Especificações Técnicas para Consulta Pública

I. Descrição da necessidade da contratação,

Após o ataque hacker ocorrido em agosto de 2022, em que afetou todas as áreas de negócios da Prefeitura que utilizam da rede corporativa para acesso a sistemas informatizados e de recursos computacionais como ferramenta de trabalho para realização de suas atividades diariamente, a Prefeitura do Rio vem investimento em soluções de segurança, com a implementação de softwares e procedimentos que protejam a rede corporativa contra invasões, acessos a sites maliciosos e uso de ferramentas inapropriadas, visando o bloqueio de tráfegos maliciosos pela rede corporativa.

Contudo, as diversas soluções adquiridas precisam ser monitoradas de forma que os eventos e logs sejam centralizados em uma solução de SIEM (Gerenciamento de Informações e Eventos de Segurança) para monitoração contínua, detecção de ameaças, tratamento das vulnerabilidades e aplicar soluções de contorno para controlar e mitigar os riscos inerentes no ambiente de TI.

A atuação em segurança, requer profissionais capacitados em segurança e, com a redução do quadro técnico de profissionais de TIC da IPLANRIO, em que vem sofrendo perdas de mão de obra frequentemente, há uma sobrecarga de funções da equipe de TIC, além de não possuírem experiências e qualificações necessárias para atuarem em segurança tecnológica, na qual requer especializações especificas e dedicação para implementação de controles que sejam amparados pelas políticas, procedimentos e padrões de segurança a serem ser adotadas em toda a Prefeitura.

A monitoração voltada para eventos de segurança, requer a implementação de processo estruturado de operação, com diversos controles, mão de obra qualificada que atuem em regime de 24 horas x 7 dias da semana x 365 dias, para que monitorem todos os tráfegos, eventos, logs e comportamentos anormais que possam acarretar um novo ataque cibernético.

Um Centro de Operações de Segurança (SOC) contempla uma equipe dedicada, formada por analistas de segurança de TI que atuam em prevenções aos riscos com automação das ações, aceleram o processo de detecção de eventos classificados como ameaças de segurança cibernética em tempo real e com isto conseguem atuar de forma rápida e eficiente na contenção de um ataque.

Se contássemos com um Centro de Operações de Segurança (SOC) monitorando de maneira centralizada o ambiente da Prefeitura durante o ataque hacker ocorrido em agosto de 2022, a resposta para remediação do problema ou contenção do ataque teria sido imediata. Isso resultaria em uma significativa redução nos efeitos e consequências do incidente.

A contratação destes serviços visa a ampliar a observabilidade do ambiente quanto à segurança de dados, ativos de rede e de toda a Prefeitura, pois o processo de monitoramento de segurança deve ser contínuo e de toda a infraestrutura da organização, em 24/7/365, incluindo os aplicativos, sistemas, dispositivos, servidores, softwares, redes de computadores, internet e tudo que possuir um endereço IP em rede interna ou externa, devendo ter ações para prevenir, detectar, analisar e responder as ameaças cibernéticas e incidentes de segurança. Assim como o controle de acessos aos recursos de TI e bases de dados, devem ser protegidos quanto ao uso indevido, capturas e perda/roubo de dados.

A reputação da Prefeitura e da Iplanrio foi severamente prejudicada pelo ataque hacker, e a implementação de um Centro de Operações de Segurança (SOC) trará como benefício principal o aumento da confiança nas áreas afetadas. Além disso, contribuirá para fortalecer a conformidade da organização no que diz respeito à aplicação de políticas, normas de segurança e procedimentos operacionais voltados para a proteção da instituição.

