DEFINIÇÕES E RESPOSTAS ÀS SUGESTÕES APRESENTADAS PELAS EMPRESAS PARTICIPANTES DA CONSULTA PÚBLICA REALIZADA NO DIA 09/08/2010, VISANDO DISCUSSÃO DA MINUTA DO EDITAL - PARA CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SEGURANÇA DA INFORMAÇÃO PARA FORNECIMENTO E IMPLANTAÇÃO DE LICENÇAS DE USO OU APPLIANCES E LICENÇAS DE USO DE FERRAMENTA DE GERENCIAMENTO DE EVENTOS, INCLUÍDOS SERVIÇOS DE TREINAMENTO PARA CAPACITAÇÃO DE PESSOAL TÉCNICO E GARANTIA JUNTO A REDE DA SEF/MG, NAS CONDIÇÕES PREVISTAS NO EDITAL E SEUS ANEXOS.

QUESTIONAMENTO 1 - Quantos dispositivos serão monitorados?

Atualmente, há necessidade de que sejam monitorados 38 dispositivos. No entanto a solução ofertada deve permitir expansão futura do número de dispositivos monitorados.

Questionamento 2 - Qual será o tempo de retenção (6 meses, 1 ano, 2 anos)?

Tempo de retenção on-line de 3 meses.

Questionamento 3 - Qual o volume estimado de EPS (eventos por segundo)?

500 eps.

Questionamento 4 – Quais as possíveis plataformas utilizadas pela SEF?

A solução deve ter minimamente de forma nativa suporte aos seguintes ativos: roteadores Cisco; switches core Juniper, Extreme Networks e Cisco; firewall Checkpoint; storages HDS, SUN, HP, NetApp e EMC; sistemas operacionais SUN/Oracle Solaris, Linux e MS Windows; IDS/IPS Chekpoint; Websense Web Security; Cisco Ironport; bancos de dados Oracle, IBM DB2 e MS-SQL Server; balanceadores de carga (servidores e Links WAN) das marcas F5, Brocade, Cisco e Radware; servidores de aplicação Oracle Application Server, Oracle WebLogic Server, Jboss e Web Container Tomcat, software de gerenciamento de filas Websphere MQ Series.

Questionamento 5 – Quais os documentos devem ser entregues pelo fornecedor da solução?

Os produtos fornecidos deverão estar acompanhados de documentação técnica completa original, em língua portuguesa ou inglesa. A documentação deverá ser fornecida em meio eletrônico.

Questionamento 6 – Será exigido suporte a ambientes virtualizados?

Não será requerido suporte a ambientes virtualizados.

Questionamento 7 – Quanto à capacidade de processamento e normalização haverá um número mínimo de campos que devem ser tratados?

Não será estabelecido um número mínimo de campos que devem ser tratados em cada registro de eventos. No entanto, a solução ofertada deve possibilitar a remoção de campos desnecessários (filtro de informações relevantes nos registros de eventos).

Questionamento 8 – A atualização de base de conhecimento de segurança deve ser feita de forma automática pela internet?

As atualizações de base de conhecimento de segurança deverão estar disponíveis, preferencialmente, na modalidade de "live update", ou em até 03 (três) dias para qualquer outro mecanismo de atualização das versões, durante todo o período de garantia.

<u>Questionamento 9</u> – A solução deve possibilitar a verificação de conformidade com as políticas, controles e normas internas da SEF?

Sim. A solução deve permitir adequação às normas internas da SEF.

Deverá ser feita a integração da solução fornecida com os ativos especificados na tabela abaixo:

Dispositivos	Quantidade
Servidores de aplicação - SUN X4450 - Unix Solaris 10	4
Servidores de banco de dados - SUN T2000 - Unix Solaris 10	4
Instâncias de banco de dados - Oracle 10g	4
Servidor de backup - Unix Solaris 10	1
Appliances - LinkProof AS3000	2
Appliances - Server iron (Foundry/Brocade)	2
Firewall - Checkpoint FW1/R70	4
IPS - Checkpoint IPS-1	2
Switch - Alpine	2
Switch - Summit	2
Switch - Alcatel 10Gbps	2
Switch SAN - Brocade	2
Switch SAN - Sanbox	2
Switch SAN - CISCO	2
Roteador - CISCO	2
NAS - NETAPP V3100	1

A SEF encontra-se em fase de aquisição de novos switches core para substituição das duas switches Alpine. Caso as switches já tenham sido substituídas no momento da instalação/integração dos ativos com a solução adquirida de SIEM (gerenciamento de logs) o fornecedor deverá garantir a integração dos novos switches cujos fabricantes estejam elencados dentre as possíveis plataformas utilizadas pela SEF (resposta ao item D).

