REQUISIÇÃO DE COMPRA: 3000658911
PROCESSO N° WS1862777269
MODALIDADE: ATO CONVOCATÓRIO
USO DE PLATAFORMA ELETRÔNICA ARIBA
TIPO: MENOR PREÇO
OBJETO DA SELEÇÃO: Contratação de empresa especializada para o fornecimento de licenças e a prestação de serviços relacionados a uma Plataforma de Monitoração e Operação de Cibersegurança, abrangendo o fornecimento de licenças em modelo de subscrição SaaS para solução de SIEM (Security Information and Event Management) com recursos de Inteligência Artificial para análise e correlação de eventos, bem como a prestação de serviços de SOC (Security Operation Center) na modalidade MSS (Managed Security Services), com monitoramento contínuo (24h x 7 dias por semana)

Data e Hora – Evento Envelope: 13.01.2026 às 11:00 (Horário de Brasília)
Data e Hora - Evento de Simulação (Etapa de Lances): 13.01.2026 às 15:00 (Horário de Brasília)

Data e Hora - Evento de Negociação (Etapa de Lances): 14.01.2026 às 11:00 (Horário de Brasília)

Questionamento 01:

Referente ao item do TR 6.1.1.8. Suporte para criação de regras customizadas em Yara-L.

Considerando que as regras YARA são para o Google, solicitamos a confirmação se o requisito “YARA-L” admite linguagens funcionalmente equivalentes de detecção e correlação em logs, tais como: Sigma, SPL ou KQL, ou se o atendimento está restrito exclusivamente ao Google Security Operations?

RESP **FB:**

A exigência constante do item 6.1.1.8 tem como objetivo assegurar que a solução SIEM seja capaz de realizar correlação avançada de eventos, criação de regras customizadas, detecção de ameaças e casos de uso complexos, compatíveis com operações de SOC maduras.

Dessa forma, a exigência será considerada atendida caso a licitante apresente solução que possua linguagem própria de correlação, motor de regras ou rule engine, desde que esta permita:

Criação de regras customizadas;

Correlação temporal e contextual de eventos;

Suporte a casos de uso avançados de detecção e threat hunting;

Capacidade técnica equivalente ou superior à pretendida.

Assim, não há obrigatoriedade de adoção exclusiva da sintaxe proprietária Yara-L, sendo admitidas soluções tecnicamente equivalentes.

Questionamento 02:

Referente ao item do TR 6.1.1.45. Arquitetura baseada em infraestrutura cloud nativa com escalabilidade comprovada para volumes massivos de dados de segurança.

Entendemos que não há restrição referente a localidade da arquitetura. Está correto nosso entendimento?

RESP FB: A Solução deverá está hospedado no Brasil, sendo a contingência hospedada fora do pais. Conforme item 6.1.1.2 a Solução de SIEM deverá ser SAAS, não sendo aceito PaaS ou IaaS. Dessa forma entende-se que no caso de solução Saas a escalabilidade é realizada de forma transparente quando necessário sem a necessidade de paradas ou indisponibilidades para manutenções.

Questionamento 03:

Referente ao item 6.1.1.1. SIEM (Security Information and Event Management) Ao final do contrato, a CONTRATADA deverá entregar à CONTRATANTE todos os dados, configurações, regras de correlação, modelos de inteligência artificial treinados e demais ativos técnicos gerados durante a operação, conforme previsto contratualmente, garantindo a plena autonomia operacional e a continuidade do uso da tecnologia por parte da CONTRATANTE ao final do contrato, a CONTRATADA deverá entregar à CONTRATANTE todos os dados, configurações, regras de correlação, modelos de inteligência artificial treinados e demais ativos técnicos gerados durante a operação, conforme previsto contratualmente.

A. Entendemos que a obrigação se aplica exclusivamente as informações produzidas e/ou customizadas durante a execução contratual. Está correto nosso entendimento?

   RESP FB: O Entendimento está correto. Conforme item 6.1.1.2 a Solução deverá ser SAAS sendo a licença e a titularidade da assinatura do contratante. No término do contrato todas as informações que foram produzidas geradas devem permanecer em posse da Contratante

B. Entendemos que a obrigação que não se estende a patentes e conhecimentos prévios da contratação pertencentes à contratada. Está correto nosso entendimento?

   RESP FB: Informações que foram adicionadas, configuradas, personalizadas, dentro do SIEM/SOAR, assim como documentação elaboradas na vigência do contrato consideramos que é propriedades da contratada, devendo ser entregues ou mantidas na solução.

