SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Fornecimento de Solução de SOC - Security Operations Center

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

Do Objeto: Contratação de empresa especializada para o fornecimento de uma Solução de SOC como serviço por um período de 12 (doze) meses que atenda as especificações técnicas mínimas necessárias apresentadas a seguir:

1. Do Modelo de atuação

- Implementar ferramenta de correlação de eventos e LOGs afim de fornecer monitoramento 24x7 da infraestrutura de segurança de TI da SCGÁS.
- Deverá possuir centro de operações operando 24x7 na área de segurança da informação, contando com especialistas atuando presencialmente e remotamente, não sendo aceita a modalidade 100% remota ou plantão.

1.1 Da Ferramenta de SIEM e XDR

- O CONTRATADO deverá implementar plataforma corporativa de correlação de LOGs e eventos para detecção e resposta a incidentes de segurança com no mínimo as características abaixo:
- A solução deverá ser entregue como serviço pelo contratado e deverá possuir suporte ativo do fabricante da solução para abertura de chamados envolvendo BUG FIXES e disponibilização periódica de minor e major releases contendo melhorias, não sendo aceitas soluções baseadas em software livre (open source);
- Ser fornecida em modelo cloud híbrida. Para soluções baseadas em cloud o fornecedor deve possuir certificações como SOX e SOC 2 Type 2.
- Deve permitir a instalação de coletores on-premise.
- Deve possuir capacidade de identificar e monitorar o comportamento de usuários (UEBA).
- Deve possuir a capacidade de identificar e monitorar o comportamento de atacantes baseados em IOCs do próprio fabricante e de terceiros (threat intelligence).
- Deve possuir a capacidade de ingestão de dados de outras ferramentas de threat intel como IPs, domínios, MD5, de maneira manual ou por API.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Fornecimento de Solução de SOC - Security Operations Center

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Deve possuir a capacidade licenciada de instalar honeypots, honey credentials, honey files para identificar possíveis brechas e identificar movimentos suspeitos / maliciosos.
- Deve monitorar ativamente fontes de eventos como: AD, DNS, DHCP, LDAP e servidores / workstations com uso de agentes.
- Os agentes deverão monitorar as máquinas em tempo real, todas as vezes que tiverem conexão com a internet, estando elas dentro ou fora do domínio.
- Os agentes deverão monitorar pelo menos:
  - brute force – asset
  - brute force - local account
  - detection evasion - event log deletion
  - detection evasion - local event log deletion
  - exploit mitigated
  - flagged hash
  - flagged process
  - honey file accessed
  - kerberos privilege elevation exploit
  - lateral movement - local administrator impersonation
  - lateral movement - local credentials
  - local honey credential privilege escalation
  - malicious hash
  - new local user account created
  - protocol poisoning
  - remote file execution
- A solução deverá ter a capacidade de identificar e quantificar no Active Directory ou via protocolo LDAP, a quantidade de usuários ativos, quantidade de contas de usuários marcados como service account, usuários configurados como senhas que “non expiring users”, usuários desabilitados e usuários com privilégios de administradores.
- Deve permitir cadastrar usuários VIP’s, para monitorá-los com thresholds específicos e toda ação em torno deste usuário.
- Deve possuir a capacidade de identificar e correlacionar logs de servidores e workstations, para identificar comportamentos anômalos em logs que aconteçam localmente na máquina.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Fornecimento de Solução de SOC - Security Operations Center

