Estudo Técnico do Projeto

Prestação de Serviços de Monitoramento de Ambiente Tecnológico

SOC (Security Operations Center)

NOC (Network Operations Center)

Justiça Federal da 3ª Região – JF3R

Tribunal Regional Federal da 3ª Região – TRF3

Versão 1.3
Agosto/2022

Histórico de Revisões

DATA	VERSÃO	DESCRIÇÃO	AUTOR
Março/2022	1.0	Abertura	Anderson Alves Chieregat
Junho/2022	1.1	Revisão	Anderson Alves Chieregat
Julho/2022	1.2	Revisão	Anderson Alves Chieregat
Agosto/2022	1.3	Revisão	Anderson Alves Chieregat

1. Introdução

Este documento visa o estudo de contratação de empresa especializada na prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center) na Justiça Federal da 3ª. Região – JF3R.

2. Situação Atual

No âmbito da Justiça Federal da 3ª Região – JF3R, as crescentes demandas na área de Tecnologia da Informação e Comunicação - TIC, principalmente dos sistemas processuais eletrônicos, requerem cada vez mais ferramentas e soluções que proporcionem segurança, alta disponibilidade, eficiência, escalabilidade e ganho de desempenho.

Conforme a edição de 2020 do Panorama de Ameaças na América Latina (janeiro a setembro de 2020), a Kaspersky identificou que 2 em cada 3 ataques na América Latina são contra empresas e apenas 1 em 3 é direcionado a pessoas comuns, evidenciando que empresas são mais atacadas que os cidadãos.

Segundo o relatório, o Brasil é líder absoluto como o país que mais foi alvo de ataques, sendo que recebeu 56% dos ataques destinados a pessoas comuns, bem como dos ataques destinados a empresas.

Considerando o coeficiente de risco para as empresas, o Brasil ocupa o segundo lugar, somente atrás da Argentina, evidenciando que se tornou um ambiente hostil para a sobrevivência dos negócios que dependem da TIC.

Fonte: https://prezi.com/view/bEFMzi8MdxxxxPyeiEqH/

O ciberataque tem crescimento ascendente em todo mundo, evidenciando-se no Brasil em dois grandes eventos recentes. Ao fim de 2020, instituições governamentais brasileiras sofreram ataques por ransomware que geraram o vazamento de dados e a indisponibilidade dos órgãos, promovendo um grande impacto no negócio. No início de 2021, dois megavazamentos de informações pessoais sensíveis de brasileiros foram detectados, sendo a exposição

de 223 milhões de dados expostos no primeiro e 100 milhões de dados expostos no segundo.

Fonte: https://canaltech.com.br/seguranca/stj-e-alvo-de-ataque-cibernetico-confira-tudo-o-que-sabemos-ate-agora-174162/

Fonte: https://canaltech.com.br/seguranca/mais-um-novo-vazamento-expoe-dados-de-102-milhoes-incluindo-bolsonaro-178825/

A JF3R é um dos maiores órgãos do Poder Judiciário brasileiro em volume de processos e tem como objetivo principal garantir o princípio constitucional do acesso à justiça, adotando medidas que visam à alta disponibilidade e a proteção dos ativos de TIC que estão sob a sua custódia.

No dia 30 de março de 2022 foram detectados pela equipe técnica da Secretaria de Tecnologia da Informação – SETI, responsável por gerir o ambiente tecnológico da JF3R, eventos maliciosos na infraestrutura de redes da JF3R.

De forma imediata, a equipe técnica começou a atuar no incidente identificando tratar-se de um ataque cibernético, executando as medidas de isolamento e contenção de danos potenciais, a fim de preservar a segurança e a integridade das informações contidas nos ativos de TIC da JF3R, esse ataque ocasionou a indisponibilidade total de sistemas eletrônicos da JF3R impossibilitando o acesso aos usuários externos e internos, afetando as atividades jurisdicionais da JF3R.

Diante da gravidade da situação, a equipe técnica atuou na tentativa da solução do problema, mas devido à extensão dos danos causados no ambiente tecnológico houve a necessidade de apoio de uma empresa especializada em segurança cibernética, com expertise principalmente na subárea de resposta a incidentes e suporte para segurança da informação, visando auxiliar nos trabalhos de investigação, recuperação e mitigação de danos.

A contratação emergencial da empresa especializada em Segurança da Informação de TIC foi realizada através de Dispensa de Licitação n. º 8659875/2022 e resultou no restabelecimento dos serviços jurisdicionais da JF3R, bem como agregou serviços de monitoramento de ambiente através de implantação de SOC e subscrição de ferramentas de SI pelo período de 6 (seis) meses.

Diante do crítico cenário atual de SI, do crescente volume de dados operacionalizados em sistema processuais, da amplitude e diversidade do parque

tecnológico da JF3R e da grande dependência do negócio a disponibilidade e qualidade dos serviços de TIC, faz-se necessário proteger as atividades jurisdicionais da JF3R por meio da continuidade dos serviços de SOC já implantados na JF3R, bem como ampliar do gerenciamento do parque tecnológico através de serviços de NOC.

Há de se considerar também que os prejuízos de uma nova paralização das atividades da JF3R são incalculáveis em relação à imagem da instituição, que passa a receber o descrédito em relação à sua capacidade de atuação diante das tentativas de ataque e, principalmente, em relação ao comprometimento da atuação jurisdicional do órgão, por ter sua principal atividade finalística comprometida.

