Termo de especificação de requisitos para contratação de serviços gerenciados de Segurança da Informação e Cibersegurança

Disposições Iniciais

1. As propostas devem compreender a formação de preços de acordo com as seguintes orientações:
   1.1. O preço deverá ser informado de acordo com os itens requisitados.
2. Avaliação das propostas será baseada do ponto de vista de atendimento aos requisitos apresentados e de valor proposto, sendo considerado o que melhor atender as necessidades do CNPEM.
3. Os Proponentes deverão apresentar no mínimo 3 atestados de capacidade técnica de execução dos serviços solicitados, com escopo similar ao apresentado nos requisitos. Esta avaliação deverá possuir caráter classificatório para a concorrência.
4. Os valores deverão ser expressos considerando pagamentos mensais e contratos de 12, 24 e 36 meses.

Item 1 – Pacote de serviço de Gestão de Cibersegurança

1.1 SOC - Security Operation Center (N1, N2 e N3 + SIEM)

Objeto: Contratação de serviços gerenciado de monitoração de eventos de Segurança Cibernética, executando atividades de SOC (Security Operation Center) Nível 1 para comunicação, tratamento e resposta a incidentes, através da identificação, análise e registro de possíveis incidentes de segurança e acionamento do SOC N2/N3 com utilização de ferramenta SIEM.

Escopo

Escopo	Qtd
Active Directory Servers (AD/AzureAD) Microsoft	4
Cofre de Senhas Opensource/Syspass	1
DNS Servers Opensource/Microsoft	4
DHCP Servers Microsoft	4
Firewall (DataCenter/Core) Fortinet	3
Roteadores CORE	20
WAF Fortinet	1
File Server	4
Banco de Dados	13
Servidores Backup	4
Servidores Publicados na Internet	8

Requisitos para o Serviço Gerenciado

- Monitorar e identificar e comunicar eventos de segurança cibernética com níveis de atendimento (N1, N2 e N3);
- O monitoramento deverá atender no modelo 24x7x365;
- Estabelecimento de SLA compatível com tempos hábeis para comunicação, acionamento, escalonamento e abertura de chamado conforme sugerido tabela a seguir:

Serviço	Criticidade	Tempo de acionamento	Escalonamento	Abertura de chamado
SOC N1/N2/N3	Desastre	Imediatamente	5 minutos (quando sem resposta)	Imediatamente
	Crítico	5 Minutos	10 minutos (quando sem resposta)	5 Minutos
	Alto	10 Minutos	15 minutos (quando sem resposta)	10 Minutos
	Médio	15 Minutos	20 minutos (quando sem resposta)	15 Minutos

- Realizar a triagem dos eventos de segurança;
- Classificar os eventos de segurança identificados de acordo com sua criticidade;
- Elaborar scripts de casos de uso (rules);
- Realizar identificação de falso positivo;
- Identificar e comunicar desvios de comportamento na infraestrutura monitorada;
- Propor a criação, alteração, customização, renomeação e/ou remoção de regras, para melhorar os alertas, diminuir a quantidade falsos-positivos, aumentar sua qualidade/efetividade;
- Sugerir elaboração, mudanças e manutenção de scripts para cada caso de uso;
- Sugerir elaboração de planos de melhorias no processo de análise de potenciais incidentes;
- Orientar e auxiliar no tratamento de eventos de segurança identificados pelo SOC;
- Realizar abertura de tickets para os eventos de segurança através de plataforma de Gestão de Serviço fornecida pela Proponente;
- Estabelecer canais de comunicação e cadeia de acionamento junto ao CNPEM;
- O serviço será prestado de maneira remota;
- O CNPEM deverá ter acesso a interface de monitoramento via internet através de um usuário e senha com permissão apenas de visualização fornecido pela Proponente;
- O Proponente deverá
- **Entregáveis:**
    - **Plataforma de gerenciamento de chamado e comunicação;**
    - **Reuniões periódicas (cada 15 dias) para repasse e alinhamento;**
    - **Relatório periódico (mensal) executivo de ações realizadas no período;**

- **Dashboard online para acompanhamento em tempo real dos indicadores de segurança suportados pelo Item 1 deste termo de requisitos**