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Deve criar timeline (linha do tempo) do ataque com evidências.
- Deve possuir a capacidade de monitorar a integridade de arquivos (FIM).
- Deve possuir funcionalidade de automação relacionada a usuários do AD,
- A solução deve ter capacidades de contenção de ameaças maneira rápida.
- Deve possuir a capacidade de monitorar tráfego de rede para detecção de:
    - Atividade inbound
    - Atividade outbound
    - Conexões RDP inbound
    - Conexões TLS inbound
    - Atividade de portas Inbound e outbound
- Junto com o monitoramento do tráfego de rede, a solução deve possuir regras de IDS incluídas para correlacionar e trazer as informações sobre possíveis anomalias / ataques no nível de rede.
- Deve atender o escopo da quantidade 250 de assets com armazenamento mínimo de 250 GB/Mês e com retenção de dados para consulta rápida de no mínimo 365 dias, cobrindo 100% do ambiente relacionado a estações de trabalho e servidores, devendo ainda estar licenciada para receber LOGs de:
    - Firewalls
    - IPS / IDS
    - Web filtering
    - Antivirus
    - Active Directory
    - DNS
    - DHCP
    - LDAP
    - O365
    - Azure
    - AntiSPAM
    - Servidores
    - Estações de trabalho
- Deverá permitir também a criação de alertas customizados seja baseado em um comportamento específico ou em um contexto de combinação de eventos (parser)
- Deverá permitir adição de logs a incidentes / alertas detectados

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Deve permitir criar investigações customizadas, sem a necessidade da própria plataforma ter gerado um alerta
- Deverá permitir a criação de dashboards e reports baseados em bibliotecas prontas ou também customizados.

1.2 Do escopo de serviços

- Deverá utilizar plataforma de ticket management integrada à plataforma de SIEM e XDR, para gerenciar os alertas gerados e SLAs de atendimento da operação;
- Deverá possuir ferramentas de automação para o envio de alertas via grupos de comunicação no Whatsapp, Microsoft Teams e e-mail.
- Deverá manter uma base de conhecimentos para incidentes conhecidos e já aceitos pela organização.
- Atuação ilimitada na resposta a incidentes de segurança com atendimento 24x7 ou 8x5, conforme detalhamento abaixo:
  - **Do escopo de atendimento 24x7:**
    - Deverá realizar a triagem de todos os alertas gerados pela ferramenta de correlação de eventos, classificando os mesmos pelo nível de severidade e direcionando os alarmes para os times de atendimento;
    - Tomar ações como: quarentenar hosts, subir agentes, bloquear usuários;
    - Notificações de eventos através de escalation list disponibilizado pela SCGAS;
    - Declarar crise e estabelecer sala de guerra com time multi-disciplinar para resposta a incidentes de segurança de severidade crítica e alta;
  - **Do escopo de atendimento 8x5:**
    - Tomando medidas para reduzir recorrência dos alarmes classificados como falso positivos;
    - Análise de causa raiz de incidentes (altos/críticos);
    - Análise de artefatos;
    - Melhorias nas automações do SIEM;
    - Alimentação da base de conhecimento do SIEM;
    - Remediação de incidentes de segurança com severidade médias e baixas;
    - Consultoria em Cyber Segurança limitado a 6 horas mês não cumulativas, que serão demandadas pelo time de governança corporativa para construir o plano de resposta a incidentes e aperfeiçoar as políticas de segurança da informação;

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Na ocorrência de um incidente de segurança, caso seja necessário o contratado deverá possuir áreas técnicas certificadas de apoio complementar ao time de segurança da informação, para atuar na resolução de incidentes no que tange, mas não se limita as seguintes tecnologias (Microsoft Cloud e on-primeses, Linux, Bancos de dados Microsoft e Oracle, Redes e firewalls Cisco e Fortinet) em regime de atuação 24x7.
- O CONTRATADO deverá realizar um PEN TEST GREYBOX do ambiente monitorado pelo serviço de SOC.
- Deverá possuir pessoal capacitado para atuar na engenharia reversa e análise de malware e artefatos.

