PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

KALINA LUCIA COSTA DO NASCIMENTO MELO
16/01/2024 11:13

Termo de Referência

Registro de Preços para contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, pelo período de 24 meses.

PROAD nº 9.605/2021

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

1 OBJETO

1.1 Descrição do Objeto

Registro de Preços para contratação de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, pelo período de 24 (vinte e quatro) meses.

2 FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1 Motivação da Contratação

O monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, bem como o gerenciamento de eventos e informações de segurança de TIC são essenciais para o rastreamento de atividades de usuários dos sistemas, sem o qual o uso abusivo (com desvio de finalidade) ou malicioso (malwares) de recursos computacionais tornam-se mais difíceis ou demorados para serem detectados e tratados.

Quando a Coordenadoria de Segurança de TIC foi instituída no TRT2, procurou-se estabelecer possíveis ferramentas que auxiliassem a equipe na visibilidade e tratamento de incidentes cibernéticos no parque computacional do Tribunal. Nesse ínterim, após várias reuniões com diferentes fornecedores, foi considerado que o custo de uma solução como essa seria muito elevado, para aquele momento, frente a maturidade da equipe, recém estabelecida, e que ainda angariava experiência na área de segurança da informação.

Dessa forma, optou-se pelo uso ferramentas de código aberto como ELK (Elasticsearch, Logstash e Kibana - três ferramentas comumente usadas em conjunto e que permitem extrair logs, visualizá-los e consultá-los), além da criação de scripts em shell Linux para alguns monitoramentos, onde a forma de alerta seria o envio de e-mails. No entanto, pelo tamanho reduzido da equipe, essa construção foi sendo realizada aos poucos e até hoje controles são implementados dessa maneira. Ao longo do tempo, apesar de ter trazido amadurecimento para a equipe, essa forma de realizar o monitoramento demonstrou-se precária, insuficiente e onerosa para a equipe. Dentre os pontos de atenção em relação ao modelo em uso, destacam-se:

- Dificuldade de se configurar a ferramenta para tratar os diversos tipos de fontes de dados que podem ser enviados;
- Complexidade para se criar correlacionamentos diversos, mesmo entre os registros de um mesmo tipo de fonte de dado;

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

- Não possui um conjunto mínimo de regras de detecção e de correlação, ou seja, todas devem ser criadas integralmente, quando possível;
- Não possui suporte nativo a uma série de ferramentas de apoio como: registro de incidentes, criação e automação de playbooks, inteligência de ameaças, entre outras;
- Não possui suporte técnico, ainda mais quando se trata dos scripts em shell Linux que foram desenvolvidos;
- Em um ambiente com muitos equipamentos e heterogêneo como é o do TRT2, muitas são as origens dos registros de auditoria, o que demanda tempo para a visualização, filtragem e correlacionamento de eventos que permitem detectar e analisar os usos abusivos ou maliciosos.

Mais recentemente, o CNJ estabeleceu a ENSEC-JT (Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário) onde se determina, entre seus diversos pontos de importância:

> *Art. 11. Para elevar o nível de segurança das infraestruturas críticas, deve-se:*
>
> *IV – utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança;*
>
> *V – utilizar tecnologia que permita a inteligência em ameaças cibernéticas em redes de informação; especialmente em fóruns, inclusive da iniciativa privada e comunidades virtuais da internet;*

Diante de oportunidade renovada, não só pela ENSEC-JT, mas também pelo estabelecimento de contratações nacionais por meio do Subcomitê Nacional de Segurança Cibernética do CSJT (SNSec), onde um “Serviço de Correlação de Logs de Segurança” ficou a cargo do TRT2, procurou-se restabelecer o contato com os fornecedores de SIEM. No entanto, durante a prospecção de mercado, levantou-se que a tecnologia avançou de SIEM para XDR (eXtended Detection and Response) e, desta forma, foram necessárias várias rodadas de reuniões com diversos fornecedores para que se estabelecesse um entendimento desse novo ferramental e que uma especificação fosse redigida de forma a, não somente haver a possibilidade de contratação de uma solução que atingisse as expectativas da Justiça do Trabalho, mas que também fosse possível de ser atendida pelo mercado.

Com a experiência obtida e diante ampla gama de especializações necessárias para o atingimento dos resultados esperados, também verificou-se que, além de uma ferramenta de

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

XDR, seria importante que um serviço de SOC (Centro de Operações de Segurança, do inglês Security Operation Center) fosse contratado de forma que, além de haver um monitoramento 24 horas por dia, 7 dias por semana, ele fosse feito por uma equipe de especialistas em cibersegurança, o que aumentou a complexidade da solução, exigindo, assim, um maior esforço na análise e consolidação dos requisitos.

Por conta dessa necessidade, o CSJT determinou a criação de um grupo de trabalho entre o TRT2 e membros do SNSec para a realização de uma análise mais criteriosa da especificação que havia sido redigida. Durante este trabalho houve a criação de um grupo no Google Space com a participação de outros Regionais e com o Tribunal Superior do Trabalho (TST), proporcionando a todos maior clareza da contratação que estava sendo efetuada, além de permitir que sugerissem alterações que julgassem importantes. Esse trabalho culminou em mais algumas reuniões, inclusive com novos fornecedores, que trouxeram ainda mais maturidade para o documento, permitindo a elaboração de uma especificação técnica completa e robusta, incluindo todas as necessidades levantadas por todos os Regionais e TST e permitindo a ampla competitividade entres os principais fornecedores do mercado que validaram as novas alterações propostas. Para permitir o levantamento de dados de dimensionamento (quantidade de ativos de cada Tribunal), foi aberto pelo CSJT o JIRA EGPTI-3212, onde todos os tribunais puderam se manifestar.

As atividades realizadas pelo grupo de trabalho permitiram o amadurecimento da compreensão de que por meio da implantação de uma solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, é possível prover ao ambiente computacional, 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 Tribunal, utilizando-se da coleta, processamento e correlação dos logs de eventos, dados de telemetria e/ou de rede dos ativos monitorados e do tráfego de rede.

Considerando que existe uma tendência preocupante para o cenário de segurança cibernética nas infraestruturas críticas e sistemas de informação governamentais, é imprescindível a disponibilização de serviço técnico especializado de monitoramento de ameaças cibernéticas em regime 24x7, com resposta a incidentes de segurança, de modo a minimizar os impactos de possíveis ocorrências de incidentes de segurança cibernética.

Nesse contexto, a consolidação do PJe vem proporcionando grandes avanços para a prestação jurisdicional da JT. Com o processo judicial existindo e tramitando exclusivamente no meio

eletrônico, além de vários outros sistemas utilizados, a tecnologia da informação passou a ser componente essencial para a continuidade dos serviços prestados pelo TRT2.

Aliado a isso, o cenário tecnológico atual coloca o Brasil como um dos principais alvos cibernéticos no mundo[1], tendo o governo como o principal alvo dos hackers[2]. Muitas notícias de ataques cibernéticos a órgãos governamentais foram veiculadas nos últimos anos, como o ataque ao STJ ocorrido em 2020[3], o ataque ao TRT-4 ocorrido em 2021[4] e o ataque ao TRT-17 ocorrido em 2022[5]. Pesquisas também apontam que os ataques de ransomware aumentaram 51% em um ano, colocando o país na primeira posição como sendo o mais atacado da América Latina[6]. Quando exitosos, estes ataques podem causar grande indisponibilidade nos sistemas computacionais, além de colocar em risco a integridade e o sigilo das informações armazenadas.

