PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2.16. Para detectar incidentes, a solução também deverá suportar o recebimento e processamento de eventos de tráfego de rede e, opcionalmente, flow de rede, provendo as seguintes informações, no mínimo:

- 2.16.1. Sistemas com maior atividade baseada em volume de tráfego;
- 2.16.2. Principais aplicações e protocolos trafegados, baseado em volume de dados enviados e recebidos entre endpoints da rede;
- 2.16.3. Atividades de rede baseada em porta de destino e endereços de origem e destino;
- 2.16.4. Relação dos usuários ou ativos que mais consomem banda de rede, baseado em volume de tráfego.
- 2.16.5. Servidores DNS em uso;
- 2.16.6. Relação das principais aplicações em uso na rede;
- 2.16.7. Identificação de picos de consumo de banda de acesso à rede;
- 2.16.8. Relação de dispositivos, servidores e serviços que operam na rede.

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

- 2.17.1. De forma nativa (sem a necessidade de customização de parsers):
  - 2.17.1.1. Checkpoint para proteção de perímetro (Firewall);
  - 2.17.1.2. Fortinet FortiGate para proteção de perímetro (Firewall);
  - 2.17.1.3. Forcepoint para proteção de perímetro (Firewall);
  - 2.17.1.4. Microsoft Active Directory para serviços de diretório.
- 2.17.2. De forma nativa (sem a necessidade de customização de parsers) ou não:
  - 2.17.2.1. Open LDAP para serviços de diretório;
  - 2.17.2.2. OpenVPN;
  - 2.17.2.3. Citrix;
  - 2.17.2.4. RDP e RDPWeb;
  - 2.17.2.5. Senha Segura para serviços de gerenciamento de acesso privilegiado;
  - 2.17.2.6. Cyberark para serviços de gerenciamento de acesso privilegiado
  - 2.17.2.7. Hashicorp Vault e Hashicorp Boundary para serviços de gerenciamento de acesso privilegiado;
  - 2.17.2.8. Keycloak para gerenciamento de identidade e acesso;
  - 2.17.2.9. midPoint para segurança de identidades (identity security);
  - 2.17.2.10. ForeScout CounterACT (eyeSight e eyeControl) para serviços de NAC (Network Access Control);
  - 2.17.2.11. Loqed;
  - 2.17.2.12. Varonis;
  - 2.17.2.13. IBM Spectrum Protect Plus para proteção de dados;
  - 2.17.2.14. Kaspersky para proteção de endpoint;
  - 2.17.2.15. Blackberry Cylance para proteção de endpoint.
  - 2.17.2.16. Check Point Harmony para proteção de endpoint;
  - 2.17.2.17. Tenable One para gerenciamento de exposição (exposure management platform);
  - 2.17.2.18. Tenable.ep / Nessus para gerenciamento de vulnerabilidades;
  - 2.17.2.19. Tenable.ad para proteção do Active Directory;
  - 2.17.2.20. Trivy para varredura de vulnerabilidades;

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2.17.2.21. VMware/vCenter para virtualização de máquinas;