II. Objeto da contratação:

ITEM	DESCRIÇÃO	QTDE
1	Serviço de centro de Operações de Segurança (SOC), operação e monitoramento de eventos e logs, pelo período de 24dx7dx365d, com equipe de suporte remoto (CSIRT) de nível 1, nível 2 e nível 3; Gestão de detecção de ameaças e incidentes de segurança (Threat Intelligence), Gestão de serviços de orquestração, automação e resposta de segurança (SOAR); Serviço de governança e gestão de riscos de segurança, incluindo solução de gerenciamento de eventos, deduplicação, compressão, agregação de dados de informações de segurança da contratante (SIEM), com dimensionamento para os ativos de TI da contratante, alvo de monitoração e proteção de segurança.	24 meses

- A entrega do serviço deve atender ao acordo de níveis de serviço, cabendo à prestadora do serviço o dimensionamento adequado da equipe, para que não haja impacto no serviço prestado;
- Nível1: atendimento, triagem, monitoramento em tempo real, coleta de dados;

- Nível 2: análise de incidentes, coordenação de resposta a incidentes, analise forense e ameaças avançadas, analisar as vulnerabilidades do ambiente e mitigação;
- Manutenção de todos os sensores, appliances, uso de inteligência artificial, automação, scripts, auditoria e armazenamento;
- Nível 3: analise de tendências, alertas de zero-day, identificarção de comportamento de segurança, escaneamento de rede e ativos, realização de testes de invasão, avaliação de segurança dos produtos, relatórios de segurança;
- Para cenário de eventuais de crise, deverá disponibilizar equipe de Nível 3 para deslocamento até o Datacenter da Iplanrio ou sala virtual de crise.

III. Requisitos, critérios e práticas de sustentabilidade:

- Uma Governança de TI eficiente, requer um alinhamento estratégico entre o tático e operacional, tendo a politica de segurança um papel importante neste contexto de segurança, em que define as diretrizes de segurança para toda a organização que devem seguir as orientações, procedimentos e regulamentos que visam a proteção de dados, da rede corporativa e principalmente da imagem corporativa da Prefeitura.

- A escolha da solução deve compreender a implantação de uma solução de gerenciamento de eventos e correlacionamento com informações de segurança em ambiente de nuvem, na modalidade de serviços, que devem manter atualizado o Inventário dos ativos que devem ser protegidos e coletar todos os dados essenciais dos ativos de rede, aplicações, banco de dados, servidores, serviços de rede, cloud, endpoints, e demais ferramentas de segurança existente no Datacenter da Iplanrio, tais como firewall, VPN, antivírus, correio eletrônico, microsegmentação, balanceador de carga/ WAF (F5), servidores windows/Linux, controladores de domínios, Aplicações web, ambientes de virtualização e etc.

- Deve fornecer profissionais qualificados e com especializações em segurança para desenvolver integrações através de scripts, api rest/xml, netflow, syslog, arquivos de log, eventos, banco de dados e demais formas de automação para coletar dados dos ativos do inventário a ser protegido, composto de diversas soluções de fabricantes distintos, de forma contínua para agregação, consolidação para entrada de dados do SIEM, para que a solução possa atuar com Inteligência artificial e analisar os dados coletados, identificar e classificar de acordo com a reputação, ameaça, riscos que deverão ser disponibilizados em painéis de alertas, status, relatórios e dashboard que devem ser atualizados em

tempo real e que servirão como objetos de monitoração pela central de operação de segurança para identificar os comportamentos suspeitos e ameaças que possam oferecer algum riscos e comprometer o funcionamento da organização.

- Deverá ter uma central de operação de segurança (SOC) em ambiente externo/próprio da contratada e redundante, com alta disponibilidade, com toda a infraestrutura física, lógica e recursos de TI e de mão de obra para operação de forma ininterrupta, em 24 horas por dia durante 7 dias por semana, com profissionais de SOC de nível 1, nível 2 e nível 3, durante a vigência do contrato;

- Deverá esta interligada de forma dedicada ao Datacenter da IPLANRIO, para realizar os serviços de monitoração, análise, detecção de comportamentos suspeitos ou alertas de segurança e responder imediatamente em incidentes e/ou notificar aos demais níveis de especialização para que possam analisar e mitigar o incidente, de forma a controlar e restabelecer a operação da Organização.