Considerando a tendência preocupante no cenário de segurança cibernética nas infraestruturas críticas e sistemas de informação governamentais, é fundamental a instituição de cenário seguro e compatível para defesa cibernética.

Reconhecendo este cenário, a implantação da solução proposta é congruente com as novas demandas de segurança da informação que enfrentamos atualmente, corroborada pela Resolução nº 396 de 07/06/2021 do CNJ.

2.2 Objetivos

A contratação de serviço técnico especializado de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, tem como objetivo o monitoramento contínuo e ininterrupto dos ativos computacionais a fim de prevenir tentativas de acesso não autorizados, bem como identificar eventos suspeitos ou incomuns relativos a ataques, violações de conformidade e comportamento suspeito que possam comprometer os serviços tecnológicos deste Regional e dos demais Tribunais coparticipantes da licitação. Com isso, espera-se também minimizar os impactos de uma possível ocorrência de grande magnitude.

[1] https://www.cnnbrasil.com.br/tecnologia/por-que-o-brasil-e-um-dos-principais-alvos-de-ataques-ciberneticos-do-mundo/
[2] https://canaltech.com.br/seguranca/governo-e-o-principal-alvo-de-ataques-ciberneticos-no-brasil-revela-analise-189050/
[3] https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml
[4] https://www.trt4.jus.br/portais/trt4/modulos/noticias/474900
[5] https://g1.globo.com/es/espirito-santo/noticia/2022/02/21/tribunal-regional-do-trabalho-do-es-sofre-ataque-cibernetico.ghtml
[6] https://www.cisoadvisor.com.br/maioria-das-empresas-que-usam-rdp-estao-expostas-a-ransomware/

2.3 Benefícios

O resultado pretendido é a contratação de uma solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, com suporte e treinamento, no qual permitirá a atuação das equipes técnicas da SETIC de forma rápida e ágil frente aos diversos tipos de incidentes cibernéticos, tais como uso indevido de recursos computacionais, infecção de malwares, ransomwares, execução remota de código, entre outros, evitando ou minimizando os prejuízos ao Tribunal e aos magistrados, servidores e jurisdicionados.

2.4 Alinhamento

Esta solução encontra-se alinhada com os seguintes objetivos:

PEI (Plano Estratégico Institucional) - 2021-2026:

- Objetivo 10: Aprimorar a Governança de TIC e a proteção de dados;

Também está de acordo com a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ):

- Art. 6º São objetivos da ENSEC-PJ:

  II – aumentar a resiliência às ameaças cibernéticas;

- Art. 9º São ações da ENSEC-PJ:

  I – fortalecer as ações de governança cibernética;

  II – elevar o nível de segurança das infraestruturas críticas.

E de acordo com a Estratégia Nacional de Tecnologia de Informação e Comunicação do Poder Judiciário (ENTIC-JUD):

- Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados.

2.5 Referência aos Estudos Preliminares

Este Termo de Referência baseia-se nos estudos preliminares constantes do processo PROAD nº 9.605/2021.

2.6 Impactos Diretos e Indiretos da Contratação

Na medida do necessário, serão disponibilizados recursos humanos da Coordenadoria de Segurança de TIC da SETIC para apoio durante a implantação da solução. Além disso será necessário também alocar um grupo de servidores para a realização dos treinamentos e administração da solução.

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2.7 Relação entre a Demanda Prevista e a Quantidade

A contratação de empresa especializada em prestação de serviço de SOC (Centro de Operações de Segurança) com solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, com implantação, suporte e treinamento para o TRT da 2ª Região e demais Regionais coparticipantes da contratação pelo período de 24 (vinte e quatro) meses, atende a demanda prevista atualmente.

2.8 Análise de Mercado

Para obtenção de uma estimativa atualizada de custos no mercado, foram contatadas, com o objetivo de garantir uma ampla pesquisa de mercado, as seguintes empresas prestadoras dos serviços: Blue Eye, BRLink/Ingram Micro, Cisco, Claro, Compwire, Crowdstrike, EverCo, Fast Help, Future, Hillstone, Innovatex, Intelliway, ISH, IT Protect, Lanlink, LCM Consulting/FastHelp, Leadcomm, LTA-RH, MW Microware, Network Secure, NTSec, Oakmont, Petacorp, Sencinet, Service IT, Suporte Informática, Tecno-IT, Teletex e Viwsec, das quais, até o momento, enviaram propostas as empresas Intelliway, Petacorp, Service IT, Suporte Informática e Network Secure, conforme orçamentos anexos e demonstrativos abaixo. Para a escolha das empresas a serem consultadas para solicitação de propostas, foram consideradas as que participaram em outras contratações públicas similares, como a realizada pelo TRT da 17ª Região, potenciais fornecedores contatados em eventos de tecnologia da informação como o ENASTIC-JT, bem como aqueles consultados durante a fase de prospecção de mercado de outros projetos de TIC. Por se tratar de um projeto conduzido em nível nacional, o TRT2 recebeu diversos contatos de empresas interessadas em participar, indicadas por outros Tribunais, e que também foram consultadas durante a elaboração dos estudos para validação das especificações técnicas e para o envio de propostas comerciais.

Proposta Comercial - Intelliway

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 249,14	R$ 247.645,16	R$ 495.290,32
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 242,10	R$ 3.675.562,20	R$ 7.351.124,40
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 227,01	R$ 6.422.566,92	R$ 12.845.133,84
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 222,39	R$ 6.885.194,40	R$ 13.770.388,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 216,22	R$ 2.345.122,12	R$ 4.690.244,24

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 0,00	R$ 0,00	R$ 0,00
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 0,00	R$ 0,00	R$ 0,00
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 31.156,36	R$ 1.246.254,40	R$ 1.246.254,40
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 81.282,92	R$ 2.032.073,00	R$ 2.032.073,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 53.431,30	R$ 641.175,60	R$ 1.282.351,20
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 74.051,19	R$ 8.886.142,80	R$ 17.772.285,60
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 109.809,60	R$ 10.541.721,60	R$ 21.083.443,20
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 157.758,30	R$ 9.465.498,00	R$ 18.930.996,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 172.566,00	R$ 2.070.792,00	R$ 4.141.584,00
							Valor Total	R$ 105.641.169,00

Proposta Comercial - Petacorp

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 469,12	R$ 466.305,28	R$ 932.610,56
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 399,41	R$ 6.063.842,62	R$ 12.127.685,24
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 364,32	R$ 10.307.341,44	R$ 20.614.682,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 382,61	R$ 11.845.605,60	R$ 23.691.211,20

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 359,65	R$ 3.900.763,90	R$ 7.801.527,80
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 190.638,93	R$ 20.779.643,37	R$ 41.559.286,74
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 300.638,93	R$ 1.803.833,58	R$ 3.607.667,16
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 50.000,00	R$ 2.000.000,00	R$ 2.000.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 180.000,00	R$ 4.500.000,00	R$ 4.500.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 28.500,00	R$ 342.000,00	R$ 684.000,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 39.000,00	R$ 4.680.000,00	R$ 9.360.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 48.000,00	R$ 4.608.000,00	R$ 9.216.000,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 63.000,00	R$ 3.780.000,00	R$ 7.560.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 70.000,00	R$ 840.000,00	R$ 1.680.000,00
							Valor Total	**R$ 145.334.671,58**