A implantação de um NOC (Network Operations Center) em datacenter da JF3R visa o monitoramento do ambiente tecnológico da JF3R, em regime de 24 (vinte e quatro) horas x 7 (sete) dias da semana e em feriados, e tem como objetivo prever e evitar falhas em equipamentos de rede e/ou serviços de TIC e sistemas críticos ao negócio da JF3R, impossibilitando ou minimizando à indisponibilidade ou degradação dos mesmos.

A implantação de um SOC (Security Operations Center) em datacenter da JF3R pós-cenário de desastre visa o monitoramento do ambiente tecnológico da JF3R e tem como objetivo prover serviços e soluções de detecção e validação de incidentes, análise comportamental e detecção de tráfego malicioso na infraestrutura de rede, gerenciamento de incidentes, validação e verificação de vulnerabilidade e ações de resposta imediata que visam restabelecer os serviços de TIC, em regime de 24 (vinte quatro) horas x 7 (sete) dias da semana e em feriados.

A implementação dos serviços de NOC e SOC se dará por meio de técnicos especializados disponíveis 24 (vinte quatro) horas x 7 (sete) dias da semana e em feriados, tanto em regime remoto quanto presencial, e ferramentas de software que permitirão o monitoramento e análise de comportamento do parque tecnológico da JF3R.

Ressalta-se que a manutenção dos serviços de SOC anteriormente contratados de forma emergencial, ampliados neste momento pelos serviços de NOC, previnem eventos de desastre em TI que comprometem a continuidade dos serviços da JF3R, visto que, sem o devido monitoramento integral do ambiente, se está sujeito à exploração de vulneráveis e, por conseguinte, a novos ataques.

3. Plano Inicial do Projeto

Objetivo

Demonstrar a proposta para a contratação de empresa monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center)

Público Alvo

Usuários internos (Desembargadores, Magistrados e Servidores Públicos) e externos que se utilizam das informações dos sistemas processuais e administrativos armazenadas em ativos de infraestrutura de rede.

Análise e Planejamento de Capacidade

A demanda prevista é a contratação de empresa especializada na prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center) na Justiça Federal da 3ª. Região – JF3R.

O Quantitativo a ser registrado será:

Item	Descrição	Unidade	Quantidade Mínima	Quantidade Total
Grupo 1				
1	Subscrição SaaS de solução Rapid 7 IDR Advanced para prestação de Serviços Gerenciados de Monitoramento, Detecção e Notificação de Ataques Cibernéticos – Para 6.500 assets, para 36 (trinta e seis) meses.	Subscrição	1	1
2	Subscrição SaaS de solução Rapid 7 IVM para prestação de Serviços Gerenciados de Gestão de Vulnerabilidades, Riscos e Conformidade de Infraestrutura – Para 600 assets, para 36 (trinta e seis) meses, para 36 (trinta e seis) meses.	Subscrição	1	1
3	Subscrição SaaS de solução Rapid 7 AppScan para prestação de Serviços Gerenciados de Gestão de Vulnerabilidades de Aplicações Web – Para 3 Aplicações FQDN (Full Qualified Domain Name), para 36 (trinta e seis) meses.	Subscrição	1	1

Item	Descrição	Unidade	Quantidade Mínima	Quantidade Total
4	Subscrição SaaS de solução Rapid 7 InsightConnect - Para 2 workflows, para 36 (trinta e seis) meses.	Subscrição	1	1
Grupo 2				
1	Serviços Gerenciados de Monitoramento de Ambiente Tecnológico e Segurança da Informação – NOC/SOC por 43 (quarenta e três) meses	Serviço	1	1
2	Serviços de Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense de Incidentes de Segurança, sob demanda	Hora	80	800

Para a situação de um novo evento de desastre, faz-se necessária a contratação de 800 (oitocentas) horas para os serviços de Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense de Incidentes de Segurança serão contratados sob demanda e foram estimados considerando que para a operação emergencial de recuperação de desastre do ataque hacker sofrido pela JF3R foram utilizadas cerca de 600 (seiscentas) horas na contratação emergencial.

Embora a atual solução seja justamente para impedir a realização de exploração de alguma vulnerabilidade que resulte em evento de indisponibilidade e/ou sequestro de dados, tem-se que levar em consideração a possibilidade de que a JF3R possa estar sob o foco destes grupos hacker que podem querer realizar uma nova investida no parque tecnológico, tendo em vista que o ataque anterior foi consumado.

Para demandar a contratação das horas, deverá emitir Ordem de Serviço contendo as atividades a serem executadas, total de horas estimadas para a execução de cada atividade.

Os projetos que se utilizam das 800 (oitocentas) horas poderão tem suas atividades gerais estimadas:

- Serviços de preparação, detecção, análise, contenção, erradicação, recuperação em situação emergencial e em pós-incidente: 500 (quinhentas) horas.
- Serviços de recomendações, apoio, assessoria e investigação: 300 (trezentas) horas.

Por se tratarem de atividades de segurança da informação onde o escopo do projeto não pode ser definido, tendo em vista que a motivação é futura, deverá ser

possível redimensionar a estimativa de horas alocada para as atividades gerais acima descritas, desde que justificadas em Ordem de Serviço.