Requisitos para o fornecimento da ferramenta SIEM

- O licenciamento da ferramenta SIEM deverá ser de responsabilidade da Proponente;
- A ferramenta SIEM deverá ser fornecida no modelo CLOUD (SAAS);
- A ferramenta SIEM deverá atender aos seguintes requisitos (mínimos, mas não se limitando a):
  - **Coleta Multifonte de Dados**: A capacidade de coletar logs e dados de uma variedade de fontes, como sistemas operacionais, aplicativos, firewalls, roteadores, dispositivos de segurança e mais.
  - **Normalização e Correlação de Eventos**: A ferramenta deve ser capaz de normalizar e correlacionar eventos de diferentes fontes para identificar relacionamentos e padrões de atividade suspeita.
  - **Detecção de Ameaças Avançada**: Recursos como análise de comportamento anômalo, detecção de ataques conhecidos e desconhecidos, além de detecção de insider threat, para identificar atividades maliciosas.
  - **Monitoramento em Tempo Real**: Capacidade de monitorar eventos em tempo real, gerando alertas imediatos sobre atividades suspeitas ou eventos anormais.
  - **Análise e Investigação**: Recursos avançados de análise de dados que permitem aos analistas investigarem incidentes com eficácia, traçar a cadeia de eventos e determinar a extensão do comprometimento.
  - **Resposta a Incidentes**: Possibilidade de automatizar respostas a incidentes, como bloqueio de tráfego malicioso ou isolamento de dispositivos comprometidos.
  - **Geração de Relatórios**: Capacidade de gerar relatórios detalhados e personalizados para fins de conformidade, auditoria e compartilhamento com partes interessadas.
  - **Integração com Outras Ferramentas**: A habilidade de integrar com outras ferramentas de segurança, como firewalls, antivírus, soluções EDR, para obter uma visão completa do ambiente.
  - **Gerenciamento de Incidentes**: Recursos que facilitam o rastreamento e a resolução de incidentes, incluindo atribuição de tarefas, acompanhamento do status e documentação.
  - **Armazenamento e Retenção de Dados**: Capacidade de armazenar e reter dados de eventos por no mínimo 1 ano (365 dias), para análises futuras e para atender a requisitos de conformidade.
  - **Escalabilidade**: A ferramenta deve ser capaz de lidar com um grande volume de eventos e dados à medida que a organização cresce.
  - **Usabilidade e Interface Amigável**: Uma interface intuitiva que permita que analistas de segurança utilizem a ferramenta efetivamente sem uma curva de aprendizado extensa.

- **Personalização e Flexibilidade**: A possibilidade de criar regras personalizadas, consultas de pesquisa e painéis de controle adaptados às necessidades da organização.
- **Suporte a Padrões de Conformidade**: Deve ser capaz de atender aos padrões regulatórios relevantes, como PCI DSS, GDPR, HIPAA, fornecendo relatórios e recursos específicos.

- **Entregáveis:**
  - **Acesso a plataforma de gestão de eventos (SIEM);**

1.2 Gestão de Vulnerabilidades

Objetivo

O objetivo deste serviço é examinar de forma minuciosa os ativos de tecnologia do CNPEM a fim de identificar possíveis vulnerabilidades, patches e configurações e propor correções para mitigar os riscos que possam ser exploradas por ameaças cibernéticas.

Escopo

Escopo	Qtd
Endpoints (Windows, Linux, MacOS)	2200
Servidores (Windows, Linux)	220
Conectividade (segmentos de rede)	255

Requisitos para prestação do Serviço de Gestão de Vulnerabilidade

- **Varredura de Vulnerabilidades**: Deve ser capaz de realizar varreduras regulares e abrangentes em sistemas, redes, aplicativos e ativos de TI para identificar vulnerabilidades.
- **Avaliação de Riscos**: Deve permitir avaliar o risco associado a cada vulnerabilidade com base em critérios como probabilidade de exploração e impacto.
- **Priorização Automatizada**: Deve ter recursos que permitam a priorização automática das vulnerabilidades com base em suas características e nível de risco.
- **Integração com Fontes de Dados**: Deve integrar feeds de inteligência de ameaças, bancos de dados de vulnerabilidades e scanners externos para obter informações atualizadas (ex: MISP, VirusTotal, NVD, VulDB, CVE, CVSS, OWASP).
- **Geração de Relatórios Detalhados**: Deve gerar relatórios detalhados sobre as vulnerabilidades identificadas, incluindo descrições, classificações de risco e recomendações de correção.

