CARLOS COSTA JORDÃO
23/10/2026 18:26
MAURICIO ANTONIOLI SCHMITZ
23/10/2026 18:28
GEOVANE DUTRA DE SOUZA
23/10/2026 18:56
NATACHA MORAES DE OLIVEIRA
23/10/2026 19:41
ALBERTO DANIEL MULLER
23/10/2026 21:41
CAROLINE ROCHA MOLINA
24/10/2026 12:37

TERMO DE REFERÊNCIA

1 DEFINIÇÃO DO OBJETO

1.1. Contratação de Solução integrada de Detecção e Resposta Estendidas a ataques cibernéticos (XDR) e Detecção e Resposta a Ameaças de Identidade (ITDR), incluindo serviços de treinamento, implantação, operação, monitoramento e sustentação, pelo período de 36 meses., conforme condições, quantidades e exigências estabelecidas neste instrumento.

1.2. Detalhamento dos bens e serviços que compõem a solução:

Item	Descrição	Unidade	Quantidade compra inicial	Quantidade total do registro
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses	Ativo monitorado	0	68.800
2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses	Usuários ativos	0	60.170
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Tokens	0	834.300
4	Ingestão de logs externos	Franquia de Gigabyte por dia	0	10.590
5	Serviço de treinamento na solução proposta	Serviço único, por turma de treinamento	0	23
6	Serviço de implantação da solução proposta	Serviço único por contratante	0	18
7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Serviço fixo para 2000 ativos monitorados por mês	0	18
8		Serviço para 1000 ativos adicionais monitorados por mês	0	39

1.3. Os itens do objeto devem ser agrupados em grupo[1]?

(x) Sim - Justificativa para o não parcelamento do objeto:

A contratação em lote único justifica-se pela interdependência técnica dos componentes da solução de segurança cibernética, que exige perfeita integração tecnológica entre os módulos, compartilhamento de informações e funcionamento coordenado dos recursos de monitoramento, detecção, investigação e resposta a incidentes.

( ) Não

2 PREVISÃO NO PLANO DE CONTRATAÇÕES DE TIC

2.1. A demanda está prevista no Plano de Contratações de TIC de 2026 e no Plano de Contratações Anual do Tribunal (PCA), conforme ID SGTI-18/2026 e 67/2026.

3 FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. A fundamentação da presente contratação faz parte dos estudos técnicos preliminares constantes nos seguintes documentos:

3.1.1 Documento de Oficialização da Demanda;

3.1.2 Estudos Técnicos Preliminares;

3.1.3 Mapa de Riscos.

4 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO[2]

4.1. A solução compreende a contratação integrada de subscrições de software para Detecção e Resposta Estendidas (XDR) e Detecção e Resposta a Ameaças de Identidade (ITDR), incluindo recursos de automação e orquestração de respostas, ingestão de logs externos e serviços de implantação, treinamento, suporte e monitoramento gerenciado de segurança cibernética em regime 24x7x365.

---

1 O parcelamento do objeto deverá ser adotado sempre que a sua divisão seja tecnicamente viável e economicamente vantajosa e não represente perda de economia de escala. O não parcelamento do objeto deverá ser devidamente justificado com a demonstração das razões técnicas, administrativas e econômicas que o inviabilize.

Devem ser considerados:

- a responsabilidade técnica;
- o custo para a Administração de vários contratos frente às vantagens da redução de custos, com divisão do objeto em itens.

2 A descrição da solução como um todo deverá considerar o ciclo de vida do objeto, na sua totalidade, inclusive a especificação da garantia, quando couber, e as exigências relacionadas à manutenção e à assistência técnica, quando for o caso, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação.

4.2. A solução deverá proporcionar visibilidade unificada do ambiente tecnológico do TRT, permitindo a correlação de eventos, a investigação de incidentes e a execução coordenada de ações de contenção e resposta a ameaças.

4.3. A contratada deverá assegurar garantia e suporte integrais durante toda a vigência contratual, abrangendo todos os componentes da solução, correção de falhas, atualizações e suporte técnico corretivo, proativo e consultivo, com atendimento 24x7x365, sem limitação de chamados ou custos adicionais.

4.4. A vigência inicial de 36 meses justifica-se pela natureza continuada dos serviços e pela necessidade de assegurar estabilidade operacional, continuidade da proteção e aproveitamento dos investimentos realizados na implantação e integração da solução, evitando os custos e riscos decorrentes de substituições frequentes de tecnologias críticas de segurança.

5 ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

5.1. Especificações técnicas

5.1.1 As especificações técnicas constam no Anexo I.

CRITÉRIOS DE SUSTENTABILIDADE

5.2. A contratação possui critérios de sustentabilidade e/ou observou as práticas sustentáveis do Guia de Contratações?

( ) Não

(x) Sim - Discrimine a seguir:

5.2.1 A solução a ser contratada promove a transformação digital ou racionalização de serviços atualmente realizados por meio de análise humana, especificamente através de recursos de inteligência artificial para a correlação de eventos e geração de relatórios.

5.2.2 Toda a documentação de software e base de conhecimento deverá estar disponível na internet, de forma a evitar impacto sobre recursos naturais decorrentes de produção de material de impressão, de pacotes e de desfazimento futuro;

5.2.3 Assinatura digital é um ato de transformação digital, portanto, sustentável;

5.2.4 A realização de treinamentos de forma remota racionaliza o consumo de recursos orçamentários do Tribunal e evita o deslocamento dos servidores, contribuindo para a sustentabilidade nesses dois aspectos.

6 MODELO DE EXECUÇÃO DO OBJETO

6.1. Prazos e Condições:

6.1.1 A vigência do contrato terá início com sua assinatura e encerra-se no prazo de **36 meses** contados da data de início da prestação dos serviços (data do recebimento definitivo do objeto), podendo ser prorrogado, na forma dos artigos 106 e 107 da Lei nº 14.133/2021.

6.1.1.1 Na hipótese de serem celebrados contratos posteriores para qualquer item ou serviço diverso do Item 1, a vigência desses contratos se findará no mesmo dia de encerramento do contrato do Item 1.

6.1.2 No prazo máximo de **10 dias**, contados da assinatura do contrato, deverá ser realizada a reunião inicial de gestão do contrato.

6.1.2.1 Deverão estar presentes na reunião o preposto e um integrante da equipe técnica da contratada.

6.1.2.2 A pauta da reunião deverá abordar o planejamento detalhado da implantação da solução contratada, além das condições contratuais.

6.1.3 A disponibilização das subscrições e serviços (itens 1, 2, 3 e 4), e a execução completa da Implantação da Solução (item 6) devem ocorrer em até **60 dias** a contar da assinatura do contrato.

6.1.4 A vigência das subscrições dos itens 1 e 2 será de **36 meses**, contados a partir da data de emissão do Termo de Recebimento Definitivo do objeto, após a conclusão da implantação e a entrada da solução em produção, em pleno funcionamento, de acordo com as especificações do fabricante da solução e em conformidade com os requisitos da contratação.

6.1.4.1 As subscrições poderão ser disponibilizadas de forma anual, hipótese em que cada disponibilização deverá assegurar o período de vigência correspondente, observadas as condições estabelecidas na contratação.

6.1.4.2 Durante a etapa de implantação, é facultado à contratada o uso de licenças temporárias (trial), visando não onerá-la antes da efetiva entrada em produção, evitando o cômputo precoce do prazo de vigência das subscrições, desde que tais licenças não apresentem limitações ao uso inicial da solução.

6.1.4.3 Eventuais atrasos na implantação motivados pelo Contratante não postergarão o início da vigência das subscrições já adquiridas e disponibilizadas, desde que estas estejam efetivamente disponíveis para uso, conforme as condições estabelecidas na contratação.

6.1.4.4 Caso a contratação das subscrições referentes ao Item 2 ocorra em data posterior à contratação do Item 1, a vigência das subscrições do Item 2 deverá ser ajustada de modo que sua data de encerramento coincida com a data de encerramento das subscrições do Item 1.

6.1.4.4.1 Na hipótese prevista no subitem anterior, o valor das subscrições do Item 2 será calculado proporcionalmente ao período efetivo de sua vigência, com base no preço unitário contratado.

6.1.5 O serviço gerenciado (itens 7 e 8) terá início imediatamente após o recebimento definitivo do objeto e possuirá vigência de 36 meses.

6.1.6 O treinamento (item 5) deverá ser concluído no prazo máximo de 180 dias a contar da assinatura do contrato.

6.2. Garantia

6.2.1 A solução como um todo, englobando software, módulos, coletores, sensores, integrações e serviços associados, deverá contar com garantia e suporte integrais prestados pela CONTRATADA com respaldo do fabricante (Garantia Compreensiva), durante todo o período de vigência contratual.

6.2.2 A garantia deve cobrir a correção de quaisquer bugs, falhas de funcionamento, erros de código, atualizações de assinaturas, atualizações de versão (major e minor releases), patches e hotfixes, sem nenhum custo adicional para o CONTRATANTE.

6.3. Serviço de Suporte Técnico

6.3.1 O suporte técnico inclui todos os serviços técnicos necessários para assegurar o pleno funcionamento da solução conforme as especificações do objeto, sem qualquer custo adicional para o CONTRATANTE.

6.3.2 Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, garantir o fornecimento e instalação de novas versões, patches e hotfixes (tanto de componentes on premises quanto em nuvem), análise de dúvidas sobre melhores práticas de configuração, entre outros.

6.3.3 A abertura de chamados pelo CONTRATANTE deve poder ser efetuada:

6.3.3.1 Pela plataforma web, em sistema de atendimento da CONTRATADA;

6.3.3.2 Pelo envio de mensagem de correio eletrônico;

6.3.3.3 Por meio do módulo de gestão de incidentes de segurança da

solução ofertada;

6.3.3.4 Por telefone.

6.3.4 O atendimento aos chamados deve estar disponível em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

6.3.5 Não poderá haver quaisquer restrições de quantidade de abertura de chamados no suporte técnico.

6.3.6 Todo tipo de comunicação e documentação relacionados aos atendimento de chamados devem ser em Português.

6.3.7 A assistência técnica em garantia deve assegurar o fornecimento de acesso irrestrito (24 horas por dia, 7 dias da semana) do CONTRATANTE à área de suporte do fabricante, especialmente ao endereço eletrônico (web site) e a toda a documentação técnica pertinente (guias de instalação e configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

6.3.8 Para a aferição e a avaliação dos níveis de serviço, a CONTRATADA deverá apresentar mensalmente à fiscalização do contrato, um relatório gerencial de serviços, até o quinto dia útil do mês subsequente ao da prestação do serviço. O relatório deverá conter, entre outras informações, a medição dos indicadores/metas de níveis de serviço, recomendações técnicas, e demais informações relevantes para a gestão contratual.

6.3.9 Os prazos de solução dos chamados deverão atender aos seguinte critérios:

Severidade	Classificação	Prazo de Solução
A0 - Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado.	2 horas a contar da abertura do chamado
A1 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	6 horas a contar da abertura do chamado
A2 - Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente.	2 dias úteis contar da abertura do chamado
A3 - Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto, dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, Impacto mínimo para os usuários.	5 dias úteis a contar do próximo dia útil da abertura do chamado
A4 - Pesquisa	Chamados com objetivo de melhorar a ferramenta, implantar novas funcionalidades ou configurações que demandem tempo e planejamento	10 dias úteis a contar do próximo dia útil da abertura do chamado

6.4. Serviço de suporte a incidentes

6.4.1 O serviço de operação e gestão da solução deverá classificar os incidentes de segurança conforme a seguir:

Prioridade	Descrição do impacto	Peso
P0 - Crítico	Alertas de invasão de ativos classificados como críticos; Comprometimento em massa de dados sensíveis; Comprometimento de credenciais administrativas; Movimentação lateral no ambiente;	**4**
P1 - Alto	Degradação de ativos classificados como críticos; Comprometimento parcial de dados sensíveis; Comprometimento de credenciais não administrativas;	**3**
P2 - Médio	Comprometimento ou degradação de ativos classificados como não críticos; Comprometimento de dados não sensíveis;	**2**
P3 - Baixo	Comprometimento ou degradação de ativos classificados como de baixa relevância. Representa uma oportunidade de melhoria no ambiente.	**1**

* 'Dado pessoal sensível' terá o significado da LGPD. A criticidade da informação observará adicionalmente a política de segurança da informação do CONTRATANTE.

6.4.2 Os seguintes Indicadores de Nível de Serviço de incidentes de segurança serão considerados:

Prioridade	Tempo máximo de percepção do incidente de segurança (MTTD)	Tempo máximo de resposta ao incidente de segurança	Tempo máximo de contenção (MTTR)
P0 - Crítico	15 min	35 min	90 min
P1 - Alto	30 min	90 min	150 min
P2 - Médio	2 horas	6 horas	10 horas
P3 - Baixo	4 horas	12 horas	24 horas

6.4.2.1 Tempo máximo de percepção do incidente de segurança: é o limite contratual (SLA) que estabelece o tempo máximo aceitável para que a plataforma ou serviço correlacione a telemetria e identifique uma atividade maliciosa, medindo o intervalo entre a primeira evidência técnica do ataque no ambiente e a geração do alerta qualificado para os analistas. Essa métrica atua como o teto para o tempo de detecção (MTTD), visando minimizar a

permanência velada do atacante na rede (dwell time) e servindo como parâmetro objetivo de conformidade e aplicação de penalidades ao fornecedor.

6.4.2.2 Tempo máximo de resposta ao incidente de segurança: é o limite contratual de tempo (SLA) exigido para que, a partir do momento em que uma ameaça é detectada e qualificada, sejam executadas as medidas operacionais e automatizadas de contenção e mitigação interrompendo ativamente a progressão do ataque e minimizando o impacto no ambiente antes que a remediação definitiva seja concluída.

6.4.2.3 Tempo Máximo de Contenção: é o limite temporal estabelecido para que a equipe de analistas investigue, realize a triagem e confirme a veracidade de um alerta gerado pela plataforma, medindo o intervalo entre a emissão do alerta e a sua classificação definitiva como um incidente real (verdadeiro positivo) ou um alarme falso (falso positivo).

6.4.2.4 Todos os tempos serão contados a partir do início do incidente de segurança. O tempo de início é medido a partir do momento que há registros das atividades maliciosas ou a partir do momento que houver impacto resultante da atividade maliciosa - o que ocorrer primeiro.

6.4.2.4.1 Os tempos serão aferidos com base nos registros de data e hora do sistema de gestão de incidentes, correlacionados aos registros da plataforma, disponibilizados para auditoria.

6.4.2.5 Quando o atendimento de um incidente depender de providência a cargo do CONTRATANTE, a contagem do tempo para cumprimento do SLA será suspensa durante o período de efetiva dependência dessa providência, sendo retomada a partir de seu atendimento pelo CONTRATANTE.

6.4.2.5.1 A suspensão da contagem somente será admitida quando houver dependência objetiva de providência do CONTRATANTE, devidamente registrada pela CONTRATADA, com indicação da ação requerida, da data e hora do acionamento, das evidências correspondentes e da data e hora do atendimento da solicitação pelo CONTRATANTE. Não será admitida a suspensão retroativa da contagem.

6.4.2.5.2 Quando o período de suspensão ultrapassar o dobro do tempo máximo previsto para validação e houver mais de um acionamento do CONTRATANTE para a mesma finalidade, a justificativa para a duração da suspensão deverá ser formalmente

registrada e submetida à validação do CONTRATANTE. A suspensão somente será considerada válida se comprovada a efetiva necessidade do tempo utilizado para as validações, não sendo admitida sua utilização indevida para afastar ou reduzir a responsabilidade da CONTRATADA pelo cumprimento dos níveis de serviço estabelecidos.

6.4.2.5.3 Não serão incluídos na contagem de totais os incidentes abertos e fechados de forma automática. Em caso de um incidente fechado de forma automática se mostrar como verdadeiro-positivo, este será tratado como se houvesse descumprimento de SLA.

6.4.2.6 O descumprimento de qualquer um dos tempos descritos no item 6.4.2 será considerado como incidente de segurança não atendido no prazo.

6.4.2.7 O descumprimento dos níveis descritos implicará em glosa a ser aplicada sobre a parcela total mensal dos itens 7 e 8, conforme tabela a seguir:

6.4.2.7.1 Periodicidade de medição: Mensal

6.4.2.7.2 Fórmula: somatória ponderada dos incidentes que descumpriram o SLA dividido pela somatória ponderada de todos os chamados.

6.4.2.7.3 ICSLA = (QTin / Tin) * 100

6.4.2.7.4 ICSLA = Índice de Conformidade de SLA

6.4.2.7.5 QTin = Quantidade de incidentes de segurança atendidos nos prazos: $\Sigma_{\text{Incidentes com SLA cumprido}}$(P0 * peso P0 + P1 * peso P1 + P2 * peso P2 + P3 * peso P3)

6.4.2.7.6 Tin = Total de incidentes de segurança registrado: $\Sigma_{\text{incidentes}}$(P0 * peso P0 + P1 * peso P1 + P2*peso P2 + P3 * peso P3)

6.4.2.7.7 Apuração e Glosa:

Faixa	Níveis Alcançados	Glosa
1	ICSLA => 95%	Sem glosa
2	90% <= ICSLA < 95%	5%
3	85% <= ICSLA < 90%	10%
4	ICSLA < 85%	20%

6.4.2.8 Todo incidente do tipo P0 e P1 (crítico e alto) deverá ser comunicado por telefone, além do registro no sistema de tíquetes;

6.4.2.9 Para P0/P1, a CONTRATADA apresentará relatório com linha do tempo, vetor, MITRE ATT&CK quando aplicável, ativos afetados, evidências, causa-raiz/hipóteses, contenção, remediação, impacto, lições, recomendações, responsáveis e prazos.