Proposta Comercial - Service IT

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 477,32	R$ 474.456,08	R$ 948.912,16
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 409,21	R$ 6.212.626,22	R$ 12.425.252,44
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 371,54	R$ 10.511.609,68	R$ 21.023.219,36
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 386,01	R$ 11.950.869,60	R$ 23.901.739,20
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 369,76	R$ 4.010.416,96	R$ 8.020.833,92

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 192.456,97	R$ 20.977.809,73	R$ 41.955.619,46
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 305.987,11	R$ 1.835.922,66	R$ 3.671.845,32
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 60.000,00	R$ 2.400.000,00	R$ 2.400.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 187.950,00	R$ 4.698.750,00	R$ 4.698.750,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 30.100,00	R$ 361.200,00	R$ 722.400,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 41.240,00	R$ 4.948.800,00	R$ 9.897.600,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 52.185,00	R$ 5.009.760,00	R$ 10.019.520,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 64.890,00	R$ 3.893.400,00	R$ 7.786.800,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 72.280,00	R$ 867.360,00	R$ 1.734.720,00
							Valor Total	**R$ 149.207.211,86**

Proposta Comercial - Suporte Informática

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 843,32	R$ 838.260,08	R$ 1.676.520,16
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 843,32	R$ 12.803.284,24	R$ 25.606.568,48
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 843,32	R$ 23.859.209,44	R$ 47.718.418,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 843,32	R$ 26.109.187,20	R$ 52.218.374,40
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 843,32	R$ 9.146.648,72	R$ 18.293.297,44

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	109	R$ 23.308,74	R$ 2.540.652,66	R$ 5.081.305,32
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	6	R$ 12.830,50	R$ 76.983,00	R$ 153.966,00
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 24.000,00	R$ 960.000,00	R$ 960.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 200.000,00	R$ 5.000.000,00	R$ 5.000.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 15.950,00	R$ 191.400,00	R$ 382.800,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 31.900,00	R$ 3.828.000,00	R$ 7.656.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 79.950,00	R$ 7.675.200,00	R$ 15.350.400,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 127.600,00	R$ 7.656.000,00	R$ 15.312.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 191.400,00	R$ 2.296.800,00	R$ 4.593.600,00
							Valor Total	**R$ 200.003.250,68**

Proposta Comercial - Network Secure

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 3.359,42	R$ 3.339.263,48	R$ 6.678.526,96
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 3.110,06	R$ 47.216.930,92	R$ 94.433.861,84
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 2.507,85	R$ 70.952.092,20	R$ 141.904.184,40
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 2.102,12	R$ 65.081.635,20	R$ 130.163.270,40

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 1.709,94	R$ 18.546.009,24	R$ 37.092.018,48
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	25	R$ 850.000,00	R$ 21.250.000,00	R$ 42.500.000,00
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente				
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 680.000,00	R$ 27.200.000,00	R$ 27.200.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 1.250.000,00	R$ 31.250.000,00	R$ 31.250.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 78.975,00	R$ 947.700,00	R$ 1.895.400,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 131.625,00	R$ 15.795.000,00	R$ 31.590.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 210.600,00	R$ 20.217.600,00	R$ 40.435.200,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 263.250,00	R$ 15.795.000,00	R$ 31.590.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 315.900,00	R$ 3.790.800,00	R$ 7.581.600,00
							Valor Total	**R$ 624.314.062,08**

Obs.: A proposta comercial apresentada pela empresa Network Secure possui valor único para o monitoramento do tráfego de rede, independente do volume, pois conforme explicado pela empresa, a entrega de sua solução para atender a este item é com a instalação de uma subscrição de software de máquina virtual para cada Tribunal.

Há também os valores da licitação realizada pelo Tribunal Regional do Trabalho da 17ª Região em 15/03/2023, para contratação de solução similar a que se pretende contratar, pelo período de 6 meses, conforme segue abaixo:

Item	Descrição	Quantidade	Preço Unitário	Preço Total
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos,	Ativo monitorado semestralmente	N/A	R$ 350.000,00

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	considerando um parque de até 2000 ativos monitorados.			
2	Serviço de treinamento na solução proposta para 8 alunos.	1 turma	R$ 10.000,00	R$ 10.000,00
3	Serviço de implantação da solução proposta	1 execução	R$ 20.000,00	R$ 20.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, considerando um parque de até 2000 ativos monitorados.	Mensal – vigência do contrato - 6 meses	R$ 45.000,00	R$ 270.000,00
			Total	**R$ 650.000,00**

Com o objetivo de atender a demanda de todos os Tribunais Regionais do Trabalho e do Tribunal Superior do Trabalho, recomenda-se que seja realizada licitação para geração de uma ata de registro de preços. Serão registrados 5 tipos de faixas, com diferentes quantitativos de ativos a serem monitorados. As quantidades totais a serem registradas foram obtidas através da planilha de dimensionamento da solução (Anexo II), que foi preenchida por todos os Tribunais.

Desta forma, uma estimativa de custo poderá ser elaborada considerando as médias dos valores das 3 menores propostas recebidas para os itens 1, 2, 3 e 4.

A análise dos valores recebidos nas propostas comerciais para o monitoramento do tráfego diário de rede apresentou uma significativa desproporcionalidade entre os custos para volume de tráfego de rede monitorado de 10Gbps (Gigabits por segundo) e de 1Gbps, sendo que, de acordo com as propostas recebidas, a contratação de 2Gbps já representaria um custo superior em relação a contratação de 10Gbps.

No dimensionamento realizado pelos Regionais, apenas dois apresentaram demanda equivalente a 1Gbps, porém há de se considerar uma previsão de crescimento estimada em 20% no tráfego de rede em todos os Tribunais para os próximos anos, conforme planilha de dimensionamento da solução (Anexo II) e, desta forma, todos os Regionais demandariam, no mínimo, a contração de 2 subscrições de 1Gbps, ou a combinação de subscrições de 10Gbps e mais 2 de 1Gbps.

Partindo deste entendimento, o volume de tráfego apontado pelos Regionais foi reavaliado e adequado para aquisições exclusivas de subscrições de 10Gbps, totalizando a necessidade de 33 unidades ao invés das 109 subscrições de 1Gbps e 6 de 10Gbps anteriormente solicitados para fornecimentos de propostas.

Conforme será verificado nas tabelas a seguir, em relação a proposta comercial enviada pela empresa Network Secure, não haverá alteração de valores, pois possui valor único para o monitoramento do tráfego de rede, independente do volume, com a instalação de uma subscrição de software de máquina virtual para cada Tribunal.

