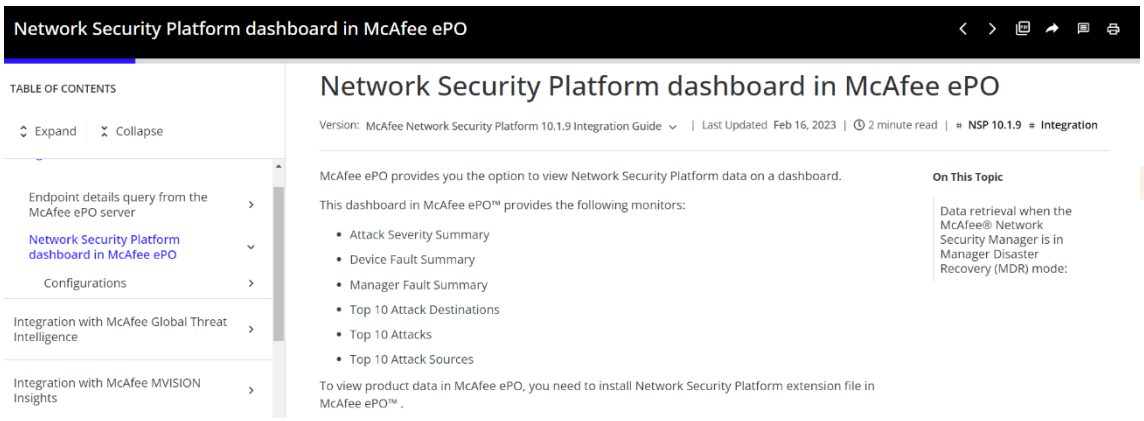
Em suma, caso um objeto suspeito seja identificado na camada de endpoint, esta informaria à plataforma de XDR, porém a solução de visibilidade de rede não conseguiria consumir determinada informação, pois o compartilhamento é unidirecional. Além disso, como consequência, as ações de resposta entre camadas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



https://docs.trellix.com/bundle/network-security-platform-10.1.x-integration-guide-unmanaged/page/GUID-49A572C7-6564-4AA3-B0C8-286D0C877102.html



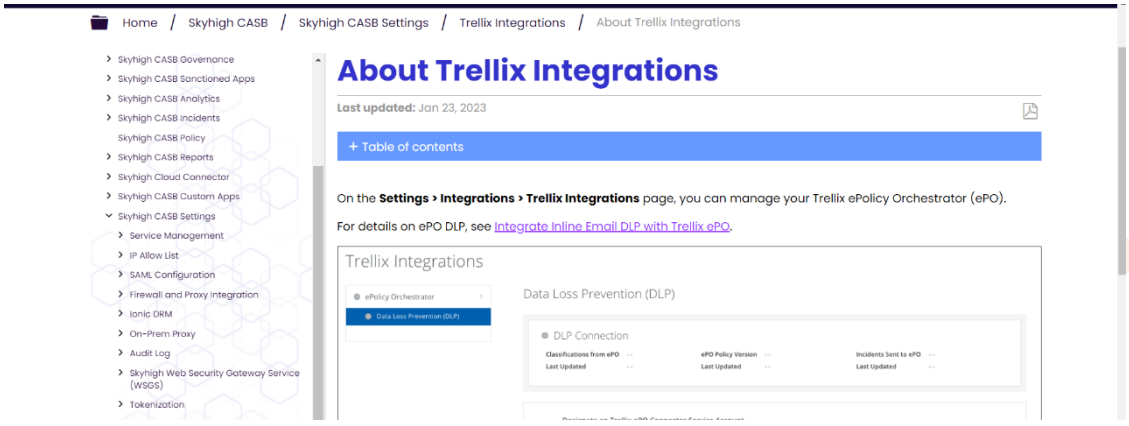
https://docs.trellix.com/bundle/network-security-platform-10.1.x-integration-guide-unmanaged/page/GUID-78DE7E07-A490-49BA-A671-9FF9FF9ADB52.html