6.4.2.10 A classificação A0–A4 aplica-se exclusivamente ao suporte técnico. P0–P3 aplica-se aos incidentes de segurança. Em sobreposição, prevalecerá a classificação de incidente de segurança.

6.5. Índice de disponibilidade

6.5.1 A disponibilidade mensal da solução será apurada com base nos registros da própria plataforma e, quando disponível, em mecanismo independente de monitoramento. A perda de coleta de dados, de telemetria ou de cobertura dos ativos monitorados deverá ser aferida por indicadores próprios.

6.5.2 O índice mensal de disponibilidade da solução deverá ser igual ou superior a 99,8%.

6.5.3 Caso o índice mensal de disponibilidade seja inferior a **99,8%**, será aplicada glosa no percentual correspondente a 10 vezes a diferença entre a disponibilidade medida no mês e a disponibilidade mínima contratada, sobre o valor mensal dos itens 7 e 8.

6.6. Deveres e Responsabilidades do Tribunal:

6.6.1 Proporcionar as facilidades indispensáveis à boa execução dos serviços.

6.6.2 Relatar, por escrito, com a devida comprovação, as eventuais irregularidades na prestação de serviços;

6.6.3 Sustar a execução de quaisquer trabalhos por estarem em desacordo com o especificado ou por qualquer outro motivo que caracterize a necessidade de tal medida;

6.6.4 Efetuar os pagamentos devidos.

6.7. Deveres e Responsabilidades da Contratada:

6.7.1 Indicar um preposto para o contrato, sendo este o interlocutor da contratada junto ao Tribunal para os assuntos relativos ao cumprimento das cláusulas contratuais e para participar de reuniões de acompanhamento, sempre que solicitado pelo CONTRATANTE

6.7.2 Responsabilizar-se técnica e administrativamente pelo objeto contratado, não sendo aceita, sob qualquer pretexto, a transferência de responsabilidade a

outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

6.7.3 Responder integralmente por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras combinações contratuais ou legais a que estiver sujeita.

6.7.4 Fornecer a seus empregados todos os instrumentos necessários à execução dos serviços.

6.7.5 Informar a relação dos empregados que prestarão serviços nas dependências deste Regional.

6.7.6 Responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez que estes não têm nenhum vínculo empregatício com o Tribunal.

6.7.7 Responder por valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional.

6.7.8 Garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que venham a ter acesso em razão dos serviços prestados, não podendo, sob qualquer pretexto, revelá-los, divulgá-los ou reproduzi-los, conforme o Termo de Compromisso com a Segurança da Informação (Anexo II).

6.7.9 Manter, durante toda a vigência do contrato, as condições de habilitação exigidas na contratação.

6.7.10 Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual.

6.7.11 Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária.

6.7.12 Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de Tecnologia da Informação e Comunicação (TIC).

6.8. Subcontratação:

6.8.1 É vedada a subcontratação do objeto contratual, não sendo considerada subcontratação a atuação do fabricante da solução nas atividades inerentes ao fornecimento, operação, manutenção, atualização e suporte técnico especializada da plataforma, permanecendo a contratada integralmente responsável pelo cumprimento das obrigações contratuais.

6.9. Consórcio:

6.9.1 Não será admitida a participação de empresas reunidas em consórcio, nos termos do art. 15 da Lei nº 14.133/2021, visando assegurar a execução integrada e coordenada do objeto e evitar a fragmentação das responsabilidades entre o fornecimento das subscrições de software e os serviços de implantação, treinamento, suporte, monitoramento, detecção, investigação e resposta a incidentes.

7 MODELO DE GESTÃO DO CONTRATO

7.1. Indicação da Equipe de Gestão e Fiscalização do Contrato:

Integrante	Titular	Substituto	Unidade
Gestor:	Carlos Costa Jordão	Charles Ferreira Falcao	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Técnico:	Maurício Antonioli Schmitz	Carlos Augusto Nantes de Castilho Rivilino	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Demandante:	Rodrigo Zarth	Mateus Both	Coordenadoria de Segurança da Informação e Proteção de Dados
Fiscal Administrativo:	Alberto Daniel Müller	Ricardo Krause Kurylenko	Coordenadoria de Gestão e Apoio à Governança de TIC

7.2. Procedimentos de Gestão e Fiscalização do Contrato:

7.2.1 O gestor do contrato ficará responsável por:

7.2.1.1 Organizar a reunião inicial;

7.2.1.2 Encaminhar alterações contratuais;

7.2.1.3 Controlar prazos e indicadores contratuais;

7.2.1.4 Atestar notas fiscais;

7.2.1.5 Tratar eventuais irregularidades constatadas na execução contratual;

7.2.1.6 Realizar o recebimento definitivo, emitindo o respectivo termo;

7.2.1.7 Verificar obrigações previstas no encerramento do contrato.

7.2.2 O Fiscal Administrativo do contrato ficará responsável por:

7.2.2.1 Participar da reunião inicial;

7.2.2.2 Conferir cumprimento de prazos contratuais;

7.2.2.3 Conferir o atendimento dos níveis de serviços contratados;

7.2.2.4 Conferir documentação exigida no contrato;

7.2.2.5 Verificar a conformidade do faturamento do objeto contratado;

7.2.2.6 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados;

7.2.3 O fiscal demandante do contrato ficará responsável por:

7.2.3.1 Participar da reunião inicial;

7.2.3.2 Acompanhar a execução do objeto de acordo com o contrato;

7.2.3.3 Monitorar cumprimento de prazos contratuais;

7.2.3.4 Encaminhar demandas para a contratada por meio de ordens de serviço e/ou chamados;

7.2.3.5 Aferir as entregas da execução em relação ao objeto contratado;

7.2.3.6 Atestar se os requisitos de negócio da contratação foram atendidos;

7.2.3.7 Informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

7.2.4 O fiscal técnico do contrato ficará responsável por:

7.2.4.1 Participar da reunião inicial;

7.2.4.2 Acompanhar a execução do objeto de acordo com o contrato;

7.2.4.3 Monitorar cumprimento de prazos contratuais;

7.2.4.4 Encaminhar demandas para a contratada por meio de ordens de serviço e/ou chamados;

7.2.4.5 Aferir as entregas da execução em relação ao objeto contratado;

7.2.4.6 Atestar se os requisitos técnicos da contratação foram atendidos;

7.2.4.7 Assinar o ateste de fiscalização do contrato, quando cabível;

7.2.4.8 informar ao gestor do contrato qualquer irregularidade na execução do objeto ou descumprimento dos níveis de serviços contratados.

7.3. Mecanismos Formais de Comunicação

7.3.1 Será realizada uma reunião inicial do contrato com a participação da contratada, do gestor e fiscais do contrato.

7.3.2 O mecanismo formal de comunicação utilizado no contrato será o e-mail, conforme detalhamento a seguir:

Assunto	E-mail
Envio de notas fiscais	Deve ser feito através do sistema SIGEO-JT
Informações sobre faturamento	sgti.contratos@trt4.jus.br
Informações técnicas	setic.csipd@trt4.jus.br

8 CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

8.1. O objeto será recebido da seguinte forma:

8.1.1.1 Provisoriamente, com verificação posterior da conformidade do objeto com os requisitos da contratação, e;

8.1.1.2 Definitivamente, após a verificação do atendimento dos requisitos da contratação.

8.2. Detalhamento dos Critérios de Medição e Pagamento

Item	Descrição	Forma de Recebimento	Prazo	Forma de pagamento
1	Entrega das subscrições de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
2	Entrega das subscrições de Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR)	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	Ateste na nota fiscal	mensal	Pagamento mensal dos tokens efetivamente consumidos
4	Disponibilização da ingestão de logs externos	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento anual após o recebimento definitivo do objeto
5	Realização do Treinamento	Ateste na nota fiscal	180 dias da assinatura do contrato	Pagamento único após a realização do treinamento
6	Conclusão do serviço de implantação	Termo de Recebimento Definitivo	60 dias da assinatura do contrato	Pagamento único após o recebimento definitivo do objeto

7 e 8	Prestação do serviço mensal de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Ateste na nota fiscal	mensal	Pagamento mensal após a realização do serviço

8.3. Os itens 1, 2 e 4 serão pagos em 3 (três) parcelas anuais, de igual valor, condicionadas à disponibilização anual das respectivas licenças e observados os seguintes marcos de pagamento: a primeira parcela será paga após a emissão do respectivo Termo de Recebimento Definitivo; a segunda, em até 12 (doze) meses após o pagamento da primeira; e a terceira, em até 12 (doze) meses após o pagamento da segunda. A segunda e a terceira parcelas são reajustáveis pelo ICTI (Índice de Custo de Tecnologia da Informação).

8.4. O item 3 será pago mensalmente com base nos registros de consumo disponibilizados pela própria solução, devendo a CONTRATADA apresentar a memória de cálculo juntamente com o relatório mensal de medição.

8.4.1 O faturamento ficará limitado ao consumo efetivamente registrado no período e ao quantitativo máximo contratado, sendo vedada a cobrança de tokens não utilizados.

8.5. O pagamento dos itens 7 e 8 será realizado mensalmente, após a execução dos serviços e entrega ao CONTRATANTE, pela CONTRATADA, dos resultados dos indicadores apurados.

8.6. A contratada deverá efetuar cadastro no Portal do SIGEO - JT para apresentação dos Documentos Fiscais (Notas Fiscais) com vistas à liquidação e pagamento das faturas.

8.6.1 Por meio do link https://sigeo.jt.jus.br/ajuda, a contratada terá acesso ao link do SIGEO – JT e a um guia detalhado das funcionalidades do sistema.

9 REAJUSTE CONTRATUAL

9.1. O reajuste contratual, quando cabível, será aplicado de acordo com o Índice de Custo da Tecnologia da Informação (ICTI), estabelecido no guia da Resolução 468 do CNJ.

10 ESTIMATIVA DO VALOR DA CONTRATAÇÃO

10.1. O valor total estimado para a contratação é de R$ 83.484.004,70

10.2. O detalhamento da pesquisa de preços realizada consta no Anexo III do Termo

de Referência.

11 ADEQUAÇÃO ORÇAMENTÁRIA

( ) Programa de Apreciação de Causas da Justiça do Trabalho;

( ) Manutenção do Sistema Nacional de TI

(x) Segurança da Informação nas Unidades do Poder Judiciário - SIUPJ

( ) Outra:

12 FORMA DE SELEÇÃO DO FORNECEDOR

Forma de Seleção
(x) Pregão Eletrônico
( ) Concorrência
( ) Dispensa de Licitação
( ) Outra:

Hipóteses para utilização do Sistema de Registro de Preços:
( ) Necessidade de contratações permanentes ou frequentes devido às características do objeto.
( ) É conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, por quantidade de horas de serviço ou em regime de tarefa.
(x) É conveniente para atendimento a mais de um órgão ou entidade.
( ) Não é possível definir previamente o quantitativo a ser demandado pela administração, devido à natureza do objeto.
Execução de obras e serviços de engenharia: ( ) Existência de projeto padronizado, sem complexidade técnica e operacional; ( ) Necessidade permanente ou frequente de obra ou serviço a ser contratado.
( ) Não será utilizado Sistema de Registro de Preços.
Deverá ser prevista no Edital a renovação dos quantitativos no caso de prorrogação da Ata de Registro de Preços? ( ) Sim (x) Não

Critério de Julgamento
( ) Menor preço por item
( ) Menor preço por grupo de itens
(x) Menor preço global
( ) Maior desconto
( ) Outro:

13 CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. Os critérios de habilitação jurídica, fiscal, social, trabalhista e econômico-financeira serão previstos no edital.

13.2. Os critérios de habilitação técnica a serem atendidos pelo fornecedor serão:

13.2.1 Qualificação técnico-profissional:

13.2.1.1 Pelo menos 3 (três) profissionais da equipe técnica da CONTRATADA, responsáveis pela sustentação da solução, deverão ter certificação oficial do fabricante da solução proposta de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (itens 1 a 4 da contratação). Não serão aceitos certificados de participação em cursos ou workshops.

13.2.1.2 Os profissionais da equipe técnica da CONTRATADA, responsáveis pela **detecção, notificação e investigação de ataques cibernéticos**, deverão possuir certificação em segurança ofensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

13.2.1.3 CompTIA PenTest+;

13.2.1.4 EC-Council Licensed Penetration Tester (LPT);

13.2.1.5 IACRB Certified Expert Penetration Tester (CEPT);

13.2.1.6 GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

13.2.1.7 GIAC Reverse Engineering Malware (GREM);

13.2.1.8 Offensive Security Certified Professional (OSCP);

13.2.1.9 Ethical Hacking Post Exploitation (EHPX);

13.2.1.10 Offensive Security Experienced Penetration Tester (OSEP);

13.2.1.11 Offensive Security Web Expert (OSWE);

13.2.1.12 Certified Red Team Expert (CRTE);

13.2.1.13 Offensive Security Certified Expert (OSCE);

13.2.1.14 Certified Ethical Hacker (CEH).

13.2.2 Os profissionais da equipe técnica da CONTRATADA, responsáveis pela **resposta a ataques cibernéticos**, deverão ter certificação em segurança defensiva, detendo, individualmente ou em conjunto, pelo menos 3 (três) das seguintes certificações, contabilizando no máximo 2 (dois) certificados por profissional:

13.2.2.1 Certified Information Security Manager (CISM);

13.2.2.2 GIAC Experienced Cybersecurity Specialist (GX-CS);

13.2.2.3 GIAC Reverse Engineering Malware (GREM);

13.2.2.4 Ethical Hacking Post Exploitation (EHPX);

13.2.2.5 CompTIA Security+;

13.2.2.6 CompTIA Advanced Security Practitioner;

13.2.2.7 EC-Council Security Analyst (ECSA);

13.2.2.8 Certified Information Systems Security Professional (CISSP);

13.2.2.9 CompTIA CYSA+ - Cybersecurity Analyst.

13.2.3 É de responsabilidade da CONTRATADA dimensionar a quantidade de profissionais para a adequada prestação dos serviços previstos e delimitados por esta especificação, principalmente no que se refere aos acordos de níveis de serviço e metas estabelecidas.

13.2.4 Os profissionais cuja documentação for apresentada pela licitante deverão ser alocados na execução dos serviços.

13.2.5 Excepcionalmente, a contratada poderá substituir o profissional para a execução dos serviços, desde que comprovadas as condições de qualificação exigidas, condicionadas à prévia avaliação dos requisitos de qualificação e aceite por parte do CONTRATANTE.

13.2.6 A CONTRATADA deverá promover, no prazo máximo de 3 (três) meses, a atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.

13.2.7 Até a data do início dos serviços, a contratada deverá comprovar que os profissionais que prestarão os serviços integram o quadro de pessoal permanente da contratada. A comprovação deverá ser feita mediante apresentação de:

13.2.7.1 Documento que comprove vínculo de emprego, ou

13.2.7.2 Documento que comprove ser o profissional sócio da empresa, ou

13.2.7.3 Contrato civil de prestação de serviços.

13.2.8 Qualificação técnico-operacional

13.2.8.1 A empresa a ser contratada deverá possuir experiência compatível com a complexidade da solução pretendida, mediante apresentação da documentação que segue:

13.2.8.1.1 Atestado(s) de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, no qual esteja expressa a aptidão do interessado no fornecimento, implantação e prestação de serviço gerenciado de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos do mesmo fabricante que ofertar na presente contratação, para uma quantidade mínima de 40% da quantidade prevista no item 1.

13.2.8.1.1.1 A organização emitente do atestado de capacidade técnica deverá ser usuária do objeto fornecido, não sendo aceitos atestados emitidos por quaisquer intermediários.

13.2.8.1.1.2 Alternativamente ao atestado de capacidade técnica, será aceita declaração emitida pelo fabricante da solução, atestando que a licitante possui capacidade técnica e operacional para fornecer e prestar os serviços de implantação e serviço gerenciado previstos no objeto.

13.2.8.1.2 Comprovação de conformidade do fabricante da solução ofertada com padrões internacionais de segurança em ambiente de nuvem mediante a apresentação de Relatório SOC 2 Type II.

14 SANÇÕES APLICÁVEIS

14.1. As sanções relativas a advertências, inexecução total ou parcial, impedimento de licitar e contratar e, se for o caso, declaração de inidoneidade serão previstas no edital;

14.2. Na hipótese de atraso na disponibilização das subscrições e serviços (itens 1, 2, 3, 4, 7 e 8) e na execução da implantação da solução (item 6), a contratada estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor da obrigação objeto do atraso, limitada a 10% (dez por cento) do respectivo valor.