<u>Questionamento 10</u> – Quais são as necessidades e funcionalidades da solução em relação aos filtros?

A ferramenta deve:

- Filtrar e selecionar os eventos que serão inseridos na solução, garantindo a confidencialidade e a integridade;
- Permitir a criação e alteração de filtros;
- Suprimir entrada de eventos cuja informação não é relevante para análise, geração de relatórios e armazenamento a longo prazo;

<u>Questionamento 11</u> – Quais as funcionalidades dos agentes?

O agente ou conector devem possuir as seguintes funcionalidades:

1) Em tempo próximo ao real (near real-time), coletar e aplicar parsing (segmentação do dado) nos eventos do dispositivo monitorado;

2) Normalizar e categorizar os eventos em um padrão único que será usado pela solução;

3) Filtrar e selecionar os eventos que serão inseridos na solução, permitindo a criação e alteração de filtros;

4) Fazer a agregação de eventos semelhantes que ocorrerem dentro de um limite de tempo ou quantidade de eventos específicos, permitindo agregar tanto os eventos cuja única diferença seja o horário de ocorrência quanto especificar quais campos do evento normalizado devem ser considerados para fins de agregação.

5) Armazenar os dados localmente (cache), caso em que os correlacionadores estejam indisponíveis, permitindo a configuração do tamanho do cache;

6) Deve ser capaz de enviar o evento bruto ("raw") para o armazenamento e consulta futura;

7) Deve ser capaz de ajustar o horário dos eventos, caso necessário, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através de sincronização de NTP com os servidores locais.

8) Deve ser capaz de gerar relatórios ofuscando campos sensíveis dos eventos (senhas, números de cartões de crédito, importâncias monetárias e outros similares);

9) Deve ser gerenciado centralmente (configurações, controle e atualizações), através de interface gráfica única, sem necessidades de intervenção nos equipamentos onde está instalado;

10) Deve ser capaz de marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, divisão corporativa ou similar;

11) Deve ser capaz de inserir nos eventos normalizados, informações sobre localização geográfica dos mesmos;

12) Um único conector deve ser capaz de coletar, processar e normalizar tanto os eventos de segurança quanto os eventos de conformidade do ativo monitorado;

13) Tanto os eventos de segurança quanto os de conformidade devem ser normalizados para um único padrão de eventos utilizado pela solução;

14) Deve permitir múltiplos perfis de configuração com possibilidade de parametrização em ativado/desativado, de modo automático, de acordo com um horário definido previamente;

15) Deve comprimir os eventos em pelo menos 20% antes do envio aos correlacionadores;

16) Deve ser capaz de limitar a banda a ser utilizada para o envio dos eventos para os correlacionadores, permitindo a configuração/limitação da banda a ser utilizada;

17) Deve ser capaz de enviar os eventos para o correlacionador.

Questionamento 12 – **Cabeamento lógico**.

Serão disponibilizados para o contratado 6 pontos lógicos (conexões de rede – RJ-45 fêmea) com cabeamento de par trançado não-blindado (UTP) categoria 6A e patch cords da categoria 6. Caso o número de conexões lógicas demandadas pela solução ofertada exceda esse número (6 pontos lógicos), o contratado deverá se responsabilizar pela instalação do cabeamento lógico excedente. Essa instalação deverá ser feita utilizando cabeamento de par trançado não-blindado (UTP) categoria 6 e 6A, com patch cords que deverão ser da categoria 6 e, se for o caso, fibras óticas multimodo e passivos de rede, ambos com tecnologia Systimax, a fim de preservar a certificação do ambiente onde os equipamentos serão instalados, para todos os pontos lógicos necessários ao funcionamento da solução. O fornecedor será

responsável, também, pelo detalhamento da execução, tomando como referência projeto básico indicativo a ser elaborado pela SEF. Será de sua responsabilidade, ainda, a obtenção de aprovação para o serviço de instalação a ser efetuado, a ser concedida pela empresa responsável pela construção do datacenter da SEF e por sua manutenção, a fim de garantir a manutenção da certificação pela norma ABNT NBR 15247.