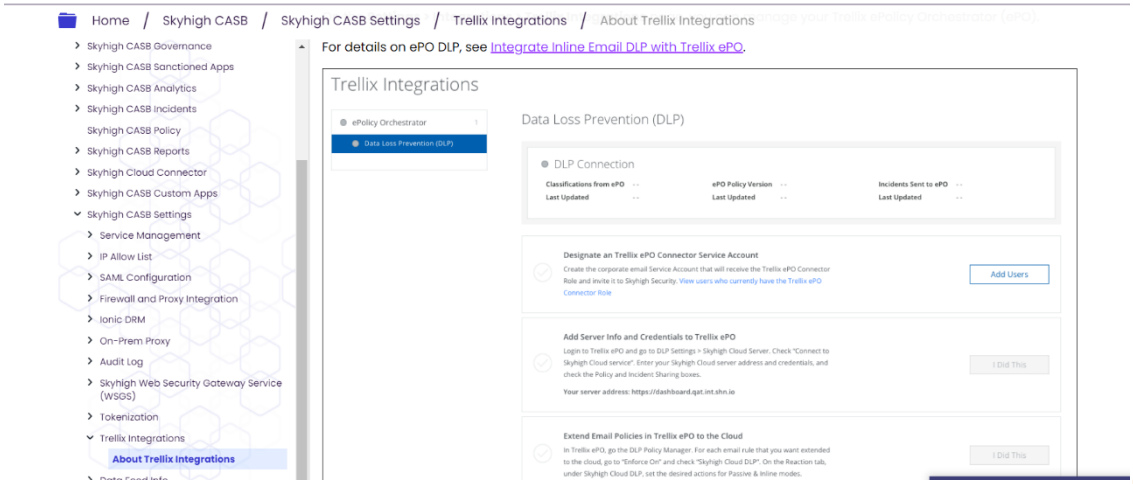
SKYHIGH CASB

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

<u>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.</u>

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.

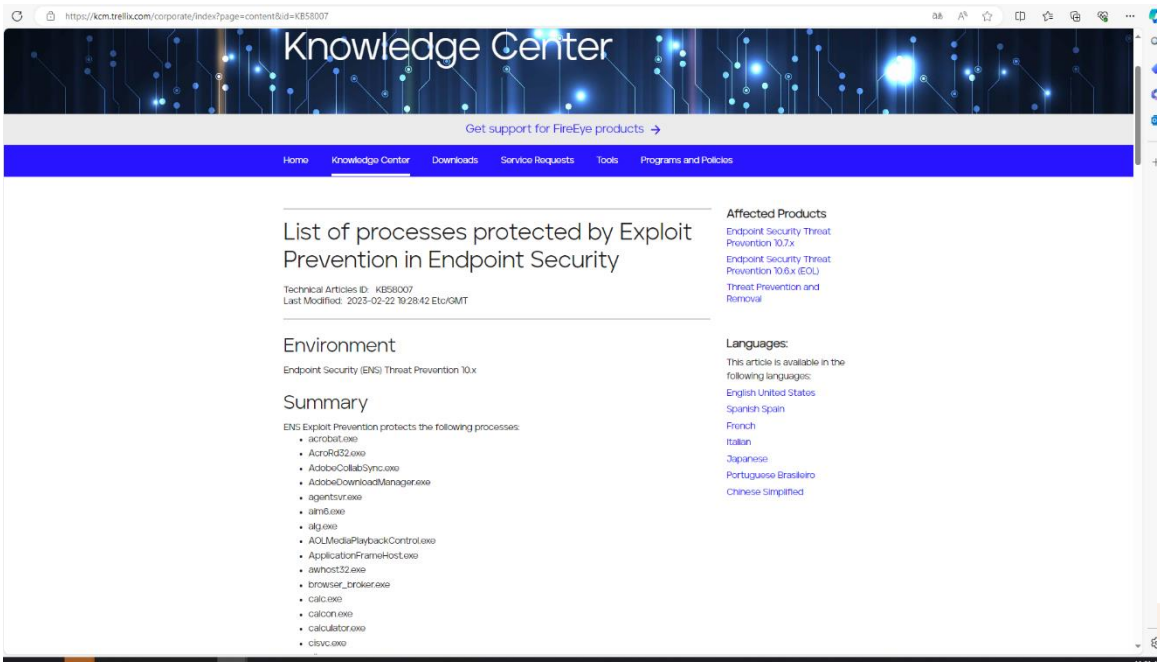
A não conformidade do item em questão pode acarretar diversas consequências negativas. Sem a capacidade de compartilhar IOCs (Indicadores de Comprometimento) com outros sensores e ferramentas, a eficácia na detecção de ameaças pode ser reduzida, levando a uma resposta inadequada ou atrasada a incidentes 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.