1.3 Dos SLAs

Tipos de SLA	Atuação	Atendimento
SLA para Triagem dos Alarmes gerados pela ferramenta:	24x7	Até 5 minutos
SLA para classificação da severidade dos alarmes e direcionando os mesmos para o time de atendimento	24x7	Até 10 minutos
SLA para resposta à Incidentes de Severidade Crítica	24x7	Até 2 horas
SLA para resposta à Incidentes de Alta Severidade	24x7	Até 4 horas
SLA para resposta à Incidentes de Média Severidade	8x5	Até 8 horas
SLA para resposta à Incidentes de Baixa Severidade	8x5	Até 24 horas

1.4 Dos Relatórios de Gestão

- Deverá apresentar mensalmente um book de gestão com minimamente as seguintes informações:
  - Volumetria de alarmes gerados no mês;
  - Tempo médio de detecção e resposta aos incidentes de segurança
  - Tratativas de recorrências (monitoramento);
  - Maiores ofensores do mês;
  - Análise de causa raiz para incidentes de severidade crítica e alta;
  - Recomendações técnicas (caso existam);

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Deverá disponibilizar relatórios detalhados sobre artefatos encontrados no ambiente a fim de auxiliar a guiar a resposta aos incidentes.

1.5 Da Implantação e Transição

- Realizar reunião de abertura do contrato, apresentando o planejamento da implantação e metodologia de prestação de serviços.
- O CONTRATADO deverá realizar um GAP Analisys e uma análise de vulnerabilidades do ambiente da SCGAS, bem como avaliar as políticas e estratégia de segurança da informação da corporação, elaborando uma matriz de risco X criticidade estruturando um roadmap de resolução de problemas;
- O CONTRATADO deverá realizar a implementação dos agentes necessários e a configuração da ferramenta 8x5;

1.6 Das Qualificações

- O CONTRATADO deverá comprovar possuir a certificação ISO 27001.
- O CONTRATADO deverá comprovar possuir no mínimo 2 (dois) profissionais com no mínimo uma das seguintes certificações (CompTIA Security+, CISSP, ECIH, GCIH, CSIH, CEH, OSCP, ISO 27002).
- O CONTRATADO deverá apresentar atestado de capacidade técnica relacionado aos serviços objeto desta contratação.

1.7 Das Obrigações do Contratado

- Executar os serviços contratados de acordo com os prazos, especificações e condições estipuladas, responsabilizando-se por eventuais prejuízos decorrentes do descumprimento de qualquer cláusula estabelecida.
- Responsabilizar-se pelos danos causados diretamente à Administração da SCGÁS ou a terceiros, decorrentes de sua culpa ou dolo, não excluindo ou reduzindo essa responsabilidade, quando da fiscalização ou o acompanhamento pela SCGÁS.
- Prestar todos os esclarecimentos que forem solicitados pela SCGÁS, obrigando-se a atender, de imediato, todas as reclamações a respeito da qualidade da prestação dos serviços.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Fornecimento de Solução de SOC - Security Operations Center

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Comunicar ao gestor do contrato, por escrito, qualquer fato que não seja conforme ao objeto do contrato, para providências por parte da SCGÁS.
- Não veicular publicidade acerca da contratação, salvo prévia autorização da SCGÁS.
- Manter, durante toda a vigência do contrato, todas as condições de habilitação e qualificação exigidas na licitação, conforme legislação vigente.
- Todas as despesas oriundas do objeto serão de responsabilidade do CONTRATADO, como por exemplo: disponibilização de profissionais, licenciamento, suporte e subscrição das ferramentas, despesas de alimentação, deslocamento, estadia, horas extras e qualquer outra aqui não mencionada.
- Obriga-se a zelar pela confidencialidade de qualquer informação a que, porventura, tenha acesso.
- Obriga-se a conhecer as normas de segurança a ela aplicáveis e a seguir os procedimentos definidos pela área competente.
- Deverá disponibilizar para a SCGÁS o backup referente os logs coletados pelo SOC quando solicitados.
- Obriga-se a colaborar com a SCGÁS para a manutenção de um ambiente de dados seguro.
- A SCGÁS poderá a qualquer momento executar ações de auditoria de forma presencial ou à distância.
- Concorda em que é responsável por ações de seus técnicos e eventuais subcontratados em tudo que diz respeito à segurança de informações.
- A ocorrência de falta relacionada à segurança de informações da SCGÁS, pelo CONTRATADO e ou integrante de sua equipe, será considerada falta grave e sujeita a aplicação de penalidade, e sua recorrência poderá dar margem à rescisão unilateral do contrato, e outras ações legais cabíveis.
- Os serviços estabelecidos por este instrumento não possuem qualquer vinculação trabalhista com a SCGAS, sendo de exclusiva responsabilidade do CONTRATADO quaisquer relações legais com o pessoal necessário à execução dos serviços, possuindo este contrato um cunho independente e devendo do CONTRATADO manter em ordem as obrigações previdenciárias decorrentes da vinculação, assumindo responsabilidade integral e exclusiva quanto aos salários e demais encargos trabalhistas e previdenciários de seus empregados/prepostos, principalmente com relação a possíveis reclamatórias trabalhistas, não existindo solidariedade entre a SCGAS e o CONTRATADO.
- Deve seguir as diretrizes de TI e SMS da SCGÁS.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Fornecimento de Solução de SOC - Security Operations Center