2.17.2.22. VMware/Horizon para virtualização de estações de trabalho;

2.17.2.23. Hyper-V para virtualização de máquinas;

2.17.2.24. Ovirt para virtualização de máquinas;

2.17.2.25. Docker e Kubernetes;

2.17.2.26. Apache HTTP Server;

2.17.2.27. HAProxy;

2.17.2.28. Ingress;

2.17.2.29. Nginx;

2.17.2.30. Switches Cisco MDS;

2.17.2.31. Switches H3C;

2.17.2.32. Switches HP;

2.17.2.33. Switches Huawei;

2.17.2.34. Roteadores Cisco;

2.17.2.35. Roteadores Juniper;

2.17.2.36. Roteadores MikroTik;

2.17.2.37. Access Points Aruba;

2.17.2.38. Access Points Ruckus;

2.17.2.39. Controladoras Virtuais Aruba;

2.17.2.40. Bacula para serviços de backup;

2.17.2.41. Commvault (software de backup);

2.17.2.42. Veeam (software de backup);

2.17.2.43. Storage Huawei;

2.17.2.44. Storage IBM;

2.17.2.45. TSM Server IBM Spectrum Protect para serviços de backup;

2.17.2.46. Dell EMC Data Domain;

2.17.2.47. Dell EMC Isilon.

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

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

2.18.1.1. AWS CloudTrail, via SQS ou API;

2.18.1.2. Google Cloud Platform, via API;

2.18.1.3. Google Workspace/Google Apps, via API;

2.18.1.4. Microsoft Office 365, via API.

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

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

2.19.1.1. Windows 7;

2.19.1.2. Windows 8.1;

2.19.1.3. Windows 10;

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2.19.1.4. Windows 11;
2.19.1.5. Windows Server 2008 R2;
2.19.1.6. Windows Server 2012;
2.19.1.7. Windows Server 2012 R2;
2.19.1.8. Windows Server 2016;
2.19.1.9. Windows Server 2019;
2.19.1.10. Windows Server 2022;
2.19.1.11. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.4;
2.19.1.12. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 8.5;
2.19.1.13. Red Hat Enterprise Linux / Oracle Enterprise Linux / Rocky Linux 9.0;
2.19.1.14. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 7;
2.19.1.15. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.0;
2.19.1.16. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.1;
2.19.1.17. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.2;
2.19.1.18. Red Hat Enterprise Linux / Oracle Enterprise Linux / CentOS 8.3;
2.19.1.19. Amazon Linux;
2.19.1.20. Debian Linux;
2.19.1.21. Ubuntu Linux.

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

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

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

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

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

2.24.1. Requisição a domínio suspeito;
2.24.2. Execução de processos suspeitos;
2.24.3. Requisição de dados de registro do sistema de nome de domínio (DNS);
2.24.4. Comunicação com servidores Command & Control;
2.24.5. Tentativa de desabilitar recursos de Sysmon;
2.24.6. Execução de processos LSASS (Local Security Authority Subsystem Service) com objetivo de detectar dump de memória para acessar possíveis credenciais armazenadas;
2.24.7. Detecção do uso de msrsc.exe - Microsoft Terminal Services Client;
2.24.8. Detecção do uso de comandos estruturados consistentes pela ferramenta Impacket e Impacket-Obfuscation;
2.24.9. Detecção de atividade de linha de comando da execução da função GetSystem, usada pelo Meterpreter ou Cobalt Strike;
2.24.10. Detecção de execução do Mimikatz e variações;

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

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

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

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

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

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

2.29. A solução deve permitir o enriquecimento de dados relacionados a endereços IPs, buscando informações adicionais em fontes de OSINT (Open Source Intelligence).

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

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

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

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

2.31. A solução deve possuir nativamente a capacidade de "deception" ou permitir que se implemente capacidade similar por meio de ferramenta complementar e integrada a solução proposta, possibilitando a marcação de ativos, credenciais, usuários e arquivos específicos como sendo "iscas" a fim de, quando acessados, gerarem alertas, facilitando o monitoramento e auditoria contínuos.

2.31.1. Honeypot: máquina projetada para capturar informações sobre tentativas de acesso e exploração. Deve permitir a instalação de, ao menos, 05 (cinco) máquinas no ambiente;

2.31.1.1. Os honeypots devem ser fornecidos em formato OVA – virtual appliance.

2.31.2. Honey Credential: configuração de um conjunto de credenciais falsas na memória de um ativo;

2.31.3. Honey User: usuário falso que não está associado a uma pessoa real dentro da organização e, portanto, nunca deve ser acessado – monitoramento do Microsoft Active Directory;

2.31.4. Honey File: arquivo falso localizado em um compartilhamento de arquivos de rede.

2.31.5. A solução deve ser capaz de detectar o vetor de entrada da ameaça na rede, identificar o caminho utilizado pelo invasor até o ativo, credencial, usuário ou arquivo específico e apresentar as vulnerabilidades exploradas no ativo (quando for o caso).

