Ata de Registro de Preços Nº 2/2022 - PJPI/TJPI/PRESIDENCIA/SECGER/SLC/SLC-APOIO

ATA DE REGISTRO DE PREÇOS Nº 2/2022-PJPI/TJPI/SLC

PREGÃO ELETRÔNICO Nº 4/2022

SEI Nº 21.0.000032562-4

O TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ - 040105, **CNPJ nº 10.540.909/0001-96,** com sede na Praça Des. Edgard Nogueira, s/n, Centro Cívico, Bairro Cabral, em Teresina-Piauí, CEP 64.000-830, neste ato representado pelo Presidente do Tribunal de Justiça, o Sr. Desembargador **JOSÉ RIBAMAR OLIVEIRA**, doravante designado simplesmente **ADMINISTRAÇÃO**, no uso das atribuições que lhe são conferidas pelo Regimento Interno do TJPI, em face das propostas apresentadas no **Pregão Eletrônico nº 4/2022,** resolve:

REGISTRAR PREÇOS a favor da empresa **APPROACH TECNOLOGIA LTDA**, inscrita no CNPJ nº 24.376.542/0001-21, Inscrição Estadual nº 257.926.879, estabelecida na AV. PREFEITO OSMAR CUNHA, 416, SL 303,CEP 88015-100 – Florianópolis/SC, Telefone para contato: (48) 4009-2160, site/e-mail: https://approachtec.com.br//kent@approachtec.com.br, neste ato representada por **Kent Johann Modes**, CPF nº 047.478.629-35 e RG nº 4.826.448 SSP-SC, doravante denominada, **BENEFICIÁRIA DO REGISTRO**, sujeitando-se as partes às determinações das Leis Federais n° 8.666, de 21.06.93, e 10.520, de 17.07.2002, Decretos nº 10.024/2019, nº 7.892/2013, nº 3.555/2000; nº 3.784/2001; da Resolução TJ/PI Nº 19/2007, de 11.10.2007, com as suas alterações e toda legislação vigente aplicável, instrumento convocatório e às seguintes cláusulas.

1. DO OBJETO

1.1. FORMAÇÃO DE REGISTRO DE PREÇOS para eventuais contratações por período de 12 (doze) meses, sendo possível prorrogação por períodos iguais ou superiores limitado a 48 (quarenta e oito) meses conforme preconiza o art. 57, inc. IV, da Lei n° 8.666 de 1993, **de Solução de Proteção avançada de endpoints Palo Alto Cortex XDR e serviços de implantação e configuração da solução (incluindo Hands On) com direito de atualização e suporte, em português do Brasil, por meio de licenças de subscrição por *endpoint***, visando atender todas as unidades integrantes do Tribunal de Justiça do Estado do Piauí, incluindo a Corregedoria Geral de Justiça e a EJUD, de acordo com as especificações, condições e quantidades estimadas, descritas no Termo de Referência Nº 161/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC (2931266).

ARP Nº 2/2022				
Item	**Especificação do Objeto**	**Unidade**	**Qtd Registrada**	**Valor Unitário**

Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses.

SOLUÇÃO DE PROTEÇÃO AVANÇADA DE ENDPOINT (XDR) 1. Aquisição de licenças de solução de segurança para proteção avançada de endpoints (estação de trabalho e servidores) no combate a vírus, malwares conhecidos e desconhecidos, vulnerabilidades conhecidas e desconhecidas com características estendidas de detecção e resposta; 2. As funcionalidades de proteção que compõe a solução de segurança, funcionam em múltiplos equipamentos e/ou softwares desde que obedeçam a todos os requisitos desta especificação; 3. A solução possui a capacidade e vem licenciada para integrar-se com a solução de firewall do fabricante Palo Alto Networks, implantada no órgão, permitindo utilizá-la como parte da solução de segurança suportando o monitoramento do tráfego de rede e correlacionando os eventos de segurança da camada de rede com os eventos ocorridos nos endpoints protegidos de modo centralizado, proporcionando uma análise de risco mais assertiva e completa; 4. Estão inclusas na proposta todas as licenças necessárias para o pleno funcionamento da solução, conforme as especificações elencadas; 5. A solução vem licenciada para retenção de logs pelo período mínimo de 30 dias, o que deve incluir o cluster de Firewall da Palo Alto Networks, modelo PA-5220, composto por 2 appliances, além dos logs dos agentes de proteção de endpoint, inerentes à solução. 5.1. A solução permite a expansão desse período de retenção de logs, conforme as necessidades da instituição, devendo ser licenciado posteriormente, conforme o caso. 6. A solução possui subscrição pelo período mínimo de 12 (doze) meses, permitindo, durante este período, acesso ilimitado à console central de gerenciamento na nuvem, acesso a todas as atualizações, serviços de segurança e assinaturas de proteção da solução e o pleno funcionamento do agente de proteção instalado nos endpoints. **CARACTERÍSTICAS GERAIS** 1. Entende-se por Endpoint uma estação de trabalho, servidor de rede ou dispositivo móvel; 2. A proteção avançada dos endpoints é feita através da instalação de agentes nos endpoints, suportando, pelo menos os seguintes sistemas operacionais: 2.1. Android 6 e superiores; 2.2. Windows Vista; 2.3. Windows 7; 2.4. Windows 8; 2.5. Windows 8.1; 2.6. Windows 10; 2.7. Mac OS X 10.13 e superiores; 2.8. Windows Server 2003; 2.9. Windows Server 2003 R2; 2.10. Windows Server 2008; 2.11. Windows Server 2008 R2; 2.12. Windows Server 2012; 2.13. Windows Server 2012 R2; 2.14. Windows Server 2016; 2.15. Windows Server 2019 2.16. Windows Server Datacenter 2.17. RHEL/CentOS/Oracle Linux 6 e superiores; 2.18. Debian Linux 9 e superiores; 2.19. Ubuntu Linux 12 e superiores; 3. Suporta e possuir agente para máquinas virtuais instaladas em ambiente VMware; 4. Proteção contra desinstalação não autorizada dos agentes de endpoint que compõem a solução; 5. Proteção contra a desativação não autorizada dos serviços que compõem a solução; 6. É eficaz na prevenção de vulnerabilidades e malwares mesmo quando estiver sem conectividade com servidores de gerenciamento e/ou recursos baseados em nuvem; 7. O agente de endpoint continua funcionando e aplicando políticas de controle mesmo se houver interrupção da comunicação com o gerenciamento centralizado; 8. Impede executável malicioso, sem requerer nenhum conhecimento prévio do artefato; 9. Previne contra ameaças conhecidas baseado em assinatura; 10. Previne contra ameaças baseada em comportamento através do monitoramento das atividades realizadas pelo endpoint;11. Previne contra ameaças através do uso de machine learning através da análise local de arquivos desconhecidos; 12. Possibilidade de colocar arquivos, diretórios e processos em listas de exclusões para não serem verificados pela proteção em tempo real; 13. Possui funcionalidades que permitem o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados; 14. A solução permite implementação em modo de monitoramento ou aprendizado do ambiente em fase inicial de instalação; 15. A solução fornece a capacidade de configurar listas brancas globais para permitir que determinados arquivos executáveis sejam executados dentro de determinadas condições da instituição; 16. A solução tem a capacidade de criar, a partir de incidentes, uma regra de exceção para permitir que um processo seja executado em um determinado endpoint; 17. Permite bloquear nos endpoints o uso de dispositivos portáteis USB como pen drives, discos, drives de CD/DVD/BluRay a fim de prevenir contra a transferência de arquivos maliciosos por meio destes dispositivos; 18. Possui firewall de host permitindo o controle da comunicação do endpoint através de regras de permissão e bloqueio do tráfego; 19. A solução armazena as informações de alertas, incidentes e suas respectivas atividades e ações e demais dados relacionados aos eventos de segurança detectados por um período mínimo de 30 (trinta) dias;
PROTEÇÃO CONTRA VULNERABILIDADES 1. A solução suporta a proteção de processos e aplicativos em execução no sistema operacional; 2. A solução suporta a adição de aplicações proprietárias e personalizadas na lista de aplicações protegidas; 3. A solução é capaz de fornecer prevenção em tempo real contra exploração de vulnerabilidades de aplicações, bloqueando em