IV. Atribuições do SOC (identificação, proteção, detecção, reação e recuperação do ambiente):

- Detectar as vulnerabilidades de segurança no ambiente,
- Acompanhar os sites técnicos dos fabricantes, de acordo com os padrões e regulamentos do uso de softwares, cloud e demais recursos tecnológicos;
- Aplicar padrões de conformidade técnicas;
- Monitorar as ameaças e incidentes cibernéticos, com base em reputação online de domínios;
- Avaliações de riscos, tomar medidas de contenção, erradicação, recuperação e investigação e respostas aos incidentes;
- Realizar teste de invasão, visando encontrar e explorar vulnerabilidades no ambiente, com intuito de aumentar o nível de segurança;
- Desenhar e implementar ações de mitigação de vulnerabilidades e ataques;
- Gerenciamento e Suporte aos produtos/soluções de segurança existentes, com aplicações de correções e realizar upgrades de softwares disponibilizados pelos fabricantes;
- Analisar e atualizar as whitelist e blacklist de domínios suspeitos;
- Sugerir atualizações na politica e nos procedimentos de segurança;
- Desenvolver, documentar e manter o plano de resposta a incidente atualizado, com as atividades, as funções e responsabilidades em caso de ameaça ou incidentes e medir os tempos de resposta;
- Verificar o status das integrações, e realizar os ajustes quando necessários;

- Detectar, investigar e responder a incidentes ou ameaças;
- Recuperar o ambiente, em caso de invasão;
- Monitoramento continuo dos status, eventos e das ameaças em tempo real, em regime 24hx7dx365 dias;
- Analise de causa raiz, implementar ou propor resolução ou mitigação para o problema investigado, bem como classificar o risco;
- Resposta a incidentes de segurança não documentado;
- Realizar Análise Forense;
- Governança do serviço de segurança, liderança de equipe dedicada para a prestação do serviço;
- Dispor de profissionais capacitados, qualificados em segurança, e alocação destes profissionais de acordo com os perfis de capacitação para atuar nos diversos níveis de SOC, em quantidades suficientes para atender aos serviços contratados;
- Desenvolver conectores, integrações, API Rest/XML, scripts e novas funcionalidades para integração da solução de SIEM com as diversas fontes de dados de coleta de eventos de segurança;
- Investigação e detecção de fragilidades, desenhar novos procedimento para gestão de mudança para remediar a vulnerabilidade;
- Revisar, Ajustar e Documentar os novos incidentes, para que os níveis de suporte básico atuem imediatamente;
- Acionar o suporte avançado dos fornecedores de softwares de segurança ou adicional aos produtos administrados;
- Registrar, documentar os tickets abertos e tratados de todos os alertas, incidentes e vulnerabilidades detectadas em ferramenta da contratante;
- Investigação de rede, sistemas operacionais, em busca de ameaças e fragilidades que possam comprometer o ambiente corporativo;
- Elaborar relatórios de causa-raiz e planos de ação para mitigar os riscos detectados;
- Elaborar dashboard operacionais e estratégicos para demonstrar o nível de exposição de riscos;
- Reuniões programadas para definir métricas, alertas, relatórios e evolução do serviço prestado;
- Emitir relatórios com informes periódicos sobre as tendências de segurança, inteligência de ameaças e ocorrências de ataques cibernéticos obtidos em fontes diversas confiáveis, inclusive dark web, dewp web, redes sociais e etc.

V. Indicador para mensuração do resultado da contratação:

- Falta de solução de um incidente;
- Chamado aberto e não atendido dentro do SLA;
- Nível de satisfação de resposta e de prestação do serviço;

- Falta de resposta a um email, chamado, consulta ou questionamento;
- Falta de atuação de algum time de SOC, dentro do prazo estipulado;
- Disponibilizar painel de monitoração de situação do risco, eventos e alertas categorizados;
- Ausência de registro de tickets na solução de ITSM;
- Ausência de documentação dos incidentes na solução de ITSM;
- Não atender aos prazos (SLA) definidos para os Incidentes, severidade e impacto;
- Não requerer autorização para ações de manutenção emergenciais, corretivas, preventivas ou programadas;
- Não notificar aos responsáveis técnicos os incidentes de segurança;
- Não entregar os relatórios de prestação de serviços;
- Não entregar os relatórios de atividades globais de ataques e vulnerabilidades exploradas;