4. Resultado Esperado

Os resultados a serem alcançados com a solução serão:

- **Prover segurança contínua ao parque tecnológico da JF3R:** Mitigar de forma continua, preventiva e reativa, possíveis ameaças ao ambiente computacional da JF3R que possam promover perda de dados.
- **Prover monitoramento contínuo ao parque tecnológico da JF3R:** Monitorar todos os ativos de TIC, visando aplicar as políticas de segurança em um ambiente tecnológico complexo.
- **Controlar individualmente os ativos de TIC:** Controlar individualmente os ativos da JF3R no que tange as vulnerabilidades detectadas e a disponibilidade, promovendo uma política de segurança ativa.
- **Prover robustez:** Prover resiliência e disponibilidade ao ambiente suportado quando por ventura sofra com algum tipo de ataque, mantendo-se funcional e com qualidade.
- **Prover economia dos recursos públicos:** Compor a prestação de serviços com requisitos técnicos mínimos que possam promover a concorrência pública, visando à economia nos recursos financeiros investidos, garantindo que os recursos disponibilizados pelos cidadãos sejam aplicados com eficiência e eficácia.

5. Análise de Requisitos Técnicos

Para a devida execução da solução do projeto faz-se preciso compor a solução com seguintes requisitos:

Tipo de Contratação

- **Nova Licitação**

Não há contratação vigente para o serviço de SOC, que é prestado pela equipe técnica em regime comercial.

Há contratação vigente para o serviço de SOC de caráter emergencial (Dispensa de Licitação n. º 8659875/2022) com prazo de 6 (seis) meses.

- **Contratação via Ata de Registro de Preços**

Tendo em vista a existência de item que será contratado via demanda, a contratação será realizada via Ata de Registro de Preços que será utilizada pelo órgão gerenciador Tribunal Regional Federal da 3ª. Região - TRF3 com vigência de 12 (doze) meses.

Vigência

- **Vigência dos Itens 1,2,3 e 4 do GRUPO 1**: O contrato terá como vigência o prazo de 36 (trinta e seis) meses e 15 (quinze) dias corridos, compreendendo:05 (cinco) dias para entrega , 05 (cinco) dias corridos para emissão do Termo de Recebimento Provisório, 5 (cinco) dias corridos para emissão do Termo de Recebimento Definitivo e 36 (trinta e seis) meses de validade para uso das ferramentas de software por parte da CONTRATANTE.
- **Vigência do Item 1 do GRUPO 2:** O contrato terá como vigência o prazo de 43 (quarenta e três) meses, compreendendo a prestação mensal de serviços por igual período, contados a partir de 01/10/2022 ou, se posterior, após a assinatura do Termo de Contrato.
- **Vigência do Item 2 do GRUPO 2:** O contrato terá vigência de 18 (dezoito) meses a contados partir da sua assinatura, pois trata-se de serviço contratado sob demanda mediante Ordem de Serviço emitida pelo GESTOR DO CONTRATO, visando a execução de atividades de preparação, detecção, análise, contenção, erradicação, recuperação em situação emergencial, entre outras, conforme especificação técnica. A vigência compreende o tempo necessário para execução das atividades selecionadas em Ordem de Serviço, 05 (cinco) dias corridos para emissão do Termo de Recebimento Provisório, 05 (cinco) dias corridos para emissão do Termo de Recebimento Definitivo e 30 (trinta dias) para o

pagamento e também corresponde ao prazo máximo de validade da nota de empenho.

Requisitos da Prestação de Serviços

As especificações técnicas para a plena prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center) são:

1.1. Considerações Gerais:

1.1.1. A CONTRATADA deverá realizar todo o planejamento para implementar a solução, dispondo de todos os recursos necessários (pessoas, materiais e ferramentas), sem ônus adicional à CONTRATANTE.

1.1.2. O acesso às informações do ambiente tecnológico de TIC da CONTRATANTE será de responsabilidade da CONTRATADA e poderá ser realizado através de conectividade por meio de VPN ou instalação de link dedicado, com velocidade compatível ao tráfego utilizado, em Data Center da CONTRATANTE.

1.1.2.1. Na comunicação dos dados trafegados deve ser garantida a integridade, confidencialidade e autenticidade das informações trafegadas.

1.2. Item 1: Subscrição de ferramentas software:

Software de Serviços Gerenciados de Segurança da Informação:

A CONTRATADA deverá implementar software automatizado corporativo, instalados em NUVEM ou em DATACENTER da CONTRATANTE, que permitam o monitoramento dos ativos e serviços de TIC visando suportar os Serviços Gerenciados de Segurança da Informação – SOC.

O gerenciamento de segurança da informação dos ativos de TIC será realizado pelas plataformas:

Plataforma Rapid 7 IDR Advanced: Para prestação de serviços gerenciados de monitoramento, detecção e notificação de ataques cibernéticos para 6.500 ativos de TIC.

Plataforma Rapid 7 IVM: Para prestação de serviços gerenciados de gestão de vulnerabilidades, riscos e conformidade de infraestrutura para 600 ativos de TIC.

Plataforma Rapid 7 AppScan: Para prestação de Serviços Gerenciados de Gestão de Vulnerabilidades de Aplicações Web para 3 Aplicações FQDN (Full Qualified Domain Name.

Plataforma Rapid 7 InsightConnect: Para 2 workflows.

As ferramentas de softwares que compõem o ITEM 2 deverão ser licenciadas junto aos seus devidos FABRICANTES e com suporte ativo em regime 24 (vinte e quatro) horas x 7 (sete) dias da semana durante a vigência do contrato.

A CONTRATADA é responsável, durante a vigência contratual, por dar manutenção e atualizar as versões dos softwares, mantendo sempre a versão mais estável disponível pelo FABRICANTE, bem como acionar o suporte do Fabricante, caso se faça necessário.

A CONTRATADA deverá garantir que as ferramentas de software que darão o suporte à prestação de serviços da solução não irão indisponibilizar e/ou degradar o funcionamento dos Ativos de TIC do ambiente tecnológico da CONTRATANTE.