tempo real a exploração, não limitadas a falhas de lógica de software, corrupção de memória e sequestro de DLL; 4. A solução é capaz de proteger contra explorações de quaisquer vulnerabilidades não descobertas (desconhecidas) dos aplicativos através do bloqueio de métodos (técnicas e subtécnicas) utilizados para exploração; 5. Ao impedir ou bloquear uma técnica de exploração, a solução congela o processo, coletar informações forenses, de no mínimo, nome do processo, origem e caminho do arquivo, data/hora, dump de memória, versão do SO, usuário, versão vulnerável do aplicativo; 6. Ao impedir ou bloquear uma técnica de exploração, a solução finaliza apenas o processo específico alvo do ataque; 7. A solução utiliza módulos de métodos de exploração para prevenir ou bloquear tentativas de exploração. Os módulos de métodos de exploração protegem aplicações conhecidas, bem como aplicações desconhecidas e desenvolvidas internamente pela instituição; 8. A solução é capaz de criar regras de exclusão para excluir endpoints específicos e processos específicos do log de eventos de ameaças de segurança da console de gerenciamento da solução; 9. Suporta detecção e bloqueio de, no mínimo, os seguintes métodos, sendo capaz de: 9.1. Impedir execução de dados na memória; 9.2. Impedir acessos não autorizados a DLLs do sistema; 9.3. Prevenir utilização de DLLs protegidas com fim de ganhar controle de processos e carregar arquivos CPL (painel de controle) maliciosos; 9.4. Interromper a ocorrência de heap sprays após detecção de exceções suspeitas ou indicativos de tentativas de exploração no host monitorado; 9.5. Prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração em processadores de texto; 9.6. Prevenir o acionamento de vulnerabilidades que resultem na corrupção da área heap na memória. Exemplo: “free() double”; 9.7. Prevenir o uso de novas técnicas que possam evadir o DEP (prevenção de execução de dados em memória) e ASLR (randomização do layout de endereçamento em memória); 9.8. Obrigar a realocação de módulos do sistema operacional, protegendo-os de tentativas de exploração; 9.9. Ser capaz de detectar e prevenir instâncias de heap spray usando algoritmo de detecção de aumento de consumo de memória, indicando execução de exploração de vulnerabilidade; 9.10. Prevenir mapeamento de código no endereço zero (início da memória) do espaço de memória do sistema operacional, dessa forma impedindo uso de explorações de referência nula para execução de código arbitrário, exposição de informações de debug, etc; 9.11. Proteger o acesso a metadados de bibliotecas críticas do sistema operacional quando estas são descompactadas em memória; 9.12. Agir preventivamente contra heap spray ao checar periodicamente a zona heap da memória virtual; 9.13. Prevenir a exploração de vulnerabilidade através da préalocação aleatória do layout de memória de processos no sistema operacional; 9.14. Prevenir uso de programação orientada a retorno (return oriented programming) protegendo APIs (interface de programação de aplicação) usadas em cadeias de ROP e técnicas de exploração usando compilações “Just-in-time” (JIT); 9.15. Mitigar o abuso e captura das estruturas de gerenciamento de exceções (SEH) em memória, impedindo a execução de código malicioso arbitrário no sistema operacional; 9.16. Reservar e proteger determinadas áreas da memória comumente utilizadas para armazenamento de cargas (payload) e instruções maliciosas usando técnicas como heap spray, por exemplo; 9.17. Prevenir vulnerabilidades lógicas na estrutura de atalhos (links) de sistemas operacionais Windows, onde o carregamento impróprio de atalhos permite execução arbitrária de código em memória; 9.18. Prevenir contra vulnerabilidades utilizadas em ataques de escalação de privilégios no sistema operacional explorando a instrução sys.exit para retornar ao nível de execução de usuário, após execução de código em nível de sistema (privilege level 0); 9.19. Aprimorar ou implementar a randomização do layout de endereços em memória (ASLR), garantindo maior aleatoriedade e robustez. Deve também ser capaz de tornar obrigatório o uso da função ASLR; **PROTEÇÃO CONTRA MALWARE** 1. A solução suporta a proteção contra a execução de arquivos maliciosos; 2. A solução fornece a capacidade de fazer controle e restringir os parâmetros sobre como executáveis podem executar incluindo proteção contra criação de processos filhos; 3. A solução é capaz de fornecer prevenção contra malware desconhecido usando análise dinâmica em ambiente de sandbox; 4. A solução possui integração com o serviço de análise de malwares desconhecidos em nuvem (sandbox) para uma análise mais profunda dos arquivos; 4.1. Fornece veredito e relatório informando o resultado da análise em sandbox; 5. O serviço de análise em nuvem é do mesmo fabricante da solução de proteção avançada de endpoint ou de fabricantes terceiros devendo ser fornecidas todas as licenças necessárias para seu pleno funcionamento; 6. O serviço de análise de malwares desconhecidos em nuvem possui a capacidade de realizar a análise dos arquivos em ambientes bare metal para detectar malwares VM-aware, que possuem a capacidade de detectar que estão em um ambiente virtual e nesta situação não realizam as atividades maliciosas para as quais foi desenvolvido; 7. O serviço de análise de malwares desconhecidos em nuvem realiza a análise de, no mínimo, os seguintes tipos de arquivos: arquivos executáveis, DLLs arquivos Word (.doc, .docm e docx) e Excel (.xls, .xlsm e .xlsx) que contenham macros, arquivos DMG e arquivos ELF; 8. A solução fornece a capacidade de criar exceções para hash

1	específicos de arquivos analisados em nuvem na solução de sandbox; 9. A solução fornece a capacidade de impedir a execução de um arquivo quando seu valor de hash for desconhecido pela solução de sandbox; 10. A solução fornece a capacidade de impedir a execução de um arquivo quando o hash do arquivo for desconhecido por cache local e o mesmo não tiver comunicação com o servidor de gerência; 11. Permite executar a varredura no endpoint em busca de arquivos infectados por malware a partir da console central de gerenciamento e a partir do próprio agente instalado no endpoint. É possível também configurar varreduras agendadas; 12. Caso um malware seja detectado, é possível o envio do mesmo para quarentena automaticamente através de política pré-definida na gerência centralizada; 13. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo e não apenas por sua extensão; 14. Extrai o hash de arquivos executáveis e verificar se o mesmo já foi analisado na solução de sandbox de forma automática sem necessidade de scripts externos ou adaptações não nativas da solução. Caso o malware já tenha apresentado comportamento malicioso em sandbox, o mesmo é impedido de ser executado no endpoint; 15. Possui mecanismos para detectar, em tempo real, ataques LotL – Living off the Land, ataques baseados em scripts e ataques fileless (sem arquivos); 16. Permite ao administrador reportar falsos positivos na análise de malwares em sandbox. A solução informa ao administrador o resultado desta análise e exibir a correção na gerência da solução; 17. Avisa o usuário quando a execução de um arquivo for bloqueada incluindo casos quando não houver veredito da sandbox sobre o arquivo e o seu status estiver definido como desconhecido; 18. Possibilita o bloqueio automático de malwares já descobertos através da sandbox do fabricante em outros endpoints do órgão; 19. É capaz de restringir a execução de arquivos específicos somente em diretórios conhecidos e protegidos, tanto na máquina local quanto em drives remotos; 20. Previne execução de arquivos não assinados; 21. Previne a execução de arquivos em mídia externa; 22. É capaz de controlar executáveis não assinados por meio do uso de WhiteLists; 23. É capaz de restringir a execução de processos; 24. Possui a capacidade de controlar e limitar a criação de processos filhos; 25. Possibilita o controle de arquivos conhecidos e não conhecidos; 26. É capaz de definir e classificar Hashs conhecidos. **COLETA DE INFORMAÇÕES FORENSES** 1. A solução coleta dados forenses capturados pelo agente de endpoint, contemplando, pelo menos, os seguintes: 1.1. Dump de memória; 1.2. Arquivos Acessados; 1.3. Módulos carregados; 1.4. URIs acessadas; 1.5. Local de execução do arquivo; 1.6. Tempo de execução; 1.7. Nome do arquivo; 1.8. Hash do arquivo; 1.9. Nome do usuário relacionado; 1.10. Nome do computador; 1.11. Endereço IP; 1.12. Versão de sistema operacional; 1.13. Histórico de arquivos maliciosos; **GERENCIAMENTO** 1. A console de gerenciamento é baseada em nuvem e acessada através de navegadores web, devendo conter de forma centralizada os recursos para a monitoração e controle da proteção dos dispositivos; 2. A console apresenta Dashboard com o resumo do estado de proteção dos dispositivos protegidos, bem como indicar os alertas de eventos de criticidades alta, média e baixa; 3. Possui mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM; 4. A console permite, dentro da estrutura de gerenciamento, a organização dos dispositivos protegidos em grupos; 5. Permite a aplicação de regras diferenciadas baseadas em dispositivos ou grupos de dispositivos; 6. A console de gerenciamento permite a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs; 7. A solução é compatível, no mínimo, com os navegadores (web browsers) Firefox e Chrome; 8. Caso a solução necessite de Banco de Dados (Ex. SQL Server Enterprise), estarão inclusas na proposta as licenças necessárias para seu pleno funcionamento; 9. A comunicação entre a console de gerenciamento e os clientes gerenciados é feita através do uso de protocolos seguros e protegidos por criptografia; 10. É possível realizar acesso direto aos endpoints protegidos a partir da console central de gerenciamento da solução, a fim de permitir a execução de ações para investigação e reposta aos incidentes de segurança como: visualizar e encerrar processos, apagar, mover e renomear arquivos, prover interface de linha de comando capaz de executar comandos do sistema operacional e executar scripts e comandos python nos endpoints; 11. É possível salvar um relatório contendo todas as atividades realizadas durante a sessão de acesso aos endpoints gerenciados; 12. É possível realizar, a partir da console de gerenciamento, a execução simultânea de scripts nos diversos endpoints de forma centralizada; 13. A solução permite, a partir da console central de gerenciamento, isolar um endpoint impedindo a comunicação do mesmo com a rede para evitar que um possível ataque se propague pela rede; 14. Possui mecanismo de comunicação prédefinido, em tempo determinado e configurável pelo administrador, entre os agentes nos endpoints e a console de gerenciamento, provendo a consulta de novas configurações, políticas ou conteúdo; 15. Permite a criação de, no mínimo, três perfis de acesso distintos para os usuários administradores da solução; 16. Registra nos logs as alterações realizadas pelos administradores da solução, provendo auditoria de mudanças; 17. A solução é capaz de exportar seus logs no formato syslog para outras soluções de gerenciamento de logs; 18. A atualização do motor de detecção de ameaças é realizada de forma transparente para o usuário; 19. Permite	unidade	4.500	R$ 310,00

integração com soluções de SIEM enviando logs no formato Syslog ou compatível; 20. Se comunica, por meio de logs de incidentes e ataques ou informações de inteligência, com os elementos de segurança do ambiente, como por exemplo, mas não se limitando a: Firewalls, Proxies, Filtros de Conteúdo; 21. Exibe lista com todos os alertas de incidentes detectados na console central de gerenciamento. Deve mostrar, para cada alerta da lista, no mínimo, a data e hora que o incidente ocorreu, o nome ou endereço IP envolvido, a ação tomada pelo agente com relação ao incidente e a categoria do incidente informando se o mesmo se trata de exploit ou malware, por exemplo; 22. Permite notificar eventos ao administrador por e-mail; 23. Permite a criação de políticas para prevenção e mitigação de: 23.1. Vulnerabilidades conhecidas e desconhecidas (Exploits); 23.2. Códigos Maliciosos (Malware); 23.3. Restrições de execução; 24. Centraliza e gerencia na console de administração qualquer evento de segurança detectado, seja na camada de rede ou nos endpoints protegidos; 25. É exibida também, na console central de gerenciamento, a lista de CVE – Common Vulnerabilities and Exposures – conhecidos e permitir visualizar quais endpoints estão sendo afetados por uma determinada CVE; 26. Identifica e gera log de qualquer interferência no serviço de proteção nas estações e servidores protegidos, como por exemplo: 26.1. Tentativa de encerramento do processo de proteção; 26.2. Tentativa de encerramento do serviço de proteção; 26.3. Logs de sistema relacionados a tentativa de interferência com o serviço, processo ou arquivos do sistema de proteção; 27. É possível visualizar, em uma linha do tempo, a cadeia de processos e eventos, desde a execução do primeiro processo responsável pela execução dos demais, que geraram um alerta de incidente. Para cada processo executado é possível visualizar, no mínimo, o caminho onde o processo estava localizado, o nome do usuário que iniciou o processo e o tempo em que o processo ficou em execução informando a data e hora do início e do fim da execução do mesmo; 28. Além dos processos executados são exibidas informações sobre conexões de entrada e saída, conexões fracassadas e download e upload de dados; 29. A solução permite o ajuste de políticas de coleta de informações forenses, dentro da console de gerenciamento centralizado, com definições do tipo de informações sobre o incidente que serão coletadas quando uma ameaça ou ataque for identificado; 30. Possui ferramenta de busca para a investigação de incidentes permitindo a realização de buscas com base em, no mínimo, processos executados, em arquivos criados, alterados e deletados, em atributos de rede como endereço IP, nome do host, porta e protocolo, em registros criados, modificados e deletados, em eventos de log do Windows e do Linux. Permite também realizar a busca através da combinação destes atributos; 31. É possível a realização de busca com base no caminho completo onde o arquivo pode estar localizado e também com base no hash do arquivo gerado pela solução. 32. A solução permite realizar a configuração de alertas com base em incidentes e em indicadores de comprometimento, como nome do arquivo, domínio e endereço IP de destino. A solução permite importar listas de indicadores de comprometimento de serviços externos de inteligência contra ameaça, além de permitir a criação destes indicadores; 33. A solução permite realizar a configuração de alertas baseados no comportamento do endpoint. Os tipos de comportamentos detectados são, no mínimo, execução de processos, manipulação de privilégios em arquivo, ofuscação do tipo do arquivo, atividade de reconhecimento na rede escalonamento de privilégio e movimentos laterais na rede; 34. A solução permite realizar a atualização de versão dos agentes instalados nos endpoints a partir da console central de gerenciamento; 35. A solução recebe e distribui atualizações contendo ajustes finos de políticas de proteção, de módulos de proteção e novos modelos matemáticos para uso de aprendizagem de máquina (Machine Learning) para análise de código antes da execução; RELATÓRIOS 1. A solução fornece visualização das ameaças em formato Web; 2. A solução suporta exportação no formato CSV dos eventos relacionados à ameaças, bem como o status dos agentes de endpoints; 3. Capacidade de geração de relatórios, estatísticas e gráficos contendo no mínimo os seguintes tipos pré-definidos: 3.1. As 10 máquinas com maior ocorrência de códigos maliciosos; 3.2. Os 10 usuários com maior ocorrência de códigos maliciosos; 3.3. Localização dos códigos maliciosos; 3.4. Sumário das ações realizadas; 3.5. Número de infecções detectadas diária, semanal e mensalmente; 4. Abrange os códigos maliciosos detectados; 5. A solução tem os seguintes dashboards nativos para monitorar a postura de segurança e o status da instituição: 5.1. Relatório de restrição de acesso a arquivos e processos; 5.2. Técnicas de Malwares utilizadas; 5.3. Técnicas de exploração utilizadas; 5.4. Informações Forenses coletadas. 6. .6. A solução tem os seguintes dashboards de controle para monitorar a situação dos endpoints da instituição: 6.1. Detalhes da saúde dos agentes de endpoints; 6.2. Dashboard de controle do histórico de regras dos endpoints; 6.3. Dashboard de controle da Política de Segurança instalada nos endpoints; 6.4. Dashboard de controle do histórico de status do serviço nos endpoints; Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos.
Garantia: 12 meses
Procedência: Estados Unidos