Questionamento 13 – Qual o padrão de rack utilizado pela SEF?

O Licitante vencedor deverá realizar a instalação dos servidores em rack padrão EIA 19"(dezenove polegadas) incluindo o kit de montagem e ocupando no máximo 04 RUs (rack units).

Questionamento 14 – Qual será o número de participantes do treinamento?

O treinamento básico deverá ser ministrado no ambiente da SEF/MG, com material (apostilas fornecidas), para 6 (seis) servidores indicados pela Superintendência de Tecnologia da Informação – STI/SEF-MG, compreendendo as fases de instalação, configuração e manutenção da solução fornecida – mínimo de 8 horas, com instrutor certificado.

O treinamento oficial deverá ser agendado para ser realizado até 90 dias após a emissão do Termo de Aceite Técnico relativo aos serviços de instalação, configuração, testes e ajustes em ambiente de produção da SEF-MG. O treinamento oficial deverá ser ministrado para 6 (seis) servidores indicados pela Superintendência de Tecnologia da Informação – STI/SEF-MG.

Questionamento 15 – O treinamento deve ser realizado pelo fabricante e com exigência de certificação ISO 27001?

O treinamento oficial, a ser ministrado em língua portuguesa por instrutor certificado pelo fabricante da solução ofertada, deverá ser agendado para ser realizado até 90 dias após a emissão do Termo de Aceite Técnico relativo aos serviços de instalação, configuração, testes e ajustes em ambiente de produção da SEF-MG.

Não há exigência de certificação ISO 27001 para o fabricante.

Questionamento 16 – Definição da prestação dos serviços de suporte e manutenção.

O Licitante vencedor deverá prover garantia original de fábrica para toda a solução ofertada, pelo período mínimo de 48 (quarenta e oito) meses contados da data de expedição do Aceite Técnico definitivo, ou seja, a partir da data em que foi dada como concluída a instalação, configuração, testes em produção e ajustes da solução fornecida. No caso do fornecedor não ser o próprio fabricante da solução fornecida – software e hardware – deverá provar de forma inequívoca a contratação da garantia estendida junto ao fabricante, transferível à SEF-MG, ou apresentar declaração do fabricante concordando com todas as exigências da garantia exigida, específica para este processo, antes da assinatura do instrumento.

a) Inclui-se na garantia o suporte técnico (orientação à equipe técnica da SEF-MG) e manutenção corretiva da ferramenta compreendendo o diagnóstico e identificação de problemas, correção de erros, defeitos (bugs) ou mau funcionamento sobre qualquer funcionalidade ou decorrente de qualquer customização efetuada pela contratada durante a fase de implantação.

b) A garantia deverá cobrir todo componente de hardware e software da solução fornecida onde, entende-se por hardware e software:

- Servidores ou appliances utilizados como plataforma dos componentes da solução ofertada;
- Estações de monitoração e administração da solução ofertada;

- Sistemas operacionais dos servidores, appliances (se aplicável) e estações de monitoração e administração da solução ofertada;
- Software para os componentes: Coletores, Correlacionador e Armazenamento.

c) Durante a vigência do contrato, o fornecedor deverá substituir, por sua conta e risco, no prazo máximo de até 10 (dez) dias úteis, contados a partir do recebimento da notificação da SEF-MG ou da constatação do defeito, o produto ou o serviço que apresentar quaisquer defeitos, que impeçam ou prejudiquem a sua utilização.

d) No caso do software, a garantia deve incluir, além da atualização, patches de correção e novos releases, também a disponibilização de novas versões lançadas durante o período de garantia contratado, sem qualquer custo adicional para a SEF-MG.

e) As atualizações de software deverão estar disponíveis, preferencialmente, na modalidade de "live update", ou em até 03 (três) dias para qualquer outro mecanismo de atualização das versões, durante todo o período de garantia. Ao final do prazo de garantia, a SEF-MG terá direito às licenças de uso dos softwares por tempo indeterminado, na última versão disponível quando do término da garantia.