- **Integração com Soluções de TI**: Deve ser capaz de integrar com ferramentas de gerenciamento de ativos de TI para manter informações sobre sistemas e aplicativos atualizadas.
- **Detecção de Ativos**: Deve ser capaz de identificar e rastrear ativos, incluindo servidores, estações de trabalho, dispositivos de rede e aplicativos.
- **Workflow de Correção**: Deve fornecer um fluxo de trabalho para acompanhar o progresso da correção das vulnerabilidades, atribuindo tarefas e responsabilidades.
- **Acompanhamento de Ciclo de Vida**: Deve permitir o acompanhamento das vulnerabilidades desde a identificação até a correção completa.
- **Integração com Sistemas de Ticketing**: Deve se integrar com sistemas de gerenciamento de tickets para garantir uma comunicação eficiente entre equipes de segurança e TI.
- **Análise de Resultados**: Deve permitir análise e interpretação detalhada dos resultados das varreduras, incluindo correlação de eventos.
- **Suporte a APIs**: Deve oferecer APIs para integração com outras ferramentas e sistemas.
- **Visualização de Dados**: Deve fornecer painéis e gráficos para visualizar o status das vulnerabilidades e tendências ao longo do tempo.
- **Suporte a Automação**: Deve permitir a automação de tarefas, como agendamento de varreduras e geração de relatórios.
- **Conformidade e Regulamentações**: Deve ajudar na conformidade com padrões de segurança e regulamentações, fornecendo relatórios específicos.
- **Suporte a Multiplataforma**: Deve ser capaz de identificar vulnerabilidades nas seguintes plataformas:
    - Windows Client (XP, 7, 8, 10, 11)
    - Windows Server (2008, 2012, 2016, 2019, 2022)
    - Linux (Ubuntu, CentOS, Debian, Suse, Oracle Linux)
    - MacOS
    - Switch (Cisco Catalyst, Nexus)
    - Wireless (Aruba Clearpass, Mobility, Controllers)
    - VMWare (ESXi)
- **Notificações e Alertas**: Deve enviar notificações e alertas em tempo real sobre vulnerabilidades críticas através de plataforma de gerenciamento de chamados (tickets).
- **Gerenciamento de Patches**: Deve auxiliar na identificação e no gerenciamento de patches e atualizações para correção de vulnerabilidades.
- **Segurança e Privacidade**: Deve seguir práticas de segurança e proteção de dados, garantindo que as informações sobre vulnerabilidades sejam tratadas com responsabilidade.

- **Entregáveis**:
    - **Acesso a plataforma de gestão de vulnerabilidade**;
    - **Relatórios periódicos (mensal) com os resultados dos scans realizados**;

- **Reuniões periódicas (mensal) com equipe técnica para orientação sobre atendimento e mitigação das vulnerabilidades identificadas**;
- **Plataforma de gestão para controle e registro das vulnerabilidades identificadas nos ativos**.

1.3 Pentest

Objetivo e Escopo

Realizar avaliação de segurança periódica e abrangente nos ativos e sistemas do CNPEM, a fim de identificar vulnerabilidades e riscos de segurança.

Requisitos para prestação do serviço Pentest

- O serviço deverá ser fornecido na modalidade banco de horas com 40 horas mensais;
- O serviço será executado sob demanda, baseado no saldo de horas disponíveis contratadas;
- O Banco de horas poderá ser compartilhado para outras finalidades dentro deste Item 1 – Pacote de serviço de Gestão de Cibersegurança;
- O Pentest deverá ser executado na modalidade “Black Box”;
- Deverá ser capaz de:
    - Identificar vulnerabilidades de segurança que possam ser exploradas para acesso não autorizado.
    - Avaliar a eficácia das medidas de segurança existentes.
    - Testar a capacidade de resposta a incidentes.
    - Avaliação de vulnerabilidades em aplicações web (SQLi, XSS, RCE).
    - Verificar a configuração segura de dispositivos de rede e servidores.
    - Avaliar a segurança das autenticações e autorizações implementadas.
    - Analisar a conformidade com padrões de segurança relevantes.

- **Entregáveis:**
    - **Relatório detalhado deverá ser entregue após a conclusão do teste, contendo descrições das vulnerabilidades, evidências, impacto e recomendações de mitigação;**

<u>Item 2 – Plataforma para Campanhas de Phishing e programas de conscientização</u>

Objetivo

O principal objetivo desta contratação é elevar a conscientização e a preparação dos colaboradores do CNPEM no que diz respeito à segurança cibernética, por meio da execução de uma campanha de simulação de Phishing e da implementação de programas educativos abrangentes.