	Fabricante: Palo Alto Networks Modelo: Cortex XDR Pro Part Numbers: 1 x PAN-XDR-ADV-EP Links de comprovação: Palo Alto Cortex XDR Website https://www.paloaltonetworks.com/cortex/cort ex-xdr Palo Alto Cortex XDR Datasheet https://www.paloaltonetworks.com/resources/datasheets/cortex-xdr Palo Alto Cortex XDR TechDocs Website https://docs.paloaltonetworks.com/cortex/cort ex-xdr.html Palo Alto Cortex XDR Pro Administrator's Guide https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-pro-admin/cortex-xdr-proadmin.pdf Palo Alto Cortex XDR API Reference https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-api/cortex-xdr-api.pdf Palo Alto Networks Compatibility Matrix https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/compatibilitymatrix/compatibility-matrix.pdf			
2	**Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses** **GERENCIAMENTO DE VULNERABILIDADES E INVENTÁRIO** 1. Provê informações capazes de enriquecer a análise de segurança do ambiente, aumentando a visibilidade e fornecendo melhor compreensão dos riscos; 2. Provê elementos capazes de neutralizar rapidamente ameaças à segurança institucional; 3. Reduz os esforços do diagnóstico ao fornecer informações abrangentes e suficientes permitindo melhorar o tempo de resposta dos incidentes; 4. Provê, de forma rápida e simples, recurso capaz de realizar a busca e a remoção do arquivo malicioso de todos os endpoints gerenciados; 5. Possui o recurso de inventário, sendo capaz de exibir, em detalhes, diversas informações dos sistemas dos endpoints; 6. Exibe detalhes sobre os aplicativos instalados que requerem e receberam permissões especiais para habilitar uma câmera, microfone, recursos de acessibilidade, acesso total ao disco ou capturas de tela; 7. Exibe detalhes sobre executáveis que iniciam automaticamente quando o usuário efetua login ou inicializa o sistema operacional do dispositivo protegido; 8. A solução exibe informações sobre autoruns que são configurados no registro do endpoint, pastas de inicialização, tarefas agendadas, serviços, drivers, daemons, extensões, tarefas Crond, itens de login, ganchos de login e logout; 9. Para cada execução automática, a solução lista o tipo e a configuração da execução automática, como método de inicialização, CMD, detalhes do usuário e caminho da imagem; 10. Exibe, pelo menos os seguintes detalhes, para cada daemon existente no endpoint gerenciado: 10.1. Nome, tipo, caminho e estado, indicando se está carregado, em execução ou não; 11. Exibe detalhes sobre cada volume de disco existentes em um endpoint, como os seguintes: 11.1. Tipo de unidade, nome, sistema de arquivos, espaço livre e tamanho total; 11.2. Mostrar informações como nome, tipo, caminho, modo e estado de todos os drivers instalados em um dispositivo gerenciado; 12. Exibe detalhes sobre todas as unidades, volumes e discos que foram montados no endpoint, a exemplo das seguintes: 12.1. Lista o diretório do ponto de montagem, o tipo de sistema de arquivos, especificações da montagem e GUID; 13. Detalha, para cada serviço em execução em um endpoint, informações como: 13.1. Nome, tipo, caminho, status do tempo de execução, se o serviço está em execução e qual é o estado do tempo de execução, se o serviço pode ser parado, pausado ou atrasado seu horário de início, se o serviço requer interação com a área de trabalho do endpoint, o nome do usuário que iniciou o serviço e o modo de início 14. Mostra detalhes sobre cada pasta compartilhada em rede como: 14.1. Tipo de pasta de rede compartilhada: Disk Drive, Print Queue, Device, IPC, Disk Drive Admin, Print Queue Admin, Device Admin, IPC Admin; 14.2. Nome da pasta, descrição e caminho; 14.3. Se a pasta está limitada a um número máximo de compartilhamentos e o número máximo de compartilhamentos permitidos; 15. Apresenta informações gerais sobre o hardware do endpoint, como fabricante, modelo, memória física, arquitetura de processadores e CPU; 16. Apresenta informações sobre o sistema operacional e a release em execução no endpoint; 17. A solução fornece a lista de usuários cujas credenciais estão armazenadas no endpoint; 18. Fornece informações sobre as contas de usuários, quais estão ativas e o tipos de cada uma; 19. Informa detalhes sobre a senha definida para cada conta de usuário, como se ela é necessária para fazer login, se tem uma data de validade ou se pode ser alterada; 20. Mostra informações de conexões dos ativos em forma de gráficos a fim de simplificar a investigação e proporcionar ganho de eficiência. 21. É capaz de identificar e quantificar as vulnerabilidades de segurança (CVEs) existentes para as aplicações instaladas nos endpoints; 22. Oferece visibilidade em tempo real da exposição às vulnerabilidades e dos níveis de patch atuais dos endpoints, aperfeiçoando a	unidade	4.500	R$ 39,50

	análise de gravidade dos riscos e permitindo priorizar a mitigação. 23. É uma solução eficaz no gerenciamento de vulnerabilidade, devendo ser simples de utilizar, escalonável e do mesmo fabricante da solução avançada de proteção de endpoint. Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos Garantia: 12 meses Procedência: Estados Unidos Fabricante: Palo Alto Networks Modelo: Host Insights Add-on for Cortex XDR Part Number: 1 x PAN-XDR-HOST-INST Links de comprovação: Palo Alto Cortex XDR Website https://www.paloaltonetworks.com/cortex/cort ex-xdr Palo Alto Cortex XDR Datasheet https://www.paloaltonetworks.com/resources/datasheets/cortex-xdr Palo Alto Cortex XDR TechDocs Website https://docs.paloaltonetworks.com/cortex/cort ex-xdr.html Palo Alto Cortex XDR Pro Administrator's Guide https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-pro-admin/cortex-xdr-proadmin.pdf Palo Alto Cortex XDR API Reference https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-api/cortex-xdr-api.pdf Palo Alto Networks Compatibility Matrix https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/compatibilitymatrix/compatibility-matrix.pdf			
3	**Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro.** **SERVIÇO DE IMPLANTAÇÃO** 1. Os serviços são executados pela CONTRATADA, por técnicos comprovadamente credenciados pelo fabricante; 2. A CONTRATADA informará nome, e-mail e telefone dos componentes da equipe técnica responsável pela solução, ou seja, do gerente do projeto, técnico e do responsável comercial; 3. Após o recebimento do Pedido de Compra, a CONTRATADA tem o prazo máximo de 15 (quinze) dias para realizar a Reunião de Alinhamento do Projeto, que será feita de forma remota, onde a CONTRATADA apresentará os técnicos responsáveis pela implantação e suas respectivas documentações exigidas neste Termo de Referência. Nessa mesma reunião será definido o cronograma de implantação/migração da solução; 3.1. O licenciamento da solução será disponibilizado a partir da data de início da execução do cronograma. O Recebimento definitivo fica condicionado à entrega de todos os agentes instalados e licenciados, conforme definido na Reunião de Alinhamento, observadas as considerações dos itens 5.1.2.2.4.1. e 5.1.2.2.4.2. 4. A implantação inicial consiste em aplicar as regras de acordo com a Política de Segurança da Informação do Tribunal de Justiça do Estado do Piauí, podendo ainda serem definidas e criadas novas regras de acordo com as necessidades informadas pela equipe técnica de TI do TJPI, sempre levando em consideração as melhores práticas estabelecidas no mercado; 4.1. É de responsabilidade da CONTRATADA a implantação da solução contemplando todos os itens apresentados neste Termo de Referência ou selecionados de acordo com as necessidades apresentadas pela equipe técnica do TJPI, incluindo todas as configurações necessárias à implantação e integração da solução ao ambiente de segurança do TJPI, sempre com acompanhamento e apoio da equipe técnica do TJPI. 4.1.1. A instalação dos agentes da solução contratada nos endpoints do PJPI será feita em conjunto com a equipe da STIC. 4.2. Todas as configurações a são feitas e aplicadas pela CONTRATADA no ambiente de infraestrutura do TJPI serão previamente apresentadas para a equipe técnica da CONTRATANTE no momento da implantação/configuração da solução. 4.2.1. Tais configurações só poderão ser aplicadas com o aval da equipe técnica de TI do TJPI; 5. No caso de inadequação técnica, o Tribunal de Justiça do Estado do Piauí encaminhará à CONTRATADA os critérios inadequados encontrados nos serviços no prazo máximo de 03 (três) dias úteis; 6. A CONTRATADA avaliará, e, após confirmação das inadequações, deverá ser agendada com o Tribunal de Justiça do Estado do Piauí a manutenção para efetuar as devidas correções; 7. Durante todo o processo de implantação a CONTRATADA prestará suporte em eventuais dificuldades que venham a surgir, sem custo adicional para a CONTRATANTE; 8. Todas as configurações de implantação serão revisadas pelos analistas do Tribunal de Justiça do Estado do Piauí, antes de serem inseridas na nova solução; 9. Todas as etapas das configurações da nova solução serão supervisionadas pela equipe de TI do tribunal; 10. O planejamento da implantação/migração será acordado na reunião de alinhamento do projeto e apresentado antes do início das atividades à equipe responsável da CONTRATANTE, incluindo, mas não se limitando, a análise	unidade	1	R$ 160.000,00

	do ambiente de infraestrutura atual do Tribunal de Justiça do Estado do Piauí e o planejamento da implantação da nova solução. 11. Ao final da implantação e configuração da solução, será realizado o repasse de informações hands-on, apresentando as configurações implementadas na solução, de no mínimo 8 (oito) horas. 12. Todas as despesas referentes aos serviços de implantação são de responsabilidade da CONTRATADA. Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos			

2. DO FORNECIMENTO

2.1. Esta Ata não obriga a ADMINISTRAÇÃO a firmar contratações com a BENEFICIÁRIA**,** podendo ocorrer licitações específicas para a aquisição dos produtos/serviços registrados, observada a legislação pertinente, sendo assegurada preferência de fornecimento ao BENEFICIÁRIO do registro em igualdade de condições.