Desta forma, as propostas comerciais das empresas Intelliway, Petacorp, Service IT e Suporte Informática passariam a ter os seguintes valores:

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Proposta Comercial - Intelliway - Com quantidade ajustada referente ao monitoramento do tráfego de rede

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 249,14	R$ 247.645,16	R$ 495.290,32
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 242,10	R$ 3.675.562,20	R$ 7.351.124,40
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 227,01	R$ 6.422.566,92	R$ 12.845.133,84
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 222,39	R$ 6.885.194,40	R$ 13.770.388,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 216,22	R$ 2.345.122,12	R$ 4.690.244,24
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 0,00	R$ 0,00	R$ 0,00
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 31.156,36	R$ 1.246.254,40	R$ 1.246.254,40
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 81.282,92	R$ 2.032.073,00	R$ 2.032.073,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 53.431,30	R$ 641.175,60	R$ 1.282.351,20
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 74.051,19	R$ 8.886.142,80	R$ 17.772.285,60
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 109.809,60	R$ 10.541.721,60	R$ 21.083.443,20
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 157.758,30	R$ 9.465.498,00	R$ 18.930.996,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 172.566,00	R$ 2.070.792,00	R$ 4.141.584,00
							Valor Total	**R$ 105.641.169,00**

Proposta Comercial - Petacorp - Com quantidade ajustada referente ao monitoramento do tráfego de rede

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 469,12	R$ 466.305,28	R$ 932.610,56
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 399,41	R$ 6.063.842,62	R$ 12.127.685,24
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 364,32	R$ 10.307.341,44	R$ 20.614.682,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 382,61	R$ 11.845.605,60	R$ 23.691.211,20
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 359,65	R$ 3.900.763,90	R$ 7.801.527,80
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 300.638,93	R$ 9.921.084,69	R$ 19.842.169,38
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 50.000,00	R$ 2.000.000,00	R$ 2.000.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 180.000,00	R$ 4.500.000,00	R$ 4.500.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 28.500,00	R$ 342.000,00	R$ 684.000,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 39.000,00	R$ 4.680.000,00	R$ 9.360.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 48.000,00	R$ 4.608.000,00	R$ 9.216.000,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 63.000,00	R$ 3.780.000,00	R$ 7.560.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 70.000,00	R$ 840.000,00	R$ 1.680.000,00
							Valor Total	**R$ 120.009.887,06**

Proposta Comercial - Service IT - Com quantidade ajustada referente ao monitoramento do tráfego de rede

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento,	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 477,32	R$ 474.456,08	R$ 948.912,16

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 409,21	R$ 6.212.626,22	R$ 12.425.252,44
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 371,54	R$ 10.511.609,68	R$ 21.023.219,36
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 386,01	R$ 11.950.869,60	R$ 23.901.739,20
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 369,76	R$ 4.010.416,96	R$ 8.020.833,92
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 305.987,11	R$ 10.097.574,63	R$ 20.195.149,26
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 60.000,00	R$ 2.400.000,00	R$ 2.400.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 187.950,00	R$ 4.698.750,00	R$ 4.698.750,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 30.100,00	R$ 361.200,00	R$ 722.400,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 41.240,00	R$ 4.948.800,00	R$ 9.897.600,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 52.185,00	R$ 5.009.760,00	R$ 10.019.520,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 64.890,00	R$ 3.893.400,00	R$ 7.786.800,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 72.280,00	R$ 867.360,00	R$ 1.734.720,00
							Valor Total	**R$ 123.774.896,34**

Proposta Comercial - Suporte Informática - Com quantidade ajustada referente ao monitoramento do tráfego de rede

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 843,32	R$ 838.260,08	R$ 1.676.520,16
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 843,32	R$ 12.803.284,24	R$ 25.606.568,48

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

	resposta a ataques cibernéticos	Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 843,32	R$ 23.859.209,44	R$ 47.718.418,88
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 843,32	R$ 26.109.187,20	R$ 52.218.374,40
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 843,32	R$ 9.146.648,72	R$ 18.293.297,44
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 12.830,50	R$ 423.406,50	R$ 846.813,00
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 24.000,00	R$ 960.000,00	R$ 960.000,00
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 200.000,00	R$ 5.000.000,00	R$ 5.000.000,00
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 15.950,00	R$ 191.400,00	R$ 382.800,00
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 31.900,00	R$ 3.828.000,00	R$ 7.656.000,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 79.950,00	R$ 7.675.200,00	R$ 15.350.400,00
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 127.600,00	R$ 7.656.000,00	R$ 15.312.000,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 191.400,00	R$ 2.296.800,00	R$ 4.593.600,00
							Valor Total	**R$ 195.614.792,36**

Diante da ampla faixa de valores totais das propostas recebidas, buscou-se analisar a distribuição dos valores individuais de cada um dos itens nas propostas comerciais recebidas em relação aos valores totais cobrados, ou seja, a porcentagem que cada item representa no custo total da proposta.

Tendo em vista que a proposta da empresa Network Secure apresenta um valor 490% superior ao da menor proposta, considera-se que a mesma não pode ser considerada para a análise e estimativa de custo da demanda.

Desta forma, verifica-se que nas propostas das empresas Petacorp, Service IT, Suporte Informática e Network Secure possuem porcentagens aproximadas se comparadas com a proposta da empresa Intelliway, que possui distribuição dos valores diferente das demais, conforme se demonstra nas tabelas a seguir:

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Proposta Comercial - Intelliway - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Intelliway	Porcentagem em relação ao valor total da solução Intelliway
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 495.290,32	0,47%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 7.351.124,40	6,96%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 12.845.133,84	12,16%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 13.770.388,80	13,04%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 4.690.244,24	4,44%
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 0,00	0,00%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 1.246.254,40	1,18%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 2.032.073,00	1,92%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 1.282.351,20	1,21%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 17.772.285,60	16,82%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 21.083.443,20	19,96%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 18.930.996,00	17,92%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 4.141.584,00	3,92%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

TOTAIS	**R$ 105.641.169,00**	100,00%

Proposta Comercial - Petacorp - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Petacorp	Porcentagem em relação ao valor total da solução Petacorp
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 932.610,56	0,78%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 12.127.685,24	10,11%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 20.614.682,88	17,18%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 23.691.211,20	19,74%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 7.801.527,80	6,50%
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 19.842.169,38	16,53%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 2.000.000,00	1,67%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 4.500.000,00	3,75%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 684.000,00	0,57%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 9.360.000,00	7,80%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 9.216.000,00	7,68%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 7.560.000,00	6,30%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 1.680.000,00	1,40%
					TOTAIS	**R$ 120.009.887,06**	100,00%

Proposta Comercial - Service IT - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Service IT	Porcentagem em relação ao valor total da solução Service IT
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 948.912,16	0,77%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 12.425.252,44	10,04%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 21.023.219,36	16,99%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 23.901.739,20	19,31%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 8.020.833,92	6,48%
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 20.195.149,26	16,32%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 2.400.000,00	1,94%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 4.698.750,00	3,80%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 722.400,00	0,58%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 9.897.600,00	8,00%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 10.019.520,00	8,09%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 7.786.800,00	6,29%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 1.734.720,00	1,40%
					TOTAIS	**R$ 123.774.896,34**	100,00%

Proposta Comercial - Suporte Informática - Com distribuição em percentual para cada um dos itens

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor TOTAL – Suporte Informática	Porcentagem em relação ao valor total da solução Suporte Informática
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 1.676.520,16	0,86%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 25.606.568,48	13,09%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 47.718.418,88	24,39%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 52.218.374,40	26,69%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 18.293.297,44	9,35%
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 846.813,00	0,43%
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 960.000,00	0,49%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 5.000.000,00	2,56%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 382.800,00	0,20%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 7.656.000,00	3,91%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 15.350.400,00	7,85%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 15.312.000,00	7,83%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 4.593.600,00	2,35%
					TOTAIS	**R$ 195.614.792,36**	100,00%

Após essa etapa, passou-se a analisar os custos totais de cada proposta, de forma que, para composição da média das propostas, também não foi considerada a proposta da empresa Suporte Informática por apresentar valor superior à 85% em relação a proposta de menor valor, da empresa Intelliway.

