CONSULTA PRELIMINAR AO MERCADO DAG/DPDO N.º 24/2024

Implementação de Solução SOAR

Nota legal:

Esta apresentação é apenas uma versão preliminar do projeto pretendido, partilhada apenas para fins de informação geral, não podendo ser considerada versão final, nem vinculativa.

As informações contidas neste documento podem estar sujeitas a alterações, não comprometendo nem vinculando os Serviços Partilhados do Ministério da Saúde, EPE e/ou quaisquer outros serviços e/ou órgãos do Ministério da Saúde ou do Serviço Nacional de Saúde.

I. ENQUADRAMENTO

A SPMS tem por missão a prestação de serviços partilhados nas áreas de compras e logística, serviços financeiros, recursos humanos e sistemas e tecnologias de informação e comunicação às entidades com atividade especifica na área da saúde, de forma a "*centralizar, otimizar e racionalizar*" a aquisição de bens e serviços no Serviço Nacional de Saúde.

Os Sistemas de Informação na Saúde permitem a cooperação, a partilha de conhecimentos e informação, bem como o desenvolvimento de atividades de prestação de serviços nas áreas dos sistemas e tecnologias de informação e comunicação. Desempenham um papel importante na reforma do sistema de saúde, tendo como principais objetivos a melhoria da acessibilidade, eficiência, qualidade e continuidade dos cuidados e o aumento da satisfação dos profissionais e cidadãos.

À SPMS cabe, ainda, a garantia da operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação do Ministério da Saúde, promovendo a definição e a utilização de normas, metodologias e requisitos que garantam a interoperabilidade e interconexão dos sistemas de informação da saúde entre si, e com os sistemas de informação transversais à Administração Pública, visando desenvolver e proteger a saúde dos cidadãos.

II. OBJETIVO

Pretende assim a SPMS, EPE vir a adquirir uma plataforma SOAR (*security orchestration automation and response*) e os respetivos serviços de implementação e manutenção, pelo que com vista à preparação do

SPMS – Serviços Partilhados do Ministério da Saúde, E.P.E. Av. da República, nº 61 | 1050-189 Lisboa | Tel.: 211 545 600| Fax: 211 545 649

respetivo procedimento aquisitivo, e fazendo uso do disposto no artigo 35.º-A do Código dos Contratos Públicos, a SPMS, EPE vem, nos termos da denominada "consulta preliminar ao mercado", solicitar informações sobre o objeto do contrato.

Assim, na presente consulta preliminar ao mercado, pretende-se identificar:

1. O preço base a considerar pela entidade adjudicante face à solução SOAR pretendida;
2. O preço base a considerar pela entidade adjudicante para os serviços de implementação;
3. O preço base a considerar pela entidade adjudicante para os serviços de manutenção e suporte;
4. Previsão de custos de suporte e manutenção a 3 e 10 anos;
5. Prazo considerado necessário para a entrega da solução, bem como o plano de implementação;
6. Informação do equipamento, serviço ou do seu portefólio, com os detalhes que considerar relevante para o objeto da consulta preliminar;

A consulta preliminar será constituída por:

Secção I - Plataforma SOAR - Requisitos técnicos e funcionais

1. A solução deve incluir a sua própria gestão centralizada de todos os componentes e funções administrativas, a partir de uma interface gráfica de utilizador baseada na web e intuitiva;
2. A solução deve permitir a visualização de incidentes, ações efetuadas a partir da solução, comandos para APIs, entre outros, em tempo real;
3. A solução deve assegurar análises estratégicas e de ameaças mais impactantes, usando o mapeamento da Framework MITRE ATT&CK, de forma a melhorar a análise das causas-raiz;
4. A solução deve ser capaz de interligar vários incidentes (automaticamente ou manualmente), podendo usar inteligência artificial e automação para otimizar e acelerar as investigações;
5. A solução deve permitir o bloqueio de entrada de eventos provenientes de integrações a partir a partir de filtros customizados;
6. A solução deve permitir a pesquisa de incidentes a partir de *queries* com linguagem semelhante à natural e deverá permitir a pesquisa de incidentes através de campos de informação presentes nos mesmos;
7. A solução deve ser capaz de priorizar alertas com base em tipo de ativo, conta, comunicação com IOCs, etc;