1.3. Item 2: Serviços Gerenciados de Monitoramento de Ambiente Tecnológico e Segurança da Informação – NOC/SOC:

Características Gerais:

O NOC/SOC deve ser planejado pela CONTRATADA em conformidade com as melhores práticas de gerenciamento de serviços de TIC.

O NOC/SOC deve estar disponível em regime integral de 24 (vinte e quatro) horas x 7 (sete) dias na semana e em feriados.

O NOC/SOC deverá operar remotamente em ambiente da CONTRATANTE.

A equipe de colaboradores que operam no NOC/SOC deve ser capacitada tecnicamente e dimensionada pela CONTRATADA de modo a atender todos os requisitos técnicos deste Termo de Referência.

Atividades do NOC/SOC:

Executar rotinas e procedimentos técnicos diários de modo a prevenir/detectar incidentes/problemas no ambiente tecnológico de TIC da CONTRATANTE de forma proativa.

Manter os softwares que compõem a solução sempre com informações atualizadas e fidedignas do ambiente tecnológico de TIC da CONTRATANTE.

Promover o Gerenciamento de Incidente, realizando a comunicação, identificação, tratamento, resolução e/ou escalonamentos de todos os alertas oriundos do ambiente tecnológico de TIC da CONTRATANTE, integrando as equipes necessárias pelo atendimento.

Promover o Gerenciamento de Problema, realizando a comunicação, identificação, tratamento, resolução e/ou escalonamentos necessários de todos os alertas oriundos do ambiente tecnológico de TIC da CONTRATANTE, integrando as equipes necessárias pelo atendimento.

Realizar a abertura de chamado junto às empresas contratadas pela CONTRATANTE em caso de indisponibilidade e/ou degradação do ambiente tecnológico da CONTRATANTE, integrando as equipes necessárias pelo atendimento.

Apresentar relatórios gerais oriundos dos sistemas que compõem a solução em qualquer tempo e sempre que solicitado pela CONTRATANTE.

Realizar atividades de liberação de Sistemas Críticos:

Executar e/ou Acompanhar a homologação e a liberação das atualizações de aplicações críticas que suportam o negócio da CONTRATANTE (Ex.: PJe-1G, PJe-2G, etc.), conforme solicitado pela CONTRATANTE.

Tais atividades deverão ser detalhadas, em modo passo a passo, em documento fornecido pela CONTRATADA e poderão ser executadas aos fins de semana e fora do horário comercial.

Tais atividades poderão ser executadas após o horário comercial, inclusive aos finais de semana, em regime presencial e/ou remoto.

A CONTRATADA não poderá alegar indisponibilidade de profissionais para a execução dos trabalhos programados, desde que comunicada pela CONTRATANTE com até 12 (doze) horas de antecedência da execução das atividades.

Serviços Gerenciados de Monitoramento de Ambiente Tecnológico - NOC:

Composição dos serviços gerenciados de monitoramento de ambiente tecnológico:

Monitoramento de Rede.

Monitoramento de Servidores.

Monitoramento de Nuvem.

Monitoramento de Máquina Virtual.

Monitoramento de Aplicativos.

Monitoramento de Banco de Dados.

A CONTRATADA deverá monitorar o parque tecnológico utilizando-se da ferramenta atual em produção.

No presente, a ferramenta atual em produção é a plataforma ZABBIX Community, cabendo a CONTATANDA adequar o seu corpo técnico em caso de troca de plataforma por parte da CONTRATANTE.

O Gerenciamento administrativo, bem como a abrangência de itens de configuração alvo da ferramenta de monitoramento do parque tecnológico será de responsabilidade da CONTRATANTE.

Serviços Gerenciados de Segurança da Informação - SOC:

Composição dos serviços gerenciados de monitoramento, detecção e notificação de ataques cibernéticos para resposta a incidentes:

Inclui Subscrição para até 6.500 servidores, estações, ativos de rede, ativos de segurança e Cloud Computing, via solução automatizada de SIEM/XDR.

Coleta e Correlação de Eventos de Ativos por meio de SIEM (Security Information Event Management / XDR (eXtended Detection and Reponse).

SOAR (Orquestração, automação e resposta de segurança) para Active Directory e Agentes Instalados.

Módulo NTA (Network Trafic Analysis) para tráfego não criptografado.

Detecção e Análise de Comportamento Anômalo, por meio de SIEM com capacidades de UEBA (User and Entity Behavior Analysis).

Dashboard de Monitoramento, Alertas, Incidentes e Investigações.

Desenvolvimento e/ou adequação de Processo de Monitoramento de Segurança da Informação.

Integração SIEM/XDR e Microsoft AD/Azure, quando licenciados.

Franquia 40 horas para Resposta Proativa a Incidentes de Segurança.

Composição dos Serviços Gerenciados de Red Team:

Testes de Invasão de Rede Externa (Perímetro Internet): Trimestral.

Testes de Invasão de Rede Interna: Semestral.

Testes de Email-Phishing: Semestral.

Password & Credential Assessment: Mensal.

As análises e testes serão realizados tanto por meio de ferramentas automatizadas quanto atuação de equipe especializada de Red Team.

As vulnerabilidades identificadas serão registradas e publicadas em um sistema WEB, com acesso seguro, criptografado e devidamente autenticado. Cada vulnerabilidade registrada no sistema deverá estar acompanhada das informações necessárias para a sua adequada correção.

Composição dos serviços gerenciados de gestão de vulnerabilidades, riscos e conformidade de infraestrutura e aplicações web:

Inclui Subscrição para até 600 servidores, ativos de rede, ativos de segurança e cloud computing, via solução de gestão de vulnerabilidades - varredura contínua, modelo SaaS.