14.3. Na hipótese de atraso na solução dos chamados de suporte técnico, a contratada estará sujeita a multa nos percentuais descritos a seguir, sobre o valor

mensal dos itens 7 e 8, limitada a 10% (dez por cento) do respectivo valor:

14.3.1 Severidade A0 (crítica): 1% (um por cento) por hora de atraso

14.3.2 Severidade A1 (alta): 0,5% (cinco décimos) por hora de atraso

14.3.3 Severidade A2 (média): 0,5% (cinco décimos) por dia útil de atraso

14.3.4 Severidade A3 (baixa): 0,2% (dois décimos) por dia útil de atraso

14.3.5 Severidade A4 (pesquisa): 0,1% (um décimo) por dia útil de atraso

14.4. Na hipótese de atraso na realização do treinamento (item 5), a contratada estará sujeita a multa diária de 0,5% (cinco décimos por cento) sobre o valor do item em atraso, limitada a 10% (dez por cento) do respectivo valor.

<table>
<tr><th colspan="2">APROVAÇÃO DO TERMO DE REFERÊNCIA</th></tr>
<tr><th colspan="2">Equipe de Planejamento da Contratação</th></tr>
<tr><td>Documento assinado digitalmente
CARLOS COSTA JORDÃO
Integrante Demandante</td><td>Documento assinado digitalmente
MAURÍCIO ANTONIOLI SCHMITZ
Integrante Técnico</td></tr>
<tr><td>Documento assinado digitalmente
GEOVANE DUTRA DE SOUZA
Integrante Administrativo da Secretaria de Administração</td><td>Documento assinado digitalmente
ALBERTO DANIEL MÜLLER
Integrante Administrativo da Secretaria-Geral de Tecnologia e Inovação / Requisitante</td></tr>
<tr><th colspan="2">Autoridade máxima da área de TIC / Subcomitê de TIC</th></tr>
<tr><td colspan="2">Documento assinado digitalmente
NATACHA MORAES DE OLIVEIRA
Coordenadora do Subcomitê de Tecnologia da Informação e Comunicações
Secretária-Geral de Tecnologia e Inovação</td></tr>
</table>

Anexo I

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1. Definições para fins desta especificação:

1.1. Define-se “Ativo monitorado” como sendo uma estação de trabalho, notebook, dispositivo móvel, servidor, container, firewall, ativo de rede ou qualquer equipamento similar ao listado que possua endereço IP próprio e distinto e que deverá ser monitorado pela solução proposta. Poderá ser físico ou virtual e poderá estar hospedado em ambiente local (on-premise) ou em nuvem.

1.1.1. Relativo a container, deverá ser contabilizado como “Ativo monitorado” o host que hospeda o(s) container(s), para efeito de subscrição.

1.1.2. As licenças para *container* estarão limitadas a 4% de todos ativos contratados.

1.2. Caso o ativo possua mais de um endereço IP, será contabilizado um único “Ativo monitorado” para efeito de subscrição.

1.3. Para os dados do ambiente do CONTRATANTE que serão coletados pela solução proposta, compreende-se as seguintes definições:

1.3.1. “Dados de logs”, “logs de evento” ou simplesmente “log”: informações produzidas sobre eventos ocorridos nos sistemas operacionais, aplicações, servidores, endpoints, ativos de rede ou outros componentes do ambiente computacional.

1.3.2. “Dados de telemetria”: informações produzidas pelos agentes a serem instalados nos ativos monitorados (quando a solução fizer uso de agentes).

1.3.3. “Dados de rede”: informações sobre o tráfego de rede.

1.4. Tokens: Unidades de consumo de Inteligência Artificial, utilizados em agentes inteligentes para automação de tarefas.

1.5. Usuários ativos: usuários que fazem uso dos recursos do Active Directory, pertencentes a uma organização ou restritos a uma ou mais OUs (Unidades Organizacionais) dentro da subárvore do Active Directory.

1.6. Define-se “Área de Armazenamento” como sendo a área disponibilizada por meio da solução contratada para armazenamento dos logs em ambiente SaaS, coletados pela solução.

1.7. Será utilizado a métrica de GB/dia (gigabytes por dia) para a ingestão de logs no SIEM da solução contratada, sendo que:

1.7.1. O volume de logs ingeridos no SIEM a partir dos demais módulos da solução do fabricante ofertadas na proposta não deverão ser contabilizados;

1.7.2. Serão contabilizados a ingestão de apenas fontes externas vindas de outros fabricantes, cuja cobrança será baseado no consumo

médio de GB/dia;

1.7.3. Caberá à CONTRATADA estimar e controlar o volume de logs de fontes externas ingeridos na solução, se desejar fazer uso deste recurso;

1.7.4. A ingestão de logs externos no volume de até 10 GB/dia será considerado isento de cobrança;

1.7.5. Considera-se o arredondamento bancário para as frações de GB/dia aferidos.

1.8. Os itens 2, 3 e 4 estão vinculados à contratação do item 1 e não podem ser contratados separadamente.

2. ITENS 1 a 4 – Requisitos mínimos da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

2.1. A solução contratada visa o monitoramento contínuo e ininterrupto dos ativos computacionais do CONTRATANTE (supramencionados como “Ativos monitorados”) por meio das etapas de, mas não se limitando à, coleta, processamento e correlação de logs de eventos, dados de telemetria e/ou de rede de tais ativos, com o objetivo de, após análise contextualizada das etapas mencionadas, identificar eventos suspeitos ou incomuns, direcionados ao CONTRATANTE e permitir ações de proteção de forma automatizada ou manual.

2.2. A solução deve possuir as características mínimas constantes nesta especificação, devendo ser constituída de softwares, licenças, subscrições e garantias, de tal forma que haja a total compatibilidade entre seus componentes.

2.3. A CONTRATADA deve prover, ao ambiente, soluções de segurança cibernética que permitam a visibilidade de logs, dados de telemetria, tráfego de rede e de informações correlatas, capazes de identificar eventos suspeitos ou incomuns que possam comprometer os serviços tecnológicos do CONTRATANTE, por meio da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.

2.4. Para a prestação desse serviço, deve ser utilizada uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, com capacidades de Coleta e Correlacionamento de Logs e Mecanismos de Detecção de Comportamento Anômalo de Usuários e Aplicações (UEBA – User and Entity Behavior Analytics). Neste caso, entende-se por “Aplicações” como sendo os softwares instalados nos ativos monitorados.

2.5. A solução permitirá monitorar em regime 24x7 (vinte e quatro horas por dia, sete dias por semana) eventos de segurança cibernética, identificando incidentes relativos a ataques, violações de conformidade e comportamento suspeito nas aplicações, rede e ativos computacionais do CONTRATANTE, compreendendo:

2.5.1. Analisar, classificar, categorizar, correlacionar e notificar os eventos e incidentes classificados como ameaças à segurança cibernética, ou que sejam

considerados relevantes de acordo com diretrizes estabelecidas pelo CONTRATANTE;

2.5.2. Registrar e comunicar os incidentes de segurança cibernética para o CONTRATANTE, com as respectivas recomendações para tratamento e mitigação das ameaças, conforme especificação técnica contida neste documento;

2.5.3. Elaborar procedimentos padronizados contendo as melhores práticas para tratamento e resposta dos incidentes confirmados, que serão posteriormente executados pelas equipes responsáveis do CONTRATANTE;

2.5.4. Registrar os incidentes no módulo de gestão de incidentes da solução ofertada, cujo acesso deverá estar disponível para o CONTRATANTE.

2.5.4.1. O módulo de gestão de incidentes deverá ser nativo da solução ofertada ou ser implementado por meio de ferramenta de ITSM (IT Service Management), complementar e integrado à solução ofertada. As funcionalidades do módulo ou da ferramenta devem conter os dados dos alertas, incidentes e chamados além de informações sobre SLA para acompanhamento do tratamento dos chamados.

2.5.4.1.1. O módulo ou ferramenta deve ser capaz de, minimamente:

2.5.4.1.1.1. Permitir a criação e acompanhamento de incidentes cibernéticos, de forma manual e automática, com no mínimo as seguintes características:

2.5.4.1.1.1.1. Sumário do incidente, incluindo título, sumário, detalhes, e a fonte geradora do incidente. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados e, opcionalmente, prioridade e analistas envolvidos;

2.5.4.1.1.1.2. Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;

2.5.4.1.1.1.3. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;

2.5.4.1.1.1.4. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;

2.5.4.1.1.1.5. Permitir inserir evidências coletadas de eventual análise forense de host e rede como um complemento da análise do incidente;

2.5.4.1.1.1.6. Permitir registrar ações de remediação que incluam contenção, erradicação, educação de usuários e melhorias no programa do SOC;

2.5.4.1.1.1.7. Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.

2.5.4.1.1.2. Permitir o recebimento de alertas de segurança, de forma automática, com no mínimo as seguintes características:

2.5.4.1.1.2.1. Nome do alerta, fonte geradora, prioridade, data de criação, data original do alerta, categoria, ação, tipo, nível de severidade, descrição, serviço afetado, e

detalhes do alerta;

2.5.4.1.1.2.2. Dados de origem e destino: IPs e portas; quando disponível, informações de contexto de negócio de cada dispositivo de origem e destino: domínios, endereços MAC, nomes dos dispositivos, tipos, unidades de negócio, geolocalização, índices de criticidade e conformidade e proprietários;

2.5.4.1.1.2.3. Capacidade de incluir arquivos anexos, de acordo com a necessidade de aprofundamento de detalhes dos alertas.

2.5.4.1.1.3. Gerar relatórios mensais do acordo de nível de serviço (SLA – Service Level Agreement).

2.5.4.1.1.3.1. Os relatórios gerados deverão ser encaminhados para o CONTRATANTE.

2.5.5. O módulo ou ferramenta de ITSM deverá estar licenciado para o CONTRATANTE, devendo ser hospedado em regime SaaS (Software as a Service) pela CONTRATADA, bem como deve estar protegida por autenticação do tipo MFA - Multi-Factor Authentication e acesso criptografado ponto a ponto.

2.6. A solução deve ser fornecida no modelo Software as a Service (SaaS) permitindo a instalação de múltiplos coletores e agentes on-premises e em nuvem, a fim de realizar a implantação distribuída da arquitetura.

2.6.1. Deve ter instância própria para cada CONTRATANTE, isto é, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

2.6.2. Todas as licenças e subscrições necessárias para o pleno funcionamento da solução deverão ser fornecidas pela CONTRATADA, conforme as quantidades e faixas discriminadas nesta especificação.

2.6.3. Coletores de logs: o software dos coletores de logs, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes eventualmente necessários para a coleta e centralização de logs de eventos e/ou dados de telemetria deverão ser fornecidos pela CONTRATADA;

2.6.4. O CONTRATANTE disponibilizará, no máximo, os seguintes recursos em ambiente virtual a serem usados pelos coletores de logs (os recursos podem ser distribuídos entre diversas máquinas virtuais - uma para cada coletor, se necessário):

2.6.4.1. 12 vCPUs;

2.6.4.2. 32Gb vRAM;

2.6.4.3. 200GB de espaço em disco.

2.6.5. Caso os recursos em ambiente virtual necessários para o pleno funcionamento da solução extrapolem os recursos disponibilizados pelo CONTRATANTE, a CONTRATADA deve demonstrar, por meio de documento técnico do fabricante e/ou de boas práticas, a necessidade de aumento dos recursos, que serão disponibilizados pelo CONTRATANTE conforme comprovação apresentada. Caso não haja comprovação, a critério do CONTRATANTE, a CONTRATADA deverá providenciar, sem custos adicionais

para o CONTRATANTE, a entrega da infraestrutura (total ou remanescente) e em conformidade com a estrutura computacional do CONTRATANTE.

2.6.6. Agentes: software de baixo consumo de processamento que é instalado nos ativos suportados para centralizar e monitorar os dados de segurança cibernética. O agente oferece visibilidade e detecção de ataques nos endpoints, coletando informações on-line do sistema, incluindo informações básicas de identificação de ativos, processos em execução, logs e outros dados de telemetria e as enviando de volta à solução para análise.

2.6.7. O console de gerência deve ser acessado via web, de forma segura (HTTPS) e deve possuir compatibilidade com, no mínimo, os seguintes navegadores:

2.6.7.1. Google Chrome;

2.6.7.2. Microsoft Edge

2.6.8. O console de gerência deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

2.6.8.1. Caso a solução seja composta por diversas ferramentas, a console de gerência principal deve permitir a visibilidade integrada e total do monitoramento, detecção, notificação, investigação e resposta aos ataques cibernéticos detectados e sendo tratados em todo o ambiente computacional.

2.6.8.2. As demais ferramentas podem estar hospedadas em ambiente provisionado pela CONTRATADA, sem custos adicionais para o CONTRATANTE.

2.6.8.3. Os ambientes utilizados pela solução, inclusive os do fabricante, devem estar localizados no Brasil ou em país que confira grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709/2018 (LGPD), assim entendido o país que possua legislação geral de proteção de dados pessoais de conteúdo equivalente à LGPD ou ao Regulamento (UE) 2016/679 (GDPR) e autoridade de controle independente com poderes de fiscalização e sanção.

2.6.8.4. É vedado utilizar dados, logs, telemetria, incidentes, prompts ou resultados para treinamento, ajuste ou desenvolvimento de modelos próprios ou de terceiros, salvo autorização expressa do CONTRATANTE. Subprocessadores deverão ser previamente informados.

2.6.9. O console de gerência deve possuir a capacidade de autenticação multifator (MFA - Multi-Factor Authentication).

2.7. A solução deve ser fornecida dimensionada para a quantidade de ativos a serem monitorados de forma a abranger o escopo completo de ativos do CONTRATANTE, conforme conceito apresentado nesta especificação técnica.

2.8. Armazenamento da totalidade da telemetria ingerida — endpoint, rede, nuvem e identidade — em camada de armazenamento quente (hot storage), com disponibilidade imediata para consulta e correlação por meio da linguagem de busca nativa da plataforma, sem necessidade de reidratação, restauração ou

processamento prévio, por período mínimo de 30 (trinta) dias;

2.8.1. As análises realizadas e alertas devem estar disponíveis de forma integral por pelo menos 90 dias.

2.8.2. Retenção de logs de auditoria da plataforma e de artefatos coletados pelos agentes por período mínimo de 180 (cento e oitenta) dias.

2.8.3. Os logs do SIEM deverão ser armazenados por 30 dias para correlação com os dados de telemetria.

2.8.4. Em caso de encerramento do contrato, substituição da solução ou mediante solicitação do CONTRATANTE durante o processo de transição, a CONTRATADA deverá permitir a exportação em lote de todos os logs, dados de telemetria, eventos e dados de rede do CONTRATANTE que ainda estejam armazenados na solução e abrangidos pelo período de retenção contratado, formato aberto, como xml, csv ou texto puro, podendo ser abertos e lidos em editores de texto sem a necessidade de softwares proprietários ou plugins.

2.8.5. A solução não deve possuir mecanismos que limitem ou onerem o CONTRATANTE com base na quantidade/volume de dados a serem exportados.

2.9. A solução deve possuir capacidade de monitorar e identificar o comportamento de usuários que representar ameaça (UEBA - User and Entity Behavior Analytics), em nível de ativos monitorados ou em nível de logs de eventos, do Microsoft Active Directory e do OpenLDAP, monitorando diferentes vetores de ataque, como:

2.9.1. Movimentação lateral com uso de credenciais locais de máquina;

2.9.2. Ataques de força bruta em contas locais de máquinas;

2.9.3. Usuários locais que tentam apagar arquivos de evento dos registros da máquina.

2.9.4. Adicionalmente, para ambientes com Microsoft Active Directory:

2.9.4.1. Movimentação lateral com uso de credenciais de domínio;

2.9.4.2. Ataques de força bruta em contas de domínio;

2.9.4.3. Usuários de domínio que tentem apagar arquivos de evento dos registros da máquina;

2.10. A solução deve permitir, para ambientes com Microsoft Active Directory, monitorar ações de todos os usuários, permitindo campanhas de caças a ameaças, auditoria e criação de alertas para usuários específicos.

2.11. A solução deve monitorar qualquer tipo de acesso de usuário:

2.11.1. Em máquinas com credenciais locais – monitoramento com uso de agente da própria solução;

2.11.2. Com credenciais do domínio – monitoramento do Microsoft Active Directory;

2.11.3. Ingress Authentication – como VPN, Google Workspace/Google Apps e Office 365;

2.11.3.1. Para autenticações vindas de fora do ambiente – Ingress Authentication – a solução deve identificar e correlacionar a informações da origem do acesso –

minimamente data, hora e IP.

2.12. A solução deve suportar IPv4 ou IPv4/IPv6.

2.13. Para detectar incidentes, a solução deverá implementar o recebimento e análise de logs, dados de telemetria e/ou de rede de, no mínimo:

2.13.1. Firewalls;

2.13.2. Web Application Firewalls;

2.13.3. IPS (Intrusion Prevention System) / IDS (Intrusion Detection System);

2.13.4. Web filtering;

2.13.5. Antivírus;

2.13.6. Microsoft Active Directory;

2.13.7. Open LDAP;

2.13.8. IAM (Identity and Access Management) / PAM (Privileged Access Management);

2.13.9. Servidores HTTP (HTTP Servers);

2.13.10. Balanceadores de Carga (Load Balancers);

2.13.11. DNS;

2.13.12. DHCP;

2.13.13. ELK Stack;

2.13.14. Sistemas Operacionais.

2.14. A solução que fizer uso de parsers para análise dos dados recebidos deve permitir a ingestão de fontes de eventos por meio de, no mínimo, o protocolo Syslog.

2.14.1. A solução deve permitir a leitura de logs e arquivos nos formatos CSV, XML, JSON e texto puro, de forma a permitir a inclusão de outras fontes de evento que não tenham conectores nativos.