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.

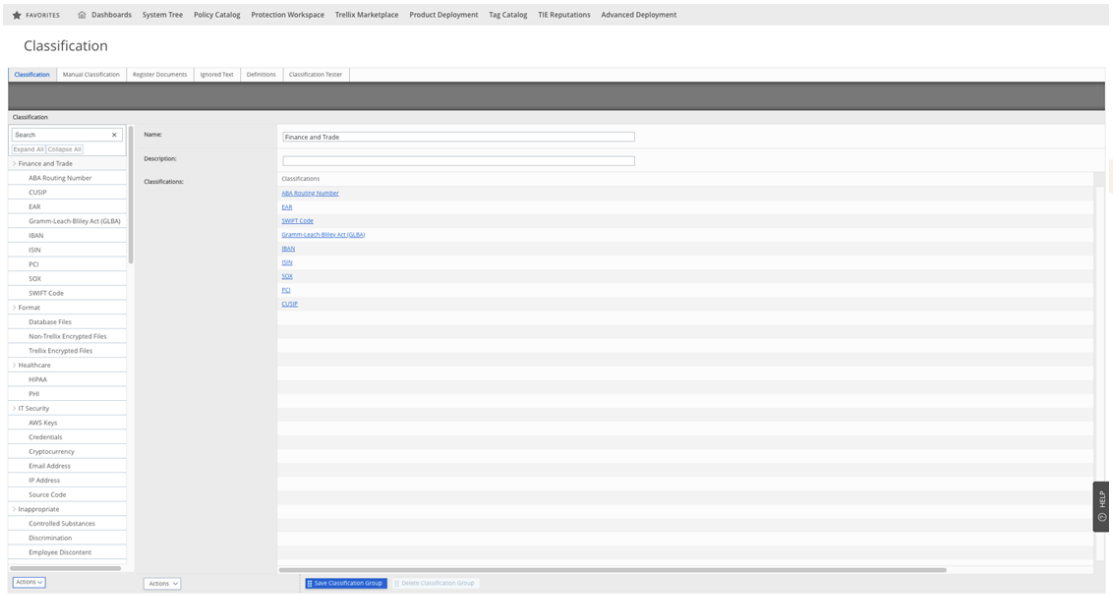
O prejuízo de não possuir esta funcionalidade é incalculável, considerando que os atacantes exploram cada vez mais vulnerabilidades conhecidas, ou seja, a TRELLIX, mais uma vez, demonstra a ineficácia de sua solução ofertada, trazendo brechas cruciais para o ambiente do CJF.