Inclui subscrição para até 3 (três) aplicações WEB, via solução de gestão de vulnerabilidades – varredura contínua, modelo SaaS.

Gestão contínua de vulnerabilidades, conformidade e riscos.

Varredura contínua de vulnerabilidades, incluindo servidores, ativos críticos e perímetro Internet.

Dashboard de riscos e conformidade (CIS Compliance).

Dashboard de projetos de ações de remediação e metas.

Composição dos serviços de Monitoramento de Informações na Deep Web:

Serviços de monitoramento de informações na Dark/Deep Web, por meio de plataforma de busca automatizada e serviços para 02 (dois) domínios da CONTRATANTE e um conjunto de até 100 derivações (emails, domínios, palavras-chave, credenciais).

Monitoramento de atividades na Dark/Deep Web, relacionadas a domínios, URLs, IPs, hashes, credenciais, e-mails, informações sensíveis, dentre outros.

Avaliação da exposição da marca.

Rastreio de comercialização de dados.

Investigação de origens de vazamentos:

Grupos de hackers.

Ameaças em fóruns.

Salas de chat reservadas.

Carteiras de bitcoins e endereços.

Registros históricos.

Notificação dos eventos monitorados.

Deve ser capaz de monitorar pelo menos 4 redes, incluindo: Telegram, TOR, ZeroNet, IRC.

Deve ter a capacidade de pesquisar sem expor a empresa na darknet.

Deve pesquisar conteúdo de sites que exigem autenticação ou outros desafios.

Deve ser capaz de coletar conteúdo em mais de 50 idiomas.

Deve ter a capacidade de enviar solicitação de coleta para sites sugeridos pelo contratante.

Deve disponibilizar acesso ao contratante via interface gráfica de usuário, bem como via API.

Mostrando a origem exata de todos os documentos.

Deve ser capaz de salvar pesquisas e gerar alertas.

Deve incluir lógica de pesquisa booleana e pesquisa de palavras-chave.

Recomendações para mitigações sobre os riscos e ameaças.

Composição dos serviços de administração, atualização, manutenção, monitoramento e suporte, em sua plenitude, das ferramentas Symantec Endpoint Security Complete - SESC nos ENDPOINTs, já licenciada pela CONTRATANTE, compreendendo, mas não se restringindo somente, as seguintes atividades:

Verificar o status do Site no SEPM (Symantec Endpoint Protection Mananger), bastando gerar um relatório para certificar-se do correto funcionamento dos servidores de rede.

Verificar as definições de vacina do SEPM, fazendo o acompanhamento diário das atualizações.

Verificar os logs e alertas do SESC, com especial atenção aos logs gerados pelo antivírus, acionando a CLRI através de chamados, caso o mesmo não consiga remover alguma ameaça detectada.

Identificar no relatório do gerenciador SESC quais são os equipamentos que estão com o Auto-Protect e o Network Threat Protection desativados, enviando o comando para ativação a fim de corrigir o problema.

Gerar relatórios semanais do SESC.

Realizar a limpeza manual dos computadores que estão com IPs e nomes duplicados.

Verificar se o backup da base de dados no SEPM programado para rodar todo domingo foi concluído com sucesso.

Realizar um scan na rede através do recurso de descoberta no SESC com a finalidade de encontrar computadores com o antivírus sem gerenciamento ou máquinas sem antivírus.

Enviar pacotes de atualizações e/ou de definições para os clientes que estiverem com estas desatualizadas.

Gerar relatórios mensais com os quantitativos de ENDPOINTs que apresentaram problemas e tiveram que ser resolvidos através de chamados.

Canal de Atendimento:

Deverá ser disponibilizado um Canal de Atendimento em regime integral de 24 (vinte e quatro) horas em 7 (sete) dias na semana e em feriados.

O Canal de Atendimento deverá ser implementado por meio de ferramentas de comunicação disponibilizadas pela CONTRATADA de modo a garantir a disponibilidade de contato, sendo, no mínimo:

Via plataforma Microsoft Teams.

Via aplicativo WhatsApp.

Via E-mail.

Via telefone, com a disponibilização de 2 (dois) números de contato.

Outros canais de comunicação poderão ser também disponibilizados pela CONTRATADA, desde que com a anuência da CONTRATANTE e sem prejuízo ao regime de atendimento especificado neste Termo de Referência.

1.4. Item 3: Serviços de Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense de Incidentes de Segurança:

Consistem em serviços de preparação, detecção, análise, contenção, erradicação, recuperação em situação emergencial e em pós-incidente, por meio de banco de horas de 800 (oitocentas) horas a serem consumidas durante a vigência contratual, sob demanda da CONTRATANTE, bem como:

Recomendação de medidas para mitigação dos ataques e ameaças detectadas (adequação de regras de firewall, proteção de endpoint, atualização de sistema operacional, dentre outros).

Apoio na implementação de ações de remediação e/ou mitigação de vulnerabilidades de segurança da informação.

Assessoria na aplicação de atualizações de segurança no ambiente, quando pertinente.

Assessoria para restauração do ambiente ao seu estado normal de operação.

Definir, propor e executar uma estratégia para a mitigação e contenção do ataque.

Investigar e identificar no ambiente alvo ameaças persistentes ou vulnerabilidades passíveis de exploração, propondo soluções para a sua mitigação e, quando possível, realizar o tratamento das ameaças identificadas.

Identificar as vulnerabilidades exploradas pelo atacante que permitiram o comprometimento do ambiente.

Monitorar o ambiente, após a sua restauração, para identificar e conter novos ataques.