Questionamento 04:

Referente aos subitens 4.1.4.4. e 13.1.1.2. do Termo de Referência, entendemos que o prazo de 5 (cinco) dias úteis para entrega da documentação dos profissionais, poderá ser prorrogado por prazo superior, considerando os princípios da razoabilidade, eficiência, competitividade e planejamento, conforme a Lei n° 14.133/2021, desde que a solicitação seja devidamente fundamentada e ocorra antes do término do prazo estabelecido, sem prejuízo à execução contratual.

RESP FB: Se trata de um item do Termo de referência, consideramos que a licitante que participa do ato convocatório já possua esse tipo de serviço contratado. Consideramos que 5 dias uteis para um serviço que a participante já tenha como um prazo razoável.

Questionamento 05:

No escopo da contratação, a licitante permanece integral e exclusivamente responsável pela prestação do serviço de SOC, abrangendo, entre outras atribuições essenciais: o monitoramento contínuo dos ambientes, a correlação e análise de eventos de segurança, a inteligência de ameaças, a definição, manutenção e execução de playbooks operacionais, a classificação e o escalonamento de incidentes, a resposta técnica, a elaboração de relatórios, o cumprimento dos níveis de serviço (SLAs) pactuados e a governança completa do serviço contratado.

Não há, portanto, qualquer hipótese de transferência, delegação ou terceirização das atividades-fim do SOC, as quais permanecem sob controle técnico, operacional, contratual e jurídico exclusivo da Contratada, que responde integralmente perante a Administração por todas as obrigações decorrentes do contrato.

O apoio no atendimento de primeiro nível configura-se exclusivamente como **arranjo operacional complementar**, destinado à execução de atividades iniciais de recepção, registro, triagem e comunicação de eventos, sempre sob estrita coordenação, supervisão e diretrizes da Contratada. Tais atividades são realizadas com base em processos, fluxos, critérios técnicos e playbooks previamente definidos, homologados e controlados pela Contratada, não havendo autonomia decisória, técnica ou operacional por parte das equipes de apoio quanto à condução de incidentes, resposta a eventos ou tomada de decisões críticas.

Ressalta-se que a adoção desse modelo visa exclusivamente aprimorar a eficiência do atendimento, garantir comunicação fluida em língua portuguesa, assegurar maior aderência cultural e operacional ao ambiente do contratante e elevar a qualidade da interação inicial, sem qualquer prejuízo à responsabilidade integral da Contratada ou à integridade do serviço prestado.

Dessa forma, requer-se o entendimento desta Comissão no sentido de que o apoio operacional no atendimento de primeiro nível, nos termos aqui expostos, **não caracteriza subcontratação do serviço de SOC**, tampouco afronta as disposições do Termo de Referência, uma vez que preserva integralmente a titularidade, a governança, a responsabilidade técnica e a execução das atividades-fim pela Contratada.

RESP FB: O Edital é taxativo ao limitar a subcontratação exclusivamente à atividade de treinamento.
As atividades descritas pela licitante como "apoio no atendimento de primeiro nível" (recepção, registro, triagem e comunicação de eventos) constituem parcela da execução técnica do objeto contratado (monitoramento e operação do SOC). Não se trata de atividades-meio ou acessórias, mas sim de etapas integrantes do fluxo de tratamento de incidentes.

O fato de a Contratada manter a responsabilidade integral e a governança (conforme já exigido pelo Art. 122, § 1º da Lei 14.133/2021) não descaracteriza a figura da subcontratação quando a execução de parte do objeto é transferida a uma terceira pessoa jurídica.

Portanto, a execução do Nível 1 (N1) por meio de outra empresa jurídica distinta da licitante configura subcontratação de parcela do objeto não autorizada pelo Edital. A licitante deverá executar tais atividades com recursos próprios (equipe integrante de seu quadro, ainda que contratada

especificamente para o projeto), vedada a interposição de pessoa jurídica terceira para a execução operacional do monitoramento/triagem.

O edital, em seu item 12.1.1.3, exige expressamente 'equipe capacitada própria'. A permissão de subcontratação restringe-se única e exclusivamente à atividade de treinamento (item 8.1.1.11), não havendo previsão legal ou editalícia para estender tal permissão à operação de monitoramento e triagem (Nível 1), que exige qualificação técnica específica (item 12.1.1.5) e constitui atividade nuclear do objeto contratado

Questionamento 06:

Em atenção às disposições do Termo de Referência e com o objetivo de assegurar a mais ampla competitividade do certame, gostaríamos de solicitar a possibilidade de criação de regras customizadas baseadas em lógica YARA-L, bem como pleitear o reconhecimento da admissibilidade de modelos de detecção complementares baseados na criação de casos de uso e comportamentos específicos do ambiente do contratante.