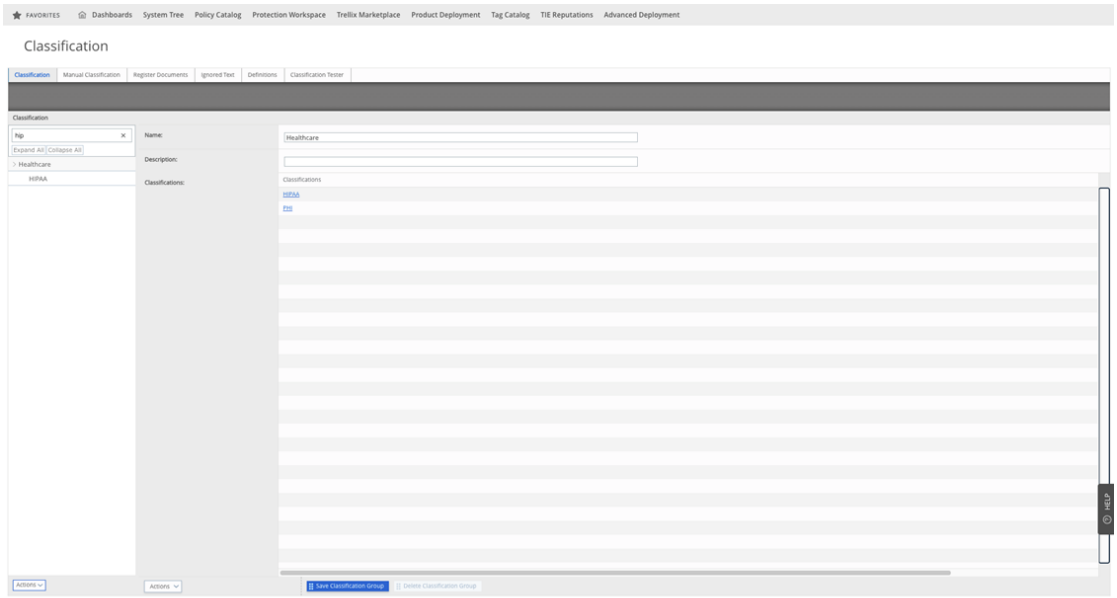
12.2.1 Deve possuir nativamente templates para atender as seguintes regulamentações: PCI/DSS, HIPA, Glba, SB-1386 e US PII.

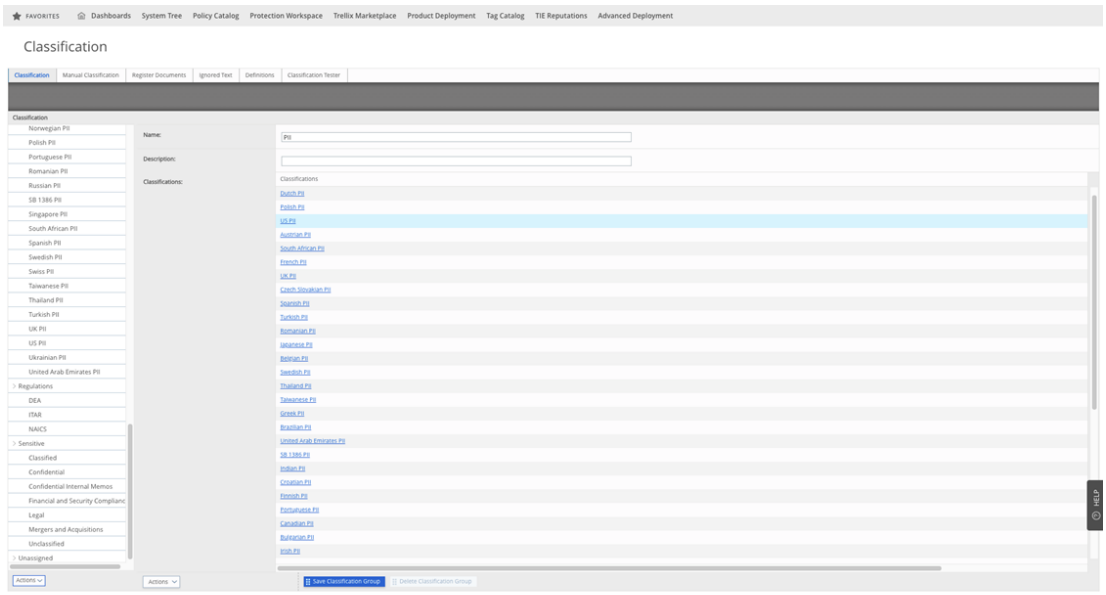
Fica evidente o não atendimento do item 12.2.1, pois não foi comprovado na planilha de comprovação técnica “Atendimento dos requisitos técnicosv2.xlsx” (ponto a ponto) e, após diligência, a LICITANTE disponibilizou algumas capturas de tela as quais não permitem identificar que tipo de solução se trata, se é um link de pesquisa ou alguma biblioteca interna. A comprovação do item não atende aos requisitos e não demonstram que possuem nativamente templates para atender as seguintes regulamentações:

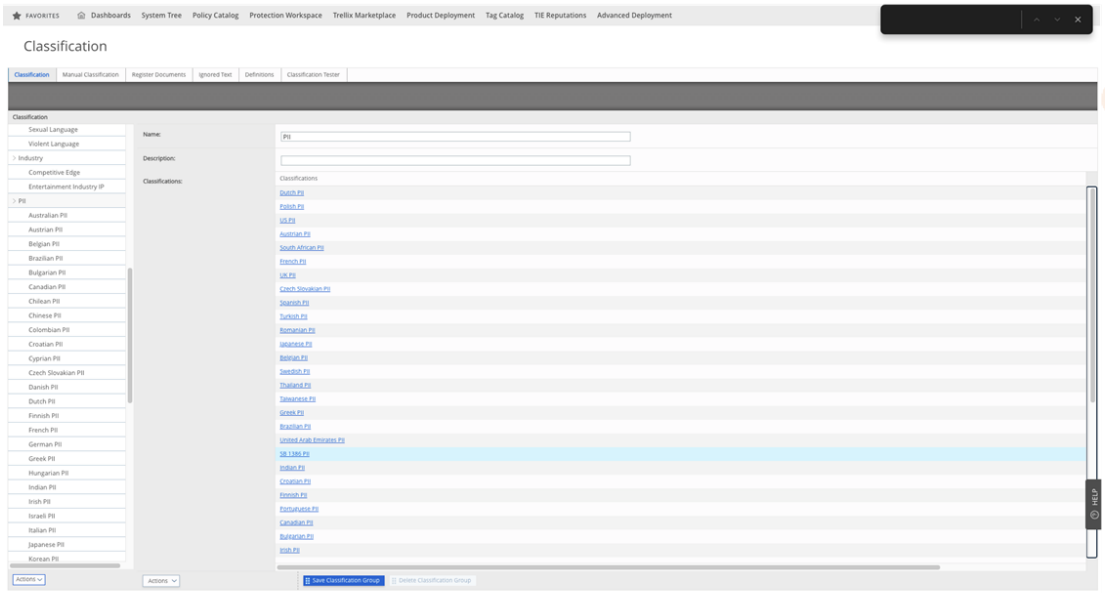
- ✓ PCI/DSS,
- ✓ HIPA,
- ✓ Glba,
- ✓ SB-1386 e
- ✓ US PII.

O não cumprimento do requisito de possuir nativamente templates para atender regulamentações específicas pode acarretar diversos riscos ao CJF. A falta de conformidade com regulamentações importantes, como o PCI/DSS, HIPAA, GLBA, SB-1386 e US PII, pode resultar em penalidades financeiras, multas e litígios. Além disso, aumenta a probabilidade de violações de dados e incidentes de segurança cibernética, expondo informações e danificando a reputação do CJF. Em resumo, o não cumprimento desse requisito representa um risco significativo, com potenciais impactos financeiros, legais, de reputação e operacionais.









d) **Prejuízo à Competitividade e impessoalidade**

O art. 5º da Lei n. 14.133/2021 é claro ao definir os princípios que devem ser observados junto ao presente certame e dentre eles, destacamos o da competitividade.

Ele é um dos pilares fundamentais que orientam as licitações públicas. Esse princípio visa assegurar que o processo licitatório seja conduzido de maneira a promover a concorrência entre os interessados em contratar com a Administração Pública. Para garantia desse princípio destacamos outro de igual importância – impessoalidade.

O princípio da impessoalidade visa garantir que as decisões e ações administrativas sejam tomadas de forma objetiva, sem favorecimentos pessoais ou discriminações.

Estes dois princípios exprimem a obrigatoriedade de tratar todos da mesma forma, sem privilegiar um em detrimento de outros. Isso não significa impor um formalismo exagerado, pelo contrário, ele delimita aquilo que pode ou não ser feito, afastando flexibilizações que tendem a beneficiar um determinado licitante.