2.32. Quando a solução não possuir capacidade de "deception", a capacidade de "Breach and Attack Simulation" (BAS) pode ser apresentada, com os seguintes critérios mínimos:

2.32.1. Caso a funcionalidade seja oferecida como um serviço, as licenças necessárias para a sua execução devem ser baseadas em vetores ou agentes, sendo um para cada tipologia: infraestrutura, network e e-mail; os 03 (três) tipos de licenças devem estar incluídas sem custos adicionais para a CONTRATANTE;

2.32.2. Deve ser executado, pelo menos, mensalmente;

2.32.3. Deve ser executado de forma automatizada, simulando ataques reais, mas que não coloquem em risco o ambiente computacional da CONTRATANTE;

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2.32.4. As simulações devem utilizar diferentes vetores de ataque;

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

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

2.34. A solução deve possuir as funcionalidades de:

2.34.1. Monitoramento de comportamento (behavior monitor);

2.34.2. Controle de aplicação;

2.34.3. Monitoramento de eventos;

2.34.4. Auditoria de alterações no sistema;

2.34.5. Resposta automatizada a ameaças com a possibilidade de, mas não se limitando a, executar as ações propostas no item 2.62.

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

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

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

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

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

2.39.1. Segura e criptografada;

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

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

2.41. A solução deve monitorar, no mínimo:

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

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

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

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

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

2.41.6. Exploração mitigada (exploit mitigated);

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

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

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

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

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

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

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

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

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

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

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

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

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

2.45.2. Identificar quais eventos devem gerar alertas;

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

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

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

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

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

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

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

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

2.51.1. Crítico;

2.51.2. Alto;

2.51.3. Médio;

2.51.4. Baixo.

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

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

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

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

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

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

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

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

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

2.58.1.1. .bat

2.58.1.2. .cfg

2.58.1.3. .conf

2.58.1.4. .config

2.58.1.5. .dll

2.58.1.6. .exe

2.58.1.7. .ini

2.58.1.8. .sys

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

2.59. Para realizar o monitoramento do tráfego de rede, a solução deve ser do tipo passiva e ser instalada em modo off-line na rede, ou seja, não ser um ativo em linha ou permitir o envio de logs e/ou dados de telemetria/de rede através de integração.

2.60. A solução deve ser capaz de inspecionar o tráfego de rede baseado no volume de tráfego em Gbps da CONTRATANTE e realizar a análise dos dados coletados.

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

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

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

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

2.62.1. Envio de e-mails.

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

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

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

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

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

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

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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2.62.4.1. Ser totalmente automática;

2.62.4.2. Aguardar uma interação humana para ser realizada.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

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

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

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

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

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

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

2.86. A solução deve permitir a realização de buscas através de strings parciais, exatas, valores nulos, coringas (wildcards) e caracteres especiais.

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

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

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

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

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

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

2.88.4.1. Alertas e incidentes mais frequentes;

2.88.4.2. Nível de risco do ambiente;

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

2.88.4.4. Top 10 (dez) ativos com incidentes;

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

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

2.88.4.7. Ativos e contas descobertas;

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

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

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

2.88.6.1. Planilha: CSV e/ou Excel;

2.88.6.2. Texto: HTML e/ou PDF.

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

2.91. A solução deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo do console.

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

2.93. A solução deve disponibilizar APIs, com documentação e sem custo adicional, para integração com outras soluções.

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

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

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

2.94.2. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar até 06 (seis) domínios DNS da CONTRATANTE e uma quantidade de no mínimo 500 (quinhentos) termos por domínio.

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

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

2.94.4.1. Na Darknet;

2.94.4.2. Em plataformas de compartilhamento de documentos;

2.94.4.3. Pelas seguintes categorias:

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

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

2.94.4.3.3. Por Geolocalização.

2.94.5. A solução de monitoramento de Deep/Dark Web deve permitir a busca de termos considerando, no mínimo, as seguintes categorias:

2.94.5.1. Domínio DNS;

2.94.5.2. Endereço de e-mail;

2.94.5.3. Endereço Bitcoin;

2.94.5.4. Endereço Ethereum;

2.94.5.5. Endereço MAC;

2.94.5.6. Hash IPFS;

2.94.5.7. IBAN (Número de Conta Bancária Internacional);

2.94.5.8. IP e CIDR;

2.94.5.9. Número de telefone;

2.94.5.10. Número do cartão de crédito;

2.94.5.11. URL.

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

2.94.8. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de filtrar e classificar os resultados das buscas:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.94.10.4. Deve ser capaz de realizar avaliação da exposição da marca e vazamentos de informações na Deep/Dark Web;