2.14.2. A solução deve possuir módulo nativo (já incluso) para realização de parsers customizados.

2.14.2.1. A solução deve permitir utilização de expressões regulares (regex) nos parsers.

2.14.2.2. A solução deve prover identificação de eventos com erro de parsing e de eventos sem suporte de coleta.

2.15. A solução deve ter funcionalidade de coleta de eventos de auditoria de bancos de dados por meio de conectores nativos, coleta de logs, dados de telemetria e/ou de rede.

2.16. Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede.

2.17. A solução deve implementar a coleta e análise de diferentes fontes de eventos. A coleta deve ser realizada para logs, dados de telemetria e/ou de rede, devendo ser possível coletar e analisar eventos das seguintes soluções presentes atualmente de forma predominante no ambiente do CONTRATANTE:

2.17.1. De forma nativa (sem a necessidade de customização de parsers):

2.17.1.1. Checkpoint para proteção de perímetro (Firewall);

2.17.1.2. Fortinet FortiGate para proteção de perímetro (Firewall);
2.17.1.3. Forcepoint para proteção de perímetro (Firewall);
2.17.1.4. Microsoft Active Directory para serviços de diretório.
2.17.2. De forma nativa (sem a necessidade de customização de parsers) ou não:
2.17.2.1. Open LDAP para serviços de diretório;
2.17.2.2. OpenVPN;
2.17.2.3. Citrix;
2.17.2.4. RDP e RDPWeb;
2.17.2.5. Senha Segura para serviços de gerenciamento de acesso privilegiado;
2.17.2.6. Cyberark para serviços de gerenciamento de acesso privilegiado
2.17.2.7. Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;
2.17.2.8. Keycloak para gerenciamento de identidade e acesso;
2.17.2.9. midPoint para segurança de identidades (identity security);
2.17.2.10. ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);
2.17.2.11. Loqed;
2.17.2.12. Varonis;
2.17.2.13. IBM Spectrum Protect Plus para proteção de dados;
2.17.2.14. Kaspersky para proteção de endpoint;
2.17.2.15. Blackberry Cylance para proteção de endpoint.
2.17.2.16. Check Point Harmony para proteção de endpoint;
2.17.2.17. Tenable One para gerenciamento de exposição (exposure management platform);
2.17.2.18. Tenable.ep / Nessus para gerenciamento de vulnerabilidades;
2.17.2.19. Tenable.ad para proteção do Active Directory;
2.17.2.20. Trivy para varredura de vulnerabilidades;
2.17.2.21. VMware/vCenter para virtualização de máquinas;
2.17.2.22. VMware/Horizon para virtualização de estações de trabalho;
2.17.2.23. Hyper-V para virtualização de máquinas;
2.17.2.24. Ovirt para virtualização de máquinas;
2.17.2.25. Docker e Kubernetes;
2.17.2.26. Apache HTTP Server;
2.17.2.27. HAProxy;
2.17.2.28. Ingress;
2.17.2.29. Nginx;
2.17.2.30. Switches Cisco MDS;
2.17.2.31. Switches H3C;
2.17.2.32. Switches HP;
2.17.2.33. Switches Huawei;
2.17.2.34. Roteadores Cisco;
2.17.2.35. Roteadores Juniper;

2.17.2.36. Roteadores MikroTik;
2.17.2.37. Access Points Aruba;
2.17.2.38. Access Points Ruckus;
2.17.2.39. Controladoras Virtuais Aruba;
2.17.2.40. Bacula para serviços de backup;
2.17.2.41. Commvault (software de backup);
2.17.2.42. Veeam (software de backup);
2.17.2.43. Storage Huawei;
2.17.2.44. Storage IBM;
2.17.2.45. TSM Server IBM Spectrum Protect para serviços de backup;
2.17.2.46. Dell EMC Data Domain;
2.17.2.47. Dell EMC Isilon.

2.18. A solução deve ser capaz de coletar e processar fontes de eventos oriundas dos seguintes serviços de Cloud:

2.18.1. De forma nativa (sem a necessidade de customização de parsers):
2.18.1.1. AWS CloudTrail, via SQS ou API;
2.18.1.2. Google Cloud Platform, via API;
2.18.1.3. Google Workspace/Google Apps, via API;
2.18.1.4. Microsoft Office 365, via API.

2.19. A solução deve suportar e implementar a coleta e o processamento de fontes de eventos oriundas, no mínimo, dos seguintes sistemas operacionais. Para as soluções que fazem uso de agentes ou outro software externo/nativo do sistema operacional, eles devem ser compatíveis com as versões 32 e 64 bits dos sistemas operacionais (quanto existirem). Caso a solução não faça uso de agentes, os dados devem ser obtidos por meio da coleta do tráfego de rede.

2.19.1. De forma nativa (sem a necessidade de customização de parsers):
2.19.1.1. Windows 10;
2.19.1.2. Windows 11;
2.19.1.3. Windows Server 2016;
2.19.1.4. Windows Server 2019;
2.19.1.5. Windows Server 2022;
2.19.1.6. Windows Server 2025;
2.19.1.7. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;
2.19.1.8. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;
2.19.1.9. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;
2.19.1.10. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;
2.19.1.11. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;
2.19.1.12. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;
2.19.1.13. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;
2.19.1.14. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;
2.19.1.15. Amazon Linux;
2.19.1.16. Debian Linux;

2.19.1.17. Ubuntu Linux.

2.20. Para os itens 2.13, 2.17, 2.18 e 2.19, as listas de soluções são do tipo "não exaustivas", devendo ser considerada pela CONTRATADA, por meio de configuração da solução, a possibilidade de inclusão ou alteração de produtos em decorrência da evolução do parque tecnológico do CONTRATANTE.

2.20.1. A inclusão ou alteração de tecnologias pertencentes ao escopo ordinário será realizada sem custo adicional. Ampliações substanciais dependerão de formalização contratual.

2.21. A solução deve ser capaz de detectar comportamentos caracterizados como maliciosos de acordo com o MITRE ATT&CK Framework levando-se em consideração os dados recebidos dos ativos monitorados e gerados pelo coletor de tráfego de rede.

2.22. A solução deve cobrir detecções nativas de, ao menos, os grupos de atacantes categorizados pelo MITRE ATT&CK.

2.23. A solução deverá informar com qual técnica e tática do MITRE ATT&CK Framework o ataque está relacionado, além de possuir link direto para o site da organização.

2.24. A solução deve possuir de maneira nativa detecções de, no mínimo, os seguintes vetores de ataque:

2.24.1. Requisição a domínio suspeito;

2.24.2. Execução de processos suspeitos;

2.24.3. Requisição de dados de registro do sistema de nome de domínio (DNS);

2.24.4. Comunicação com servidores Command & Control;

2.24.5. Tentativa de desabilitar recursos de Sysmon;

2.24.6. Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;

2.24.7. Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;

2.24.8. Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;

2.24.9. Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;

2.24.10. Detecção de execução do Mimikatz e variações;

2.24.11. Detecção de processos que utilizam resultados do comando wget via Bash, Perl e Python;

2.24.12. Detecção de tentativas de criação de reverse shells para Command & Control.

2.25. A solução deve possuir a capacidade de identificar e monitorar o comportamento de atacantes baseados em IoC’s (Indicators of Compromise) do próprio fabricante e de terceiros (threat intelligence).

2.26. A solução deve possuir listas de terceiros com informações de IoC’s com, no mínimo, IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.27. A solução deve possuir a capacidade de integração e/ou ingestão de dados de outras ferramentas de threat intelligence, de maneira manual ou por API, importando arquivos com base CSV ou STIX (Structured Threat Information Expression), através de assinatura de feeds de inteligência de ameaças de terceiros, aceitando, no mínimo, os seguintes tipos: IPs, domínios, URLs e hashes da família SHA e, opcionalmente, MD5.

2.28. A solução deve disponibilizar informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações.

2.29. A solução deve possui Inteligência de ameaças própria, reconhecida no quadrante mágico "2026 Gartner® Magic Quadrant™ for Cyberthreat Intelligence Technologies" ou permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence)

2.30. A solução deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar na defesa proativa contra ameaças.

2.30.1. A solução deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e de terceiros para ajudar na identificação de ameaças.

2.30.2. Após análise dos relatórios de ameaças pela CONTRATADA, deverá ser feita uma investigação dentro do ambiente computacional do CONTRATANTE e registrado um incidente caso sejam identificadas atividades presentes nos relatórios.

2.30.3. Cada relatório deve possuir, no mínimo, informações como: região/país alvo, plataforma alvo e campanhas de ataques relacionadas aos dados do relatório.

2.31. Ter capacidade de Gerenciamento de Superfície de Ataque e Exposição de Ameaças (ASM):

2.31.1. Capacidade de realizar o mapeamento contínuo e sem necessidade de agentes adicionais de todos os ativos da organização expostos à internet pública (endereços IP, domínios, serviços, portas e recursos em nuvem), combinado com a identificação automatizada de ativos internos e não gerenciados (*Shadow IT*) realizada pela telemetria nativa da plataforma;

2.31.2. Funcionalidade de identificação automatizada e sem interrupção de vulnerabilidades conhecidas (CVEs), portas de alto risco expostas e configurações inadequadas de segurança em tempo real, dispensando o agendamento manual ou a execução de varreduras (*scans*) invasivas tradicionais;

2.31.3. Mapeamento e visualização gráfica automatizada das rotas potenciais de exploração, identificando de forma clara como um

invasor pode se aproveitar de uma exposição externa ou vulnerabilidade local para realizar movimentação lateral e comprometer sistemas e dados críticos (*crown jewels*);

2.31.4. Cálculo dinâmico do nível de risco das exposições identificadas, correlacionando pontuação CVSS, aplicabilidade técnica no ambiente, criticidade do ativo e dados de inteligência de ameaças em tempo real (existência de exploits ativos no mundo real) para ordenar as vulnerabilidades que exigem correção imediata;

2.31.5. Integração direta entre o módulo de exposição e os fluxos de automação nativos da própria plataforma (XDR/SOAR), permitindo o disparo de ações imediatas ou guiadas de mitigação (como isolamento de host, bloqueio de portas ou alteração de políticas) diretamente a partir da console central;

2.31.6. Disponibilização de painéis consolidados em tempo real com métricas de postura de segurança, histórico de redução da superfície de ataque, cálculo de tendência de risco e exportação de relatórios executivos para suporte a auditorias e conformidade;

2.32. O serviço deve gerar um relatório mensal que indique como corrigir os problemas que venham a ser encontrados.

2.33. A solução que fizer uso de agentes deve permitir sua instalação de forma “silenciosa” nos ativos a serem monitorados.

2.34. A solução deve possuir as funcionalidades de:

2.34.1. Monitoramento de comportamento (behavior monitor);

2.34.2. Controle de aplicação;

2.34.3. Monitoramento de eventos;

2.34.4. Auditoria de alterações no sistema;

2.34.5. Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.61.

2.34.6. Capacidade de fornecer proteção contra malware desconhecido sem exigir uma conexão com o console de gerenciamento ou com a Internet;

2.34.7. Capacidade de proteção contra malware sem a necessidade de assinaturas, utilizando padrões e/ou heurísticas;

2.35. A solução deve monitorar os ativos em tempo real, estando eles dentro ou fora do domínio.

2.36. Os agentes devem poder coexistir com outras soluções de proteção, como antivírus, instaladas nos ativos monitorados sem que gerem conflito nem incompatibilidade entre os softwares.

2.36.1. Serão aceitas apenas soluções de NGAV/EDR cujo motor primário de detecção e prevenção opere por meio de análise comportamental contínua de processos e aprendizado de máquina (Machine Learning), capaz de avaliar tanto o comportamento de execução de arquivos quanto de atividades em memória (*fileless*). A solução deverá ser capaz de detectar e bloquear ameaças mesmo

quando não houver assinatura, hash, indicador de comprometimento ou conhecimento prévio específico da ameaça;

2.36.2. Não serão aceitas soluções que possuam apenas mecanismos de detecção baseados em assinaturas, hashes, reputação ou indicadores de comprometimento previamente conhecidos. A existência de módulos baseados em assinaturas será aceita como camada complementar de proteção, desde que a solução também possua, de forma nativa e habilitada, mecanismos de análise comportamental e Machine Learning para detecção e prevenção de ameaças conhecidas e desconhecidas, mesmo que tais módulos possam ser desabilitados ou parametrizados nas configurações do produto para simular o uso exclusivo do motor comportamental.

2.36.3. O agente de proteção instalado no endpoint não deverá depender do download, a atualização ou a aplicação recorrente e periódica de arquivos de vacinas, definições de vírus ou hashes estáticos para a execução da proteção preventiva em tempo real;

2.36.4. Capacidade de fornecer proteção contra malware desconhecido sem exigir uma conexão com o console de gerenciamento ou com a Internet;

2.37. Os agentes devem executar de maneira que não haja impacto na performance ou disponibilidade dos ativos monitorados.

2.37.1. Durante a implantação será estabelecido *baseline* de CPU, memória, disco e rede; degradação superior aos limites acordados será não conformidade.

2.38. Os agentes e os coletores devem, em caso de desconexão com o console, manter as informações sendo coletadas a fim de serem enviadas quando a conexão for restabelecida.

2.39. Os agentes e coletores devem enviar os dados para o console de maneira:

2.39.1. Segura e criptografada;

2.39.2. Que não haja impacto na performance ou disponibilidade da rede do CONTRATANTE.

2.40. Os agentes e coletores, ao enviarem os dados para o console, não devem degradar o tráfego de saída da rede do CONTRATANTE.

2.41. A solução deve monitorar, no mínimo:

2.41.1. Força bruta no ativo (brute force – asset);

2.41.2. Força bruta em conta local (brute force – local account);

2.41.3. Detecção de evasão - Deleção de log de evento (detection evasion – event log deletion);

2.41.4. Detecção de evasão - Deleção de log de evento local (detection evasion – local event log deletion);

2.41.5. Correspondência de Threat Intel (endpoint threat intelligence match);

2.41.6. Exploração mitigada (exploit mitigated);

2.41.7. Hash sinalizado no ativo (flagged hash on asset) - a solução deve permitir cadastrar um hash qualquer para gerar um alerta quando for acessado no ativo;

2.41.8. Processo sinalizado no ativo (flagged process on asset);

2.41.9. Exploração de elevação de privilégio Kerberos (kerberos privilege elevation exploit);

2.41.10. Movimentação lateral com personificação de administrador local (lateral movement – local administrator impersonation);

2.41.11. Movimentação lateral com credenciais locais (lateral movement – local credentials);

2.41.12. Tentativa de escalação de privilégio em honey credential local (local honey credential privilege escalation attempt);

2.41.13. Hash malicioso no ativo (malicious hash on asset) - a solução deve gerar um alerta quando um hash já conhecido como malicioso é acessado no ativo;

2.41.14. Criação de nova conta de usuário local (new local user account created);

2.42. A solução deve ser capaz de fornecer uma listagem dos ativos sendo monitorados.

2.43. A solução deve ser capaz de fornecer uma listagem dos ativos que estejam se comunicando no ambiente computacional do CONTRATANTE e que não estejam sendo monitorados.

2.44. A solução deve ser capaz de identificar acessos a URLs maliciosas além das portas padrão 80 e 443.

2.44.1. A solução deverá permitir classificar alertas relacionados a URLs em exceção para redução de falsos-positivos.

2.45. A solução deve correlacionar logs e/ou dados de telemetria/de rede dos ativos monitorados para:

2.45.1. Identificar comportamentos anômalos que aconteçam localmente no ativo monitorado;

2.45.2. Identificar quais eventos devem gerar alertas;

2.45.3. A solução deverá permitir classificar alertas relacionados a usuários e ativos em exceção para redução de falsos-positivos.

2.46. O console de correlacionamento deve estar disponível no ambiente do próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução.

2.47. A solução deve fazer uso de inteligência de ameaças do fabricante para analisar e correlacionar os dados recebidos.

2.48. A solução deve detectar ameaças conhecidas usando casos de uso de detecção constantemente atualizados, e desconhecidas por meio de conjuntos de dados aprendidos.

2.49. A solução deve prover funcionalidade de detecção de padrões em eventos coletados:

2.49.1. A solução deve prover detecção de padrões de ataque em todas as suas fases, com base no modelo Cyber Kill Chain, MITRE ou NIST;

2.50. A solução deve permitir a criação de alertas customizados baseados em um comportamento específico ou em um contexto de combinação de eventos.

2.51. Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:

2.51.1. Crítico;

2.51.2. Alto;

2.51.3. Médio;

2.51.4. Baixo.

2.52. A solução deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento.

2.53. A solução deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque.

2.53.1. Essas informações podem ser disponibilizadas por interação humana após investigação.

2.54. A solução deve permitir a visualização da correlação entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque.

2.55. A solução deve permitir o encerramento remoto de processos ativos executados nas estações de trabalho e servidores sob sua gestão.

2.56. A solução deve ser capaz de isolar uma estação de trabalho, desconectando-a da rede e permitindo se comunicar exclusivamente com a central da solução.

2.56.1. A solução deve ser capaz de restaurar a conectividade da estação de trabalho com a rede.

2.57. A solução deve ser capaz de realizar as ações dos itens 2.55. e 2.56. sem a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente (caso a solução faça uso) não possa ser instalado com direitos administrativos.