8. A solução deve garantir a possibilidade de criar ou editar *parsers* para processamento de campos de incidentes não reconhecidos automaticamente;
9. A solução deve assegurar a integridade, autenticidade e confidencialidade no transporte dos *logs*;
10. A solução deve permitir a criação de listas com vários tipos (json, csv, html);
11. A solução deve ter a capacidade de enviar e-mails (através de integração), receber e-mails para tratamento, podendo criar *templates* de resposta;
12. A componente de automação da plataforma deve basear-se no uso de *workflows* modulares e scripts. Qualquer tarefa que seja automatizada deve poder ser visualizada através de um *workflow* disponível na interface gráfica;
13. A solução deve suportar mecanismos de *Disaster Recovery*, permitindo a comutação de todos os serviços de gestão e controlo;
14. A solução deve ter o seu próprio sistema de ticketing;
15. A plataforma deve utilizar *machine learning* para identificar incidentes relacionados e detetar incidentes duplicados;
16. A solução deve ser capaz de aprender e sugerir que ações devem ser tomadas pelo analista tendo em conta a análise de incidentes prévios.

Ativos (*asset discovery*)

17. A solução deve ter capacidade de armazenar informação de ativos, sejam provenientes de uma integração com CMDB ou através de campos populados nos incidentes destinados a *hostnames,* ips, de forma que permita ingerir essa informação e armazenar na sua lista interna de assets ou indicadores, com possibilidade de criar campos customizados para dar contexto acerca do asset ou indicador;
18. A solução deve permitir atribuir pesos relativos à importância dada a determinadas redes, ativos e serviços, podendo este valor ser considerado na fórmula de cálculo do risco.

Arquitetura e integrações

19. A solução deve disponibilizar um Marketplace. Este Marketplace deve ser um local central para instalar, trocar, contribuir e gerir conteúdo da plataforma incluindo: playbooks, automações, integrações, campos, layouts, etc.
20. A solução deve ter a capacidade de integração com várias ferramentas de IT;

21. A solução deve permitir uma arquitetura em alta disponibilidade de forma integrada e nativa, de forma a disponibilizar um serviço 24x7x365;
22. A arquitetura para a solução proposta deve levar em conta o não sobrecarregar da infraestrutura de comunicações;
23. A arquitetura da solução deve permitir realizar *deployments on-premises* e *cloud*. No caso de *deployments cloud* não deve ser necessário que as ferramentas internas comuniquem diretamente com a *cloud*.
24. A arquitetura da solução deve garantir que qualquer ferramenta que necessite de comunicar com a *cloud*, o possa fazer através de um proxy disponibilizado pela solução;
25. A solução deve ser facilmente expandida para suportar necessidades adicionais, sem necessidade de reiniciar e reconfigurar a implementação existente;
26. A solução deverá disponibilizar uma API que permita a operação e gestão da própria solução;
27. A API deve permitir executar as mesmas operações que estão disponíveis via interface gráfica;
28. Deve ser utilizada uma REST API para obter informação de outras plataformas de forma a gerar incidentes;
29. Para além das integrações *out of the box*, a plataforma deve ter a funcionalidade de BYOI (Bring Your Own Integration);
30. A solução deve permitir desenvolver novas integrações de forma a integrar com ferramentas desenvolvidas *in-house*. De forma a poder criar estas integrações a plataforma deve disponibilizar um SDK;
31. A solução deve, em termos de monitorização de integrações, ter capacidade de notificar quando uma integração se encontra indisponível;
32. A solução deve ser escalável, para aglomerar o processamento de mais eventos, incorporar mais equipamentos e/ou licenciamento, não implicando a substituição dos já instalados;
33. A solução deve apresentar uma arquitetura modular e *multi-tenant* em modelo RBAC, isto é, um ambiente em que a informação originária de várias unidades lógicas se mantém segregada entre si, não havendo qualquer possibilidade de partilha/*spillage* de uma unidade para a outra;
34. A solução deve possuir uma arquitetura onde seja preservada a anonimização dos dados pessoais, estando em conformidade com o Regulamento Geral de Proteção de Dados (RGPD);
35. A solução deve suportar endereçamento IPv6 em todos os campos onde sejam suportados por endereçamento Ipv4;