2.2. A requisição dos produtos/serviços será formalizada mediante Contrato Administrativo ou Ordem de Fornecimento/Serviço, observadas as disposições contidas no referido Pregão Eletrônico.

2.3. Após a disponibilização no Sistema Eletrônico SEI, os eventuais Contratos Administrativos ou Ordem de Fornecimento/Serviço deverão ser assinados pela BENEFICIÁRIA DO REGISTRO, no prazo de 03 (três) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das penalidades previstas em Edital e Termo de Referência.

2.4. As despesas com a execução deste Registro de Preços serão atendidas com recursos consignados em dotação específica, cujo detalhamento será contido no respectivo Contrato Administrativo ou Ordem de Fornecimento/Serviço, em havendo.

2.5. O pagamento será realizado mediante crédito bancário, **em favor de APPROACH TECNOLOGIA LTDA e vinculado ao CNPJ Nº 24.376.542/0001-21**, não se admitindo, em hipótese alguma, desconto ou cobrança de título na rede bancária, e será efetivado no **Banco:ITAÚ (341) - Agência: 7197, Conta: 33207-0.**

3. DOS ENCARGOS DA BENEFICIÁRIA DO REGISTRO

3.1. O Beneficiário do Registro fica obrigado a atender todos os pedidos efetuados durante a validade desta Ata de Registro de Preços.

3.2. Manter, durante o período do registro de preços, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar à ADMINISTRAÇÃO, imediatamente, qualquer alteração que possa comprometer a manutenção desta Ata de Registro de Preços.

4. DAS OBRIGAÇÕES DA ADMINISTRAÇÃO

4.1. Proporcionar à beneficiária do registro todas as facilidades à boa execução do objeto desta Ata de Registro de Preços e designar um representante para acompanhar o eventual fornecimento dos suprimentos registrados, com a finalidade de dirimir eventuais dúvidas.

4.2. Efetuar os pagamentos devidos em função de eventual contratação realizada com base na presente Ata de Registro de Preços.

5. DA VIGÊNCIA

5.1. Esta Ata de Registro de Preços terá vigência 12 (doze) meses, a contar da data de sua publicação no Diário da Justiça TJ/PI.

6. DA REVISÃO E DO CANCELAMENTO DOS PREÇOS REGISTRADOS

6.1. A Administração realizará pesquisa de mercado periodicamente, a fim de verificar a vantajosidade dos preços registrados nesta Ata.

6.2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo do objeto registrado, cabendo à Administração promover as negociações junto à BENEFICIÁRIA DO REGISTRO.

6.3. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, a Administração convocará a BENEFICIÁRIA DO REGISTRO para negociar a redução dos preços aos valores praticados pelo mercado.

6.4. A BENEFICIÁRIA DO REGISTRO que não aceitar reduzir seu preço ao valor praticado pelo mercado será liberado do compromisso assumido, sem aplicação de penalidade.

6.5. Quando o preço de mercado tornar-se superior aos preços registrados e a BENEFICIÁRIA DO REGISTRO não puder cumprir o compromisso, o órgão gerenciador poderá:

6.5.1. Liberar a BENEFICIÁRIA DO REGISTRO do compromisso assumido, **caso a comunicação ocorra antes do pedido de fornecimento**, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

6.5.2. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

6.6. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação desta ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

6.7. O registro do fornecedor será cancelado quando:

6.7.1. Descumprir as condições da ata de registro de preços;

6.7.2. Não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

6.7.3. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

6.7.4. Sofrer sanção administrativa cujo efeito torne-o proibido de celebrar contrato administrativo.

6.8. O cancelamento de registros nas hipóteses previstas nos itens 6.7.1, 6.7.2 e 6.7.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

6.9. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:

6.9.1. Por razão de interesse público; ou

6.9.2. A pedido do fornecedor.

7. DAS CONDIÇÕES PARA ADESÃO DA ATA DE REGISTRO DE PREÇOS

7.1. Desde que devidamente justificada a vantagem, a ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da administração pública que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador.

7.2. Os órgãos e entidades que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar o órgão gerenciador da ata para manifestação sobre a possibilidade de adesão.

7.3. A manifestação do órgão gerenciador fica condicionada à realização de estudo, pelos órgãos e pelas entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública da utilização da ata de registro de preços, conforme estabelecido em ato do Secretário de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão.

7.4. O estudo de que trata o item anterior, após aprovação pelo órgão gerenciador, será divulgado no Portal de Compras do Governo federal.

7.5. Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o órgão gerenciador e órgãos participantes.

7.6. As aquisições ou as contratações adicionais de que trata este artigo não poderão exceder, por órgão ou entidade, a **cinquenta por cento dos quantitativos** dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

7.7. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, **ao dobro do quantitativo de cada item registrado** na ata de registro de preços para o órgão gerenciador e para os órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

7.8. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

7.9. Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.

7.10. É vedada aos órgãos e entidades da administração pública federal a adesão a ata de registro de preços gerenciada por órgão ou entidade municipal, distrital ou estadual.

8. DA PUBLICIDADE

8.1. Esta Ata de Registro de preços será publicado no Diário da Justiça, conforme dispõe o artigo 61, parágrafo único, da Lei nº 8.666/1993, e divulgada no site www.tjpi.jus.br.

9.DAS DISPOSIÇÕES FINAIS

9.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, bem como no Edital e suas minutas.

9.2. Caberá à BENEFICIÁRIA DO REGISTRO, observadas as condições estabelecidas nesta Ata de Registro de Preços, optar pela aceitação ou não do fornecimento a órgão ou entidade da administração pública que não tenha participado do certame, desde que esse fornecimento não prejudique as obrigações anteriormente assumidas.

9.3. O gerenciamento desta Ata de Registro de Preços caberá à Superintendência de Licitações e Contratos do tribunal de Justiça do Estado do Piauí – SLC/TJPI.

10. DO FORO

10.1. Fica eleito o Foro da Justiça Estadual do Estado da Piauí, na Comarca de Teresina, para dirimir questões oriundas deste instrumento, com renúncia expressa de qualquer outro por mais privilegiado que

seja.

E por estarem as partes, justas e acordadas, firmam o presente instrumento, assinando-o eletronicamente, conforme art. 1º, III, "b", da Lei nº 11.419/2006 e Resolução 22/2016/TJPI, para que produza seus efeitos jurídicos legais.

Documento assinado eletronicamente por **José Ribamar Oliveira**, **Presidente**, em 02/02/2022, às 13:57, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **KENT JOHANN MODES**, **Usuário Externo**, em 02/02/2022, às 15:12, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **3010258** e o código CRC **09E5D477**.

PERÍODO DE PRESTAÇÃO CONTAS: 31/03 a 09/04/2022 (10 dias)
CONSIDERANDO os poderes delegados pela Presidência do TJPI através da Portaria nº 1.831/2016, **AUTORIZO** a concessão do Suprimento de Fundos acima descritos. Fica o Suprido sujeito ao cumprimento da legislação aplicável à concessão de Suprimento de Fundos, em especial aos dispositivos que regulam sua finalidade e prazos de utilização e de prestação de contas.
PAULO SILVIO MOURÃO VERAS
Secretário Geral do TJPI

Documento assinado eletronicamente por **Paulo Silvio Mourão Veras**, **Secretário(a) Geral**, em 01/02/2022, às 13:13, conforme art. 1º, III, "b", da Lei 11.419/2006.

5. CENTRAL DE LICITAÇÕES E CONTRATOS

5.1. PUBLICAÇÃO - Extrato Nº 14/2022 - PJPI/TJPI/PRESIDENCIA/SECGER/SLC/PREG

Ref. Processo SEI nº 21.0.000032562-4.
Ato: Homologação/Procedimento Licitatório
Procedimento: Pregão Eletrônico Nº 4/2022
OBJETO: FORMAÇÃO DE REGISTRO DE PREÇOS para eventuais contratações por período de 12 (doze) meses, sendo possível prorrogação por períodos iguais ou superiores limitado a 48 (quarenta e oito) meses conforme preconiza o art. 57, inc. IV, da Lei n° 8.666 de 1993, de Solução de Proteção avançada de endpoints Palo Alto Cortex XDR e serviços de implantação e configuração da solução (incluindo Hands On) com direito de atualização e suporte, em português do Brasil, por meio de licenças de subscrição por endpoint, visando atender todas as unidades integrantes do Tribunal de Justiça do Estado do Piauí, incluindo a Corregedoria Geral de Justiça e a EJUD, de acordo com as especificações, condições e quantidades estimadas, descritas no Termo de Referência Nº 161/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC (2931266).
RESULTADO/BENEFICIÁRIA(S):
Grupo: 1 - Adjudicado para: **APPROACH TECNOLOGIA LTDA, CNPJ 24.376.542/0001-21**, pelo melhor lance de R$ 1.848.250,00, com valor negociado a **R$ 1.732.750,00**.
Item: 1 - Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses, Adjudicado para: **APPROACH TECNOLOGIA LTDA, CNPJ 24.376.542/0001-21**, pelo melhor lance de R$ 327,00, com valor negociado a **R$ 310,00** e a quantidade de **4.500 unidades**.
Item: 2 - Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses, Adjudicado para: **APPROACH TECNOLOGIA LTDA, CNPJ 24.376.542/0001-21**, pelo melhor lance de **R$ 39,50** e a quantidade de **4.500 unidades**.
Item: 3 - Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro, Adjudicado para: **APPROACH TECNOLOGIA LTDA, CNPJ 24.376.542/0001-21**, pelo melhor lance de R$ 199.000,00, com valor negociado a **R$ 160.000,00** e a quantidade de **1 unidade de serviço técnico**.
DATA DA ASSINATURA: Às 09:12 horas do dia 02 de fevereiro de 2022, após constatada a regularidade dos atos procedimentais, a autoridade competente, Sr. JOSE RIBAMAR OLIVEIRA, HOMOLOGA a adjudicação referente ao Processo nº 21.0.000032562-4, Pregão nº 00004/2022.