f) Acordo de Nível de Serviços: os prazos para solução de ocorrências e os recursos a serem disponibilizados pelo Licitante devem observar os requisitos a seguir:

⇨ Central de Atendimento: o Licitante vencedor deverá prover acesso à SEF-MG à sua Central de Atendimento ou à Central de Atendimento do Fabricante no Brasil com disponibilização de número de telefone fixo no Brasil e endereço de e-mail ou ferramenta de acesso Web para registro de chamados e respectivo acompanhamento, na modalidade 24 x 7 x 365, ou seja, 24 horas por dia, 7 dias por semana, 365 dias por ano, incluindo feriados e pontos facultativos, envolvendo todos os recursos do ambiente que será objeto do contrato com resolução de problemas, via telefone ou via ferramenta web disponibilizada à SEF-MG;

⇨ Software: prazo de atendimento de 4(quatro) horas a partir do registro do chamado, independente da garantia obrigatória de provimento de acesso à SEF-MG aos recursos on-line a correções e a novas versões de software, podendo a assistência ser do tipo remota (via web, telefone ou e-mail);

⇨ Hardware: contempla substituição de peças, mão-de-obra e atendimento on-site, com resposta aos chamados telefônicos em até 2 (duas) horas e o prazo de solução de até 48 (quarenta e oito) horas a partir do registro do chamado.

g) O registro de solicitação de serviços de suporte, manutenção em garantia e orientação poderá ser feito via website, e-mail, fax ou telefone, onde constarão as seguintes informações: data, hora, descrição da demanda, número da Ordem de Serviço, identificação do solicitante e atendente.

h) Visando garantir a efetividade do atendimento relativo à manutenção e suporte técnico, o fornecedor deve manter sempre atualizados junto à SEF-MG os meios de comunicação com a Central de Atendimento própria ou do fabricante.

i) Não deverá haver qualquer limitação para o número de solicitações de suporte de software assim como não deverá haver qualquer limitação para o número de técnicos da SEF-MG autorizados, mediante indicação da SEF-MG, a abrir chamados técnicos de software.

j) Em todas as atividades de assistência técnica ou suporte relacionados à garantia dos produtos, os técnicos da CONTRATADA deverão empregar a língua portuguesa, exceto no uso de termos técnicos e na utilização de textos técnicos, que poderão estar redigidos em Inglês.

k) Deverá ser garantido à SEF-MG o pleno acesso aos sites dos fabricantes dos produtos ofertados, com direito a consultas a quaisquer bases de dados disponíveis para usuários, e também efetuar downloads de quaisquer atualizações de software ou documentação.

l) Quaisquer atualizações das documentações elaboradas quando da instalação, configuração, testes em produção e ajustes no ambiente da SEF-MG deverão ser fornecidas, sem ônus, durante o período de garantia de todos os produtos fornecidos.

Certificações do fornecedor – software:

a - ao Licitante vencedor serão exigidas prova de que possui credenciamento para representar o fabricante do software no Brasil, bem como capacidade para realizar a instalação, configuração, manutenção e suporte por meio da apresentação de declaração do fabricante, específica para o certame, comprometendo-se com os termos e condições exigidos para garantia e suporte dos produtos ofertados. Esta exigência será aplicada como condição para o recebimento dos produtos ofertados.

Certificações do fornecedor – hardware:

a - serão exigidas do Licitante vencedor, no momento da assinatura do contrato de fornecimento, nos termos do item 3, deste Anexo I, prova de que possui credenciamento ou parceria suficiente para o fornecimento, manutenção e garantia dos equipamentos ofertados pelo prazo exigido na especificação técnica, bem como capacidade para realizar a instalação, configuração, manutenção e suporte mediante apresentação de declaração de distribuidora/revenda autorizada do fabricante, ou ainda, do próprio fabricante, específica para o certame, comprometendo-se com os termos e condições exigidos para garantia e suporte dos produtos ofertados;

b - no caso de declaração de distribuidora ou revenda autorizada, a declaração deve estar acompanhada, necessariamente, de documento do fabricante que autorize a mesma a fornecer a citada declaração, para o respectivo certame.