36. Possibilidade de criar integrações ou tarefas customizadas recorrendo para isso a linguagens de programação (Python, C++, JS, Powershell);
37. A solução deve ter a capacidade de consultar repositórios (internos ou externos) para acesso a atualizações dos seus vários componentes, bem como de elementos dinâmicos como assinaturas e regras;
38. A solução deve permitir a inclusão de *feeds* sobre reputação de endereços IP e domínios;
39. A solução deve ser capaz de obter automaticamente informação externa de bases de dados públicas de reputação de endereços IP e vulnerabilidades, entre outros;
40. A solução deve ter a capacidade de integração com um sistema de *ticketing.* As integrações devem ser bidirecionais de forma a iniciar ações para a criação de tickets assim como pesquisar e atualizar tickets existentes.;
41. A solução deve suportar a integração com o MISP;
42. A solução deve ter integração com ferramentas de SIEM (Splunk, Arcsight, Microsoft Defender);
43. A solução deve permitir a integração com ferramentas de vulnerabilidades externas, permitindo o cruzamento de informação;
44. A solução deve permitir a implementação de instâncias e/ou agentes em localizações distintas;
45. O tráfego entre a instância central e outras instâncias e/ou integrações de terceiros deverá ser encaminhado de forma segura sobre a infraestrutura de comunicações existente;
46. A solução deve suportar uma base de dados distribuída para coleta de eventos e atividades de rede, de forma que todas as informações possam ser acedidas a partir de uma única interface de utilizador;
47. Deve ser possível atualizar as integrações, os *playbooks*, os scripts de automação e os relatórios em ambientes offline;
48. Deve ser possível atualizar as integrações, os *playbooks*, os scripts de automação e os relatórios sem ter de fazer upgrade ao sistema.

Playbooks

49. Definição e configuração de *playbooks* customizados com interface simples de forma a conseguir construir fluxos de tarefas de interação com o próprio SOAR bem como com integrações terceiras para consumir informação, introduzir informação ou manipular informação;

50. A solução deve utilizar *playbooks* de forma a automatizar os passos seguidos pelos analistas para responder aos diferentes tipos de incidentes (phishing, malware, etc) desde o processo de triagem até ao fecho do incidente;
51. Por defeito, a plataforma deve ter mais de 100 *playbooks* configurados que correspondam a diferentes use cases e tipos de incidentes.
52. Os *playbooks* devem ser *opensource*. Qualquer pessoa com uma conta do GitHub deve poder submeter *updates*;
53. Não deve ser necessário desenvolver código para a criação de playbooks;
54. A configuração de playbooks deverá ocorrer através de uma interface gráfica que utilize mecanismos de drag-and-drop;
55. Deve ser possível incluir playbooks dentro de outros playbooks;
56. Os playbooks podem conter tasks manuais, tasks automatizadas, filtros, sub playbooks, tasks de recolha de dados e tasks condicionais.
57. Deve ser possível correr playbooks automaticamente assim que um incidente é gerado na plataforma. Também deve ser possível agendar playbooks para correr em determinados períodos de tempo.
58. Deve ser possível correr playbooks manualmente através da criação de um incidente no sistema e da sua associação com um playbook. Os playbooks também devem poder ser criados como "Jobs" e ser corridos em tempo real para determinados use cases (health check,etc).
59. A representação gráfica de cada componente dos playbooks deve servir como um nível de abstração para os scripts e funções automatizadas que correm no back-end.
60. Todos os outputs de um playbook devem ser documentados no sistema, assim como as atividades do analista.
61. Deve ser possível criar tasks no processo de investigação que necessitem de interação com o analista para progredir na análise do incidente.
62. A execução dos playbooks deve poder ser visualizada passo a passo em tempo real ou à posteriori de forma a permitir o debugging dos mesmos.
63. No caso de algum dos passos do playbook parar devido a um erro, deve ser possível recomeçar o playbook a partir deste passo.
64. Deve ser possível mapear nos playbooks os processos e procedimentos CSIRT atuais e futuros para "Incident Types".
65. Deve ser possível atribuir tarefas dentro de um playbook a diferentes membros da equipa.
66. O output de qualquer task dentro de um playbook deve poder ser consumido por qualquer outra task que seja executada posteriormente nesse workflow.