Escopo

O CNPEM possui aproximadamente cerca de 1400 colaboradores.

Requisitos para contratação da plataforma

- Campanha de Simulação de Phishing:
  - Planejamento e criação de diversos cenários de ataques de phishing.
  - Envio de e-mails simulados para os colaboradores e acompanhamento das respostas.
  - Análise das interações e comportamentos dos usuários diante das simulações.
- Programas de Conscientização Interativos:
  - Desenvolvimento de conteúdos educativos gamificados, como quizzes e desafios.
  - Criação de módulos de treinamento em segurança cibernética de fácil compreensão.
  - Oferecimento de recompensas virtuais para a conclusão bem-sucedida de atividades.
- Gamificação e Engajamento:
  - Implementação de elementos de gamificação, como pontuações, rankings e prêmios virtuais.
  - Uso de feedback imediato e reforço positivo para incentivar a participação ativa.
- Análise de Resultados:
  - Coleta de dados sobre o desempenho dos colaboradores nas simulações de phishing.
  - Avaliação da participação e progresso nos programas de conscientização.
  - Geração de relatórios detalhados sobre o impacto das ações na postura de segurança.
- Personalização e Adaptação:
  - Customização da plataforma para refletir a identidade e os desafios específicos da organização.
  - Adaptação dos cenários e conteúdo de treinamento de acordo com as áreas de atuação dos colaboradores.
- Suporte e Atualizações:
  - Fornecimento de suporte técnico para esclarecimento de dúvidas e resolução de problemas.
  - Atualizações regulares da plataforma para incorporar novos cenários e conteúdos educativos.
- Encerramento e Avaliação:

- Encerramento formal da campanha de simulação de phishing e programas de conscientização.
- Avaliação dos resultados alcançados, identificando melhorias na conscientização e na postura de segurança.

- **Entregáveis:**
  - **Plataforma para envio de campanhas de phishing;**
  - **Plataforma para realização das campanhas de conscientização e treinamentos focados em segurança da informação e proteção e privacidade de dados pessoais;**
  - **Consultoria para configuração e preparação da plataforma.**

_____

Dennis Massarotto Campos
Divisão de Tecnologia da Informação

_____

Rogger José de Lima
Gestão de Segurança da Informação

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Portal Vertsign. Para verificar as assinaturas clique no link: https://vertsign.portaldeassinaturas.com.br/Verificar/C7E1-9D39-B2C4-612C ou vá até o site https://vertsign.portaldeassinaturas.com.br e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: C7E1-9D39-B2C4-612C

Hash do Documento

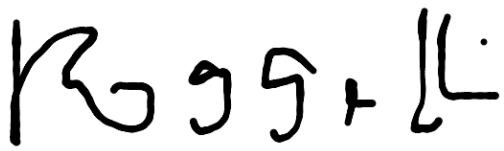
3900841E82CE5F9C7F03BA636977AF8E19E519E8C3B5F3F231F31862C9507394

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 12/09/2023 é(são) :

☑ ROGGER JOSE DE LIMA - ***.097.361-** em 12/09/2023 14:50 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Por email: rogger.lima@cnpem.br

Evidências

Client Timestamp Tue Sep 12 2023 14:50:50 GMT-0300 (Horário Padrão de Brasília)
Geolocation Latitude: -22.570632663959447 Longitude: -47.4076538563413 Accuracy: 35
IP 189.28.156.138
Assinatura:



Hash Evidências:
CFECE5536E7A640760D10CEB566147690EC640A667CB4A11D63A2D72043D96D2

☑ Dennis Massarotto Campos - ***.672.518-** em 11/09/2023 18:04 UTC-03:00
Tipo: Assinatura Eletrônica
Identificaçao: Por email: dennis.campos@cnpem.br

Evidências

Client Timestamp Mon Sep 11 2023 18:04:26 GMT-0300 (Horário Padrão de Brasília)
Geolocation Latitude: -22.846846846846848 Longitude: -47.178846797492355 Accuracy: 2000

IP 177.77.185.140
Assinatura:

Hash Evidências:
FC0902ECE85E22F35D45D04B4A3DA750B63917F3C41B532F96C7ABBD80863092