Documento assinado eletronicamente por **Fernando Moura Rêgo Nogueira Leal**, **Pregoeiro**, em 02/02/2022, às 09:32, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **3009671** e o código CRC **F3864681**.

5.2. PUBLICAÇÃO - Ata de Registro de Preços Nº 2/2022 - PJPI/TJPI/PRESIDENCIA/SECGER/SLC/SLC-APOIO

ATA DE REGISTRO DE PREÇOS Nº 2/2022-PJPI/TJPI/SLC
PREGÃO ELETRÔNICO Nº 4/2022
SEI Nº 21.0.000032562-4
O TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ - 040105, **CNPJ nº 10.540.909/0001-96,** com sede na Praça Des. Edgard Nogueira, s/n, Centro Cívico, Bairro Cabral, em Teresina-Piauí, CEP 64.000-830, neste ato representado pelo Presidente do Tribunal de Justiça, o Sr. Desembargador **JOSÉ RIBAMAR OLIVEIRA**, doravante designado simplesmente **ADMINISTRAÇÃO**, no uso das atribuições que lhe são conferidas pelo Regimento Interno do TJPI, em face das propostas apresentadas no **Pregão Eletrônico nº 4/2022,** resolve:
REGISTRAR PREÇOS a favor da empresa **APPROACH TECNOLOGIA LTDA**, inscrita no CNPJ nº 24.376.542/0001-21, Inscrição Estadual nº 257.926.879, estabelecida na AV. PREFEITO OSMAR CUNHA, 416, SL 303,CEP 88015-100 - Florianópolis/SC, Telefone para contato: (48) 4009-2160, site/e-mail: https://approachtec.com.br//kent@approachtec.com.br, neste ato representada por **Kent Johann Modes**, CPF nº 047.478.629-35 e RG nº 4.826.448 SSP-SC, doravante denominada, **BENEFICIÁRIA DO REGISTRO**, sujeitando-se as partes às determinações das Leis Federais n° 8.666, de 21.06.93, e 10.520, de 17.07.2002, Decretos nº 10.024/2019, nº 7.892/2013, nº 3.555/2000; nº 3.784/2001; da Resolução TJ/PI Nº 19/2007, de 11.10.2007, com as suas alterações e toda legislação vigente aplicável, instrumento convocatório e às seguintes cláusulas.
1. DO OBJETO
1.1. FORMAÇÃO DE REGISTRO DE PREÇOS para eventuais contratações por período de 12 (doze) meses, sendo possível prorrogação por períodos iguais ou superiores limitado a 48 (quarenta e oito) meses conforme preconiza o art. 57, inc. IV, da Lei n° 8.666 de 1993, **de Solução de Proteção avançada de endpoints Palo Alto Cortex XDR e serviços de implantação e configuração da solução (incluindo Hands On) com direito de atualização e suporte, em português do Brasil, por meio de licenças de subscrição por *endpoint***, visando atender todas as unidades integrantes do Tribunal de Justiça do Estado do Piauí, incluindo a Corregedoria Geral de Justiça e a EJUD, de acordo com as especificações, condições e quantidades estimadas, descritas no Termo de Referência Nº 161/2021 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC (2931266).

ARP Nº 2/2022				
Item	**Especificação do Objeto**	**Unidade**	**Qtd Registrada**	**Valor Unitário**
1	**Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses.** **SOLUÇÃO DE PROTEÇÃO AVANÇADA DE ENDPOINT (XDR)** 1. Aquisição de licenças de solução de segurança para proteção avançada de endpoints (estação de trabalho e servidores) no combate a	unidade	4.500	R$ 310,00

	vírus, malwares conhecidos e desconhecidos, vulnerabilidades conhecidas e desconhecidas com características estendidas de detecção e resposta; 2. As funcionalidades de proteção que compõe a solução de segurança, funcionam em múltiplos equipamentos e/ou softwares desde que obedeçam a todos os requisitos desta especificação; 3. A solução possui a capacidade e vem licenciada para integrar-se com a solução de firewall do fabricante Palo Alto Networks, implantada no órgão, permitindo utilizá-la como parte da solução de segurança suportando o monitoramento do tráfego de rede e correlacionando os eventos de segurança da camada de rede com os eventos ocorridos nos endpoints protegidos de modo centralizado, proporcionando uma análise de risco mais assertiva e completa; 4. Estão inclusas na proposta todas as licenças necessárias para o pleno funcionamento da solução, conforme as especificações elencadas; 5. A solução vem licenciada para retenção de logs pelo período mínimo de 30 dias, o que deve incluir o cluster de Firewall da Palo Alto Networks, modelo PA-5220, composto por 2 appliances, além dos logs dos agentes de proteção de endpoint, inerentes à solução. 5.1. A solução permite a expansão desse período de retenção de logs, conforme as necessidades da instituição, devendo ser licenciado posteriormente, conforme o caso. 6. A solução possui subscrição pelo período mínimo de 12 (doze) meses, permitindo, durante este período, acesso ilimitado à console central de gerenciamento na nuvem, acesso a todas as atualizações, serviços de segurança e assinaturas de proteção da solução e o pleno funcionamento do agente de proteção instalado nos endpoints. **CARACTERÍSTICAS GERAIS** 1. Entende-se por Endpoint uma estação de trabalho, servidor de rede ou dispositivo móvel; 2. A proteção avançada dos endpoints é feita através da instalação de agentes nos endpoints, suportando, pelo menos os seguintes sistemas operacionais: 2.1. Android 6 e superiores; 2.2. Windows Vista; 2.3. Windows 7; 2.4. Windows 8; 2.5. Windows 8.1; 2.6. Windows 10; 2.7. Mac OS X 10.13 e superiores; 2.8. Windows Server 2003; 2.9. Windows Server 2003 R2; 2.10. Windows Server 2008; 2.11. Windows Server 2008 R2; 2.12. Windows Server 2012; 2.13. Windows Server 2012 R2; 2.14. Windows Server 2016; 2.15. Windows Server 2019 2.16. Windows Server Datacenter 2.17. RHEL/CentOS/Oracle Linux 6 e superiores; 2.18. Debian Linux 9 e superiores; 2.19. Ubuntu Linux 12 e superiores; 3. Suporta e possuir agente para máquinas virtuais instaladas em ambiente VMware; 4. Proteção contra desinstalação não autorizada dos agentes de endpoint que compõem a solução; 5. Proteção contra a desativação não autorizada dos serviços que compõem a solução; 6. É eficaz na prevenção de vulnerabilidades e malwares mesmo quando estiver sem conectividade com servidores de gerenciamento e/ou recursos baseados em nuvem; 7. O agente de endpoint continua funcionando e aplicando políticas de controle mesmo se houver interrupção da comunicação com o gerenciamento centralizado; 8. Impede executável malicioso, sem requerer nenhum conhecimento prévio do artefato; 9. Previne contra ameaças conhecidas baseado em assinatura; 10. Previne contra ameaças baseada em comportamento através do monitoramento das atividades realizadas pelo endpoint;11. Previne contra ameaças através do uso de machine learning através da análise local de arquivos desconhecidos; 12. Possibilidade de colocar arquivos, diretórios e processos em listas de exclusões para não serem verificados pela proteção em tempo real; 13. Possui funcionalidades que permitem o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados; 14. A solução permite implementação em modo de monitoramento ou aprendizado do ambiente em fase inicial de instalação; 15. A solução fornece a capacidade de configurar listas brancas globais para permitir que determinados arquivos executáveis sejam executados dentro de determinadas condições da instituição; 16. A solução tem a capacidade de criar, a partir de incidentes, uma regra de exceção para permitir que um processo seja executado em um determinado endpoint; 17. Permite bloquear nos endpoints o uso de dispositivos portáteis USB como pen drives, discos, drives de CD/DVD/BluRay a fim de prevenir contra a transferência de arquivos maliciosos por meio destes dispositivos; 18. Possui firewall de host permitindo o controle da comunicação do endpoint através de regras de permissão e bloqueio do tráfego; 19. A solução armazena as informações de alertas, incidentes e suas respectivas atividades e ações e demais dados relacionados aos eventos de segurança detectados por um período mínimo de 30 (trinta) dias; **PROTEÇÃO CONTRA VULNERABILIDADES** 1. A solução suporta a proteção de processos e aplicativos em execução no sistema operacional; 2. A solução suporta a adição de aplicações proprietárias e personalizadas na lista de aplicações protegidas; 3. A solução é capaz de fornecer prevenção em tempo real contra exploração de vulnerabilidades de aplicações, bloqueando em tempo real a exploração, não limitadas a falhas de lógica de software, corrupção de memória e sequestro de DLL; 4. A solução é capaz de proteger contra explorações de quaisquer vulnerabilidades não descobertas (desconhecidas) dos aplicativos através do bloqueio de métodos (técnicas e subtécnicas) utilizados para exploração; 5. Ao impedir ou bloquear uma técnica de exploração, a solução congela o processo, coletar informações forenses, de no mínimo, nome do processo, origem e caminho do arquivo, data/hora, dump de memória, versão do SO, usuário, versão vulnerável do aplicativo; 6. Ao impedir ou bloquear uma técnica de exploração, a solução finaliza apenas o processo específico alvo do ataque; 7. A solução utiliza módulos de métodos de exploração para prevenir ou bloquear tentativas de exploração. Os módulos de métodos de exploração protegem aplicações conhecidas, bem como aplicações desconhecidas e desenvolvidas internamente pela instituição; 8. A solução é capaz de criar regras de exclusão para excluir endpoints específicos e processos específicos do log de eventos de ameaças de segurança da console de gerenciamento da solução; 9. Suporta detecção e bloqueio de, no mínimo, os seguintes métodos, sendo capaz de: 9.1. Impedir execução de dados na memória; 9.2. Impedir acessos não autorizados a DLLs do sistema; 9.3. Prevenir utilização de DLLs protegidas com fim de ganhar controle de processos e carregar arquivos CPL (painel de controle) maliciosos; 9.4. Interromper a ocorrência de heap sprays após detecção de exceções suspeitas ou indicativos de tentativas de exploração no host monitorado; 9.5. Prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração em processadores de texto; 9.6. Prevenir o acionamento de vulnerabilidades que resultem na corrupção da área heap na memória. Exemplo: "free() double"; 9.7. Prevenir o uso de novas técnicas que possam evadir o DEP (prevenção de execução de dados em memória) e ASLR (randomização do layout de endereçamento em memória); 9.8. Obrigar a realocação de módulos do sistema operacional, protegendo-os de tentativas de exploração; 9.9. Ser capaz de detectar e prevenir instâncias de heap spray usando algoritmo de			