Responder a eventuais novos ataques cibernéticos.

Composição dos Serviços Gerenciados de Red Team Pós Incidente:

Os serviços de Red Team Pós Incidente visam apoiar as atividades de Resposta Emergencial a Incidentes de Cibernéticos, e abrangem as seguintes atividades:

Teste de invasão do perímetro Internet e identificação de vulnerabilidades persistentes no ambiente.

Serviços de Password Assessment, para identificação de credenciais frágeis de usuário e senha de domínio AD, potencialmente exploradas por atacantes e utilizadas para comprometer o ambiente.

Níveis de Serviço

Os Níveis de Serviço estão relacionados aos Níveis de Severidade que se baseiam na relação entre IMPACTO e URGÊNCIA, sendo:

— IMPACTO relaciona-se com a abrangência do ocorrido, ou quantos usuários estão sendo afetados, classificando-se em:

- Alto: Impacta um site inteiro ou todos os usuários.
- Médio: Impacta uma equipe inteira ou um pequeno grupo de usuários.
- Baixo: afeta um único usuário ou um número desconhecido de usuários.

— URGÊNCIA relaciona-se a velocidade em que o serviço precisa ser restaurado, classificando-se em:

- Alto: Precisa ser restaurado imediatamente, pois impede que uma função ou serviço principal do negócio seja executado.
- Médio: Pode ser restaurado em uma janela de tempo maior que a de urgência alta, pois restringe a eficácia de uma função ou serviço;
- Baixo: Pode ser restaurado de maneira planejada, pois possui impacto menor nas tarefas do dia-a-dia.

O cruzamento dessas duas variáveis provê a SEVERIDADE:

SERVERIDADE (IMPACTO/URGÊNCIA)		URGÊNCIA		
		Alto	Médio	Baixo
IMPACTO	Alto	Alta	Alta	Médio
	Médio	Alta	Média	Baixa
	Baixo	Média	Baixa	Baixa

Os níveis mínimos de serviços são critérios objetivos e mensuráveis que visam aferir e avaliar diversos fatores relacionados com os serviços contratados, quais sejam: qualidade, desempenho, disponibilidade, abrangência/cobertura e segurança.

As metas devem ser medidas do primeiro ao último dia de cada mês.

Os prazos de atendimento baseiam-se no tipo de SEVERIDADE:

Severidade	Tempo de resposta	Tempo de atendimento
ALTA	15 Minutos	30 Minutos
MÉDIA	2 Horas	4 Horas
BAIXA	4 Horas	24 Horas

Os prazos de atendimento são contados a partir do registro das requisições, sendo suspensos em situações que dependam de algum fator externo a CONTRATADA.

Fica acordado entre a CONTRATANTE e a CONTRATADA o cumprimento de 90% dos atendimentos dentro dos tempos especificados.

Acompanhamento Contratual

O acompanhamento contratual se dará através de:

- **Reunião de Abertura do Projeto:** A CONTRATANTE e a CONTRATADA realizarão a Reunião de Abertura do Projeto, visando dispor sobre

os detalhes da implantação da solução em até 15 (quinze) dias após a assinatura do Termo de Contrato.

A CONTRATADA enviará por correio eletrônico a ATA da Reunião Abertura do Projeto para aprovação da CONTRATANTE.

- **Reunião:** A CONTRATANTE e a CONTRATADA realizarão reuniões de acompanhamento, visando dispor sobre os detalhes da prestação dos serviços sempre que necessário.

Apresentar equipe qualificada em segurança da informação que detenham, individualmente ou em conjunto, certificados ou certificações vigentes abaixo:

- Rapid7 InsightIDR Certified Specialist.
- Rapid7 InsightIVM Certified Specialist.
- Check Point Certified Security Administrator – CCSA.
- Symantec Certified Specialist.
- CompTIA PenTest+.

Deverá ser comprovado vínculo entre os profissionais detentores dos certificados e a empresa, seja na qualidade de sócio, através da cópia do contrato social ou ata de assembleia; como funcionário, através de cópia do livro de registro de funcionários ou cópia da carteira de trabalho contendo as respectivas anotações de contrato de trabalho; ou como contratado, por meio de contrato de prestação de serviços.

A CONTRATADA enviará por correio eletrônico a ATA da Reunião Abertura do Projeto para aprovação da CONTRATANTE.

- **Evento: Relatório de Atividades Interventivas – Item 2 do GRUPO 2:**

Deverá ser entregue o Relatório de Atividades Interventivas elencando detalhadamente as ações relacionadas a eventos de SEVERIDADE classificados como Médio e Alto ou quaisquer atividades desenvolvidas, bem como a quantidade de horas utilizadas, que impliquem na contratação do ITEM 2 do GRUPO 2, em até 10 (dez) dias corridos, contados a partir da finalização dos serviços realizados.

- **Evento: Relatório de Atividades Diário – Item 1 do GRUPO 2:**

Deverá ser entregue o Relatório de Atividades Diário elencando detalhadamente todos os eventos ocorridos e as ações adotadas pela equipe ao

longo das últimas 24 (horas) do dia anterior, relacionadas a eventos de SEVERIDADE classificados como Baixo, Médio e Alto até as 10:00 (dez) horas do dia seguinte, cumprindo esta programação mesmo em de finais de semana e feriados.

- **Evento: Relatório de Atividades Mensal – Item 1 do GRUPO 2**

Deverá ser entregue o Relatório de Atividades Mensal elencando detalhadamente todos os eventos ocorridos e as ações adotadas pela equipe ao longo do mês, relacionadas a eventos de SEVERIDADE classificados como Baixo, Médio e Alto em até 5 (cinco) dias corridos, contados a partir do último dia do mês.