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Deve executar os serviços conforme especificações deste Memorial Descritivo e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Memorial Descritivo e em sua proposta.
- Deve reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.
- Deve responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a CONTRATANTE autorizada a descontar dos pagamentos devidos ao CONTRATADO, o valor correspondente aos danos sofridos.
- Deve utilizar empregados habilitados e com conhecimentos específicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.
- Deve responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à SCGÁS.
- Atender às solicitações da SCGÁS quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Memorial Descritivo.
- Instruir seus empregados quanto à necessidade de acatar as Normas internas da Administração da SCGÁS.
- Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo Contrato, devendo o CONTRATADO relatar à SCGÁS toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.
- Relatar à SCGÁS toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.
- Não utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato, de acordo com o Termo de Confidencialidade disposto no Anexo do Contrato.
- Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para a atividade objeto da licitação, exceto quando ocorrer algum dos eventos arrolados na Legislação em vigor.
- Estar em conformidade com a Lei Nº 13.709, de 14 de agosto de 2018, a LGPD – Lei Geral de Proteção de Dados.
- Executar o serviço com profissionais devidamente capacitados e de acordo com os critérios técnicos para a prestação do serviço.

1.8 Responsabilidades da SCGAS

- Manter o CONTRATADO informado sobre quaisquer modificações ou alterações legais ou administrativas que possam afetar ou se relacionar com os serviços objetos deste documento.
- Providenciar acessos individuais aos sistemas, redes e servidores necessários para a prestação dos serviços. O CONTRATADO deve solicitar com antecedência os acessos necessários.
- Emitir a ordem de serviço, dando início à vigência do Contrato, após a verificação da realização dos procedimentos para a implementação dos serviços.
- Prestar as informações e esclarecimentos pertinentes ao objeto que venha a ser solicitado pelo CONTRATADO.
- Encaminhar todas as deliberações com relação ao pessoal do CONTRATADO através do preposto desta, respeitando o princípio da hierarquia e unidade de comando.

1.9 Prazos de Entrega:

- Os prazos de entrega incidirão sobre os serviços de implantação e treinamento.

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Os serviços somente poderão ser prestados e os prazos de entrega ter sua contagem iniciada após a emissão, por parte da CONTRATANTE, de Autorização de Serviço.
- O prazo de entrega será de 30 (trinta) dias após a assinatura do contrato.