	detecção de aumento de consumo de memória, indicando execução de exploração de vulnerabilidade; 9.10. Prevenir mapeamento de código no endereço zero (início da memória) do espaço de memória do sistema operacional, dessa forma impedindo uso de explorações de referência nula para execução de código arbitrário, exposição de informações de debug, etc; 9.11. Proteger o acesso a metadados de bibliotecas críticas do sistema operacional quando estas são descompactadas em memória; 9.12. Agir preventivamente contra heap spray ao checar periodicamente a zona heap da memória virtual; 9.13. Prevenir a exploração de vulnerabilidade através da préalocação aleatória do layout de memória de processos no sistema operacional; 9.14. Prevenir uso de programação orientada a retorno (return oriented programming) protegendo APIs (interface de programação de aplicação) usadas em cadeias de ROP e técnicas de exploração usando compilações "Just-in-time" (JIT); 9.15. Mitigar o abuso e captura das estruturas de gerenciamento de exceções (SEH) em memória, impedindo a execução de código malicioso arbitrário no sistema operacional; 9.16. Reservar e proteger determinadas áreas da memória comumente utilizadas para armazenamento de cargas (payload) e instruções maliciosas usando técnicas como heap spray, por exemplo; 9.17. Prevenir vulnerabilidades lógicas na estrutura de atalhos (links) de sistemas operacionais Windows, onde o carregamento impróprio de atalhos permite execução arbitrária de código em memória; 9.18. Prevenir contra vulnerabilidades utilizadas em ataques de escalação de privilégios no sistema operacional explorando a instrução sys.exit para retornar ao nível de execução de usuário, após execução de código em nível de sistema (privilege level 0); 9.19. Aprimorar ou implementar a randomização do layout de endereços em memória (ASLR), garantindo maior aleatoriedade e robustez. Deve também ser capaz de tornar obrigatório o uso da função ASLR; **PROTEÇÃO CONTRA MALWARE** 1. A solução suporta a proteção contra a execução de arquivos maliciosos; 2. A solução fornece a capacidade de fazer controle e restringir os parâmetros sobre como executáveis podem executar incluindo proteção contra criação de processos filhos; 3. A solução é capaz de fornecer prevenção contra malware desconhecido usando análise dinâmica em ambiente de sandbox; 4. A solução possui integração com o serviço de análise de malwares desconhecidos em nuvem (sandbox) para uma análise mais profunda dos arquivos; 4.1. Fornece veredito e relatório informando o resultado da análise em sandbox; 5. O serviço de análise em nuvem é do mesmo fabricante da solução de proteção avançada de endpoint ou de fabricantes terceiros devendo ser fornecidas todas as licenças necessárias para seu pleno funcionamento; 6. O serviço de análise de malwares desconhecidos em nuvem possui a capacidade de realizar a análise dos arquivos em ambientes bare metal para detectar malwares VM-aware, que possuem a capacidade de detectar que estão em um ambiente virtual e nesta situação não realizam as atividades maliciosas para as quais foi desenvolvido; 7. O serviço de análise de malwares desconhecidos em nuvem realiza a análise de, no mínimo, os seguintes tipos de arquivos: arquivos executáveis, DLLs arquivos Word (.doc, .docm e docx) e Excel (.xls, .xlsm e .xlsx) que contenham macros, arquivos DMG e arquivos ELF; 8. A solução fornece a capacidade de criar exceções para hash específicos de arquivos analisados em nuvem na solução de sandbox; 9. A solução fornece a capacidade de impedir a execução de um arquivo quando seu valor de hash for desconhecido pela solução de sandbox; 10. A solução fornece a capacidade de impedir a execução de um arquivo quando o hash do arquivo for desconhecido por cache local e o mesmo não tiver comunicação com o servidor de gerência; 11. Permite executar a varredura no endpoint em busca de arquivos infectados por malware a partir da console central de gerenciamento e a partir do próprio agente instalado no endpoint. É possível também configurar varreduras agendadas; 12. Caso um malware seja detectado, é possível o envio do mesmo para quarentena automaticamente através de política pré-definida na gerência centralizada; 13. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo e não apenas por sua extensão; 14. Extrai o hash de arquivos executáveis e verificar se o mesmo já foi analisado na solução de sandbox de forma automática sem necessidade de scripts externos ou adaptações não nativas da solução. Caso o malware já tenha apresentado comportamento malicioso em sandbox, o mesmo é impedido de ser executado no endpoint; 15. Possui mecanismos para detectar, em tempo real, ataques LotL - Living off the Land, ataques baseados em scripts e ataques fileless (sem arquivos); 16. Permite ao administrador reportar falsos positivos na análise de malwares em sandbox. A solução informa ao administrador o resultado desta análise e exibir a correção na gerência da solução; 17. Avisa o usuário quando a execução de um arquivo for bloqueada incluindo casos quando não houver veredito da sandbox sobre o arquivo e o seu status estiver definido como desconhecido; 18. Possibilita o bloqueio automático de malwares já descobertos através da sandbox do fabricante em outros endpoints do órgão; 19. É capaz de restringir a execução de arquivos específicos somente em diretórios conhecidos e protegidos, tanto na máquina local quanto em drives remotos; 20. Previne execução de arquivos não assinados; 21. Previne a execução de arquivos em mídia externa; 22. É capaz de controlar executáveis não assinados por meio do uso de WhiteLists; 23. É capaz de restringir a execução de processos; 24. Possui a capacidade de controlar e limitar a criação de processos filhos; 25. Possibilita o controle de arquivos conhecidos e não conhecidos; 26. É capaz de definir e classificar Hashs conhecidos. **COLETA DE INFORMAÇÕES FORENSES** 1. A solução coleta dados forenses capturados pelo agente de endpoint, contemplando, pelo menos, os seguintes: 1.1. Dump de memória; 1.2. Arquivos Acessados; 1.3. Módulos carregados; 1.4. URIs acessadas; 1.5. Local de execução do arquivo; 1.6. Tempo de execução; 1.7. Nome do arquivo; 1.8. Hash do arquivo; 1.9. Nome do usuário relacionado; 1.10. Nome do computador; 1.11. Endereço IP; 1.12. Versão de sistema operacional; 1.13. Histórico de arquivos maliciosos; **GERENCIAMENTO** 1. A console de gerenciamento é baseada em nuvem e acessada através de navegadores web, devendo conter de forma centralizada os recursos para a monitoração e controle da proteção dos dispositivos; 2. A console apresenta Dashboard com o resumo do estado de proteção dos dispositivos protegidos, bem como indicar os alertas de eventos de criticidades alta, média e baixa; 3. Possui mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM; 4. A console permite, dentro da estrutura de gerenciamento, a organização dos dispositivos protegidos em grupos; 5. Permite a aplicação de regras diferenciadas baseadas em dispositivos ou grupos de dispositivos; 6. A console de gerenciamento permite a definição de grupos de usuários com diferentes níveis de acesso as configurações, políticas e logs; 7. A solução é compatível, no mínimo, com os navegadores (web browsers) Firefox e Chrome; 8. Caso a solução necessite de Banco de Dados (Ex.			