Após esse passo, definiu-se o valor total da contratação com base na média das propostas comerciais das empresas Intelliway, Petacorp e Service IT.

Com isso, com o objetivo de garantir a elaboração de uma estimativa de custo de forma mais equilibrada, sugere-se que seja elaborada uma média das porcentagens dos itens em relação aos valores totais das propostas recebidas das empresas, mesmo que a proposta da empresa Suporte Informática não tenha sido utilizada na composição dos valores médios estimados, pois verifica-se que possuem distribuição percentual dos itens semelhantes.

Média das Porcentagens das propostas

Item	**Descrição**	**Faixa**	**Faixa de Subscrição por Ativo**	**Unidade de Medida**	**Qtde.**	**Média das Porcentagens das Propostas**
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	0,72%
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	10,05%
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	17,68%
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	19,70%
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	6,69%
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	8,32%

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	1,32%
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	3,01%
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	0,64%
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	9,13%
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	10,89%
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	9,58%
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	2,27%
					TOTAL	**100,00%**

Por fim, para a definição da estimativa de custo de cada item da contratação, aplicou-se a média das porcentagens obtidas, conforme a tabela acima, no valor total estimado da contratação obtido por meio da média das propostas comerciais das empresas Intelliway, Petacorp e Service IT, obtendo-se assim a estimativa a seguir:

Estimativa de custo total - Média das 3 menores propostas

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 398,53	R$ 396.138,82	R$ 792.277,64
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 350,24	R$ 5.317.343,68	R$ 10.634.687,36
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 320,96	R$ 9.080.600,32	R$ 18.161.200,64
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 330,34	R$ 10.227.326,40	R$ 20.454.652,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 315,21	R$ 3.418.767,66	R$ 6.837.535,32
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 202.208,68	R$ 6.672.886,44	R$ 13.345.772,88

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 47.052,12	R$ 1.882.084,80	R$ 1.882.084,80
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 149.744,31	R$ 3.743.607,75	R$ 3.743.607,75
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 37.343,77	R$ 448.125,24	R$ 896.250,48
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 51.430,40	R$ 6.171.648,00	R$ 12.343.296,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 69.998,20	R$ 6.719.827,20	R$ 13.439.654,40
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal	5	R$ 95.216,10	R$ 5.712.966,00	R$ 11.425.932,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 104.948,67	R$ 1.259.384,04	R$ 2.518.768,08
Valor Total Estimado para todos os Tribunais								**R$ 116.475.720,15**

Obs. 1: Os valores referentes aos itens 1, 2, 3 e 4 foram calculados com base na média dos valores das 3 menores propostas comerciais recebidas das empresas Intelliway, Petacorp e Service IT. Os valores das propostas comerciais recebidas das empresas Suporte Informática e Network Secure, como já desqualificada anteriormente, não foram utilizados na estimativa de custo por estarem muito superior em relação à proposta de menor valor recebida da empresa Intelliway.

Obs. 2: Recomenda-se que os valores referentes a licitação realizada pelo TRT17 não sejam utilizados nos cálculos da estimativa de custo, por se tratar de uma contratação com escopo bem menor da que se pretende realizar, sendo feita para atender apenas a necessidade daquele Regional, bem como por não ter todos os valores dos tipos de faixas das subscrições e dos serviços de monitoramento e nem ter os valores do monitoramento do tráfego de rede. Por isso, caso sejam utilizados os valores desta licitação na composição da estimativa de custo, eles podem não ser exequíveis.

Aplicando-se as médias das porcentagens das propostas comerciais recebidas, conforme explicado acima, em relação ao valor total estimado de R$ 116.475.720,15, que foi calculado com base na média das 3 menores propostas, teremos os seguintes valores unitários e totais máximos dos itens conforme segue abaixo:

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Estimativa de custo total para todos os Tribunais

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente	994	R$ 398,53	R$ 396.138,82	R$ 792.277,64
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente	15182	R$ 350,24	R$ 5.317.343,68	R$ 10.634.687,36
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente	28292	R$ 320,96	R$ 9.080.600,32	R$ 18.161.200,64
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente	30960	R$ 330,34	R$ 10.227.326,40	R$ 20.454.652,80
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 315,21	R$ 3.418.767,66	R$ 6.837.535,32
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	33	R$ 202.208,68	R$ 6.672.886,44	R$ 13.345.772,88
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 251 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	40	R$ 47.052,12	R$ 1.882.084,80	R$ 1.882.084,80
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	25	R$ 149.744,31	R$ 3.743.607,75	R$ 3.743.607,75
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal	1	R$ 37.343,77	R$ 448.125,24	R$ 896.250,48
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal	10	R$ 51.430,40	R$ 6.171.648,00	R$ 12.343.296,00
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal	8	R$ 69.998,20	R$ 6.719.827,20	R$ 13.439.654,40
		Tipo 4	De 8001 a 8000 ativos monitorados	Serviço mensal	5	R$ 95.216,10	R$ 5.712.966,00	R$ 11.425.932,00
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 104.948,67	R$ 1.259.384,04	R$ 2.518.768,08
Valor Total Estimado para todos os Tribunais								**R$ 116.475.720,15**

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Desta forma, o valor total estimado da contratação para todos o TRTs e para o TST é de R$ 116.475.720,15 (cento e dezesseis milhões, quatrocentos e setenta e cinco mil, setecentos e vinte reais e quinze centavos) pelo período de 24 (vinte e quatro) meses.

Já o valor total estimado somente para o TRT2 será conforme segue na tabela abaixo:

Estimativa de custo total para o TRT2

Item	Descrição	Faixa	Faixa de Subscrição por Ativo	Unidade de Medida	Qtde.	Valor Unitário	Valor Total (em 12 meses)	Valor Total – (em 24 meses)
1	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente	10846	R$ 315,21	R$ 3.418.767,66	R$ 6.837.535,32
		Rede	10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente	2	R$ 202.208,68	R$ 404.417,36	R$ 808.834,72
2	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes para 8 alunos	Serviço pontual, por turma de treinamento (8 alunos por turma no máximo)	1	R$ 47.052,12	R$ 47.052,12	R$ 47.052,12
3	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual	1	R$ 149.744,31	R$ 149.744,31	R$ 149.744,31
4	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal	1	R$ 104.948,67	R$ 1.259.384,04	R$ 2.518.768,08
Valor Total Estimado para o TRT2								**R$ 10.361.934,55**

Para a composição dos quantitativos referente ao TRT2, estão sendo considerados um total de 10.846 ativos monitorados, sendo 10.170 estações de trabalho/notebooks, 615 servidores Linux e 61 servidores Windows, o que nos enquadra na faixa do tipo 5, que é de 8.001 a 12.000 ativos monitorados. Para o tráfego diário de rede monitorado anualmente, considerando que o nosso volume médio diário do tráfego da rede interna é de 17,04 Gbps, já considerando um crescimento de 20% para os próximos anos, está sendo considerada a aquisição de 2 subscrições de 10Gbps.