A solução proposta contempla, em seu escopo técnico-operacional, a capacidade de criação de regras customizadas baseadas em lógica YARA-L os quais serão importadas para dentro da nossa solução de SOC.

Contudo, adicionalmente, incorporamos um modelo mais abrangente e evolutivo de detecção, fundamentado na criação contínua de casos de uso personalizados, desenvolvidos por time técnico próprio da Contratada, sem limitação quantitativa, como parte integrante do serviço de SOC.

Enquanto provedora global de serviços de Security Operations Center (SOC), adotamos uma abordagem de engenharia de detecção orientada a risco, comportamento e contexto de negócio. Nesse modelo, a lógica YARA-L é utilizada como um dos instrumentos técnicos disponíveis, porém integrada a estruturas mais amplas de correlação, análise comportamental, priorização e resposta a incidentes.

A criação de casos de uso específicos para o ambiente do cliente permite considerar características próprias de sua arquitetura tecnológica, fluxos operacionais, perfis de usuários, padrões de acesso e criticidade dos ativos, resultando em detecções mais precisas, contextualizadas e alinhadas ao risco real do negócio. Esses casos de uso englobam não apenas regras sintáticas, mas também critérios de severidade, limiares dinâmicos, correlação de múltiplas fontes de telemetria e integração direta com playbooks de resposta.

Por outro lado, a exigência de que o próprio contratante seja responsável pela customização direta de regras em YARA-L implica a transferência de uma responsabilidade técnica complexa, que pressupõe equipe especializada, conhecimento aprofundado da linguagem, capacidade contínua de testes, validação e manutenção das regras, além de atualização permanente frente às mudanças do ambiente e do cenário de ameaças. Tal abordagem, na prática, tende a aumentar o risco de falsos positivos, gerar regras desatualizadas ao longo do tempo e comprometer a efetividade operacional do serviço.

O modelo proposto, ao centralizar a criação, manutenção e evolução das detecções em equipe especializada da Contratada, eleva o nível de maturidade de proteção do ambiente, reduz o esforço operacional do contratante, assegura padronização técnica e facilita processos de auditoria e governança, sem restringir a capacidade de customização, mas ampliando-a de forma estruturada e sustentável.

Dessa forma, requer-se o entendimento desta Comissão no sentido de que o atendimento ao item 6.1.1.8 possa ser interpretado de forma a **admitir não apenas a criação de regras customizadas em lógica YARA-L**, mas também — a opção da **criação de casos de uso personalizados e modelos de detecção comportamental**, desenvolvidos por equipe técnica própria da Contratada, como meio tecnicamente superior de cumprimento do objetivo do requisito, qual seja, a efetiva customização das detecções às necessidades específicas do ambiente do contratante.

RESP FB: A exigência constante do item 6.1.1.8 tem como objetivo assegurar que a solução SIEM seja capaz de realizar correlação avançada de eventos, criação de regras customizadas, detecção de ameaças e casos de uso complexos, compatíveis com operações de SOC maduras.

Dessa forma, a exigência será considerada atendida caso a licitante apresente solução que possua linguagem própria de correlação, motor de regras ou rule engine, desde que esta permita:

Criação de regras customizadas;

Correlação temporal e contextual de eventos;

Suporte a casos de uso avançados de detecção e threat hunting;

Capacidade técnica equivalente ou superior à pretendida.

Assim, não há obrigatoriedade de adoção exclusiva da sintaxe proprietária Yara-L, sendo admitidas soluções tecnicamente equivalentes.

Questionamento 07:

Existe contrato semelhante vigente ou recém-encerrado?

RESP FB: NÃO

Questionamento 08:

Se sim, qual o número do contrato?

RESP FB: NÃO

Questionamento 09:

Se sim, com qual empresa?

RESP FB: NÃO

Questionamento 10:

Se sim, qual o valor atual do contrato?

RESP FB: NÃO

QUESTIONAMENTO 11:

Com base no Art. 67, § 9º da Lei 14.133/2021 e no Acórdão 1923/2025-TCU, será admitido atestado de capacidade técnica do fabricante/parceiro no que se refere a venda de SIEM SaaS, uma vez que se trata de componente de alta especialização tecnológica?