	SQL Server Enterprise), estarão inclusas na proposta as licenças necessárias para seu pleno funcionamento; 9. A comunicação entre a console de gerenciamento e os clientes gerenciados é feita através do uso de protocolos seguros e protegidos por criptografia; 10. É possível realizar acesso direto aos endpoints protegidos a partir da console central de gerenciamento da solução, a fim de permitir a execução de ações para investigação e reposta aos incidentes de segurança como: visualizar e encerrar processos, apagar, mover e renomear arquivos, prover interface de linha de comando capaz de executar comandos do sistema operacional e executar scripts e comandos python nos endpoints; 11. É possível salvar um relatório contendo todas as atividades realizadas durante a sessão de acesso aos endpoints gerenciados; 12. É possível realizar, a partir da console de gerenciamento, a execução simultânea de scripts nos diversos endpoints de forma centralizada; 13. A solução permite, a partir da console central de gerenciamento, isolar um endpoint impedindo a comunicação do mesmo com a rede para evitar que um possível ataque se propague pela rede; 14. Possui mecanismo de comunicação prédefinido, em tempo determinado e configurável pelo administrador, entre os agentes nos endpoints e a console de gerenciamento, provendo a consulta de novas configurações, políticas ou conteúdo; 15. Permite a criação de, no mínimo, três perfis de acesso distintos para os usuários administradores da solução; 16. Registra nos logs as alterações realizadas pelos administradores da solução, provendo auditoria de mudanças; 17. A solução é capaz de exportar seus logs no formato syslog para outras soluções de gerenciamento de logs; 18. A atualização do motor de detecção de ameaças é realizada de forma transparente para o usuário; 19. Permite integração com soluções de SIEM enviando logs no formato Syslog ou compatível; 20. Se comunica, por meio de logs de incidentes e ataques ou informações de inteligência, com os elementos de segurança do ambiente, como por exemplo, mas não se limitando a: Firewalls, Proxies, Filtros de Conteúdo; 21. Exibe lista com todos os alertas de incidentes detectados na console central de gerenciamento. Deve mostrar, para cada alerta da lista, no mínimo, a data e hora que o incidente ocorreu, o nome ou endereço IP envolvido, a ação tomada pelo agente com relação ao incidente e a categoria do incidente informando se o mesmo se trata de exploit ou malware, por exemplo; 22. Permite notificar eventos ao administrador por e-mail; 23. Permite a criação de políticas para prevenção e mitigação de: 23.1. Vulnerabilidades conhecidas e desconhecidas (Exploits); 23.2. Códigos Maliciosos (Malware); 23.3. Restrições de execução; 24. Centraliza e gerencia na console de administração qualquer evento de segurança detectado, seja na camada de rede ou nos endpoints protegidos; 25. É exibida também, na console central de gerenciamento, a lista de CVE - Common Vulnerabilities and Exposures - conhecidos e permitir visualizar quais endpoints estão sendo afetados por uma determinada CVE; 26. Identifica e gera log de qualquer interferência no serviço de proteção nas estações e servidores protegidos, como por exemplo: 26.1. Tentativa de encerramento do processo de proteção; 26.2. Tentativa de encerramento do serviço de proteção; 26.3. Logs de sistema relacionados a tentativa de interferência com o serviço, processo ou arquivos do sistema de proteção; 27. É possível visualizar, em uma linha do tempo, a cadeia de processos e eventos, desde a execução do primeiro processo responsável pela execução dos demais, que geraram um alerta de incidente. Para cada processo executado é possível visualizar, no mínimo, o caminho onde o processo estava localizado, o nome do usuário que iniciou o processo e o tempo em que o processo ficou em execução informando a data e hora do início e do fim da execução do mesmo; 28. Além dos processos executados são exibidas informações sobre conexões de entrada e saída, conexões fracassadas e download e upload de dados; 29. A solução permite o ajuste de políticas de coleta de informações forenses, dentro da console de gerenciamento centralizado, com definições do tipo de informações sobre o incidente que serão coletadas quando uma ameaça ou ataque for identificado; 30. Possui ferramenta de busca para a investigação de incidentes permitindo a realização de buscas com base em, no mínimo, processos executados, em arquivos criados, alterados e deletados, em atributos de rede como endereço IP, nome do host, porta e protocolo, em registros criados, modificados e deletados, em eventos de log do Windows e do Linux. Permite também realizar a busca através da combinação destes atributos; 31. É possível a realização de busca com base no caminho completo onde o arquivo pode estar localizado e também com base no hash do arquivo gerado pela solução. 32. A solução permite realizar a configuração de alertas com base em incidentes e em indicadores de comprometimento, como nome do arquivo, domínio e endereço IP de destino. A solução permite importar listas de indicadores de comprometimento de serviços externos de inteligência contra ameaça, além de permitir a criação destes indicadores; 33. A solução permite realizar a configuração de alertas baseados no comportamento do endpoint. Os tipos de comportamentos detectados são, no mínimo, execução de processos, manipulação de privilégios em arquivo, ofuscação do tipo do arquivo, atividade de reconhecimento na rede escalonamento de privilégio e movimentos laterais na rede; 34. A solução permite realizar a atualização de versão dos agentes instalados nos endpoints a partir da console central de gerenciamento; 35. A solução recebe e distribui atualizações contendo ajustes finos de políticas de proteção, de módulos de proteção e novos modelos matemáticos para uso de aprendizagem de máquina (Machine Learning) para análise de código antes da execução; RELATÓRIOS 1. A solução fornece visualização das ameaças em formato Web; 2. A solução suporta exportação no formato CSV dos eventos relacionados à ameaças, bem como o status dos agentes de endpoints; 3. Capacidade de geração de relatórios, estatísticas e gráficos contendo no mínimo os seguintes tipos pré-definidos: 3.1. As 10 máquinas com maior ocorrência de códigos maliciosos; 3.2. Os 10 usuários com maior ocorrência de códigos maliciosos; 3.3. Localização dos códigos maliciosos; 3.4. Sumário das ações realizadas; 3.5. Número de infecções detectadas diária, semanal e mensalmente; 4. Abrange os códigos maliciosos detectados; 5. A solução tem os seguintes dashboards nativos para monitorar a postura de segurança e o status da instituição: 5.1. Relatório de restrição de acesso a arquivos e processos; 5.2. Técnicas de Malwares utilizadas; 5.3. Técnicas de exploração utilizadas; 5.4. Informações Forenses coletadas. 6. .6. A solução tem os seguintes dashboards de controle para monitorar a situação dos endpoints da instituição: 6.1. Detalhes da saúde dos agentes de endpoints; 6.2. Dashboard de controle do histórico de regras dos endpoints; 6.3. Dashboard de controle da Política de Segurança instalada nos endpoints; 6.4. Dashboard de controle do histórico de status do serviço nos endpoints; Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos.			

	Garantia: 12 meses Procedência: Estados Unidos Fabricante: Palo Alto Networks Modelo: Cortex XDR Pro Part Numbers: 1 x PAN-XDR-ADV-EP Links de comprovação: Palo Alto Cortex XDR Website https://www.paloaltonetworks.com/cortex/cortex-xdr Palo Alto Cortex XDR Datasheet https://www.paloaltonetworks.com/resources/ datasheets/cortex-xdr Palo Alto Cortex XDR TechDocs Website https://docs.paloaltonetworks.com/cortex/cort ex-xdr.html Palo Alto Cortex XDR Pro Administrator's Guide https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-pro-admin/cortex-xdr-proadmin.pdf Palo Alto Cortex XDR API Reference https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-api/cortex-xdr-api.pdf Palo Alto Networks Compatibility Matrix https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/compatibilitymatrix/compatibility-matrix.pdf			
2	**Add-on Host Insight para Cortex XDR Pro por endpoint. Subscrição pelo período de 12 meses GERENCIAMENTO DE VULNERABILIDADES E INVENTÁRIO** 1. Provê informações capazes de enriquecer a análise de segurança do ambiente, aumentando a visibilidade e fornecendo melhor compreensão dos riscos; 2. Provê elementos capazes de neutralizar rapidamente ameaças à segurança institucional; 3. Reduz os esforços do diagnóstico ao fornecer informações abrangentes e suficientes permitindo melhorar o tempo de resposta dos incidentes; 4. Provê, de forma rápida e simples, recurso capaz de realizar a busca e a remoção do arquivo malicioso de todos os endpoints gerenciados; 5. Possui o recurso de inventário, sendo capaz de exibir, em detalhes, diversas informações dos sistemas dos endpoints; 6. Exibe detalhes sobre os aplicativos instalados que requerem e receberam permissões especiais para habilitar uma câmera, microfone, recursos de acessibilidade, acesso total ao disco ou capturas de tela; 7. Exibe detalhes sobre executáveis que iniciam automaticamente quando o usuário efetua login ou inicializa o sistema operacional do dispositivo protegido; 8. A solução exibe informações sobre autoruns que são configurados no registro do endpoint, pastas de inicialização, tarefas agendadas, serviços, drivers, daemons, extensões, tarefas Crond, itens de login, ganchos de login e logout; 9. Para cada execução automática, a solução lista o tipo e a configuração da execução automática, como método de inicialização, CMD, detalhes do usuário e caminho da imagem; 10. Exibe, pelo menos os seguintes detalhes, para cada daemon existente no endpoint gerenciado: 10.1. Nome, tipo, caminho e estado, indicando se está carregado, em execução ou não; 11. Exibe detalhes sobre cada volume de disco existentes em um endpoint, como os seguintes: 11.1. Tipo de unidade, nome, sistema de arquivos, espaço livre e tamanho total; 11.2. Mostrar informações como nome, tipo, caminho, modo e estado de todos os drivers instalados em um dispositivo gerenciado; 12. Exibe detalhes sobre todas as unidades, volumes e discos que foram montados no endpoint, a exemplo das seguintes: 12.1. Lista o diretório do ponto de montagem, o tipo de sistema de arquivos, especificações da montagem e GUID; 13. Detalha, para cada serviço em execução em um endpoint, informações como: 13.1. Nome, tipo, caminho, status do tempo de execução, se o serviço está em execução e qual é o estado do tempo de execução, se o serviço pode ser parado, pausado ou atrasado seu horário de início, se o serviço requer interação com a área de trabalho do endpoint, o nome do usuário que iniciou o serviço e o modo de início 14. Mostra detalhes sobre cada pasta compartilhada em rede como: 14.1. Tipo de pasta de rede compartilhada: Disk Drive, Print Queue, Device, IPC, Disk Drive Admin, Print Queue Admin, Device Admin, IPC Admin; 14.2. Nome da pasta, descrição e caminho; 14.3. Se a pasta está limitada a um número máximo de compartilhamentos e o número máximo de compartilhamentos permitidos; 15. Apresenta informações gerais sobre o hardware do endpoint, como fabricante, modelo, memória física, arquitetura de processadores e CPU; 16. Apresenta informações sobre o sistema operacional e a release em execução no endpoint; 17. A solução fornece a lista de usuários cujas credenciais estão armazenadas no endpoint; 18. Fornece informações sobre as contas de usuários, quais estão ativas e o tipos de cada uma; 19. Informa detalhes sobre a senha definida para cada conta de usuário, como se ela é necessária para fazer login, se tem uma data de validade ou se pode ser alterada; 20. Mostra informações de conexões dos ativos em forma de gráficos a fim de simplificar a investigação e proporcionar ganho de eficiência. 21. É capaz de identificar e quantificar as vulnerabilidades de segurança (CVEs) existentes para as aplicações instaladas nos endpoints; 22. Oferece visibilidade em tempo real da exposição às vulnerabilidades e dos níveis de patch atuais dos endpoints, aperfeiçoando a análise de gravidade dos riscos e permitindo priorizar a mitigação. 23. É uma solução eficaz no gerenciamento de vulnerabilidade, devendo ser simples de utilizar, escalonável e do mesmo fabricante da solução avançada de proteção de endpoint. Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos Garantia: 12 meses Procedência: Estados Unidos Fabricante: Palo Alto Networks Modelo: Host Insights Add-on for Cortex XDR Part Number: 1 x PAN-XDR-HOST-INST Links de comprovação: Palo Alto Cortex XDR Website https://www.paloaltonetworks.com/cortex/cortex-xdr Palo Alto Cortex XDR Datasheet https://www.paloaltonetworks.com/resources/ datasheets/cortex-xdr Palo Alto Cortex XDR TechDocs Website https://docs.paloaltonetworks.com/cortex/cort ex-xdr.html Palo Alto Cortex XDR Pro Administrator's Guide https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-pro-admin/cortex-xdr-proadmin.pdf Palo Alto Cortex XDR API Reference https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/cortex/cortexxdr/cortex-xdr-api/cortex-xdr-api.pdf Palo Alto Networks Compatibility Matrix https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/compatibilitymatrix/compatibility-matrix.pdf	unidade	4.500	R$ 39,50
3	**Professional Services Palo Alto para Implantação e Configuração do Cortex XDR Pro.**	unidad	1	R $