Para a realização do treinamento, está sendo considerada a participação de 8 alunos, sendo necessária a contratação de 1 turma.

Para os serviços de implantação e de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos (itens 3 e 4), está sendo considerada a quantidade de 1 para cada Tribunal.

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Desta forma, a estimativa de custo total para o TRT2 será de R$ 10.361.934,55 (dez milhões, trezentos e sessenta e um mil, novecentos e trinta e quatro reais e cinquenta e cinco centavos) pelo período de 24 (vinte e quatro) meses.

2.9 Natureza do Objeto

O objeto a ser contratado possui características comuns e usuais encontradas atualmente no mercado de Tecnologia de Informação, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste documento.

A descrição do objeto a ser contratado é Solução e Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos, incluindo suporte técnico, implantação e treinamento.

Conforme decreto nº 11.462, de 31 de março de 2023, Artigo 3º, incisos III e V, o Sistema de Registro de Preços poderá ser adotado quando a Administração julgar pertinente, em especial quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas e quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração. O Tribunal poderá efetivar contratação dos itens do objeto deste documento observando a viabilidade técnica na ocasião do vencimento da garantia vigente e disponibilidade orçamentária.

Com o objetivo de se padronizar soluções, sistemas, ferramentas e contratações conjuntas, como meio de minimizar custos e maximizar a força de trabalho das equipes de TIC, será permitida a adesão/carona somente aos órgãos integrantes da Justiça do Trabalho.

2.10 Parcelamento do Objeto

Recomenda-se que o objeto não seja parcelado, uma vez que todos os produtos e serviços a serem fornecidos e prestados são componentes de uma única solução de TIC, a qual não pode ser desmembrada sem que haja perda de produtividade e economia de escala.

Cabe ressaltar também que não é viável o parcelamento dos serviços prestados, pois geraria riscos à continuidade da solução, dificultando a gestão de problemas diversos em diferentes itens da solução.

2.11 Forma de Adjudicação

Para efeito de adjudicação do objeto, recomenda-se que seja considerado o menor preço global, uma vez que todos os itens a serem fornecidos são componentes de uma única solução de TIC, a qual não pode ser desmembrada sem que haja perda de produtividade e economia de escala.

2.12 Modalidade, Tipo de Licitação e Critérios de Seleção

Verifica-se que o objeto pretendido é oferecido por alguns fornecedores no mercado de TIC e apresenta características padronizadas e usuais. Assim, se pode concluir que o objeto é comum e, portanto, sugere-se como melhor opção a utilização da licitação na modalidade pregão eletrônico do tipo menor preço.

Considerando que a demanda se enquadra nas hipóteses previstas no artigo 3º, incisos III e V do decreto nº 11.462/2023, sugere-se que seja adotado o Sistema de Registros de Preços (SRP). O Registro de Preços poderá ser adotado quando a Administração julgar pertinente, em especial quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas e quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

Além disso, recomenda-se que seja aplicado o disposto no artigo 49 da lei complementar 123/2006, considerando se tratar de serviço especializado em solução complexa e não ter sido encontrado microempresas ou empresas de pequeno porte que possam atender à demanda. Por isso, com o objetivo de não frustrar o processo licitatório, sugere-se, s.m.j., que a licitação não seja exclusiva para empresas que se enquadrem nessas categorias.

2.13 Impacto Ambiental

A Secretaria de Processamento e Acompanhamento de Contratos e Licitações, em sua Notificação Ambiental, documento 19 do PROAD 9.605/2021, dos itens 4.5 e 4.6 do Manual para Contratação de Solução de TIC e de acordo com a análise do objeto constante no presente Processo Administrativo de Contratação, informou que a Secretaria de Processamento e Acompanhamento de Contratos e Licitações e a Seção de Gestão Socioambiental verificaram, s.m.j, não haver critério de sustentabilidade a ser observado quando da contratação, conforme determinações previstas no Plano de Logística Sustentável (PLS-TRT2), no Guia de Contratações Sustentáveis do Conselho Superior da Justiça do Trabalho, Resolução nº 310/2021 ou no Guia Prático de Contratações Sustentáveis do TRT2.

Informou também que não há necessidade de participação da Seção de Gestão Socioambiental, com a indicação de integrante, no presente processo de contratação, em cumprimento ao item 4.6 do referido Manual.

2.14 Aderência da Contratação ao plano anual de compras

A contratação deverá estar prevista nas programações orçamentárias da Secretaria de Tecnologia da Informação e Comunicação para os anos de 2024 e 2025.

2.15 Conformidade com normas Técnicas e Legais

As especificações técnicas descritas no Anexo A deste Termo de Referência vislumbram a

aplicação de normas técnicas e legais específicas.

2.16 Prazo e Condições de Garantia

A CONTRATADA deve realizar a implantação, configuração e ativação da solução no prazo de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições detalhadas que constam das Especificações Técnicas em anexo.

O período de vigência deverá ser de 24 (vinte e quatro) meses a partir do Termo de Recebimento Definitivo do Serviço de implantação da solução, podendo ser prorrogado por mais 24 (vinte e quatro) meses ou até o limite legal.

2.17 Condições e Prazos de Pagamento

O pagamento relativo às subscrições de licenças do software de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos será realizado anualmente, devendo ser fornecidas conforme a quantidade de ativos definida pela CONTRATANTE e deverão ser nomeadas (para cada CONTRATANTE). A comprovação do fornecimento se dará através da Nota Fiscal e o pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação às subscrições efetivamente fornecidas em nome da CONTRATANTE, conforme volumetria mínima prevista.

O pagamento relativo aos serviços de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos será realizado mensalmente, sendo realizado somente após a emissão do termo de recebimento definitivo, descontadas eventuais glosas do período avaliado, conforme Fator de Desconto (FD) calculado no período e das multas aplicadas, quando houver.

O pagamento do serviço de implantação deve ser realizado em parcela única, após a emissão do termo de recebimento definitivo.

O pagamento do treinamento deve ser realizado em parcela única após a emissão do termo de recebimento definitivo.

Além das retenções legais, serão automaticamente descontados dos valores faturados os percentuais decorrentes da aplicação dos critérios de níveis de serviço.

2.18 Previsão de Custo

O objeto da contratação constitui despesa corrente, classificação orçamentária 3390.40.07 e 3390.40.20, estimada em R$ 116.475.720,15 (cento e dezesseis milhões, quatrocentos e setenta e cinco mil, setecentos e vinte reais e quinze centavos) para todos os TRTs e o TST e em R$ 10.361.934,55 (dez milhões, trezentos e sessenta e um mil, novecentos e trinta e quatro reais e

cinquenta e cinco centavos) para o TRT2 para um período de 24 meses de contratação, e deverá constar nas programações orçamentárias de SETIC para os anos de 2024 e 2025, sendo distribuído da seguinte forma:

Todos os TRTs e TST:

Treinamento: 3390.40.20 – R$ 1.882.084,80

Manut. Corretiva/Adaptativa e Sustentação de Softwares: 3390.40.07 – R$ 114.593.635,35

Somente TRT 2ª Região:

Treinamento: 3390.40.20 – R$ 47.052,12

Manut. Corretiva/Adaptativa e Sustentação de Softwares: 3390.40.07 – R$ 10.314.882,43

Serão necessários recursos orçamentários para os próximos exercícios, conforme segue:

Ano	Valor - Serviços	Valor - Treinamento
2024	R$ 5.232.313,37	R$ 47.052,12
2025	R$ 5.082.569,06	---------

3 Equipe de Gestão e Fiscalização da Contratação

Papel	Servidor	Matrícula	Telefone	E-mail
Gestor do Contrato	Cláudia Sant'Anna Pinheiro – Diretora da Coordenadoria de Segurança de TIC	97500	2073	seguranca-ti@trt2.jus.br
Gestor do Contrato - Substituto	Leonardo Luis Soares - Assistente Administrativo Chefe da Seção de Gestão de Riscos e Continuidade	132870	2726	riscos-ti@trt2.jus.br
Fiscal Técnico	Ramon Chiara – Assistente Administrativo Chefe da Seção de Gestão de Incidentes em Segurança da Informação	133167	2737	incidentesseg-ti@trt2.jus.br

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Fiscal Técnico - Substituto	Lucas Ihara Alves - Seção de Gestão de Incidentes em Segurança da Informação	161020	2737	lucas.alves@trt2.jus.br

3.1 Equipe de Recebimento da Contratação

O recebimento, conforme determinado pelo Ato GP 37/2018, deverá ser feito pela seguinte equipe nomeada:

Nome	Ramal	E-Mail
Ramon Chiara	2737	incidentesseg-ti@trt2.jus.br
Lucas Ihara Alves	2737	lucas.alves@trt2.jus.br
Cláudia Sant'Anna Pinheiro	2073	seguranca-ti@trt2.jus.br

O prazo para o recebimento definitivo, após a conclusão do serviço de implantação, configuração e ativação da solução, será de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato. O prazo para sanar irregularidades, no caso de entrega/disponibilização de serviço em desacordo com o solicitado, será de até 15 (quinze) dias corridos da data de comunicação.

3.2 Obrigações Contratuais

As obrigações contratuais pormenorizadas constam da especificação técnica que acompanha este termo de referência.

Destaca-se o cumprimento das obrigações e requisitos detalhados no Anexo A – Especificações Técnicas, bem como a eventual aplicação das penalidades a eles vinculadas, descritas no mesmo anexo.

4 OUTRAS INFORMAÇÕES RELEVANTES

Os produtos deverão ser registrados em Ata de Registro de Preços conforme a tabela abaixo:

Item	Descrição	Tipo de Faixa	Faixa de Subscrição	Quant. Registrada	Pedido Inicial	Pedido Mínimo	Valor Unitário Máximo	Valor Total Máximo (24 meses)
01	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados anualmente	994	0	1	R$ 398,53 p/ ano	R$ 792.277,64
		Tipo 2	De 1001 a 2000 ativos monitorados anualmente	15.182	0	1	R$ 350,24 p/ ano	R$ 10.634.687,36
		Tipo 3	De 2001 a 5000 ativos monitorados anualmente	28.292	0	1	R$ 320,96 p/ ano	R$ 18.161.200,64
		Tipo 4	De 5001 a 8000 ativos monitorados anualmente	30.960	0	1	R$ 330,34 p/ ano	R$ 20.454.652,80
		Tipo 5	De 8001 a 12000 ativos monitorados anualmente	10.846	10.846	1	R$ 315,21 p/ ano	R$ 6.837.535,32

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Item	Descrição	Tipo de Faixa	Faixa de Subscrição	Quant. Registrada	Pedido Inicial	Pedido Mínimo	Valor Unitário Máximo	Valor Total Máximo (24 meses)
		Rede	10Gbps (Gigabits por segundo) de tráfego diário monitorado anualmente	33	2	1	R$ 202.208,68 p/ ano	R$ 13.345.772,88
02	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes (Valor por turma)	40	1	1	R$ 47.052,12 p/ turma	R$ 1.882.084,80
03	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	25	1	1	R$ 149.744,31 p/ serviço	R$ 3.743.607,75
04	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados mensalmente	1	0	1	R$ 37.343,77 p/ mês	R$ 896.250,48
		Tipo 2	De 1001 a 2000 ativos monitorados mensalmente	10	0	1	R$ 51.430,40 p/ mês	R$ 12.343.296,00
		Tipo 3	De 2001 a 5000 ativos monitorados mensalmente	8	0	1	R$ 69.998,20 p/ mês	R$ 13.439.654,40
		Tipo 4	De 5001 a 8000 ativos monitorados mensalmente	5	0	1	R$ 95.216,10 p/ mês	R$ 11.425.932,00
		Tipo 5	De 8001 a 12000 ativos monitorados mensalmente	1	1	1	R$ 104.948,67 p/ mês	R$ 2.518.768,08
							TOTAL	**R$ 116.475.720,15**

Cumpre informar também que a equipe de planejamento desta contratação não identificou impedimentos em relação à aplicação do decreto nº 7.174/2010. Porém, por se tratar de um mercado restrito de soluções que atendam plenamente a demanda, não se recomenda, s.m.j, que seja restringida a licitação a apenas empresas que atendam ao disposto no artigo 5º, sob o risco de fracasso do certame.

As empresas participantes deverão apresentar, no momento da sua habilitação no processo licitatório, Atestado(s) de Capacidade Técnica (ACT) em nome da licitante e emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado ou estar prestando:

- Fornecimento de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos similar à proposta, em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;
- Fornecimento de serviço de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias ao ano), em ambiente computacional contendo no mínimo 4.000 (quatro mil) ativos monitorados;
- Para cada subitem acima, serão considerados somatórios de atestados para atingir as quantidades solicitadas.

Na fase da habilitação deverá ser apresentado: balanço patrimonial e demonstrações do resultado do exercício – DRE relativos ao último exercício social exigível, comprovando índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um),

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

em conformidade com os normativos pertinentes, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta, devendo apresentar as seguintes características:

- Estarem devidamente assinados pelo administrador da empresa e pelo profissional de Contabilidade;

- Estarem devidamente registrados na Junta Comercial do Estado correspondente ou disponibilizado pelo SPED;

- Constando Patrimônio Líquido igual ou superior a 10% (dez por cento) do valor estimado da contratação;

- Constando Capital circulante Líquido ou Capital de Giro (Ativo Circulante - Passivo Circulante) de, no mínimo, 16,66% (dezesseis inteiros e sessenta e seis centésimos por cento) do valor estimado da contratação.

A comprovação dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC) serão resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

Com o objetivo de se padronizar soluções, sistemas, ferramentas e contratações conjuntas, como meio de minimizar custos e maximizar a força de trabalho das equipes de TIC, será permitida a adesão/carona somente aos órgãos integrantes da Justiça do Trabalho.

A licitante vencedora deverá apresentar, junto com os demais documentos de habilitação, a planilha de comprovação de atendimento aos itens da especificação técnica devidamente preenchida, conforme Anexo B – Comprovação de atendimento aos itens da Especificação

Técnica, onde deverá constar a forma de atendimento a cada um dos itens mencionados no documento.

5 ESPECIFICAÇÃO TÉCNICAS

Conforme Anexo A – Especificações Técnicas.

Análises realizadas pela Equipe de Planejamento.

São Paulo, data da assinatura eletrônica.