VI. Resultados pretendidos:

- Disponibilidade, escalabilidade de recursos como serviços em nuvem para armazenamento e processamento dos dados coletados em solução de SIEM;
- Equipe especializada em segurança dedicada para monitoração, detecção, análise e recuperação do ambiente de TI da Prefeitura;
- Implementação de um processo estruturado de governança e gestão de riscos de segurança, com padrões e tecnologias adequadas para aumentar a proteção do ambiente;
- Observabilidade e mitigação de riscos de segurança em todas as camadas de infraestrutura, rede, aplicação, dados e negócios, com adoção de inteligência artificial e aprendizado de maquina;
- Redução do nível de exposição a riscos;
- Mitigar as vulnerabilidades e incidentes detectados;
- Conscientizar a comunidade de TI sobre a necessidade de evolução do ciclo de vida dos produtos;
- Redução do tempo de detecção e resposta a incidentes de segurança;
- Centralização de eventos e logs para análise e correlação para detectar ameaças;
- Coordenação de resposta a incidentes em menor tempo;
- Melhoria na gestão de vulnerabilidades, com os devidos tratamentos para mitigar os riscos;
- Acompanhar os ataques, padrões e boletins de segurança em escala global;
- Redução de custos, não haverá necessidade de capacitação da equipe de TI da Iplanrio.

VII. Descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso, acompanhada da escolha do tipo de solução:

Serviço de central de operações de segurança (SOC) nível 1,2 e 3 em ambiente externo, com toda a infraestrutura e recursos de mão de obra e de TI para operação em 24h por dia, durante 7 dias por semana;

Serviço de gestão de eventos e correlacionamento de informações de segurança (SIEM) na modalidade de serviço em nuvem, com automação e integração e coleta de dados de todas as soluções de segurança e ativos a ser protegidos existentes no Datacenter da Iplanrio;

Serviço de gestão de incidentes e a ameaças cibernéticas (THREAT INTELLIGENCE) e serviço de orquestração, automação e resposta de segurança (SOAR), detectar, notificar, registrar, tratar, mitigar os incidentes e documentar em ferramenta de ITSM da contratante (BMC Helix);

Serviço de governança e gestão de riscos de segurança de todas as ferramentas/soluções existentes no Datacenter da Iplanrio:

- Monitoramento de eventos/alertas/vulnerabilidades da solução de gestão de vulnerabilidades (Tenable), executar varreduras, detectar vulnerabilidades de alta criticidades, aplicar correções e atualizações, elaborar plano de mitigação da vulnerabilidade e notificar aos responsáveis,
- Monitoramento de eventos/alertas/incidentes da solução de microsegmentação (Guardicore), detectar, analisar e realizar o tratamento das aplicações e ativos de rede;
- Monitoramento de eventos/alertas/incidentes dos equipamentos de rede (roteadores, switches cores, switchs SAN), negação de serviços das operadoras, tentativas de acessos indevidos, uso da largura de banda e demais indicadores que possam afetar a segurança do ambiente
- Monitoração de eventos/alertas/incidentes da solução de antivírus (EDR/XDR), executar varreduras, instalar agentes, resolver problemas nos agentes, verificar arquivos suspeitos, analisar alertas e implementar bloqueios para minimizar os riscos ao ambiente, elaborar procedimentos para mitigação;
- Monitoramento de alertas/eventos/incidentes da solução de email/antispam existente na Iplanrio, vazamento de credenciais, analisar arquivos maliciosos e atualizar politicas de bloqueios de maliciosos ou indesejados;
- Monitoramento de alertas/eventos/incidentes da solução de BIG-IP/F5, WAF, AFM, ASM, detectar, analisar e tratar os eventos detectados e fragilidades encontradas;