	SERVIÇO DE IMPLANTAÇÃO 1. Os serviços são executados pela CONTRATADA, por técnicos comprovadamente credenciados pelo fabricante; 2. A CONTRATADA informará nome, e-mail e telefone dos componentes da equipe técnica responsável pela solução, ou seja, do gerente do projeto, técnico e do responsável comercial; 3. Após o recebimento do Pedido de Compra, a CONTRATADA tem o prazo máximo de 15 (quinze) dias para realizar a Reunião de Alinhamento do Projeto, que será feita de forma remota, onde a CONTRATADA apresentará os técnicos responsáveis pela implantação e suas respectivas documentações exigidas neste Termo de Referência. Nessa mesma reunião será definido o cronograma de implantação/migração da solução; 3.1. O licenciamento da solução será disponibilizado a partir da data de início da execução do cronograma. O Recebimento definitivo fica condicionado à entrega de todos os agentes instalados e licenciados, conforme definido na Reunião de Alinhamento, observadas as considerações dos itens 5.1.2.2.4.1. e 5.1.2.2.4.2. 4. A implantação inicial consiste em aplicar as regras de acordo com a Política de Segurança da Informação do Tribunal de Justiça do Estado do Piauí, podendo ainda serem definidas e criadas novas regras de acordo com as necessidades informadas pela equipe técnica de TI do TJPI, sempre levando em consideração as melhores práticas estabelecidas no mercado; 4.1. É de responsabilidade da CONTRATADA a implantação da solução contemplando todos os itens apresentados neste Termo de Referência ou selecionados de acordo com as necessidades apresentadas pela equipe técnica do TJPI, incluindo todas as configurações necessárias à implantação e integração da solução ao ambiente de segurança do TJPI, sempre com acompanhamento e apoio da equipe técnica do TJPI. 4.1.1. A instalação dos agentes da solução contratada nos endpoints do PJPI será feita em conjunto com a equipe da STIC. 4.2. Todas as configurações a são feitas e aplicadas pela CONTRATADA no ambiente de infraestrutura do TJPI serão previamente apresentadas para a equipe técnica da CONTRATANTE no momento da implantação/configuração da solução. 4.2.1. Tais configurações só poderão ser aplicadas com o aval da equipe técnica de TI do TJPI; 5. No caso de inadequação técnica, o Tribunal de Justiça do Estado do Piauí encaminhará à CONTRATADA os critérios inadequados encontrados nos serviços no prazo máximo de 03 (três) dias úteis; 6. A CONTRATADA avaliará, e, após confirmação das inadequações, deverá ser agendada com o Tribunal de Justiça do Estado do Piauí a manutenção para efetuar as devidas correções; 7. Durante todo o processo de implantação a CONTRATADA prestará suporte em eventuais dificuldades que venham a surgir, sem custo adicional para a CONTRATANTE; 8. Todas as configurações de implantação serão revisadas pelos analistas do Tribunal de Justiça do Estado do Piauí, antes de serem inseridas na nova solução; 9. Todas as etapas das configurações da nova solução serão supervisionadas pela equipe de TI do tribunal; 10. O planejamento da implantação/migração será acordado na reunião de alinhamento do projeto e apresentado antes do início das atividades à equipe responsável da CONTRATANTE, incluindo, mas não se limitando, a análise do ambiente de infraestrutura atual do Tribunal de Justiça do Estado do Piauí e o planejamento da implantação da nova solução. 11. Ao final da implantação e configuração da solução, será realizado o repasse de informações hands-on, apresentando as configurações implementadas na solução, de no mínimo 8 (oito) horas. 12. Todas as despesas referentes aos serviços de implantação são de responsabilidade da CONTRATADA. Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos	e		160.000,00

2. DO FORNECIMENTO

2.1. Esta Ata não obriga a ADMINISTRAÇÃO a firmar contratações com a BENEFICIÁRIA**,** podendo ocorrer licitações específicas para a aquisição dos produtos/serviços registrados, observada a legislação pertinente, sendo assegurada preferência de fornecimento ao BENEFICIÁRIO do registro em igualdade de condições.

2.2. A requisição dos produtos/serviços será formalizada mediante Contrato Administrativo ou Ordem de Fornecimento/Serviço, observadas as disposições contidas no referido Pregão Eletrônico.

2.3. Após a disponibilização no Sistema Eletrônico SEI, os eventuais Contratos Administrativos ou Ordem de Fornecimento/Serviço deverão ser assinados pela BENEFICIÁRIA DO REGISTRO, no prazo de 03 (três) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das penalidades previstas em Edital e Termo de Referência.

2.4. As despesas com a execução deste Registro de Preços serão atendidas com recursos consignados em dotação específica, cujo detalhamento será contido no respectivo Contrato Administrativo ou Ordem de Fornecimento/Serviço, em havendo.

2.5. O pagamento será realizado mediante crédito bancário, **em favor de APPROACH TECNOLOGIA LTDA e vinculado ao CNPJ Nº 24.376.542/0001-21**, não se admitindo, em hipótese alguma, desconto ou cobrança de título na rede bancária, e será efetivado no **Banco:ITAÚ (341) - Agência: 7197, Conta: 33207-0.**

3. DOS ENCARGOS DA BENEFICIÁRIA DO REGISTRO

3.1. O Beneficiário do Registro fica obrigado a atender todos os pedidos efetuados durante a validade desta Ata de Registro de Preços.

3.2. Manter, durante o período do registro de preços, todas as condições de habilitação e qualificação exigidas na licitação, devendo comunicar à ADMINISTRAÇÃO, imediatamente, qualquer alteração que possa comprometer a manutenção desta Ata de Registro de Preços.

4. DAS OBRIGAÇÕES DA ADMINISTRAÇÃO

4.1. Proporcionar à beneficiária do registro todas as facilidades à boa execução do objeto desta Ata de Registro de Preços e designar um representante para acompanhar o eventual fornecimento dos suprimentos registrados, com a finalidade de dirimir eventuais dúvidas.

4.2. Efetuar os pagamentos devidos em função de eventual contratação realizada com base na presente Ata de Registro de Preços.

5. DA VIGÊNCIA

5.1. Esta Ata de Registro de Preços terá vigência 12 (doze) meses, a contar da data de sua publicação no Diário da Justiça TJ/PI.

6. DA REVISÃO E DO CANCELAMENTO DOS PREÇOS REGISTRADOS

6.1. A Administração realizará pesquisa de mercado periodicamente, a fim de verificar a vantajosidade dos preços registrados nesta Ata.

6.2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo do objeto registrado, cabendo à Administração promover as negociações junto à BENEFICIÁRIA DO REGISTRO.

6.3. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, a Administração convocará a BENEFICIÁRIA DO REGISTRO para negociar a redução dos preços aos valores praticados pelo mercado.

6.4. A BENEFICIÁRIA DO REGISTRO que não aceitar reduzir seu preço ao valor praticado pelo mercado será liberado do compromisso assumido, sem aplicação de penalidade.

6.5. Quando o preço de mercado tornar-se superior aos preços registrados e a BENEFICIÁRIA DO REGISTRO não puder cumprir o compromisso, o órgão gerenciador poderá:

6.5.1. Liberar a BENEFICIÁRIA DO REGISTRO do compromisso assumido, **caso a comunicação ocorra antes do pedido de fornecimento**, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

6.5.2. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

6.6. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação desta ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.
6.7. O registro do fornecedor será cancelado quando:
6.7.1. Descumprir as condições da ata de registro de preços;
6.7.2. Não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;
6.7.3. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou
6.7.4. Sofrer sanção administrativa cujo efeito torne-o proibido de celebrar contrato administrativo.
6.8. O cancelamento de registros nas hipóteses previstas nos itens 6.7.1, 6.7.2 e 6.7.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.
6.9. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados:
6.9.1. Por razão de interesse público; ou
6.9.2. A pedido do fornecedor.
7. DAS CONDIÇÕES PARA ADESÃO DA ATA DE REGISTRO DE PREÇOS
7.1. Desde que devidamente justificada a vantagem, a ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da administração pública que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador.
7.2. Os órgãos e entidades que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar o órgão gerenciador da ata para manifestação sobre a possibilidade de adesão.
7.3. A manifestação do órgão gerenciador fica condicionada à realização de estudo, pelos órgãos e pelas entidades que não participaram do registro de preços, que demonstre o ganho de eficiência, a viabilidade e a economicidade para a administração pública da utilização da ata de registro de preços, conforme estabelecido em ato do Secretário de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão.
7.4. O estudo de que trata o item anterior, após aprovação pelo órgão gerenciador, será divulgado no Portal de Compras do Governo federal.
7.5. Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o órgão gerenciador e órgãos participantes.
7.6. As aquisições ou as contratações adicionais de que trata este artigo não poderão exceder, por órgão ou entidade, a **cinquenta por cento dos quantitativos** dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.
7.7. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, **ao dobro do quantitativo de cada item registrado** na ata de registro de preços para o órgão gerenciador e para os órgãos participantes, independentemente do número de órgãos não participantes que aderirem.
7.8. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata.
7.9. Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.
7.10. É vedada aos órgãos e entidades da administração pública federal a adesão a ata de registro de preços gerenciada por órgão ou entidade municipal, distrital ou estadual.
8. DA PUBLICIDADE
8.1. Esta Ata de Registro de preços será publicado no Diário da Justiça, conforme dispõe o artigo 61, parágrafo único, da Lei nº 8.666/1993, e divulgada no site www.tjpi.jus.br.
9.DAS DISPOSIÇÕES FINAIS
9.1. As condições gerais do fornecimento, tais como os prazos para entrega e recebimento do objeto, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, bem como no Edital e suas minutas.
9.2. Caberá à BENEFICIÁRIA DO REGISTRO, observadas as condições estabelecidas nesta Ata de Registro de Preços, optar pela aceitação ou não do fornecimento a órgão ou entidade da administração pública que não tenha participado do certame, desde que esse fornecimento não prejudique as obrigações anteriormente assumidas.
9.3. O gerenciamento desta Ata de Registro de Preços caberá à Superintendência de Licitações e Contratos do tribunal de Justiça do Estado do Piauí - SLC/TJPI.
10. DO FORO
10.1. Fica eleito o Foro da Justiça Estadual do Estado da Piauí, na Comarca de Teresina, para dirimir questões oriundas deste instrumento, com renúncia expressa de qualquer outro por mais privilegiado que seja.
E por estarem as partes, justas e acordadas, firmam o presente instrumento, assinando-o eletronicamente, conforme art. 1º, III, "b", da Lei nº 11.419/2006 e Resolução 22/2016/TJPI, para que produza seus efeitos jurídicos legais.

Documento assinado eletronicamente por **José Ribamar Oliveira**, **Presidente**, em 02/02/2022, às 13:57, conforme art. 1º, III, "b", da Lei 11.419/2006.
Documento assinado eletronicamente por **KENT JOHANN MODES**, **Usuário Externo**, em 02/02/2022, às 15:12, conforme art. 1º, III, "b", da Lei 11.419/2006.
A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **3010258** e o código CRC **09E5D477**.

6. GESTÃO DE CONTRATOS

6.1. EXTRATO DE TERMO ADITIVO

ATO/ESPÉCIE: PRIMEIRO TERMO ADITIVO AO CONTRATO Nº 149/2021
PROCESSO ADMINISTRATIVO: 22.0.000002162-1
CONTRATANTE: FUNDO ESPECIAL DE REAPARELHAMENTO E MODERNIZAÇÃO DO PODER JUDICIÁRIO DO ESTADO DO PIAUÍ - FERMOJUPI
CNPJ/CONTRATANTE: 10.540.909/0001-96
EMPRESA/CONTRATADA: IPÊ INDÚSTRIA DE MÓVEIS EIRELI
CNPJ/CONTRATADA: 33.817.864/0001-50
OBJETO/RESUMO: O presente Termo Aditivo tem por objetivo a **prorrogação do prazo de entrega do objeto do Contrato n. 149/2021.**