2.58. A solução deve possuir a capacidade de monitorar a integridade de arquivos (FIM – File Integrity Monitoring) nos servidores monitorados.

2.58.1. Nativamente, para os seguintes formatos de arquivos, no mínimo:

2.58.1.1. .bat

2.58.1.2. .cfg

2.58.1.3. .conf

2.58.1.4. .config

2.58.1.5. .dll

2.58.1.6. .exe

2.58.1.7. .ini

2.58.1.8. .sys

2.58.2. A solução deve permitir a inclusão de novos formatos de arquivos diferentes dos nativos.

2.59. O serviço de segurança cibernética de Caças Ameaças (Threat Hunting) deve se fornecido pelo fabricante da solução, ou por meio de certificações oficiais do fabricante

para a equipe da CONTRATADA e com níveis mínimos de SLA de MDR/Threat Hunting validados ou auditados pelo fabricante;

2.60. A solução deve, junto com o monitoramento do tráfego de rede (ou por meio de agentes), implementar regras de detecção de intrusão para correlacionar e trazer as informações sobre possíveis anomalias e ataques no nível de rede.

2.60.1. A solução deve permitir a criação de regras e/ou fornecer um conjunto de regras pré definidas.

2.60.1.1. No caso da solução possuir regras pré-definidas, deve haver sua atualização periódica cobrindo as informações de novas ameaças.

2.61. A solução deve possuir funcionalidade de automação na resposta de incidentes com playbooks de resposta já funcionais, devendo suportar, no mínimo, a automação das seguintes tarefas:

2.61.1. Envio de e-mails.

2.61.2. Com a utilização de agentes (não deve haver a necessidade de fornecimento de credenciais de usuário administrativo, o que não significa que o agente não possa ser instalado com direitos administrativos) ou outro mecanismo que a solução utilize para a automação:

2.61.2.1. Isolamento de uma máquina – caso seja detectado uma ameaça ou comportamento anômalo em uma máquina, deve ser possível isolá-la da rede;

2.61.2.2. Encerrar um processo malicioso – caso o agente detecte algum processo malicioso na máquina, a solução deve ter a capacidade de finalizar esse processo;

2.61.3. Com integrações para as soluções nativas indicadas no item 2.17.1:

2.61.3.1. Alertas relacionados a usuários do Microsoft Active Directory – se um alerta for gerado associado a uma credencial de domínio, a solução deve desabilitar o usuário para conter a ameaça de maneira rápida;

2.61.3.2. Sugerir e/ou criar regras no firewall – se um alerta for gerado associado a uma consulta DNS a um domínio considerado malicioso, a solução deve possibilitar a criação de regras de bloqueio no firewall ou sugerir qual regra deve ser criada para tal.

2.61.4. A solução deve permitir que cada tarefa nos playbooks de resposta de incidentes possa ser configurada de forma a:

2.61.4.1. Ser totalmente automática;

2.61.4.2. Aguardar uma interação humana para ser realizada.

2.62. Em casos de identificação de uma ameaça, a solução deve ter a capacidade de bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional ou demais aplicações instaladas no ativo.

2.63. A solução deve conter regras pré-definidas para detecção de ransomware e as principais famílias deste tipo de malware.

2.64. A solução deve possuir módulo de investigação e detecção integrados.

2.65. A solução deve apresentar os alertas de ameaças consolidados e correlacionados para melhor investigação e resposta aos incidentes.

2.66. A solução deve permitir configuração de notificações por e-mail (SMTP) e Webhooks (do Google Workspaces, no mínimo) para envio de alertas e notificações.

2.66.1. As notificações podem ser nativas ou, caso necessário, serem desenvolvidas pela CONTRATADA, sem custo para o CONTRATANTE, para viabilizar sua integração.

2.67. A solução deve permitir que as detecções sejam correlacionadas com dados recebidos dos ativos monitorados.

2.68. A solução deve, através dos dados do alerta, permitir a criação de um incidente e vinculá-lo ao alerta, possibilitando a definição da gravidade do incidente com dados de gravidade da fonte do alerta.

2.69. A solução deve permitir visualizar uma lista de incidentes e suas descrições, solicitar enriquecimentos e executar ações sobre os incidentes.

2.70. A solução deve criar uma linha do tempo (timeline) do ataque detectado, incluindo as evidências sobre cada alerta gerado e informando qual ativo gerou aquela evidência.

2.70.1. A solução deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho.

2.71. A solução deve ser capaz de classificar a relevância dos eventos, minimamente, em “crítico”, “alto”, “médio” e “baixo”.

2.72. A solução deve permitir a alteração do status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma.

2.73. A solução deve permitir visualizar as atividades suspeitas de forma a sinalizar a causa raiz, seguindo as categorias do MITRE ATT&CK.

2.74. A solução deve permitir investigar os alertas gerados pelos modelos de detecção por meio de análise de impacto e análise de causa raiz.

2.74.1. Deve ser possível ativar ou desativar qualquer modelo de detecção.

2.74.2. A solução deverá possuir todos os módulos de detecção completamente licenciados, sem custo para o CONTRATANTE, independentemente da quantidade de modelos de detecção que venham a ser disponibilizados futuramente.

2.74.3. A solução deve permitir a análise automatizada de causa raiz de qualquer alerta, incluindo os alertas de rede, se os dados do endpoint estiverem disponíveis;

2.74.4. Visualização das cadeias de execução que levam a um alerta;

2.74.5. Visualização da cadeia de execução de eventos não envolvidos com alertas (Caça de ameaça - Threat Hunt);

2.74.6. Visualização de análise da linha do tempo para ver todas as ações e alertas em uma linha do tempo;

2.74.7. Consulta de indicadores de comprometimento (IoCs) e comportamentos de endpoint;

2.74.8. Para investigação em estações ou servidores deverá ser possível o registro

minimamente dos seguintes itens:

2.74.9. 1 Processo executado, incluindo datas e horários;

2.74.10. 2 Atividades realizadas em arquivos;

2.74.11. 3 Criação e encerramento de processos;

2.74.12. 4 Threads de processo;

2.74.13. 5 Protocolos de rede utilizados: solicitações DNS, conexão HTTP, desconexão HTTP;

2.74.14. 6 Estatísticas de rede: histórico de conexões realizadas e processos associados;

2.74.15. 7 Alterações em valores do registro;

2.74.16. 8 Sessões de usuários no sistema operacional.

2.75. A solução deve permitir a criação de listas de exceção de objetos para redução de falsos positivos.

2.76. A solução deve adicionar os logs, dados de telemetria e/ou de rede coletados/correlacionados aos incidentes/alertas detectados.

2.77. A solução deve permitir o registro de incidentes por demanda, sem a necessidade de a própria solução ter gerado um alerta.

2.78. A solução deve possibilitar que, para cada incidente gerado, um analista seja vinculado ao incidente e que ele possa criar anotações sobre como está a evolução da resposta deste incidente;

2.79. A solução deve permitir que incidentes possam ser fechados após atividades serem encerradas, permitir marcação como falsos positivos e, também, que possam ser reabertos.

2.80. A solução deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, indicando criticidade e níveis de prioridade.

2.80.1. A classificação quanto ao nível de criticidade deve ser baseada nas regras do MITRE.

2.81. A solução deve ter a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções.

2.82. A solução deve permitir realizar buscas e filtros de objetos para possibilitar pesquisas e análises avançadas.

2.83. A solução deve possibilitar a interação com cada um dos objetos relacionados ao evento para análise avançada e resposta.

2.83.1. Ao clicar em quaisquer dos objetos, a solução deve permitir a realização de buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

2.84. A solução deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar, categorizar e recuperar os resultados da pesquisa.

2.85. A solução deve permitir a realização de buscas através de strings parciais,

exatas, valores nulos, coringas (wildcards) e caracteres especiais.

2.86. A solução deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas.

2.87. A solução deve permitir a criação de dashboards e relatórios baseados em bibliotecas prontas ou, também, criar do zero.

2.87.1. Deve possuir dashboards pré-configurados e permitir sua customização ou mesmo a criação de novos para refletir necessidades específicas do CONTRATANTE.

2.87.2. Deve fornecer a possibilidade de criação de relatórios e dashboards para dados de todas as fontes de dados ingeridas (endpoints, rede, e-mail, nuvem, etc.), seja por meio de criação de consultas (queries) ou a partir de cliques com o mouse.

2.87.3. Deve possuir dashboards pré-configurados que permitam a visualização executiva dos principais incidentes e atividades no ambiente com base em usuários, aplicações acessadas e estações de trabalho/servidores.

2.87.4. Deve possuir, ao menos, 15 (quinze) dashboards em sua biblioteca, incluindo dashboards de fácil visualização de:

2.87.4.1. Alertas e incidentes mais frequentes;

2.87.4.2. Nível de risco do ambiente;

2.87.4.3. Relatório dos últimos 30 (trinta) dias da detecção de incidentes;

2.87.4.4. Top 10 (dez) ativos com incidentes;

2.87.4.5. Os ativos que mais sofreram incidentes em um determinado período;

2.87.4.6. Os usuários que mais sofreram incidentes em um determinado período;

2.87.4.7. Ativos e contas descobertas;

2.87.4.8. Ameaças descobertas e classificadas conforme a cadeia de ataque.

2.87.5. Deve permitir configuração de atualização do tempo de cada dashboard.

2.87.6. Deve permitir exportação dos relatórios para os seguintes formatos:

2.87.6.1. Planilha: CSV e/ou Excel;

2.87.6.2. Texto: HTML e/ou PDF.

2.88. A solução deve permitir o gerenciamento de usuários, funções e permissões.

2.89. A solução deve permitir a criação de usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações.

2.90. A solução deve permitir uma gestão de usuários, com recursos de permissionamento RBAC, onde usuários podem ser excluídos da console sem prejuízos à auditoria ou a funcionalidades.

2.91. A solução deve registrar todas as atividades efetuadas pelos seus usuários, permitindo auditoria das ações realizadas.

2.91.1. Registros de auditoria de usuários, administradores e componentes integrarão os dados do CONTRATANTE e serão exportáveis ao encerramento.

2.92. A solução deve disponibilizar APIs, com documentação e sem custo

adicional, para integração com outras soluções.

MONITORAMENTO DEEP/DARK WEB (MONITORAMENTO DE MARCA E AMEAÇAS GLOBAIS)

2.93. A CONTRATADA deverá realizar serviços de monitoramento de Deep/Dark Web por meio da solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos ofertada (nativamente ou por meio de solução complementar). Os serviços e a respectiva solução utilizada para a realização do monitoramento de Deep/Dark Web devem atender às seguintes especificações mínimas:

2.93.1. A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas ao CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis.

2.93.2. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 6 (seis) domínios DNS do CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.

2.93.3. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

2.93.4. A solução de monitoramento de Deep/Dark Web deve realizar buscas, no mínimo:

2.93.4.1. Na Darknet;

2.93.4.2. Em plataformas de compartilhamento de documentos;

2.93.4.3. Pelas seguintes categorias:

2.93.4.3.1. Por Bucket: Darknet TOR, Whois, Usenet, Leaks, Bot Logs, Wikileaks, Public Leaks, Dumpster, Sci-Hub;

2.93.4.3.2. Por Site Público: .com, .org, .net, .info, .eu.

2.93.4.3.3. Por Geolocalização.

2.93.5. A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos

2.93.5.1. Domínio DNS;

2.93.5.2. Endereço de e-mail;

2.93.5.3. IP e CIDR;

2.93.5.4. Número de telefone;

2.93.5.5. Número do cartão de crédito;

2.93.5.6. URL.

2.93.6. Deve detectar resultados de itens pesquisa duplicados, apresentando-os de forma consolidada, otimizando a busca por informações relevantes.

2.93.7. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 1 (um) ano.

2.93.8. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de

filtrar e classificar os resultados das buscas:

2.93.8.1. Com base na data ou no tempo de publicação das informações encontradas (antigas e novas);

2.93.8.2. Com base nos domínios, e-mails e URLs encontrados;

2.93.8.3. Com base nos resultados mais relevante, menos relevante, mais recente e mais antigo;

2.93.8.4. Com capacidade de combinar ou excluir termos de pesquisa a fim de encontrar com eficiência informações relevantes no banco de dados.

2.93.9. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de manter históricos de resultados de busca.

2.93.10. A solução de monitoramento de Deep/Dark Web deve contemplar os seguintes itens:

2.93.10.1. Monitoramento de atividades na Deep/Dark Web relacionadas às informações sobre domínios, URLs, IPs, hashes, credenciais, e-mails e informações sensíveis do CONTRATANTE.

2.93.10.2. Amplitude de rastreamento contemplando dados e informações disponibilizadas na Deep/Dark Web como:

2.93.10.2.1. Monitoramento das credenciais de funcionários em listas e bases de dados de credenciais vazadas na Deep/Dark Web, marketplaces, entre outros;

2.93.10.2.2. Monitoramento do Pastebin, incluindo posts deletados e outros sites, buscando por referências sobre a empresa, domínios ou endereços IP;

2.93.10.2.3. Monitoramento de documentos vazados ou roubados da empresa em páginas da Deep/Dark Web e fóruns hackers;

2.93.10.2.4. Monitoramento de referências aos sistemas em páginas da Deep/Dark Web e fóruns hackers, além de Threat Intelligence e listas de IoC's;

2.93.10.2.5. Busca de informações sobre redes sociais e plataformas de divulgação de vulnerabilidades vazadas na Deep/Dark Web.

2.93.10.3. Deve ser possível encontrar marketplaces, fóruns e agentes de ameaças;

2.93.10.4. Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web, até um total de 20 marcas, submarcas ou nomenclaturas;

2.93.10.5. Investigação de origens de vazamentos de, no mínimo:

2.93.10.5.1. Grupos de hackers;

2.93.10.5.2. Ameaças em fóruns;

2.93.10.5.3. Salas de chats reservadas;

2.93.10.5.4. Carteira de bitcoins e endereços;

2.93.10.5.5. Registros históricos.

2.93.10.6. As investigações deverão ser realizadas por uma equipe especializada à medida que informações monitoradas forem identificadas na Deep/Dark Web.

2.93.10.7. Geração e notificação de alertas acompanhados da enumeração das ameaças e riscos relacionados e ações de mitigação sugeridas.

2.93.11. A coleta e tratamento serão limitados à finalidade de segurança

cibernética, vedada utilização diversa e observados necessidade, segurança, prevenção e responsabilização.

2.94. A solução como um todo, bem como os seus componentes devem contar com garantia e suporte integrais conforme especificado neste documento.

2.95. O serviço de segurança cibernética de Caças Ameaças (Threat Hunting) deverá ser realizado através de análise humana e operar em caráter contínuo, regime 24 horas x 7 dias da semana, em busca de ameaças cibernéticas, anomalias, comportamentos suspeitos e ou maliciosos, análise e revisão da telemetria gerada pelos dispositivos e estratégias avançadas utilizadas por atores maliciosos, sem a dependência de alertas ou detecções. Ou seja, as atividades listadas devem ocorrer independente de alertas e detecções.

REQUISITOS PARA PROTEÇÃO DE IDENTIDADES

2.96. A solução deverá fornecer capacidades de Detecção e Resposta a Ameaças de Identidade (ITDR) integradas à plataforma XDR para ambientes Active Directory (on-premises) e Entra ID (nuvem), sendo capaz de avaliar continuamente vulnerabilidades e riscos em credenciais, detectar ataques em andamento (incluindo técnicas como Password Spray, DCSync, Pass-the-Hash e Skeleton Key), prevenir ou identificar movimentações laterais associadas ao uso indevido de protocolos de administração remota e investigar comportamentos anômalos nos fluxos e acessos de autenticação que envolvam os protocolos Kerberos e NTLM.

2.97. A solução deverá suportar a detecção e monitoramento de identidades não-humanas, incluindo contas de serviço, aplicações, APIs e identidades gerenciadas.

2.98. A ferramenta deverá analisar o comportamento de cada conta de usuário e conta de computador, além de estabelecer o perfil comportamental padrão dos acessos comuns, com o intuito de alertar ou bloquear condições anormais, utilizando técnicas de User and Entity Behavior Analytics (UEBA), incluindo técnicas de análise comportamental avançada, estatística e/ou aprendizado de máquina.

2.99. A solução deverá possuir capacidade de detecção baseada em anomalia de protocolo, identificando desvios em protocolos de autenticação e comunicação de diretório que não correspondam aos padrões documentados ou ao comportamento legítimo de sistemas operacionais homologados, independentemente da assinatura de um ataque específico.

2.100. A solução deverá identificar caminhos de ataque (attack paths) que permitam a elevação de privilégios ou comprometimento de ativos críticos a partir de identidades com menor privilégio.

2.101. A solução deverá permitir a execução de ações de contenção imediata diretamente a partir do console ou de seus componentes técnicos

(sensores/coletores), incluindo, no mínimo, mecanismos de invalidação de credenciais e sessões de autenticação, tanto em ambientes on-premises quanto em nuvem, de forma imediata e centralizada, devendo abranger credenciais Kerberos, tokens de autenticação e sessões ativas.