A competitividade nas licitações públicas envolve a busca pelo melhor preço, qualidade, prazo e condições para a administração, estimulando a participação de um maior número de empresas e propiciando a escolha da proposta mais vantajosa para a Administração Pública. A ideia é criar um ambiente propício para a disputa leal entre os concorrentes, promovendo eficiência e eficácia na contratação.

A preservação desse princípio estimula a concorrência, dada a igualdade de condições, permitindo a seleção da proposta mais vantajosa a partir do cumprimento de critérios e requisitos. O chamado tratamento isonômico exige uma avaliação objetiva em relação aos padrões de qualidade exigidos, não se lhe sendo assistido reduzir requisitos ou aceitar menos do que aquilo que foi definido como características mínimas.

Ao aceitar uma proposta cuja solução deixou de atender os requisitos, esse CJF se afasta da regularidade processual e cria uma insegurança jurídica para todo o processo e partes envolvidas, colocando o interesse público em risco, deixando claro privilégios conferidos à então RECORRIDA.

e) **Autotutela administrativa**

A autotutela é um dever da Administração Pública que está previsto no artigo 53 da Lei nº 9.784/99 e na Súmula nº 473 do STF. Esse dever significa que a Administração deve revisar e anular seus próprios atos administrativos que estejam viciados por ilegalidade ou que não sejam convenientes ou oportunos. É importante lembrar que esse não é apenas um poder, mas sim uma obrigação da Administração.

A autotutela administrativa é uma prerrogativa concedida à Administração Pública para que possa rever seus próprios atos quando necessário. Essa possibilidade de rever seus atos por iniciativa própria se dá em razão da supremacia do interesse público sobre o privado. É importante destacar que a autotutela administrativa não é uma via de mão única, e a Administração Pública também pode rever seus atos por provocação, ou seja, por meio de requerimento apresentado pelo interessado.

Ressaltamos também cabe ao interessado apresentar argumentos consistentes e fundamentados para justificar e provocar uma revisão do ato administrativo. Caso contrário, é possível que o requerimento seja indeferido pela Administração Pública. No presente caso, justificamos exaustivamente a necessidade inafastável de se rever a decisão, procedendo a análise documental de acordo com os requisitos definidos pelo próprio CJF e que constam no edital, não se admitindo a inovação e nem interpretações de atestados de entes particulares aplicando-se as regras de contratações públicas.

A Administração Pública tem o dever de avaliar o presente caso e decidir com base nos princípios da legalidade, da moralidade, da eficiência, da razoabilidade e da proporcionalidade, promovendo, ainda, apuração da responsabilidade civil perante as declarações, informações e documentos apresentados e, para isso, deve evocar o princípio da autotutela administrativa.

Por fim, é importante destacar que a possibilidade de revisão de um ato administrativo por provocação é uma garantia fundamental para os cidadãos em relação à Administração Pública. Dessa forma, é fundamental que o cidadão esteja ciente de seus direitos e saiba como proceder para exercê-los, tal qual o caso em lide.

Cabe a esse CJF evocar o princípio e rever sua decisão, tendo por base todos os elementos trazidos nesta peça recursal.

V. CONCLUSÃO

Em resumo, fica evidente que a BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA não está ofertando uma solução capaz de atender os requisitos mínimos exigidos, resultando em uma oferta de solução de qualidade muito inferior ao descrito no termo de referência, como exaustivamente demonstrado, resultando em uma PROPOSTA que não atende ao EDITAL.

Qualquer alternativa que seja adotada diferente da desclassificação da mesma, estará maculando o Edital em face dos princípios constitucionais norteadores da ADMINISTRAÇÃO PÚBLICA, tais como o da moralidade, impessoalidade, isonomia, devido processo legal, entre outros mais.

A aceitação e homologação da proposta impugnada causará sérios riscos a administração pública, assim como, possibilidade de enorme prejuízo ao erário.

A participação da RECORRIDA perante o certame é desrespeitosa, ao passo que oferta solução que não atende aos requisitos e quando convocado em sede de diligenciamento, desmerece o conhecimento dos servidores envolvidos no processo, apresentando supostas comprovações que também não atendem às exigências mínimas, não conferindo a seriedade mínima necessária esperada de uma licitante.