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

2.94.10.5.1. Grupos de hackers;

2.94.10.5.2. Ameaças em fóruns;

2.94.10.5.3. Salas de chats reservadas;

2.94.10.5.4. Carteira de bitcoins e endereços;

2.94.10.5.5. Registros históricos.

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

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

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

PAGAMENTO

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

2.96. A emissão do termo de recebimento provisório será feita após a instalação e configuração do console de gerência, dos coletores de logs, dos coletores de tráfego de rede e de agentes em estações de trabalho e em servidores.

2.97. As subscrições deverão 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.

2.98. A emissão do termo de recebimento definitivo será feita após a verificação do perfeito funcionamento do console de gerência, dos coletores de logs, dos coletores de tráfego de rede, de agentes em estações de trabalho, de agentes em servidores e da integração de todos os componentes.

2.99. A quantidade de agentes a serem considerados em cada tipo de ativo nos termos de recebimento provisório e definitivo deve ser acordada na fase de Planejamento e Projeto (item 4.4.1), não sendo superior a 10% do parque computacional da CONTRATANTE.

2.100. A distribuição dos agentes (no restante do parque computacional) para os outros ativos a serem monitorados será de responsabilidade da CONTRATANTE, sem prejuízo do suporte que a CONTRATADA deve fornecer para a realização dessa etapa.

2.101. O pagamento da subscrição deve ser anual, em parcela única, sendo realizado somente após a emissão do termo de recebimento definitivo.

3. ITEM 2 – Requisitos mínimos de treinamento na solução

3.1. A CONTRATADA deve oferecer treinamento contemplando a perfeita instalação, configuração, operação e utilização da solução contratada.

3.2. O treinamento deverá proporcionar aos participantes condições de:

3.2.1. Compreender a arquitetura da solução;

3.2.2. Identificar e configurar os recursos disponibilizados no produto;

3.2.3. Configurar fontes de eventos;

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

3.2.5. Configurar honeypots, quando a solução tiver essa capacidade;

3.2.6. Configurar serviço de Breach and Attack Simulation (item 2.32), quando a solução tiver essa capacidade;

3.2.7. Configurar regras;

3.2.8. Configurar alertas;

3.2.9. Configurar playbooks;

3.2.10. Investigar incidentes;

3.2.11. Pesquisar em logs;

3.2.12. Criar dashboards;

3.2.13. Criar relatórios e agendamento de relatórios;

3.2.14. Gerenciar usuários, funções e permissões;

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

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

3.2.17. Conhecer os procedimentos para abertura de chamados técnicos;

3.2.18. Conhecer os procedimentos para obtenção de atualizações de software.

3.3. Devem ser fornecidos todos os recursos necessários para a realização do treinamento (material didático, equipamentos, instrutor, etc.). Os treinamentos serão realizados nas dependências da CONTRATANTE ou na modalidade EAD, a critério da CONTRATANTE.

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

3.5. O treinamento deve ser o treinamento oficial do fabricante ou com material oficial do fabricante.

3.6. O material didático e demais documentações deverão ser fornecidos, preferencialmente, em Português (Brasil). Em caso de não disponibilidade dessa versão, a mesma deverá ser disponibilizada em Inglês.

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

3.8. O treinamento deverá ser ministrado com carga horária mínima de 40 (quarenta) horas, com fornecimento de certificados a todos os participantes, em papel timbrado da empresa, constando: nome do treinando, identificação do treinamento, carga horária, período de ocorrência e conteúdo programático.

3.9. A critério da CONTRATANTE, o treinamento poderá ser dividido em turmas de, no mínimo, 02 (dois) alunos e, no máximo, 08 (oito) alunos.

3.10. O treinamento deverá ser ministrado em horário definido pela CONTRATANTE, em dias úteis.

3.11. O cronograma do treinamento será definido em conjunto com a CONTRATANTE, na fase de Planejamento e Projeto (item 4.4.1).