2.102. A solução deverá analisar configurações inadequadas, detalhar os riscos, o que deve ser feito para remediar, além de listar todas as identidades afetadas, incluindo minimamente:

2.103. Contas com SPN vulneráveis;

2.104. Utilização de protocolos vulneráveis como NTLMv1;

2.105. Contas configuradas para nunca expirar a senha;

2.106. Contas configuradas como uma política de senhas fraca;

2.107. Contas inativas;

2.108. Domain Controllers com o serviço Print Spooler em execução;

2.109. Caminhos onde contas regulares podem adotar para se tornarem contas privilegiadas.

2.110. Usuários com Account Lockout;

2.111. Alterações de senhas;

2.112. Alterações em contas;

2.113. Usuários desabilitados;

2.114. Usuários com senhas há muito tempo sem trocar;

2.115. Principais falhas de login;

2.116. Contas vulneráveis a Kerberoasting;

2.117. Contas vulneráveis a DCSync e Pass the Hash;

2.118. Informar se a conta KRBTGT precisa ser alterada para mitigar ataques como Golden Ticket;

2.119. Conta oculta identificada (contas que possuem configurações que impedem administradores de encontrá-las em buscas no serviço de diretório);

2.120. Identificação de permissões excessivas que possibilitem usuários comuns manipular políticas de acesso e autenticação de contas privilegiadas;

2.121. Identificar alterações no objeto AdminSDHolder;

2.122. Contas sincronizadas com o Entra ID que possuam privilégios excessivos ou MFA desabilitado;

2.123. A detecção de ameaças deverá ocorrer em tempo real ou próximo de tempo real e permitir que ações sejam tomadas para evitar que futuros ataques aconteçam, incluindo, mas não se limitando a ataques e técnicas, tais como:

2.124. Golden Ticket;

2.125. Suspicious Protocol Implementation (Pass the Hash);

2.126. NTLM Relay;

2.127. Suspicious LDAP Search (Kerberos Misconfiguration);

2.128. Suspicious LDAP search (Accounts);

2.129. DCSync;

2.130. Ataque DCSync com conta MSOL;

2.131. Ataques de DCShadow (replicação fraudulenta de objetos);
2.132. Forged PAC Attack;
2.133. Suspicious Kerberos Ticket Reuse;
2.134. Password Brute Force;
2.135. Credential Scanning;
2.136. Bronze Bit exploit;
2.137. CredSSP Vulnerability;
2.138. Skeleton Key Attack;
2.139. Pass-the-Ticket;
2.140. Overpass-the-Hash;
2.141. Token replay e abuso de tokens de autenticação;
2.142. Injeção de SID-History em contas de usuário;
2.143. Acesso incomum a um endpoint;
2.144. Acesso excessivo a múltiplos endpoints;
2.145. Atividade excessiva de acesso a múltiplos endpoints;
2.146. Acesso de um IP envolvido com outros incidentes ou qualificado como danoso pelo sistema de inteligência.
2.147. Administradores de Domínio com SPN;
2.148. Contas com senhas em branco;
2.149. Escalação de Privilégio via Grupo;
2.150. Atividades recentes vindas de contas dormentes;
2.151. Conta de computador - abuso de Serviços Kerberos para Usuário (S4U);
2.152. Para cada ataque identificado, a solução deverá minimamente fornecer as seguintes informações e possibilidades:
2.153. Data e hora da detecção;
2.154. Descrição do ataque;
2.155. Severidade;
2.156. Tática e técnica associada ao framework MITRE ATT&CK;
2.157. Conta comprometida;
2.158. Host de origem, de onde o ataque foi realizado;
2.159. Host de destino, quando o ataque está relacionado a uma movimentação lateral;
2.160. Recomendações com ações que devem ser realizadas para conter tal ataque;
2.161. Marcar o ataque como resolvido;
2.162. Marcar o ataque como falso positivo e não alertar ataques similares.
2.163. A solução deverá permitir a configuração de políticas de acesso para minimamente os seguintes cenários:
2.164. Em caso de detecção de um ataque pré-definido (como DCSync ou Pass the Hash), a solução deverá automaticamente adicionar a conta comprometida a uma lista de contenção; e, em seguida, bloquear ou restringir autenticações e sessões desta mesma conta, mediante aprovação manual ou configuração prévia

de políticas de automação baseadas em níveis de confiança, com o fim de interromper uma movimentação lateral;

2.165. Impedir a autenticação (Logon) de usuários incluídos em lista de contenção;

2.166. Alertar ou bloquear quando usuários privilegiados sejam utilizados em horários fora do normal (como fora do horário comercial).

2.167. A solução deverá fornecer capacidades de investigação de contas de usuários e acessos suspeitos, permitindo minimamente a visualização de:

2.168. Autenticações realizadas, incluindo sucesso e falha, com capacidade de filtragem por usuário, origem e destino;

2.169. Eventos de replicação de domínio, Account Lockout e acesso RPC;

2.170. Acessos realizados por contas de serviço e por contas com privilégios específicos (como Domain Admin);

2.171. Capacidade de listar em tempo real todas as sessões ativas de um usuário em múltiplos endpoints.

2.172. Deverá ser possível emitir relatórios para as funcionalidades de proteção de identidade minimamente dos seguintes indicadores:

2.173. Account Lockouts por endpoint;

2.174. Account Lockouts por usuário;

2.175. Uso de NTLM por usuário;

2.176. Uso de NTLM por endpoint;

2.177. Resumo de novos incidentes de segurança relacionados às identidades;

2.178. Top 10 incidentes por severidade;

2.179. Top 10 usuários com riscos significativos;

2.180. Usuários que nunca efetuaram Logon no domínio;

2.181. Administradores inativos;

2.182. Administradores com privilégios ocultos.

2.183. A solução deverá possuir capacidade de detectar, correlacionar, alertar e responder a ameaças relacionadas a autenticações e identidades em tempo real ou próximo de tempo real, utilizando mecanismos nativos, integrações ou ações automatizadas compatíveis com sua arquitetura.

2.184. A solução deverá permitir ações de contenção e resposta a incidentes relacionados a identidades, de forma automatizada ou manual, utilizando recursos nativos e/ou integração com plataformas de segurança, autenticação ou orquestração

2.185. As ações de bloqueio, restrição ou contenção de autenticação deverão ser executadas diretamente pela solução, não dependendo exclusivamente de integrações externas para sua efetivação.

2.185.1. As ações automatizadas serão classificadas como automáticas, dependentes de aprovação ou proibidas, conforme Matriz de Autonomia definida pelo CONTRATANTE.

2.186. A capacidade de detecção e resposta a ameaças de identidade deverá estar disponível de forma nativa, não dependendo da criação manual de regras ou correlações para identificação de ataques conhecidos.

2.187. A solução não deverá depender exclusivamente da instalação de agentes em endpoints para detecção de ameaças de identidade, devendo ser capaz de analisar autenticações diretamente a partir de controladores de domínio, serviços de diretório ou tráfego de autenticação.

2.188. A solução deverá prover visibilidade e proteção de identidades mesmo em sistemas que não suportam instalação de agentes, incluindo sistemas legados, dispositivos de rede e aplicações, por meio da análise de autenticações e credenciais.

2.189. A solução deverá apresentar encadeamento de eventos (timeline) permitindo a visualização da cadeia de ataque relacionada a uma identidade comprometida.

2.190. A solução deverá correlacionar eventos provenientes de múltiplas fontes, incluindo diretórios, autenticações, endpoints e sistemas integrados, para identificação de ataques complexos.

2.191. A solução deverá permitir o monitoramento e a rastreabilidade de alterações relacionadas a identidades, grupos e permissões no ambiente de diretório, incluindo registro e consulta de eventos associados.

2.192. A solução deverá fornecer evidências e contexto detalhado para cada detecção, permitindo a rastreabilidade e compreensão do motivo do alerta.

2.193. A solução deverá permitir a priorização de incidentes com base em risco agregado, considerando múltiplos fatores, como comportamento, exposição e criticidade da identidade.

2.194. A solução deverá identificar quando um usuário desativado tenta autenticar;

2.195. A solução deverá possuir capacidade de identificar comportamentos anômalos relacionados à autenticação e acesso às identidades, incluindo desvios de comportamento, padrões incomuns de acesso ou eventos suspeitos correlacionados;

2.196. A solução deverá identificar tentativas suspeitas relacionadas à autenticação NTLM, destacando comportamentos anômalos, como coleta de credenciais e volume incomum de autenticações em hosts de destino, permitindo a análise desses eventos em diferentes janelas de tempo, incluindo a última hora;

2.197. A solução deverá identificar quando um host procura se registrar como um novo controlador de domínio e alertar quando houver tráfego de sincronização de dados de um controlador de domínio legítimo;

2.198. A solução deverá identificar quando um usuário tenta se autenticar em um host via NTLM e não o fez nos últimos 30 dias;

2.199. Realizar Análise de Caminhos de Ataque, que é o mapeamento de como um invasor poderia realizar elevação de privilégio ou fazer movimentação lateral;

2.200. A solução deverá identificar comportamento que caracteriza uma quantidade excessiva de logins;

2.201. A solução deverá possuir módulo que seja capaz de identificar Brute Force em usuário e senha;

2.202. A solução deverá identificar contas de usuário que possuem permissões administrativas diretas (ACLs) em objetos do serviço de diretório, sem que estas contas pertençam formalmente a grupos de administradores;

2.203. A solução deverá fornecer uma pontuação de Risco por Usuário, calculado com base no comportamento e nas exposições da identidade, permitindo priorizar a investigação de contas com maior probabilidade de comprometimento;

2.204. A detecção de ameaças não deverá depender exclusivamente da ingestão de logs, devendo a solução ser capaz de identificar atividades maliciosas de forma independente, inclusive em cenários de evasão, como limpeza, manipulação ou ausência de logs. Todas as comunicações entre componentes da solução e os Controladores de Domínio devem priorizar o uso de protocolos seguros (como Kerberos ou LDAPS), evitando a utilização de protocolos legados sempre que tecnicamente possível (como NTLM).

2.205. A solução deverá funcionar em sua plenitude (com todos os recursos), sem depender de reboots nos Domain Controllers.

2.206. A solução deverá possuir capacidade de integração com ferramentas de segurança e infraestrutura, como SIEM, SOAR, EDR/XDR e soluções de gestão de identidade, por meio de APIs ou conectores nativos.

2.207. A solução deve possuir APIs documentadas para integração com ferramentas de orquestração (SOAR), permitindo que ações de contenção sejam disparadas de forma externa;

2.208. A solução deverá possuir mecanismos para identificação de tentativas suspeitas de enumeração, acesso indevido, movimentação lateral ou abuso de credenciais privilegiadas, podendo utilizar recursos nativos de detecção, análise comportamental, correlação ou tecnologias complementares;

MÓDULO DE SOAR AGÊNTICO

2.209. A solução deve dispor de agentes virtuais baseados em Inteligência Artificial integrados à solução capazes de interpretar alertas, formular hipóteses de investigação e tomar decisões de roteamento sem a necessidade de fluxogramas totalmente pré-configurados.

2.209.1. A utilização de IA não transfere à Administração responsabilidade pelas ações da plataforma. A CONTRATADA responderá pela operação, controles e rastreabilidade dos agentes.

2.210. O uso de módulo de SOAR agêntico consumirá *tokens* para execução de suas funções;

2.211. A CONTRATADA deve fornecer exemplos de cenários de uso de agentes inteligentes e seu consumo estimado de tokens;

2.212. Deverá existir alertas graduais (p. ex: 50%, 80%, 90%) o consumo e a possibilidade de bloqueios automáticos no uso da ferramenta a fim de evitar oneração imprevista acima do teto estabelecido pelo CONTRATANTE;

2.213. A quantidade de tokens contratados poderá ser utilizada durante todo o período contratual, sendo que o faturamento será sobre o número de tokens efetivamente consumidos dentro do mês e até o limite previamente estabelecido.

2.214. A solução deve operar de forma integrada combinando automações determinísticas (playbooks de regras fixas para execução previsível) e automações agênticas (IA adaptativa baseada em objetivos).

2.214.1. Alterações de playbook decorrentes de mecanismo agêntico deverão ser versionadas e registradas e observar a política de autorização antes de ações de alto impacto.

2.215. Capacidade de criar, implantar e gerenciar múltiplos agentes de IA autônomos e especializados (ex: Agente de Triagem, Agente de Investigação de Nuvem, Agente de Threat Hunting e Agente de Remediação).

2.216. Os agentes virtuais de inteligência artificial devem ser capazes de colaborar entre si, compartilhando contexto, dividindo tarefas complexas e orquestrando o fluxo de trabalho do incidente do início ao fim.

2.217. A solução deve permitir a criação automática de playbooks ou adaptação do fluxo de resposta em tempo real com base no raciocínio da IA, eliminando a dependência de manutenção de regras estáticas.

2.218. A solução deve permitir análise automatizada do alerta no momento de sua geração, atribuindo um índice de confiança (*confidence score*) e determinando se trata-se de um falso positivo ou uma ameaça real.

2.219. O agente deve ter capacidade de investigar árvores de processos, logs de chamadas de API em nuvem (ex: AWS, Azure, GCP), eventos de rede e telemetria de identidade de forma automatizada para correlacionar o ataque.

2.220. A solução deve permitir a identificação e mapeamento automático das táticas, técnicas e procedimentos (TTPs) utilizadas pelo atacante durante a investigação do incidente.

2.221. A solução deve permitir a geração automática de narrativas detalhadas e resumos executivos do incidente em Português (Brasil) ou Inglês, cobrindo causa-raiz, cronologia dos fatos, ativos e identidades impactadas.

2.221.1. Resultados automatizados de causa-raiz serão apresentados como hipótese, acompanhados das evidências, grau de confiança e validação do analista.

2.222. A solução deve prover interface conversacional de suporte ao analista que permite realizar perguntas operacionais e investigativas sobre o ambiente de segurança em linguagem natural em Português ou inglês;

2.223. A solução deve sugerir os próximos passos de mitigação e remediação mais adequados com base no contexto específico da infraestrutura.

2.224. A solução deve permitir mecanismos de governança para limitar o nível de autonomia que cada agente de IA possui sobre a infraestrutura.

2.225. A solução deve permitir a possibilidade de configurar travas operacionais obrigatórias para que ações de contenção/resposta de alto risco (ex: isolar servidor crítico, revogar acesso de usuário VIP) dependam de autorização prévia por um operador humano.

2.226. A solução deve dispor de mecanismos nativos de sanitização e proteção contra sequestro de objetivos (*goal hijacking*) e ataques de injeção de prompt manipulados por malwares ou atacantes.

2.227. A solução manterá registro auditável dos eventos, entradas relevantes, regras/políticas, agente, ação, resultado, data/hora e justificativa operacional, sem exigir exposição de raciocínio interno proprietário do modelo.

3. ITEM 5 – Requisitos mínimos de treinamento na solução

3.1. Deve ser realizado treinamento de administração e de operação da solução para até 10 (dez) profissionais da CONTRATANTE, contemplando, ao menos, os seguintes temas: instalação, configuração, operação e utilização da solução contratada.

3.1.1. O treinamento deve contemplar todos os recursos e configurações existentes na solução ofertada.

3.2. O treinamento deverá proporcionar aos participantes condições de:

3.2.1. Compreender a arquitetura da solução;

3.2.2. Identificar e configurar os recursos disponibilizados no produto;

3.2.3. Configurar fontes de eventos;

3.2.4. Instalar e configurar agentes, coletores e outros módulos necessários para o perfeito funcionamento da solução;

3.2.5. Configurar funcionalidade de deception, quando a solução tiver essa capacidade;

3.2.6. Configurar regras;

3.2.7. Configurar alertas;

3.2.8. Configurar playbooks;

3.2.9. Investigar incidentes;

3.2.10. Pesquisar em logs;

3.2.11. Criar dashboards;

3.2.12. Criar relatórios e agendamento de relatórios;

3.2.13. Gerenciar usuários, funções e permissões;

3.2.14. Identificar as possíveis causas de problemas e atuar na sua resolução;

3.2.15. Monitorar o funcionamento da solução (analisar mensagens de log, efetuar acesso remoto, atualizar os componentes que fazem parte da solução, administração e utilização dos recursos disponibilizados);

3.2.16. Conhecer os procedimentos para abertura de chamados técnicos;
3.2.17. Conhecer os procedimentos para obtenção de atualizações de software.

3.3. O treinamento deve ser oficial ou autorizado pelo fabricante da solução, devendo ser realizado na plataforma online do fabricante ou do centro autorizado de treinamento.
3.3.1. O conteúdo do treinamento poderá seguir o padrão de treinamento utilizado pelo fabricante para os módulos ofertados na solução, enquanto demais conteúdos que extrapolem o contexto padronizado do fabricante pode ser complementado pela CONTRATADA através de treinamento próprio.

3.4. O treinamento deve ser ministrado por pessoa certificada na solução.

3.5. A CONTRATADA deverá apresentar, juntamente à documentação técnica, a programação, conteúdo programático e carga horária do curso, a fim de serem ajustados às necessidades do CONTRATANTE.

3.6. É de responsabilidade da CONTRATADA todo material audiovisual, didático e eletrônico para a realização do treinamento.

3.7. O treinamento deve ter duração mínima de 40 horas.

3.8. O treinamento deverá ser ministrado em horário definido pelo CONTRATANTE, em dias úteis.
3.8.1. A critério da CONTRATANTE e havendo disponibilidade da CONTRATADA, o treinamento poderá ser realizado em meio-turno ou turno inteiro.

3.9. O treinamento deverá ser ministrado em língua portuguesa do Brasil.

3.10. O material escrito (PDF, apresentações, imagens etc) deverá ser fornecido, preferencialmente, em Português (Brasil). Em caso de não disponibilidade dessa versão, a mesma deverá ser disponibilizada em Inglês.

