

## ANEXO IV - CARACTERÍSTICAS DA FERRAMENTA DE SIEM

### 1- Objetivo da Ferramenta de SIEM

- 1.1.** O objetivo do SIEM (Security Information and Event Management) ou Gerenciamento e Correlação de Eventos de Segurança, não é apenas proteger o perímetro da rede, mas também proteger as áreas de negócio das Contratantes. Para tal proteção, é essencial entender quem está na rede, quais dados eles estão vendo e quais ações eles estão tomando com esses dados, conhecidos como monitoramento de usuários, monitoramento de dados e monitoramento de aplicativos.

### 2. Descrição da correção de eventos SIEM

- 2.1. (Requisito Técnico Obrigatório)** A solução a ser ofertada deverá constar no quadrante mágico do Gartner como Líder;
- 2.2. (Requisito Técnico Obrigatório)** A solução deverá ser ofertada em nuvem, como Serviço;
- 2.3.** A solução deverá garantir que os dados enviados pelos agentes, utilizam apenas metadados, não podendo, sob nenhuma hipótese, encaminhar dados sensíveis da Contratante;
- 2.4.** O prazo admitido para implantação da solução é de 90 dias;
- 2.5.** O Correlacionar os logs de eventos de todos os itens de configuração que fazem parte dos serviços críticos de tecnologia da informação de maneira a alarmar possíveis ameaças e vulnerabilidades que coloquem em risco o perfeito funcionamento e a integridade dos serviços;
- 2.6. (Requisito Técnico Obrigatório)** O serviço deverá funcionar em modo próximo ao real (near real-time) e de forma ininterrupta;
- 2.7. (Requisito Técnico Obrigatório)** Deve ser gerenciado centralmente (configurações, controle e atualizações), através de interface gráfica única, sem necessidades de intervenção nos equipamentos onde está instalado;
- 2.8. (Requisito Técnico Obrigatório)** Deve ser capaz de marcar (através de tag, label ou similar) os eventos;
- 2.9. (Requisito Técnico Obrigatório)** Deve ser capaz de inserir nos eventos, informações sobre localização geográfica dos mesmos;
- 2.10. (Requisito Técnico Obrigatório)** A visualização deverá ser possível através de dashboards customizáveis;
- 2.11. (Requisito Técnico Obrigatório)** Deverão ser configurados, alarmes por nível de criticidade;

- 2.12. (Requisito Técnico Obrigatório)** Deverá ser capaz de receber e correlacionar as informações coletadas do Active Directory, tais como criação de contas, alterações e falhas de logins.
- 2.13. (Requisito Técnico Obrigatório)** A solução deverá monitorar aproximadamente 2.500 ativos.
- 2.14. (Requisito Técnico Obrigatório)** A solução deverá armazenar todos os logs dos ativos monitorados durante o período de contrato, possibilitando o acesso a direto, ou seja, sem a necessidade de restore, a todos os registros dos últimos 6 meses.
- 2.15.** Se solicitado pela Contratante, deverá possibilitar o acesso a qualquer um dos logs armazenados individualmente.
- 2.16.** Caso sejam necessários, conectores específicos deverão ser desenvolvidos pela Contratada sem custos extras.
- 2.17.** A implantação deverá ser realizada pela Contratada.