PAGAMENTO

3.12. A emissão do termo de recebimento provisório do treinamento será feita após a conclusão do treinamento.

3.13. A emissão do termo de recebimento definitivo do treinamento será feita após a avaliação dos participantes, com o preenchimento da Planilha de Avaliação de Treinamento, devendo ser obtida média superior a 70%, caso contrário a CONTRATANTE poderá solicitar a realização de novo treinamento com a reformulação que achar necessária.

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

4. ITEM 3 – Requisitos mínimos de implantação da solução

4.1. A fase de ativação dos serviços deverá ser conduzida e concluída nos primeiros 45 (quarenta e cinco) dias corridos contados a partir da assinatura do contrato, quando serão executados o planejamento para implantação das ferramentas e a adequação de processos de gestão de segurança cibernética que nortearão a prestação de serviços do Centro de Operações de Segurança Cibernética (SOC).

4.1.1. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 45 (quarenta e cinco) dias corridos, contados a partir da assinatura do contrato, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

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

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

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

4.4.1. Planejamento e Projeto:

4.4.1.1. Reunião de kick-off;

4.4.1.2. Coleta de dados e requisitos complementares;

4.4.1.3. Detalhamento de cronograma;

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

4.4.2. Implantação, Configuração e Ativação da solução:

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

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

4.4.2.3. Instalação e ativação dos coletores de logs e dos coletores de tráfego de rede;

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

4.4.2.5. Testes e homologação.

4.4.3. Definição de Processos e Outras Configurações:

4.4.3.1. Implementação dos processos e recursos propostos;

4.4.3.2. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

4.4.3.3. Configuração e correto funcionamento da coleta, processamento e correlação de logs de eventos em que haja a necessidade de customização de parsers para tal funcionamento (item 2.17.2).

4.4.3.4. Testes e homologação;

4.4.3.5. Desenvolvimento de um plano de continuidade que contemple minimamente a exportação de:

4.4.3.5.1. Base de incidentes em aberto (em tratamento);

4.4.3.5.2. Playbooks implementados.

4.4.4. Treinamento de equipes.

4.4.5. Operação, Sustentação e Melhoria Contínua:

4.4.5.1. Sustentação/On-Going;

4.4.5.2. Reunião mensal;

4.4.5.2.1. Relatórios periódicos;

4.4.5.2.2. Acompanhamento de indicadores;

4.4.5.2.3. Melhoria contínua.

4.5. A lista de soluções constantes nos itens 2.13, 2.17, 2.18 e 2.19 não é exaustiva, de forma que, conforme houver evolução do parque tecnológico ao longo do contrato, a CONTRATADA deve, como parte da operação, sustentação e melhoria contínua da solução (item 4.4.5), realizar a configuração para o correto

funcionamento de parsing (quando houver), coleta, processamento e correlação de logs de eventos gerados pela novas soluções incluídas/alteradas no ambiente computacional.

RESPONSABILIDADES DA CONTRATADA

4.6. São responsabilidades da CONTRATADA:

4.6.1. Prestar os serviços conforme previsto e delimitados por esta especificação, dentro das normas e especificações técnicas aplicáveis à espécie;

4.6.2. Respeitar as normas e regulamentos da CONTRATANTE, inclusive aqueles relativos ao acesso, permanência e trânsito de pessoas e materiais, no estabelecimento desta, as quais deverão lhe ser fornecidas previamente e por escrito;

4.6.3. Observar integralmente a legislação e normas infralegais aplicáveis aos serviços, inclusive aqueles referentes à segurança cibernética e medicina do trabalho;

4.6.4. Zelar pela disponibilidade da infraestrutura de TI da CONTRATADA durante a realização dos serviços propostos;

4.6.5. Realizar a manutenção de software e hardware de sua propriedade e utilizados para a prestação dos serviços propostos.

4.7. A implantação, configuração, ativação e atualização da solução será de responsabilidade da CONTRATADA, bem como as despesas diretas ou indiretas para a execução das atividades pela sua equipe técnica.

4.8. A instalação e atualização dos softwares nos ativos monitorados (item 1.1.1) poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE.