67. Tasks que façam parte do workflow de um playbook devem poder consumir outputs gerados por sub-playbooks que tenham sido executados previamente nesse workflow.
68. Deve ser mantido o histórico de todos os playbooks e tasks executados no sistema.
69. Deve ser possível exportar playbooks.
70. Todos os playbooks devem manter um sistema de "versioning".
71. Devem existir playbooks específicos para lidar com incidentes de ransomware.
72. Devem existir playbooks específicos para lidar com incidentes relacionados com GDPR.
73. A plataforma deve disponibilizar out of the box playbooks para use cases fora do mundo tradicional da segurança, nomeadamente: Onboarding de novos empregados, Offboarding de empregados, ativar utilizadores na AD, atribuição de acessos a novos utilizadores, Shadow IT, etc.

Autenticação, Perfis e *logging*

74. A solução deve ter a capacidade de criação de perfis de utilizador de forma a permitir a segregação de permissões dentro do SOAR de acordo com as funções do utilizador. (ex: analista e administrator de plataforma);
75. A solução deverá permitir o acesso simultâneo de, pelo menos, cinco analistas de segurança.
76. A identificação, sincronização e autenticação dos utilizadores das consolas de SOAR deverá ser feita através de um diretório central LDAPS, podendo ser *Microsoft Active Directory* com ligação segura;
77. Os acessos à solução deverão também ser possíveis utilizando o protocolo SAML e/ou OAUTH;
78. A solução deve permitir definir acessos baseados em perfis (RBAC) a várias áreas funcionais da solução, incluindo a capacidade de restringir o acesso de um utilizador a funcionalidades específicas da solução que não estão dentro do âmbito de uma função do utilizador, incluindo, mas não se limitando a, administração, relatórios, filtragem de eventos, criação de playbooks e/ou visualização do painel;
79. A solução deve permitir a criação de perfis com determinados privilégios de visualização de informação;
80. A solução deverá permitir implementar o princípio de privilégios mínimos para os utilizadores que operam a solução, ou seja, os utilizadores não devem ter mais privilégios do que que os estritamente necessários para a sua função;
81. A solução deve ter a capacidade de registar em log as atividades de administração da solução;
82. A solução deve ter a capacidade de registar em log as atividades dos utilizadores que nela operam.

Backups

83. A solução deverá ter capacidades de *backup* completo diário (ou frequência inferior) de todos os componentes SOAR.
84. A solução deverá permitir a realização de *backups* locais, mas deverá permitir também a realização de backup centralizado de forma regular;
85. A solução terá de gerir um tempo de retenção online e offline de todos os dados em bruto (r*aw data)* de, pelo menos:
    - Retenção Online: mínimo 90 dias
    - Retenção Offline: 365 dias, sendo que informação estatística deve ser armazenada por 2 anos (730 dias)
86. A solução deverá ser capaz de gerir alterações nos termos de retenção, quer na *storage* online, quer no offline.