3.11. Deve ser realizado na modalidade telepresencial síncrona.

3.12. O prazo para execução do treinamento é de até 180 dias após a assinatura do contrato.

3.13. Deve fornecer, ao término, certificado de realização, em português do Brasil, para cada participante, contendo, no mínimo: nome do curso, carga horária, conteúdo programático, nome do instrutor e período de realização.

3.14. A CONTRATANTE poderá solicitar, sem custo adicional, a repetição total ou parcial do treinamento quando forem identificadas, mediante critérios objetivos de avaliação, falhas no cumprimento da carga horária, conteúdo programático, condições de realização ou requisitos mínimos estabelecidos neste Termo de Referência, devendo a CONTRATADA realizar a nova capacitação em prazo acordado entre as partes.

3.15. O treinamento será aceito após comprovação da carga horária, conteúdo, participação e entrega dos materiais.

4. ITEM 6 – Requisitos mínimos de implantação da solução

4.1. A fase de ativação dos serviços deverá ser conduzida e concluída nos primeiros 60 dias dias corridos contados a partir da assinatura do contrato, quando serão executados o

planejamento para implantação das ferramentas e a adequação de processos de gestão de segurança cibernética que nortearão a prestação de serviços do Centro de Operações de Segurança Cibernética (SOC).

4.1.1. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 60 dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

4.2. As atividades que propiciarão criar, alterar e manter controles de segurança cibernética, além de medir a eficiência e eficácia dos serviços de SOC quanto à sua utilização dentro do negócio, serão adequadas nesta fase de ativação do contrato, conforme parâmetros (baseline) a serem acordados entre as partes.

4.3. Os papéis e responsabilidades das partes nos processos de gestão de segurança cibernética, bem como indicadores necessários para medir e melhorá-los continuamente, serão definidos também com base nos referidos parâmetros (baseline).

4.4. As atividades de implantação e ativação do contrato poderão ocorrer de forma remota e deverão contemplar, no mínimo, as seguintes fases:

4.4.1. Planejamento e Projeto:

4.4.1.1. Reunião de kick-off;

4.4.1.2. Coleta de dados e requisitos complementares;

4.4.1.3. Detalhamento de cronograma;

4.4.1.4. Apresentação de parâmetros (baseline) e adequação de processos de gestão de segurança cibernética.

4.4.2. Implantação, Configuração e Ativação da solução:

4.4.2.1. Instalação e ativação da solução on-line e console de gerência;

4.4.2.2. Instalação e ativação dos agentes, coletores, console de gerência e demais componentes da solução (pertinentes aos ativos monitorados) no ambiente computacional do CONTRATANTE: servidores, estações de trabalho, firewalls, servidores de diretório e cloud;

4.4.2.3. Instalação e ativação dos coletores de logs;

4.4.2.4. Configuração e o correto funcionamento da coleta, processamento e correlação de logs de eventos em que a solução possua conectores nativos, ou seja, que não necessitem de customização de parsers para tal funcionamento (os conectores nativos devem contemplar a coleta, processamento e correlação de logs para os ambientes que constam nos itens 2.17.1, 2.18.1 e 2.19.1;

4.4.2.5. Testes e homologação.

4.4.3. Definição de Processos e Outras Configurações:

4.4.3.1. Implementação dos processos e recursos propostos;

4.4.3.2. Desenvolvimento de playbooks de resposta a ataques cibernéticos;
4.4.3.3. Configuração e correto funcionamento da coleta, processamento e correlação de logs de eventos em que haja a necessidade de customização de parsers para tal funcionamento (item 2.17.2).
4.4.3.4. Testes e homologação;
4.4.3.5. Desenvolvimento de um plano de continuidade que contemple minimamente a exportação de:
4.4.3.5.1. Base de incidentes em aberto (em tratamento);
4.4.3.5.2. Playbooks implementados.
4.4.4. Treinamento de equipes.
4.4.5. Operação, Sustentação e Melhoria Contínua:
4.4.5.1. Sustentação/On-Going;
4.4.5.2. Reunião mensal;
4.4.5.2.1. Relatórios periódicos;
4.4.5.2.2. Acompanhamento de indicadores;
4.4.5.2.3. Melhoria contínua.

4.5. A lista de soluções constantes nos itens 2.13, 2.17, 2.18 e 2.19 não é exaustiva, de forma que, conforme houver evolução do parque tecnológico ao longo do contrato, a CONTRATADA deve, como parte da operação, sustentação e melhoria contínua da solução, realizar a configuração para o correto funcionamento de parsing (quando houver), coleta, processamento e correlação de logs de eventos gerados pela novas soluções incluídas/alteradas no ambiente computacional.

5. ITENS 7 e 8 – Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

5.1. Para o item 7, considera-se que o valor trata-se de custo fixo mensal referente à construção da infraestrutura mínima necessária para atendimento aos requisitos do item presentes neste edital, considerando 2.000 ativos por mês monitorados;

5.2. O item 8 refere-se ao monitoramento de ativos além da quantidade basal prevista para o item 7. A unidade de medida será mensurada em múltiplos de 1.000 ativos monitorados por mês, proporcional à quantidade de ativos monitorados. Por exemplo: uma contratação de 3200 ativos do item 1, implicam em 1 unidade do item 7 e 2 unidades do item 8;

5.3. Os serviços deverão ser prestados por meio do Centro de Operações de Segurança Cibernética (SOC) da CONTRATADA, em regime 24x7x365, que deverá atender os seguintes requisitos mínimos:

5.3.1. A prestação dos serviços deverá ser feita a partir de Centro de Operações de Segurança Cibernética especializado, sendo remoto às instalações do CONTRATANTE.

5.3.2. A equipe do SOC poderá, a critério da CONTRATADA, ser compartilhada com outros clientes, incluindo outros Órgãos da Justiça do Trabalho, de modo a otimizar os esforços, respeitando a confidencialidade das informações relativas ao objeto deste edital.

5.3.3. A solução contratada deve ter instância própria para o CONTRATANTE, exclusiva e dedicada para cada Tribunal e sem compartilhamento com outros clientes da CONTRATADA.

5.3.4. A CONTRATADA deve indicar, formalmente, quando da assinatura do contrato, PREPOSTO TITULAR e substituto que tenham capacidade gerencial para tratar de todos os assuntos previstos no instrumento contratual e coordenação da equipe para a execução dos serviços contratados.

5.3.5. O PREPOSTO deve, entre outras atividades, promover os contatos com o gestor do contrato bem como deve prestar atendimento aos profissionais em serviço, tais como:

5.3.5.1. Assegurar de que as determinações do CONTRATANTE sejam disseminadas junto aos profissionais alocados com vistas à execução dos serviços contratados;

5.3.5.2. Informar ao gestor do contrato sobre problemas de qualquer natureza que possam impedir o bom andamento dos serviços contratados;

5.3.5.3. Desenvolver atividades administrativas de responsabilidade da CONTRATADA, principalmente quanto ao controle de informações relativas ao seu faturamento mensal e apresentação de documentos quando solicitado;

5.3.5.4. O PREPOSTO não pode ser contabilizado como profissional para execução dos serviços contratados.

5.3.6. Os serviços de operação e gestão da solução deverão ser fornecidos diretamente pela CONTRATADA com expressa autorização do fabricante da solução XDR para fornecer serviço de MDR (Managed Detection and Response).

5.3.7. O compartilhamento de profissionais não poderá comprometer capacidade, SLAs ou segregação lógica. A CONTRATADA manterá controles de acesso e menor privilégio.

5.3.8. A CONTRATADA deverá disponibilizar um canal de comunicação por telefone, celular ou 0800 com o serviço de SOC em regime 24x7;

5.4. A CONTRATADA deve possuir um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança – grupo de pessoas com a responsabilidade de identificar, receber, analisar e investigar as notificações e atividades relacionadas a incidentes de segurança cibernética nos ativos monitorados e orientar o CONTRATANTE quanto ao que deve ser feito para resolver o incidente de segurança cibernética.

5.5. Os incidentes de segurança cibernética são os relacionados aos eventos de segurança dos ativos monitorados como: ataques de movimentação lateral, escalação de privilégios, acessos indevidos, instalações de códigos maliciosos, ataques por força bruta, ou qualquer outra ação passível de monitoramento pela solução proposta e que possa comprometer a confidencialidade, disponibilidade, integridade ou privacidade das informações do CONTRATANTE.

5.6. Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação do CONTRATANTE, levando à perda de um ou mais princípios básicos de segurança cibernética: confidencialidade, integridade, disponibilidade ou privacidade.

5.7. O processo de notificação de incidentes de segurança se inicia sempre que um evento adverso for submetido por qualquer ferramenta de segurança, podendo o corpo técnico de segurança deste CONTRATANTE a qualquer momento, abrir um incidente de segurança junto à CONTRATADA.

5.8. O CONTRATANTE deverá ser informado sobre os incidentes detectados através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1).

5.9. As solicitações de serviços e as notificações de incidentes de segurança cibernética reportadas pela solução proposta ou pelo CONTRATANTE deverão ser registradas no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4).

5.10. Todo tipo de comunicação e documentação relacionados aos tratamentos de incidentes devem ser em Português.

OPERAÇÃO E SUSTENTAÇÃO

5.11. Os serviços de operação e sustentação da solução contemplam todas as atividades de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos identificados pela solução ofertada, bem como a sustentação da mesma, mediante a sua operação por parte da CONTRATADA.

5.12. Os seguintes serviços deverão ser realizados pela equipe da CONTRATADA para a operação da solução proposta:

- 5.12.1. Ativação e configuração dos módulos contratados;
- 5.12.2. Integração dos componentes contratados com o ambiente do CONTRATANTE;
- 5.12.3. Gestão do ciclo de vida da solução, contemplando a sua implantação e operação, além da inclusão, alteração e exclusão de ativos monitorados;
- 5.12.4. Abrir e fazer a triagem de chamados de segurança cibernética;
- 5.12.5. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;
- 5.12.6. Atender incidentes simples, os quais possuem instruções indicadas em playbooks (knowledge Base do ITSM);
- 5.12.7. Elaborar consultas(queries)/scripts de rastreamento quando

necessário e/ou solicitados pelo CONTRATANTE;

5.12.8. Elaborar manual de usuário das atividades que se fizerem necessários e/ou solicitados pelo CONTRATANTE;

5.12.9. IPs externos deverão ser analisados e contextualizados conforme sua criticidade;

5.12.10. Fazer passagem de turno, acompanhar os incidentes e realizar “follow-ups”, de modo que haja acompanhamento integral dos tickets abertos;

5.12.11. Prestar suporte/apoio ao processo de automação das atividades relacionadas à resposta e tratamento de incidentes cibernéticos;

5.12.12. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

5.12.13. Configuração de fontes de eventos;

5.12.14. Configuração de usuários VIP e usuários de serviço;

5.12.15. Criação de alertas customizados;

5.12.16. Configuração de coletores de eventos;

5.12.17. Configuração de monitoramento de arquivos e diretórios;

5.12.18. Liberação de acesso à solução para usuários autorizados pelo CONTRATANTE;

5.12.19. Geração de indicadores de performance (KPI) definidos neste documento e acordados na fase de Planejamento e Projeto (item 4.4.1);

5.12.20. Zelar e empregar todos os esforços necessários para garantir o atendimento ao SLA estabelecido neste edital, tanto que se refere aos serviços quanto às soluções contratadas;

5.12.21. Atualização da solução, quando necessário/aplicável e/ou solicitados pelo CONTRATANTE;

5.12.22. Resolução de chamados de suporte junto ao(s) fabricante(s) da solução.

5.13. A equipe da CONTRATADA deve ter, no mínimo, uma pessoa responsável pelos assuntos técnicos (líder técnico) e que será o ponto de contato com a equipe de segurança cibernética do CONTRATANTE. O líder técnico tem, entre outras responsabilidades:

5.13.1. Após a assinatura do contrato, conhecer o parque tecnológico e as atividades em andamento, visando à preparação da equipe que prestará os serviços, conhecer os modelos de serviços realizados, as normas internas, procedimentos de segurança e a definição dos requisitos necessários;

5.13.2. Fazer uma reunião semanal com a equipe do CONTRATANTE para acompanhamento dos resultados (a frequência da reunião poderá ser revista oportunamente, a critério do CONTRATANTE).

5.13.3. Fazer a entrega e apresentação dos relatórios mensais, conforme especificação técnica contida neste documento (item 5.17);

5.13.4. Esclarecer dúvidas em relação às requisições, alertas, incidentes, relatórios, prazos de atendimento e outras atividades de responsabilidade da equipe da CONTRATADA;

5.13.5. Estar disponível por telefone e e-mail, de segunda a sexta-feira, das 9 (nove) às 18 (dezoito) horas e acessível por contato telefônico em qualquer outro horário (incluindo sábados, domingos e feriados).

INTELIGÊNCIA DE AMEAÇAS

5.14. A equipe da CONTRATADA deve prover serviços de pesquisa e desenvolvimento de inteligência (threat intelligence) para proteção contra ataques cibernéticos, sendo responsável por:

5.14.1. Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela CONTRATADA;

5.14.2. Criar, em colaboração com a equipe de segurança cibernética do CONTRATANTE, casos de uso (regras) que devem ser implementados na solução fornecida;

5.14.3. Revisar, sempre que necessário e/ou solicitados pelo CONTRATANTE, as regras da solução fornecida, realizando as adaptações e evoluções necessárias;

5.14.4. Produzir e entregar informação de inteligência acionável, na forma de procedimentos para triagem de alertas e procedimentos para notificação de incidentes correspondentes às regras da solução ofertada;

5.15. A equipe da CONTRATADA deve fornecer serviço de Password e Credential Assessment (avaliação de credenciais em serviços de diretório e banco de dados):

5.15.1. A solução deve avaliar o nível de dificuldade de quebra de senhas.

5.15.2. A solução deve avaliar possíveis vazamentos de credenciais na Dark/Deep Web.

5.15.3. O serviço deve poder ser executado sob demanda.

5.15.4. O serviço deve ser executado sem que senhas sejam fornecidas.

MONITORAMENTO E DETECÇÃO DE AMEAÇAS E ATAQUES

5.16. A equipe da CONTRATADA deve atuar no monitoramento dos incidentes detectados pela solução e serviços propostos, sendo responsável por:

5.16.1. Monitorar equipamentos e softwares componentes das soluções de segurança do CONTRATANTE, envolvendo identificação, classificação e análise de eventos que possam comprometer a disponibilidade, integridade e confidencialidade dos serviços.

5.16.2. Focar suas ações nos eventos significativos, classificando-os corretamente conforme as categorias abaixo:

5.16.2.1. Informativos: são eventos que não requerem ação, utilizados para verificação de funcionalidades dos ativos monitorados, ou seja, tem por objetivo identificar se as ferramentas e soluções estão tendo o comportamento esperado. São úteis para gerar informações acerca do ambiente monitorado como, por exemplo, quantidade de eventos gerados nas últimas 24 (vinte e quatro) horas.

5.16.2.2. Avisos: são eventos utilizados para classificar comportamentos anômalos comparados à linha de base de operação do ambiente, porém que ainda não gerou impacto ao ambiente do CONTRATANTE como, por exemplo, espera-se que ocorram 10 bloqueios de um determinado hash diariamente e, entretanto, nos últimos 2 (dois) dias ocorreram 100 bloqueios, sendo que a ferramenta de antivírus continua bloqueando sem que haja qualquer impacto ou degradação no ambiente.

5.16.2.3. Exceções: são eventos que podem indicar que houve impacto em um ou mais dos pilares da segurança da informação (confidencialidade, integridade e disponibilidade) como, por exemplo, a ferramenta de antivírus não bloqueou a ação de um ransomware e dados do CONTRATANTE foram criptografados. Caso um evento seja classificado como "Exceção", o processo de resposta a incidentes de segurança deve ser iniciado imediatamente.

5.16.3. Comunicar, à equipe de segurança cibernética do CONTRATANTE, as informações iniciais sobre o incidente de segurança e quais serão as linhas de atuação para sua resolução.

5.16.4. Informar ao CONTRATANTE, através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto (item 4.4.1), sobre os incidentes detectados.

5.16.5. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações ao CONTRATANTE:

5.16.5.1. Alertas e notificações;

5.16.5.2. Quantidade de incidentes por categoria;

5.16.5.3. Quantidade de incidentes por criticidade (severidade);

5.16.5.4. Quantidade de incidentes que geraram crise;

5.16.5.5. Porcentagem dos incidentes originários do monitoramento;

5.16.5.6. Quantidade de incidentes tratados/fechados;

5.16.5.7. Quantidade de incidentes registrados.

5.16.6. Relativo ao monitoramento de Deep/Dark Web, a CONTRATADA deverá prover, no mínimo, os seguintes serviços:

5.16.6.1. Monitoramento e envio de notificações para a equipe técnica do CONTRATANTE contendo os alertas identificados no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

5.16.6.2. Serviço de investigação pela equipe técnica da CONTRATADA, contendo os alertas identificados e sugestões de mitigação, em regime 8x5 (oito horas por dia, cinco dias por semana);

5.16.6.3. Envio de um relatório ao fim do mês ao CONTRATANTE contendo, no mínimo, as informações a seguir:

5.16.6.3.1. Vazamento de dados do CONTRATANTE que foram encontrados na Deep/Dark Web, através do monitoramento de domínios, IPs, e e-mails.