RESP FB: Conforme item 12.1.1.2 A Empresa deverá apresentar o atestado de capacidade técnica do objeto dessa contratação. Sendo sinalizado a venda das licenças e o serviço SOC

QUESTIONAMENTO 12:

Considerando que o SIEM SaaS é o insumo/ferramenta para a prestação do SOC, serão aceitos atestados de capacidade técnica que comprovem a operação de serviços de SOC utilizando ferramenta de SIEM do cliente, independentemente da empresa ter sido a fornecedora originária das licenças em contratos anteriores? Caso negativo, a exigência de atestado de venda de software, não restringe indevidamente a competitividade

RESP FB: Conforme item 12.1.1.2 A Empresa deverá apresentar o atestado de capacidade técnica do objeto dessa contratação. Sendo sinalizado a venda das licenças e o serviço SOC

QUESTIONAMENTO 13:

Yara-L é uma linguagem de detecção de ameaças proprietária e exclusiva da solução Google Security Operations (anteriormente Google Chronicle). Diferente da linguagem YARA padrão (open source), a versão "L" é específica para a arquitetura de dados desta ferramenta.

UDM (Unified Data Model) é a nomenclatura específica e proprietária do modelo de dados utilizado pela mesma ferramenta (Google Chronicle).

Ao exigir nominalmente "Yara-L" e "UDM", o Edital implicitamente exclui todos os demais fabricantes líderes de mercado (como Fortinet/FortiSIEM, IBM QRadar, Splunk, Elastic, entre outros) que utilizam suas próprias linguagens de correlação e modelos de normalização de eventos, igualmente ou mais eficientes.

A Lei nº 14.133/2021 veda, em seu Art. 9º, inciso I, a admissão de condições que comprometam, restrinjam ou frustrem o caráter competitivo do processo licitatório, bem como o estabelecimento de preferências por marcas específicas (salvo justificativa técnica robusta, que não consta no instrumento).

DO PEDIDO

Diante do exposto, para garantir a lisura e a competitividade do certame, entendemos que o objetivo da Fundação Butantan é contratar uma solução capaz de realizar correlação avançada e normalização de dados, independentemente da nomenclatura proprietária utilizada pelo fabricante.

Desta forma, perguntamos:

Está correto o entendimento de que a exigência do item 6.1.1.8 (Yara-L) será considerada atendida se a licitante ofertar solução que possua linguagem própria de correlação e criação de regras customizadas (parser/rule engine) com funcionalidades equivalentes ou superiores, sem se limitar à sintaxe proprietária de um único fabricante?

RESP FB: Item 6.1.1.8 – Suporte para criação de regras customizadas

A exigência constante do item 6.1.1.8 tem como objetivo assegurar que a solução SIEM seja capaz de realizar correlação avançada de eventos, criação de regras customizadas, detecção de ameaças e casos de uso complexos, compatíveis com operações de SOC maduras.

Dessa forma, a exigência será considerada atendida caso a licitante apresente solução que possua linguagem própria de correlação, motor de regras ou rule engine, desde que esta permita:

Criação de regras customizadas;

Correlação temporal e contextual de eventos;

Suporte a casos de uso avançados de detecção e threat hunting;

Capacidade técnica equivalente ou superior à pretendida.

Assim, não há obrigatoriedade de adoção exclusiva da sintaxe proprietária Yara-L, sendo admitidas soluções tecnicamente equivalentes.

Está correto o entendimento de que a exigência do item 6.1.1.10 (UDM) será considerada atendida se a solução ofertada possuir um Modelo de Dados Normalizado (Normalized Event Data) capaz de padronizar logs de múltiplas fontes, conforme é padrão nas soluções de SIEM de mercado?

RESP FB: Item 6.1.1.10 – Suporte a buscas em eventos normalizados e Raw Log Scan

A exigência do item 6.1.1.10 visa garantir que a solução possua modelo de dados normalizado, capaz de padronizar logs provenientes de múltiplas fontes, bem como permitir buscas estruturadas sobre eventos normalizados e consultas em logs brutos (raw logs).

Dessa forma, a exigência será considerada atendida caso a solução ofertada possua um Modelo de Dados Normalizado (Normalized Event Data), com estrutura, tipificação e semântica adequadas à correlação, detecção e investigação de incidentes, conforme práticas consolidadas nas soluções de SIEM de mercado.

Não é requisito que o modelo de dados seja denominado especificamente como Unified Data Model (UDM), desde que as capacidades técnicas requeridas sejam plenamente atendidas.

FUNDAÇÃO BUTANTAN
Gestão é uma ciência

Fundação Butantan
Rua Alvarenga, 1396
Butantã, São Paulo/SP
CEP: 05509-002

www.fundacaobutantan.org.br