1.10 Da Lei Geral de Proteção de Dados Pessoais:

- Para a devida garantia da privacidade e da proteção de dados pessoais, as partes comprometem-se a observar e cumprir as disposições previstas na Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), durante a execução deste Contrato e tratamento de dados pessoais decorrente deste.
- As partes obrigam-se a:
- Tratar, usar e atender os requisitos de coleta mínima necessária dos dados pessoais para os fins a que se destinam, mantendo-os registrados, organizados, conservados e disponíveis para consulta.
- Limitar o tratamento de dados pessoais às finalidades para as quais tenham sido coletados.
- Manter os dados pessoais armazenados apenas durante o período estritamente necessário à execução das finalidades contratuais previstas ou pelo prazo necessário ao cumprimento de eventual obrigação legal, garantindo a sua efetiva confidencialidade, bem como manter o devido armazenamento em meios seguros, preferencialmente digitais e com rastreabilidade disponível, assim como garantir destinação final segura.
- Quando da coleta de dados pessoais sensíveis, em razão de cumprimento de obrigação acessória, armazená-los em local apartado dos demais dados pessoais e com nível de restrição ainda maior, sendo disponibilizados somente mediante requerimento formal e justificativa legítima.
- Aplicar medidas técnicas e administrativas capazes de proteger os dados contra alteração, perda, difusão, acesso ou destruição – acidental ou intencionalmente – não autorizados ou estranhos à essa relação contratual, bem como contra qualquer outra forma de tratamento irregular.
- Informar a outra parte imediatamente após a tomada de conhecimento caso haja alguma suspeita ou incidente de segurança concreto envolvendo dados pessoais, devendo prestar toda a colaboração necessária a qualquer investigação que venha a ser realizada.

SCGÁS COMPANHIA DE GÁS DE SANTA CATARINA	GETIN - Gerência de Tecnologia da Informação
	Memorial Descritivo
	Fornecimento de Solução de SOC - Security Operations Center

Resumo: **Fornecimento de Solução de SOC - Security Operations Center como serviço, por um período de 12 meses.**

- Garantir que os titulares tenham acesso facilitado às informações sobre o tratamento de seus dados mediante requerimento.
- Garantir a rastreabilidade de tratamento de tais dados durante todo o seu ciclo de vida, principalmente quanto ao download, exportação de disponibilização de documentos com dados pessoais e dados pessoais sensíveis.
- Adotar políticas para o desenvolvimento de sistemas que incluam diretrizes de acordo com a LGPD para atendimento das necessidades de tratamento de dados pessoais.
- Assegurar que todas as pessoas que venham a ter acesso a dados pessoais no contexto deste contrato tenham ciência e cumpram as disposições legais aplicáveis em matéria de proteção de dados pessoais.
- Fomentar e disponibilizar treinamento e ações de conscientização relacionadas à proteção de dados pessoais e privacidade aos responsáveis pela execução do contrato, garantindo assim a implementação de Boas Práticas e da Governança, nos termos dos artigos 50 e 51 da Lei nº 13.709/2018.
- Responsabilizar-se-á a parte que der causa a eventuais violações de dados pessoais nos termos da legislação vigente, ressalvado o direito de regresso estabelecido em lei e consideradas as circunstâncias do caso e medidas de segurança adotadas pela responsável.

Florianópolis, 13 de fevereiro de 2024.

Alison Luiz Martins Schveitzer

Assinado de forma digital por Alison Luiz Martins Schveitzer
DN: dc=br, dc=corp, dc=scgas, ou=SCGAS, ou=Usuarios, ou=Gerências, ou=GETIN, ou=Concursados, cn=Alison Luiz Martins Schveitzer, email=alison.martins@scgas.com.br
Dados: 2024.03.13 15:14:14 -03'00'

Alison Luiz Martins Schveitzer
Analista de Tecnologia da Informação

Victor Hugo Bogiano

Assinado de forma digital por Victor Hugo Bogiano
DN: dc=br, dc=corp, dc=scgas, ou=SCGAS, ou=Usuarios, ou=Gerências, ou=GETIN, ou=Comissionados, cn=Victor Hugo Bogiano, email=victor.bogiano@scgas.com.br
Dados: 2024.03.13 15:31:25 -03'00'

Victor Hugo Bogiano
Gerente de Tecnologia da Informação