5.16.6.3.2. Descrição do ambiente avaliado;

5.16.6.3.3. Tabela resumo de serviços descobertos, detecções e alertas;

5.16.6.3.4. Descrição detalhada dos alertas;

5.16.6.3.5. Descrição, evidências, screenshots relevantes e recomendações para mitigação dos riscos;

5.16.6.3.6. Testes executados e relatórios técnicos das ferramentas;

5.16.6.3.7. Apresentação técnica dos resultados, incluindo o detalhamento dos eventos identificados.

RESPOSTA E INVESTIGAÇÃO A INCIDENTES CIBERNÉTICOS

5.17. A equipe da CONTRATADA deve atuar no processo de resposta a incidentes detectados pela solução proposta, sendo responsável por:

5.17.1. Analisar, recomendar ações de remediação e contenção e documentar os eventos de segurança que, após analisados, demonstraram ser um ataque ao ambiente do CONTRATANTE, tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

5.17.2. Analisar, após um incidente de segurança ser aberto, os logs e artefatos enviados/coletados a fim de, no primeiro instante, identificar as fontes geradoras de tais eventos.

5.17.3. Identificar, uma vez realizadas as análises iniciais do incidente, quais foram os principais vetores de ataque ao ambiente do CONTRATANTE.

5.17.4. Definir, junto à equipe de segurança cibernética do CONTRATANTE, a severidade do incidente de segurança, que será obtida por meio de uma matriz GUT (Gravidade, Urgência e Tendência).

5.17.4.1. A matriz GUT será definida na fase de Planejamento e Projeto

(item 4.4.1) pela CONTRATADA em conjunto à equipe de segurança cibernética do CONTRATANTE.

5.17.5. Apoiar a equipe técnica do CONTRATANTE nos processos de mitigação, contenção de ataques e restauração do seu ambiente tecnológico.

5.17.6. Realizar, após análises iniciais do incidente e a definição de severidade, uma análise aprofundada do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

5.17.7. Documentar todo o processo de análise e resultado no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4) para que a equipe de segurança cibernética do CONTRATANTE acompanhe os passos para a solução do incidente de segurança.

5.17.8. Definir e documentar, uma vez identificado o comportamento e os principais vetores de ataque, uma estratégia para a mitigação e contenção do ataque em questão e notificá-la ao CONTRATANTE.

5.17.8.1. Qualquer tipo de alteração no parque computacional do CONTRATANTE para contenção e mitigação de incidentes de severidade alta ou crítica, deverá ser executada pelo próprio CONTRATANTE com o suporte da CONTRATADA, que deverá sugerir a melhor maneira de implantar a estratégia definida por ela para a resposta ao ataque, até a efetiva resolução do incidente.

5.17.9. Iniciar, mitigado o incidente de segurança, o processo de compilação de todas e quaisquer evidências e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo para execução de eventual análise forense do incidente de segurança.

5.17.9.1. A necessidade de análise forense será indicada pelo CONTRATANTE, seguindo os seus processos internos de gestão de incidentes de segurança, a serem apresentados na fase de Planejamento e Projeto (item 4.4.1).

5.17.9.2. Os dados coletados devem ser reunidos durante o processo de tratamento de incidente para subsidiar futura e eventual análise forense, seguindo as etapas de preservação, extração, análise e laudo. Tal análise deve ser realizada com o objetivo de identificar pessoas, locais ou eventos, correlacionando todas as informações reunidas e gerando como produto final um laudo sobre o incidente de segurança em questão.

5.17.10. Reconstruir o ataque, caso seja necessário e/ou solicitado pelo CONTRATANTE. Esta ação deve ser realizada pela CONTRATADA em ambiente controlado (como um sandbox), utilizando mecanismos

de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança cibernética.

5.17.11. Documentar, no módulo de gestão de incidentes de segurança da solução ofertada (item 2.5.4), as lições aprendidas do incidente de segurança em questão, formando, durante todo o período de vigência do contrato, uma grande base de conhecimento sobre ataques adversos.

5.17.11.1. A solução deve permitir a exportação da base de conhecimentos para formato Word ou PDF.

5.18. O regime de execução dos serviços deve ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano).

CONFIDENCIALIDADE E DESCARTE DE INFORMAÇÕES

5.19. Confidencialidade**:**

5.19.1. A CONTRATADA deve ser responsável pelo ciclo de vida das informações coletadas pela solução proposta, atendendo aos critérios definidos pelo CONTRATANTE, devendo processar, armazenar e, após o término da sua finalidade, descartar os dados de maneira segura.

5.19.1.1. A CONTRATADA obriga-se a tratar como “segredos comerciais e confidenciais” quaisquer informações, dados, processos, fórmulas, códigos, obtidos em consequência ou por necessidade desta contratação, utilizando-os apenas para as finalidades previstas no contrato, não podendo revelá-los ou facilitar a revelação a terceiros, mediante assinatura dos Termo de Compromisso com a Segurança da Informação (Anexo II);

5.19.2. Ao final do contrato, o descarte das informações deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte físico ou digital.

Anexo II

TERMO DE COMPROMISSO COM A SEGURANÇA DA INFORMAÇÃO

A empresa _____, parte CONTRATADA no contrato___/____, neste ato representado pelo(a) Sr.(a)_____, portador(a) da CI/RG n.º _____ e do CPF nº _____, compromete-se, por intermédio do presente termo, a não divulgar sem prévia autorização informações confidenciais pertencentes ou custodiadas pelo **TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO (TRT4)** às quais tiver acesso em decorrência da prestação do objeto do citado contrato, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA: Consideram-se informações confidenciais aquelas referentes a dados pessoais e dados pessoais sensíveis existentes no ambiente tecnológico ou físico do TRT4 ou por ele contratado, bases de dados, topologias, planos, políticas, processos, códigos-fonte, serviços e sistemas tecnológicos vinculados ao TRT4.

§ 1º Em relação aos dados pessoais e dados pessoais sensíveis do TRT4, a CONTRATADA deverá realizar o tratamento de acordo com o disposto nas cláusulas *de Proteção de Dados* do instrumento contratual.

§ 2º – Em caso de dúvida acerca da confidencialidade de determinada informação, a CONTRATADA deverá tratar a mesma sob sigilo até que venha a ser autorizada por escrito pelo TRT4 a tratá-la diferentemente. De forma alguma se interpretará o silêncio do TRT4 como a liberação do compromisso de manter o sigilo da informação.

§ 3º Excluem-se das disposições desta Cláusula informações que já estiverem comprovadamente disponíveis ao público em geral de qualquer forma que não em decorrência de sua revelação pela CONTRATADA.

CLÁUSULA SEGUNDA: A CONTRATADA concorda que as informações às quais terá acesso serão utilizadas exclusivamente no desempenho das atividades necessárias para execução do objeto contratado, em conformidade com o presente TERMO.

CLÁUSULA TERCEIRA: A CONTRATADA obriga-se a conhecer e observar a Política de Segurança da Informação disponível no site do TRT4.

CLÁUSULA QUARTA: A CONTRATADA compromete-se a aplicar boas práticas de mercado relacionadas à segurança da informação (como, por exemplo, ABNT NBR 27002:2022, CIS *Controls*, OWASP, NIST *Cybersecurity Framework*, dentre outras), pertinentes ao serviço prestado, para garantir a segurança do seu ambiente tecnológico de forma a atender os Acordos de Níveis de Serviços (ANS) e os Acordos de Nível Operacional (ANO) estabelecidos em contrato, bem como garantir a proteção da confidencialidade, integridade e disponibilidade das informações do TRT4 que vierem a ser tratadas em seu ambiente tecnológico.

CLÁUSULA QUINTA: A CONTRATADA determinará a todos os seus representantes - assim considerados, diretores, administradores, sócios, empregados, prepostos, agentes,

colaboradores e prestadores de serviço a qualquer título (incluindo consultores e assessores) que estejam, direta ou indiretamente, envolvidos com a prestação de serviços - a observância do presente Termo, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA SEXTA: Caso a CONTRATADA seja obrigada, em decorrência de intimação de autoridade judiciária ou fiscal, a revelar quaisquer informações, notificará por escrito ao TRT4, em até 24 horas, acerca da referida intimação, de forma a permitir que o TRT4 possa optar entre interpor a medida cabível contra a ordem judicial ou administrativa ou consentir, por escrito, com a referida revelação.

CLÁUSULA SÉTIMA: A CONTRATADA obriga-se a informar ao TRT4, em até 24 horas, qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

CLÁUSULA OITAVA: A CONTRATADA obriga-se a informar, em até 24 horas, ao TRT4 a ocorrência de incidentes, tecnológicos ou não, que possam comprometer (ou possam ter comprometido) a confidencialidade, integridade ou a disponibilidade das informações do TRT4 que são tratadas em seu ambiente tecnológico ou o cumprimento de ANS e ANO, bem como as medidas adotadas para contenção, tratamento, resposta e erradicação dos incidentes.

CLÁUSULA NONA: O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Porto Alegre, ___ de _____ de 20__.

_____

Assinatura do Representante Legal

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

versão janeiro/2026

MAURICIO ANTONIOLI SCHMITZ
23/10/2026 18:28

ALBERTO DANIEL MULLER
23/10/2026 21:41

CAROLINE ROCHA MOLINA
24/10/2026 12:37

Anexo III - FORMULÁRIO DE PESQUISA DE PREÇOS

Objeto:	Solução integrada de Detecção e Resposta Estendidas a ataques cibernéticos (XDR) e Detecção e Resposta a Ameaças de Identidade (ITDR), incluindo serviços de treinamento, implantação, operação, monitoramento e sustentação, pelo período de 36 meses.

Unidade Requisitante:	SGTI	**Responsável(is) pela pesquisa de preços:**	Maurício Antonioli Schmitz Alberto Daniel Müller

Observações:
1. A pesquisa de preços deve ser realizada de acordo com as recomendações do Guia de Pesquisa de Preços do TRT4.
2. Devem ser indicadas as páginas (folhas) que ratificam os preços lançados em cada uma das fontes utilizadas.
3. Não há necessidade de indicação do nome das fontes que originaram o valor estimado.
4. Na coluna “Metodologia de Cálculo”, deve ser indicada a metodologia utilizada para o valor estimado de cada um dos itens da contratação (média, mediana ou menor preço, etc).
5. A unidade requisitante poderá adaptar o presente formulário a sua necessidade, devendo atentar para a apresentação, no processo administrativo, em arquivo único, devidamente identificado.
6. O valor estimado (unitário e total) deve constar no Termo de Referência da contratação.
7. A data do orçamento estimado refere-se à data de análise das fontes de pesquisa, escolha da metodologia de cálculo e formação do valor total estimado da contratação.
8. O Código do Catálogo Comprasnet deve ser obtido no seguinte link: https://catalogo.compras.gov.br/cnbs-web/busca

PROAD n. 6891/2026 DOC 17. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.DGRH.LQWJ:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO

JUSTIÇA DO TRABALHO

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

VALORES ESTIMADOS PARA TODOS OS TRTs PARTICIPANTES:

							Fonte 01 (DOC. 4)	Fonte 02 (DOC. 5)	Fonte 03 (DOC. 6)	Fonte 4 (DOC. 7)	Fonte 5 (DOC. 8)	Fonte 6 (DOC. 9)	VALOR ESTIMADO		
Item	Descrição	CATMAT/ CATSERV	Classificação da Despesa	Unidade	Quantidade de compra inicial	Quantidade total do registro	Valor unitário	Valor unitário	Valor unitário	Valor unitário	Valor unitário	Valor unitário	Metodologia de cálculo	Valor unitário estimado	Valor total estimado
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses	27502	33904006 - Locação de software	Ativo monitorado	0	68.800	*1.836,00*	*541,74*	*755,43*	*1.049,00*	*1.227,72*	*1.320,00*	Média dos 2 menores valores	648,59	44.622.992,00
2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses	27502	33904006 - Locação de software	Usuários ativos	0	60.170	*216,59*	*154,17*	*101,96*	-	-	*975,00*	Média dos 2 menores valores	128,07	7.705.971,90
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	26972	33904000 Serviços de TIC - PJ	Tokens	0	834.300	*15,66*	*21,45*	*7,31*	-	-	-	Média dos 2 menores valores	11,49	9.586.107,00
4	Ingestão de logs externos - Franquia de Gigabyte por dia por 36 meses	26972	33904000 Serviços de TIC - PJ	Franquia de Gigabyte por dia	0	10.590	*12.511,80*	*930,49*	*6.680,00*	-	-	-	Menor valor	930,49	9.853.889,10
5	Serviço de treinamento na solução proposta	3840	33904020 Treinamento/capacitação em TIC	Serviço único, por turma de treinamento	0	23	*27.000,00*	*48.459,08*	*35.000,00*	*30.823,33*	-	*30.510,05*	Média dos 3 menores valores	29.444,46	677.222,58
6	Serviço de implantação da solução proposta	26972	33904000 Serviços de TIC - PJ	Serviço único por contratante	0	18	*32.400,00*	*254.864,77*	*54.500,00*	-	-	*63.588,87*	Média dos 2 menores valores	43.450,00	782.100,00
7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	25992	33904007 Manutenção corretiva/adaptativa e sustenção softwares	Serviço fixo para 2000 ativos monitorados por mês	0	18	*2.700,00*	*28.201,35*	*5.750,00*	*5.300,33*	*4.400,00*	*12.480,37*	Média, excluindo o menor e maior valor	6.982,68	4.524.776,64
8				Serviço para 1000 ativos adicionais monitorados por mês	0	39	*2.160,00*	*6.635,61*	*3.450,00*	-	-	-	Média	4.081,87	5.730.945,48
														VALOR TOTAL ESTIMADO COMPRA INICIAL	**R$ 0,00**
														VALOR TOTAL ESTIMADO REGISTRO	**R$ 83.484.004,70**
														DATA DO ORÇAMENTO ESTIMADO	**22/10/2023**
* Fonte 1: Os valores foram orçados em dólar, para comparativo de preços foi utilizado o dólar estimado pela empresa de R$ 5,40.															
* Fonte 5: no contrato o valor unitário do item 1 está para 30 meses, desta forma foi feito cálculo proporcional para 36 meses															
* Fonte 6: as subscrições são para 1 ano, desta forma foi multiplicado por 3 para completar os 36 meses.															

PODER JUDICIÁRIO

JUSTIÇA DO TRABALHO

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

VALORES ESTIMADOS PARA O TRT4:

Item	Descrição	CATMAT/ CATSERV	Classificação da Despesa	Unidade	Quantidade de compra inicial	Quantidade total do registro	Vlor unitário estimado	Total
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (XDR) pelo período de 36 meses	27502	33904006 - Locação de software	Ativo monitorado	0	6.500	648,59	4.215.835,00
2	Subscrição do Módulo de Detecção e Resposta a Ameaças de Identidade (ITDR) pelo período de 36 meses	27502	33904006 - Locação de software	Usuários ativos	0	4.500	128,07	576.315,00
3	Módulo de solução Agêntica para resposta, orquestração e triagem de eventos e incidentes	26972	33904000 Serviços de TIC - PJ	Tokens	0	72.000	11,49	827.280,00
4	Ingestão de logs externos - Franquia de Gigabyte por dia por 36 meses	26972	33904000 Serviços de TIC - PJ	Franquia de Gigabyte por dia	0	1.000	930,49	930.490,00
5	Serviço de treinamento na solução proposta	3840	33904020 Treinamento/capacitação em TIC	Serviço único, por turma de treinamento	0	1	29.444,46	29.444,46
6	Serviço de implantação da solução proposta	26972	33904000 Serviços de TIC - PJ	Serviço único por contratante	0	1	43.450,00	43.450,00
7	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	25992	33904007 Manutenção corretiva/adaptativa e sustenção softwares	Serviço fixo para 2000 ativos monitorados por mês	0	1	6.982,68	251.376,48
8				Serviço para 1000 ativos adicionais monitorados por mês	0	5	4.081,87	734.736,60
							VALOR TOTAL ESTIMADO COMPRA INICIAL	0,00
							VALOR TOTAL ESTIMADO REGISTRO	7.608.927,54

PROAD n. 6891/2026 DOC 17. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2026.DGRH.LQWJ:
https://proad.trt4.jus.br/proad/pages/consultadocumento.xhtml

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

Justificativa pela eventual não obtenção de 3 valores de mercado: [1]
Não se aplica

Justificativa pela eventual não utilização de painel de preços ou de contratos similares de outros órgãos na pesquisa de preços:
Não se aplica

Justificativa da escolha dos fornecedores que participaram da pesquisa de preços:
(x) Fornecedores que atuam no ramo empresarial relativo ao objeto da contratação;
( ) Fornecedores que mantém contrato vigente com o Tribunal;
( ) Fornecedores cadastrados no Tribunal e/ou que tenham fornecido no passado objeto similar;
( ) Fornecedores que venceram licitações de objetos similares em outros órgãos públicos;
( ) Outra:

[1] Neste campo, o requisitante deverá informar a situação que inviabilizou a obtenção de três orçamentos, mencionar as tentativas de consulta de preço empreendidas, informando os fornecedores contatados (nome e telefone) e anexando mensagens eletrônicas que tenha enviado, bem como demais documentos que entender relevantes para demonstrar tal fato, ou, ainda, informar acerca da inexistência de outros fornecedores para o objeto.