- Monitoramento de alertas/eventos/incidentes da solução de registro de nome de domínios (DNS, BIND);
- Monitoramento de alertas/eventos/incidentes da solução de Acesso Remoto;
- Monitoramento de alertas/eventos/incidentes do controlador de domínios (AD) e diretórios de nomes (LDAP), tentativas de acessos indevidos, bloqueios de contas de serviços e de administradores;
- Monitoramento de alertas/eventos/incidentes da solução de Firewall interno e externo, DDOS, Dominios/IP´s maliciosos, acessos remotos VPN, IPS/IDS, Spam, Bot, Phishing, Filtros de conteúdos, e etc;
- Monitoramento de alertas/eventos/incidentes de arquivos de Logs de servidores Windows/Linux, e banco de dados, web e demais softwares servidores;
- Monitoramento de alertas/eventos/incidentes de solução de proxy/filtro de conteúdo, detectar saída de dados e acessos indevidos a conteúdos impróprios e indesejados;
- Monitoramento de balanceamento de carga, WAF, ASM, AFM, DDOS, DNS;
- Monitoramento de alertas/eventos/incidentes de solução de virtualização, Vmware, Citrix e demais soluções de acessos remotos;
- Monitoramento de alertas/eventos/incidentes de trafego de rede (Netflow), SNMP;
- Monitoramento de alertas/eventos/incidentes de solução de banco de dados
- Monitoramento de alertas/eventos/incidentes de servidores de aplicações cliente/servidor, WEB (IIS / Apache / NGINX), Samba/NFS/CIFS e servidores de aplicações ou ativos que possuem endereço IP;
- Monitoramento de alertas/eventos /incidentes de solução de monitoramento de ativos de rede (Zabbix).

VIII. Exigências do serviço a ser contratado:

- Certificação SOC2
- Interligação entre os sites do Datacenter e do SOC
- Disponibilidade de 99,99%do SOC
- Certificação dos profissionais de SOC N1,N2 e N3
- Comprovar que possui processos implementados com base na norma ABNT NBR ISSO/IEC 270001

- A prestação do serviço pode gerar vínculos empregatícios com a contratante;

- Todos os recursos de infraestrutura, espaço físico, equipamentos, licença de softwares e ferramentas, custos de mão de obra, materiais de consumos e demais insumos serão de responsabilidade da prestadora de serviços.

IX. Estimativa das quantidades a serem contratadas:

- Para fins de cálculo foram identificados os ativos de rede que devem ser protegidos, contabilizados e estimado o valor atual alocado para armazenamento de logs bruto, acrescido de margem de crescimento.
- Os dados de eventos e logs deverão ser consolidados e descartados após o período de 180 dias, exceto os casos excepcionais que podem ser solicitado a preservação de salva de um período pré-definido destes eventos/logs.
- A extração dos dados deverá ser realizada em tempo real, ou em períodos curtos, todo o processo de captura, compactação e envio devem ser executados on-premise, para posterior envio de dados tratados em link dedicado para o SIEM como serviço em nuvem, e deve suportar capacidades mínimas previstas de 20 (vinte) Terabytes de volume de dados trafegados, por dia.

Ativos a serem protegidos	ATIVOS/Throughput	Volume de Eventos/Log por dia (EVS)
Operadoras de rede	3	500 GB
Ativos de rede(roteador/switches)	1500	1.000 GB
Servidores Windows/Linux	1.017 hosts	1.000 GB
Aplicações web	1.500 apps	1.000 GB
Kubernets		500 GB
Banco de dados	132	1.000 gb
Controladores de domínio	11.000 contas 11.000 desktops	1.000 GB
Domínios	2.000	500 GB
Email	42.000 contas	1.000 GB
Firewall	60 Gbps	1.000 GB
Antivirus	22.000	500 GB
Microsegmentação	1.500	500 GB
BigIP/F5	60 Gbps	500 GB
Scanner Vulnerabilidades	1.000	500 GB
OUTROS		1.500 GB
TOTAL TRAFEGO DE LOGS/EVENTOS POR DIA		12.000 GB

- Não cabe parcelamento da solução, que deve ser integralmente fornecida por um único fornecedor, tendo em vista a natureza da contratação, em que os itens do objeto se relacionam com o produto a ser ofertado.