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

Anexo A - Especificação Técnica

1. Objeto

Ata de registros de preços visando a contratação de solução de Monitoramento, Detecção, Notificação, Investigação e Resposta a Ataques Cibernéticos, bem como serviços de treinamento, implantação e sustentação da solução proposta, pelo período de 24 meses, conforme a tabela seguinte:

Item	Descrição	Tipo de Faixa	Faixa de Subscrição	Unidade de Medida
01	Subscrição de solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos	Ativo monitorado anualmente
		Tipo 2	De 1001 a 2000 ativos	Ativo monitorado anualmente
		Tipo 3	De 2001 a 5000 ativos	Ativo monitorado anualmente
		Tipo 4	De 5001 a 8000 ativos	Ativo monitorado anualmente
		Tipo 5	De 8001 a 12000 ativos	Ativo monitorado anualmente
		Rede	1Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente
			10Gbps (Gigabits por segundo)	Tráfego diário monitorado anualmente
02	Serviço de treinamento na solução proposta	-	Treinamento sobre a solução e seus componentes	Serviço pontual, por turma de treinamento
03	Serviço de implantação da solução proposta	-	Serviço de implantação e ativação da solução e seus componentes	Serviço pontual
04	Serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos	Tipo 1	Até 1000 ativos monitorados	Serviço mensal
		Tipo 2	De 1001 a 2000 ativos monitorados	Serviço mensal
		Tipo 3	De 2001 a 5000 ativos monitorados	Serviço mensal
		Tipo 4	De 5001 a 8000 ativos monitorados	Serviço mensal
		Tipo 5	De 8001 a 12000 ativos monitorados	Serviço mensal

1.1 Definições para fins desta especificação:

1.1.1 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.

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

1.1.1.2 Caso o ativo possua mais de um endereço IP, será contabilizado um único "Ativo monitorado" para efeito de subscrição.

1.1.2 Define-se "Tráfego diário monitorado" como sendo volume médio diário do tráfego da rede interna (em Gbps - Gigabits por segundo) que deverá ser monitorado pela solução proposta.

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

1.1.3.1 "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.

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

1.1.3.3 "Dados de rede": informações sobre o tráfego de rede.

1.2 Para soluções cuja subscrição seja baseada em EPS (Eventos Por Segundo), a CONTRATADA deve licenciar a solução para uma quantidade mínima de EPS suficiente para atender 100% dos ativos da CONTRATANTE e garantir a escalabilidade da solução, independentemente da quantidade de EPS gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de EPS igual a 8 vezes a referida quantidade de ativos monitorados.

1.2.1 A CONTRATADA deverá aferir mensalmente o consumo de EPS e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para a CONTRATANTE.

1.3 Para soluções cuja subscrição seja baseada em volumetria de logs, a CONTRATADA deve licenciar a solução para uma quantidade mínima de Área de Armazenamento em modalidade SaaS, suficiente para atender 100% dos ativos da CONTRATANTE e garantir a escalabilidade da solução, independentemente do volume de logs, dados de telemetria e de rede gerados pelos ativos monitorados, observando-se o limite de licenciamento mínimo de GB (gigabytes) igual a 2 vezes a referida quantidade de ativos monitorados e a retenção dos logs estipulada no item 2.8.

1.3.1 A CONTRATADA deverá aferir mensalmente a volumetria e provar que a quantidade ofertada está comportando a quantidade de eventos ingerida pela solução, realizando correções no quantitativo se necessário, sem custo para a CONTRATANTE.

1.3.2 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.

2. ITEM 1 – 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 da 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 à CONTRATANTE.

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 da 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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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 da 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 pela CONTRATANTE;

2.5.2. Registrar e comunicar os incidentes de segurança cibernética para a 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 da CONTRATANTE;

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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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) dos alertas, incidentes e chamados.

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

2.5.4.1.2. O módulo ou ferramenta de ITSM deverá estar licenciado para a 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. O fabricante da solução proposta para monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos deve ser atestado SOC 2 Type II;

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

2.6.3. 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.

2.6.4. 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, podendo ser de fabricantes distintos da solução.

2.6.5. Coletores de tráfego de rede: o software dos coletores de tráfego de rede, bem como os respectivos sistemas operacionais, sistemas gerenciadores de banco de dados, entre outros componentes (de software ou hardware) eventualmente necessários para a coleta e centralização de dados de tráfego de rede deverão ser fornecidos pela CONTRATADA, podendo ser de fabricantes distintos da solução, devendo ser compatíveis com a infraestrutura da CONTRATANTE (interfaces de rede de 1Gbps e 10Gbps).

2.6.5.1. O tráfego de rede deverá ser mensurado de acordo com o ambiente da CONTRATANTE.

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

2.6.6.1. 12 vCPUs;

2.6.6.2. 32Gb vRAM;

2.6.6.3. 200GB de espaço em disco.

2.6.7. Caso os recursos em ambiente virtual necessários para o pleno funcionamento da solução extrapolem os recursos disponibilizados pela 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 pela CONTRATANTE conforme comprovação apresentada. Caso não haja comprovação, a critério da CONTRATANTE, a CONTRATADA deverá providenciar, sem custos adicionais para a CONTRATANTE, a entrega da infraestrutura (total ou remanescente) e em conformidade com a estrutura computacional da CONTRATANTE.

2.6.8. 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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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.

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

2.6.9.1. Google Chrome;

2.6.9.2. Mozilla Firefox.

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

2.6.10.1. 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.

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

2.6.10.3. Os ambientes utilizados pela solução (incluindo do fabricante) devem possuir, ao menos, uma cópia das informações localizadas no Brasil.

2.6.11. 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 ou para a quantidade de eventos por segundo (conforme item 1.2) ou para o volume de armazenamento de logs em ambiente SaaS (conforme item 1.3) de forma a abranger o escopo completo de ativos da CONTRATANTE, conforme conceito apresentado nesta especificação técnica. Assim, é obrigatório que a solução cubra 100% do ambiente da CONTRATANTE, incluindo estações de trabalho, notebooks, dispositivos móveis, servidores físicos e virtuais, containers, firewalls, ativos de rede ou qualquer equipamento similar ao listado, e não somente parcialmente, de forma a prover uma visibilidade plena da segurança cibernética do ambiente.

2.7.1. A solução deve suportar picos de EPS (Eventos Por Segundo) ou GB (gigabytes) acima do licenciado em até 30%.

2.7.1.1. Caso os picos de EPS ou GB ultrapassem o limite de 30%, a solução não deve descartar os eventos de forma que sejam processados posteriormente.

2.8. A solução deve possuir retenção mínima de 03 (três) meses de registros prontamente acessíveis (“Logs Quentes”). Após este período, a solução deve suportar, no mínimo, 09 (nove) meses de registros arquivados (“Logs Frios”) - totalizando 12 (doze) meses de registros - bem como permitir a exportação destes logs/dados de telemetria/de rede para armazenamento em ambiente de propriedade da CONTRATANTE.

2.8.1. As análises realizadas e alertas devem estar disponíveis de forma integral por pelo menos 06 (seis) meses.

2.8.2. Deve haver a opção de exportação de logs/dados de telemetria/de rede em formato aberto (plain text) podendo ser abertos e lidos em editores de texto sem a necessidade de softwares proprietários ou plugins.

2.8.3. A solução não deve possuir mecanismos que limitem ou onerem a 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 Open LDAP, 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;

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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 ou de terceiros;

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.