4.9. O processo de implantação, configuração, ativação e atualização da solução deverá ser realizado por técnicos capacitados da CONTRATADA, acompanhados por servidores da CONTRATANTE.

PAGAMENTO

4.10. A emissão do termo de recebimento provisório será feita após a conclusão da fase de Implantação, Configuração e Ativação da solução (item 4.4.2);

4.11. A emissão do termo de recebimento definitivo será feita após a conclusão da fase de Definição de Processos e Outras Configurações (item 4.4.3);

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

5. ITEM 4 – Requisitos mínimos do serviço de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos

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

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

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

OPERAÇÃO E SUSTENTAÇÃO

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

5.10.1. Ativação e configuração dos módulos contratados;

5.10.2. Integração dos componentes contratados com o ambiente da CONTRATANTE;

5.10.3. Gestão do ciclo de vida da solução, contemplando a sua implantação e operação, além da inclusão, alteração e exclusão de ativos monitorados;

5.10.4. Abrir e fazer a triagem de chamados de segurança cibernética;

5.10.5. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;

5.10.6. Atender incidentes simples, os quais possuem instruções indicadas em playbooks (knowledge Base do ITSM);

5.10.7. Elaborar consultas(queries)/scripts de rastreamento quando necessário e/ou solicitados pela CONTRATANTE;

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

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

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

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

5.10.12. Desenvolvimento de playbooks de resposta a ataques cibernéticos;

5.10.13. Configuração de fontes de eventos;

5.10.14. Configuração de usuários VIP e usuários de serviço;

5.10.15. Criação de alertas customizados;

5.10.16. Configuração de coletores de eventos;

5.10.17. Configuração de monitoramento de arquivos e diretórios;

5.10.18. Liberação de acesso à solução para usuários autorizados pela CONTRATANTE;

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

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

5.10.21. Atualização da solução, quando necessário/aplicável e/ou solicitados pela CONTRATANTE;

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

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

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

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

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

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

5.11.5. Estar disponível por telefone e e-mail, de segunda a sexta-feira, das 09 (nove) às 18 (dezoito) horas e acessível por contato telefônico em qualquer outro horário (incluindo sábados, domingos e feriados).

INTELIGÊNCIA DE AMEAÇAS

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

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

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

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

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

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

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

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

5.13.3. O serviço deve poder ser executado sob demanda.

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

MONITORAMENTO E DETECÇÃO DE AMEAÇAS E ATAQUES

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

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

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

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

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

PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

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

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

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

5.14.5. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações à CONTRATANTE:

5.14.5.1. Alertas e notificações;

5.14.5.2. Quantidade de incidentes por categoria;

5.14.5.3. Quantidade de incidentes por criticidade (severidade);

5.14.5.4. Quantidade de incidentes que geraram crise;

5.14.5.5. Porcentagem dos incidentes originários do monitoramento;

5.14.5.6. Quantidade de incidentes tratados/fechados;

5.14.5.7. Quantidade de incidentes registrados.

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

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

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

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

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

5.14.6.3.2. Descrição do ambiente avaliado;

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

5.14.6.3.4. Descrição detalhada dos alertas;

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

5.14.6.3.6. Testes executados e relatórios técnicos das ferramentas;

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

RESPOSTA E INVESTIGAÇÃO A INCIDENTES CIBERNÉTICOS

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

5.15.1. Analisar, recomendar ações de remediação e contenção e documentar os eventos de segurança que, após analisados, demonstraram ser um ataque ao ambiente da CONTRATANTE,

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 2ª REGIÃO

tendo sido categorizados como "Eventos de Exceção" e, portanto, acionado o processo de resposta a incidentes cibernéticos.

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

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

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

5.15.4.1. A matriz GUT será definida na fase de Planejamento e Projeto (item 4.4.1) pela CONTRATADA em conjunto à equipe de segurança cibernética da CONTRATANTE.

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

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

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

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

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

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

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

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

5.15.10. Reconstruir o ataque, caso seja necessário e/ou solicitado pela CONTRATANTE. Esta ação deve ser realizada pela CONTRATADA em ambiente controlado (como um sandbox), utilizando mecanismos de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança cibernética.

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

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

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