Desta forma, fica claro que vários aspectos da solução oferecida pela fabricante TRELLIX, representada pela BLUE EYE SOLUÇÕES EM TECNOLOGIA LTDA, não foram atendidos. Adicionalmente, é importante destacar que, diante das necessidades especificadas pelo CJF, surgem alguns pontos críticos e de não atendimentos, entre os principais podemos citar os seguintes:

a) Inexistência de funcionalidades relacionadas ao processo de visibilidade de risco;

b) Inexistência de uma pontuação geral para cada organização;

c) Utilização de padrão próprio, passível de falha, para definição de risco;

d) Integração limitada das soluções ofertadas Skyhigh CASB e Network Security com a "plataforma central". O conceito de XDR descrito no objeto deste edital não é comprovado.

e) Possuir configuração de classificação de spam com, no mínimo, três níveis: Alto, Médio e Baixo ou escala equivalente

f) Possuir capacidade de identificar e proteger o MTA contra-ataques de Negação de Serviços (DoS)

g) Possuir capacidade para detecção de explorações de documentos, ameaças de dia zero, vulnerabilidades conhecidas e outras ameaças usadas em ataques direcionados

h) Permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.

i) Obter relatório:

   a. Relatório sobre resumo do tráfego de e-mail de todos os domínios,

   b. Relatório sobre resumo do tráfego de e-mail domínio,

   c. Relatório sobre detecções de ameaças,

   d. Relatório sobre detecções de arquivos da sandbox,

   e. Relatório sobre detecções de URL da sandbox e

   f. Relatório sobre os principais destinatários comprometidos por e-mail (BEC)

j) 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).

k) Fornecer um índice global de risco

l) Fornecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.

m) Fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos.

n) Realizar benchmarking em tempo real com comparação de nível de risco

o) Fornecer um guia para reduzir fatores de risco detectados

p) Definir um objetivo de redução de risco.

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

r) Permitir as seguintes ações para responder a riscos:

   a. Desativar/Ativar conta do usuário

b. Forçar logout

c. Redefinir senha

d. Isolar/Restaurar Endpoint

e. Monitorar tentativas de login

f. Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno

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

s) Consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.

t) Permitir alterar o status de cada evento, para no mínimo Novo, Em progresso/análise e Fechado ou escala equivalente.

u) Exibir os seguintes painéis de controle:

a. Índice de risco dar empresa;

b. MITRE ATT&CK® Mapping for Enterprise;

c. Visão geral de alertas;

d. Top 10 vulnerabilidades em risco;

e. Top 10 usuários em risco;

f. Top 10 dispositivos em risco;

v) Integrado a rede através de port mirror.

w) Permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança.

x) 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.

y) Integrar 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.

z) Detectar e responder, os IOCs poderão ser compartilhados com outros sensores do fabricante e ferramentas de terceiros, sendo estas ao menos:

a. MS Active Directory,

b. Microsoft 365

c. Fortinet.

aa) 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.

bb) Possuir nativamente templates para atender as seguintes regulamentações: PCI/DSS, HIPA, Glba, SB-1386 e US PII.

A não conformidade com esses requisitos atrai para o ambiente desse CJF uma possibilidade enorme de riscos e impactos negativos, tais como:

a) Visibilidade limitada de risco: A ausência de funcionalidades relacionadas ao processo de visibilidade de risco resulta em uma compreensão inadequada das ameaças e vulnerabilidades enfrentadas pela organização, dificultando a tomada de decisões informadas para mitigação de riscos.

b) Falta de avaliação geral de segurança: Sem uma pontuação geral para cada organização, torna difícil para os gestores avaliarem rapidamente o nível de segurança da empresa como um todo, dificultando a priorização de medidas de segurança, alocação de recursos e melhoria contínua dos processos.

c) Risco de falha de segurança: A utilização de um padrão próprio para definição de risco, passível de falhas, aumenta a possibilidade de inadequações na identificação e avaliação de ameaças, o que pode levar a falhas na proteção dos ativos e dados da organização.

d) Integração limitada das soluções: A integração limitada das soluções oferecidas com a plataforma central pode resultar em lacunas na visibilidade e no controle de segurança, dificultando a detecção e resposta eficaz a incidentes de segurança.

e) Falta de comprovação do conceito de XDR: O conceito de XDR descrito no edital não é comprovado, isso demonstra que a solução não atende aos requisitos de detecção e resposta estendidas, deixando o CJF vulnerável às ameaças avançadas que podem passar despercebidas, além de limitar a capacidade de detecção entre camadas, investigação e resposta.