Repasse de Conhecimento

A CONTRATADA deverá realizar repasse de conhecimento a equipe técnica da CONTRATANTE, via remoto, com carga horária de até 40 (quarenta horas), discorrendo de forma intermediária sobre as seguintes ferramentas de software que compõem a solução:

- Plataforma Rapid 7 IDR Advanced.
- Plataforma Rapid 7 IVM.
- Plataforma Rapid 7 AppScan.
- Plataforma Rapid 7 InsightConnect.

A CONTRATADA deverá emitir certificado com nome dos participantes, carga horária total e ementa dos assuntos abordados.

Qualificação Técnica

Atestado (s) fornecido (s) por Pessoa Jurídica de Direito Público ou Privado, comprovando a prestação de serviços em ambientes corporativos de porte médio à grande, com no mínimo 1.000 ativos, que englobem no mínimo o seguinte escopo de trabalho:

- Serviços de Monitoramento de ataques cibernéticos.
- Serviços de Gestão de Vulnerabilidades.
- Serviços de Teste de Invasão.

- Serviços de Teste de Email Phishing.
- Serviços de Resposta a Incidentes Cibernéticos.

Justificativa I: Tendo em vista a alta complexidade da solução e da especificidade dos profissionais técnicos alocados para a prestação dos serviços, a exigência de atestado de capacidade técnica tem por objetivo comprovar a experiência anterior na realização de serviços similares, proporcionais à dimensão e complexidade do objeto a ser executado, visando assegurar que a Administração contratará empresas que possam desincumbir-se adequadamente do objeto contratado.

Justificativa II: A comprovação no atestado de capacidade técnica do escopo de atividades executadas pela empresa se deve ao fato de que nem toda empresa de segurança de TI provê todos os serviços especializados em seu portfólio de trabalho que são objeto desta contratação.

Penalidades

Pela inexecução total ou parcial do objeto deste Termo de Referência, poderão ser aplicadas, além das previstas em Termo de Contrato, as seguintes sanções:

- **Advertência por escrito:** Quando do não cumprimento de quaisquer das obrigações deste Termo de Referência, conforme avaliação técnica da CONTRATANTE.
- **Multa por:**
  - **Reincidência em advertência por escrito:**
    - De 1% (um por cento) do valor mensal da prestação de serviços para os casos de reincidência por 2 (duas) vezes de advertência por escrito para a mesma falta.
    - De 10% (dez por cento) do valor mensal da prestação de serviços para os casos de reincidência superior a 2 (duas) vezes de advertência por escrito para a mesma falta.
  - **Não cumprimento de SLA Mensal:**
    - De 1% (um por cento) do valor mensal da prestação de serviços referentes ao ITEM 2, para os casos de não cumprimento de SLA Mensal.

- De 10% (dez por cento) do valor mensal da prestação de serviços referentes ao ITEM 2, para os casos de não cumprimento de SLA Mensal, por 2 (dois) meses consecutivos.
- De 10% (dez por cento) do valor contratual da prestação de serviços referentes ao ITEM 2, para os casos de não cumprimento de SLA Mensal, a partir do 3º (terceiro) mês consecutivo.
- A partir do 4º (quarto) mês consecutivo de não cumprimento do SLA Mensal, poderá ser configurado pela CONTRATANTE a inexecução total do ITEM 2, sem prejuízo da multa.

- **Não cumprimento de adequação da equipe técnica:**

- De 1% (um por cento) do valor mensal da prestação de serviços referentes ao ITEM 2, por mês, para os casos de não adequação da equipe técnica, enquanto perdurar o não cumprimento.
- A partir do 3º (terceiro) mês consecutivo de não adequação da equipe técnica, poderá ser configurado pela CONTRATANTE a inexecução total do ITEM 2, sem prejuízo da multa.

- **Indisponibilidade dos serviços de NOC/SOC:**

- De 0,1% (um décimo por cento) do valor mensal da prestação de serviços referentes ao ITEM 2, por dia, para os casos de total indisponibilidade dos serviços prestados no ITEM 2, enquanto a indisponibilidade durar até 2 (dois) dias corridos.
- De 1% (um por cento) do valor mensal da prestação de serviços referentes ao ITEM 2, por dia, para os casos de total indisponibilidade dos serviços descritos no ITEM 2, enquanto a indisponibilidade for superior à 2 (dois) dias corridos.
- A partir do 10º (décimo) dia de indisponibilidade consecutiva, poderá ser configurado pela CONTRATANTE a inexecução total do ITEM 2, sem prejuízo da multa.

As penalidades de Multa de eventos diversos serão consideradas independentes entre si.

6. Análise de Investimento

Conforme pesquisa realizada, concluímos que os valores ofertados a administração são condizentes com o praticado pelo mercado:

- Item 1,2,3 e 4 do GRUPO 1: Subscrição de ferramentas de software por 36 (trinta e seis) meses:

		INTELLIWAY Proposta		TRF 3ªR CONTRATO 04.004.10.2022	
Item	**Descrição**	**Valor Total para 12 meses**	**Valor para 36 meses**	**Valor Total para 12 meses**	**Valor para 36 meses**
1	Subscrição SaaS de solução Rapid 7 IDR Advanced para prestação de Serviços Gerenciados de Monitoramento, Detecção e Notificação de Ataques Cibernéticos – Para 6.500 assets, para 12 (doze) meses	R$ 1.561.134,71	R$ 4.683.404,13	R$ 1.502.957,58	R$ 4.508.872,74
2	Subscrição SaaS de solução Rapid 7 IVM para prestação de Serviços Gerenciados de Gestão de Vulnerabilidades, Riscos e Conformidade de Infraestrutura – Para 600 assets, para 12 (doze) meses	R$ 105.335,51	R$ 316.006,53	R$ 101.410,08	R$ 304.230,24
3	Subscrição SaaS de solução Rapid 7 AppScan para prestação de Serviços Gerenciados de Gestão de Vulnerabilidades de Aplicações Web – Para 3 Aplicações FQDN (Full Qualified Domain Name), para 12 (doze) meses	R$ 50.918,70	R$ 152.756,10	R$ 49.021,17	R$ 147.063,51
4	Subscrição SaaS de solução Rapid 7 InsightConnect - Para 2 workflows, para 12 (doze) meses	R$ 152.756,18	R$ 458.268,54	R$ 147.063,58	R$ 441.190,74

- Item 1 do GRUPO 2: Serviços Gerenciados de Monitoramento de Ambiente Tecnológico e Segurança da Informação – NOC/SOC por 43 meses:

INTELLIWAY Proposta		CDTN CONTRATO N°: 01/2022/CDTN/DIGEA	
Valor Unitário mensal	**Valor Total**	**Valor Unitário mensal**	**Valor Total**
R$ 165.320,86	R$ 7.108.796,98	R$ 66.458,30	R$ 2.857.706,90
TRT 17ªR PAe n.º 0000292-72.2022.5.17.0500		**TRF 3ªR CONTRATO 04.004.10.2022**	
Valor unitário mensal	**Valor Total**	**Valor unitário mensal**	**Valor Total**
R$ 192.335,00	R$ 8.270.405,00	R$ 200.935,87	R$ 8.640.242,41

- Item 2 do GRUPO 2: Serviços de Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense de Incidentes de Segurança, 800h sob demanda:

INTELLIWAY Proposta		TRT 17ªR PAe n.º 0000292-72.2022.5.17.0500		TRF 3ªR CONTRATO 04.004.10.2022	
Valor unitário por hora	**Valor Total**	**Valor unitário por hora**	**Valor Total**	**Valor unitário por hora**	**Valor Total**
R$ 495,00	R$ 396.000,00	R$ 275,00	R$ 220.000,00	R$ 275,00	R$ 220.000,00

- Valor total estimado da contratação:

			VALOR TOTAL A SER CONTRATADO	
Item	**Descrição**	**Quantidade**	**Valor unitário**	**Valor total**
		Grupo 1		
1	Subscrição SaaS de solução Rapid 7 IDR Advanced para prestação de Serviços Gerenciados de Monitoramento, Detecção e Notificação de Ataques Cibernéticos – Para 6.500 assets, para 36 (trinta e seis) meses.	1	R$ 4.596.138,44	R$ 4.596.138,44
2	Subscrição SaaS de solução Rapid 7 IVM para prestação de Serviços Gerenciados de Gestão de Vulnerabilidades, Riscos e Conformidade de Infraestrutura – Para 600 assets, para 36 (trinta e seis) meses.	1	R$ 310.118,39	R$ 310.118,39
3	Subscrição SaaS de solução Rapid 7 AppScan para prestação de Serviços Gerenciados de Gestão de Vulnerabilidades de Aplicações Web – Para 3 Aplicações FQDN (Full Qualified Domain Name), para 36 (trinta e seis) meses.	1	R$ 149.909,81	R$ 149.909,81
4	Subscrição anual SaaS de solução Rapid 7 InsightConnect - Para 2 workflows, para 36 (trinta e seis) meses.	1	R$ 449.729,64	R$ 449.729,64
			TOTAL DO GRUPO 1	**R$ 5.505.896,27**
		Grupo 2		
1	Serviços Gerenciados de Monitoramento de Ambiente Tecnológico e Segurança da Informação – NOC/SOC por 43 (quarenta e três) meses	43	R$ 178.827,93	R$ 7.689.600,99
2	Serviços de Resposta a Incidentes Cibernéticos, Investigação, Mitigação e Análise Forense de Incidentes de Segurança, sob demanda - horas	800	R$ 275,00	R$ 220.000,00
			TOTAL DO GRUPO 2	**R$ 7.909.600,99**
			TOTAL DA CONTRATAÇÃO	**R$ 13.415.497,26**

7. Parecer Final

Com base nos diversos benefícios apresentados neste estudo, tendo em vista também a alta relevância destes serviços para o pleno exercício jurisdicional da JF3R, existindo disponibilidade financeira, sugerimos a contratação de empresa especializada na prestação de serviços de monitoramento de ambiente tecnológico, prevenção de ameaças cibernéticas e resposta à incidentes de segurança da informação através da implantação de NOC (Network Operations Center) e SOC (Security Operations Center) na Justiça Federal da 3ª. Região – JF3R.

Simone Sanches Alves:3311
Assinado de forma digital por Simone Sanches Alves:3311
Dados: 2022.08.16 21:51:17 -03'00'

VINICIUS SOUZA BARBOSA:3341
Assinado de forma digital por VINICIUS SOUZA BARBOSA:3341
Dados: 2022.08.17 11:37:03 -03'00'

MARCOS ANTONIO DE AGUIAR:3337
Assinado de forma digital por MARCOS ANTONIO DE AGUIAR:3337
Dados: 2022.08.17 11:54:08 -03'00'

DANIEL HENRIQUE GUIMARAES:3624
Assinado de forma digital por DANIEL HENRIQUE GUIMARAES:3624
Dados: 2022.08.17 17:40:19 -03'00'