No geral, a não conformidade com esses requisitos comprometerá a eficácia da estratégia de segurança desse CJF e aumenta sua exposição à riscos de segurança cibernética.

VI. DOS PEDIDOS

Ilustríssima Pregoeira, Comissão e Assessoria Jurídica do CJF, o que foi apresentado até aqui já é mais que suficiente para demostrar um equívoco na classificação da RECORRIDA. São alegações claríssimas que sustentam a necessidade de se

promover a ANULAÇÃO da decisão e consequente desclassificação por inobservância à premissas mais básicas exigidas no edital.

A solução ofertada não atende a todas as especificações editalícias, ato que por sí só já deveria ter acarretado a desclassificação. Buscando oportunizar a demonstração, a MD. Pregoeira convocou em sede de diligenciamento, a qual mais uma vez falhou na simples missão de comprovar requisitos. O item abaixo é responsável por dirimir a questão:

> *"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****."*

A condução do processo empregou a possibilidade de usar a prerrogativa do diligenciamento, mas em sede complementar e para esclarecimento de dúvidas, sendo vedada a inclusão posterior de informação que deveria constar desde o início.

Ocorre que a proposta é justamente esse documento com informações que deveriam constar originalmente da proposta:

> *"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."*

Insistir na habilitação da RECORRIDA afronta o princípio da isonomia e igualdade e pode levar ao entendimento equivocado de predileção.

Claramente de forma desrespeitosa, a empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA não está levando o processo à sério e se comportando de forma imprudente, descuidada e negligente, induzindo a MD. Pregoeira ao erro. A RECORRIDA acredita que qualquer elemento que usar para fins de comprovação será aceito por esse CJF, mesmo não atendendo as exigências do edital, algo que esta RECORRENTE não permitirá.

Data vênia, temos que a MD. Decisão da Ilma. Pregoeira busca atender o interesse público envolvido, entretanto, há inafastável necessidade de se invocar a autotutela administrativa, revisando as comprovações sob as óticas e argumentos aqui trazidos, o que certamente levará esse CJF a recusar a proposta da empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA e a consequente convocação das demais licitantes, na ordem de classificação do certame.

Des feita, pugnamos:

a) PROVIMENTO total das presentes razões e justificativas, a fim de provocar uma revisão dos atos praticados, promovendo a desclassificação da empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA e convocação das demais licitantes;

b) Existindo dúvidas quanto a decisão a ser tomada, que a MD. Pregoeira emita parecer justificando e embasando a sua decisão e em seguida, encaminhe o processo à Autoridade Competente, para conhecimento e ciência dos riscos que sua gestão está incorrendo, caso mantenha a decisão;

c) Mantida a decisão por parte da Autoridade Competente, que os autos sejam encaminhados à Douta Consultoria Jurídica, sem prejuízo da emissão de parecer sobre o caso; e

d) Em se mantendo a decisão, que dê publicidade aos atos proferidos e seus respectivos embasamentos para que esta RECORRENTE tenha acesso às justificativas para que busque seus direitos legais.

Ademais, salientamos que a manutenção da decisão e consequente continuidade da habilitação da empresa BLUE EYE SOLUCOES EM TECNOLOGIA LTDA não prospera e não prosperará perante a justiça e nem perante o Tribunal de Contas da União - TCU e que esta empresa recorrerá à todas as instâncias possíveis para defender seus direitos, assim como evitando o cometimento de grave prejuízo ao erário.

Nesses termos,

Pede deferimento.

MURILO ROSSETTO
Representante Legal
ALLTECH SOLUÇÕES EM TECNOLOGIA