Colaboração

87. A solução deve permitir colaboração em tempo real entre os analistas de forma a acelerar o processo de resolução de um incidente;
88. A plataforma deve disponibilizar a sua própria ferramenta de colaboração para analistas. Cada incidente deve disponibilizar um "war room" onde os analistas podem colaborar entre si e partilhar informação sobre a investigação em curso;
89. O *war room* deve permitir aos analistas colaborar, documentar e executar comandos de segurança numa única consola;
90. A solução deve também integrar com plataformas externas de colaboração;
91. No caso de os analistas utilizarem uma plataforma de colaboração durante a análise de incidentes, deve ser possível integrar o conteúdo desse chat com a plataforma e o respetivo incidente;
92. Deve ser possível convidar utilizadores externos à equipa de segurança de forma a estes terem acesso à plataforma de colaboração para determinados incidentes. A interação com utilizadores externos pode ser também feita através do envio de emails que pode ser despoletado através de uma task de um playbook. Estes playbooks devem monitorizar as respostas a estes emails e tomar ações dependendo da resposta obtida;

Documentação, Reporting e relatórios

93. A solução deve ter possibilidade de consultar dados e estatísticas do sistema e dos incidentes que consome, permitindo retirar métricas;
94. A plataforma deve permitir gerir e monitorizar SLAs;
95. A plataforma deve permitir documentar todas as ações tomadas na análise de qualquer tipo de incidente;
96. Todos os incidentes devem disponibilizar uma secção na interface gráfica que documente todas as alterações efetuadas, membros da equipa envolvidos no incidente, tasks completas, IOCs, comandos executados manualmente pelos analistas, evidências, chat, notas, tasks do playbook e seu respectivo output. Esta informação deve ser apresentada, respeitando a timeline dos acontecimentos;
97. As ações dos analistas devem ser documentadas;
98. A solução deve possuir um repositório de indicadores;
99. A solução deve conter reports pré-definidos;
100. A solução deverá ter a capacidade de produzir relatórios situacionais e dashboards;
101. A solução deverá ter a capacidade de produzir relatórios com dados de histórico;
102. A solução deverá ter a capacidade de elaborar relatórios de alto nível, assim como elaborar relatórios técnicos de incidentes;
103. A solução deverá ter a capacidade de reporting em formatos standard mas também permitir a inclusão de formatos pré-definidos com base na informação pretendida.
104. A solução deverá ter capacidade de reporte de conformidade ao nível das normas ISO2700X;
105. A solução deverá ter a capacidade de reporte de conformidade ao nível do RGPD e RJSC;
106. A solução deverá, no mínimo, ter capacidade de gerar os relatórios em formato HTML, CSV e PDF;
107. A solução deverá permitir a configuração do envio dos relatórios no mínimo por e-mail e o download dos mesmos.

Secção II - Serviços de implementação

1. Como serviços de implementação deverão estar incluídos todos os trabalhos de instalação, configuração e parametrização da solução proposta, bem como todo o trabalho de integração da totalidade dos sistemas, soluções, equipamentos e utilizadores da SPMS;
2. Os serviços de implementação devem incluir, no mínimo, as seguintes atividades macro:
    a) Workshop de definição de âmbito e pré-requisitos
    b) Instalação e configuração necessária ao funcionamento da solução proposta:
        I. Identificação e integração de várias integrações uteis para tratamento de incidentes a partir do SOAR;
        II. Configuração de casos de uso, através da adaptação de casos de uso já fornecidos pelo fabricante (out-of-the-box), nomeadamente:
            - Phishing;
            - Malware identificado em Máquinas;
            - Bloqueio de Ips, URLs ou domínios automaticamente através de feeds ou alertas recebidos;
            - Bloqueio de utilizadores;
            - Bloqueio de utilizadores e reset de passwords;
            - Isolamento de máquinas na rede.
        III. Definição e configuração de *dashboards*, relatórios e alertas (em diversas plataformas)
        IV. Entre outras atividades necessárias que se afigurem necessárias.
    c) Testes de aceitação;
    d) Entrega de documentação técnica e de utilizador.
    e) Formação técnica à equipa da SPMS de forma a permitir à SPMS obter as competências técnicas necessárias para a utilização, gestão e futuras configurações da solução, garantindo assim a transferência de "know-how".

    - A formação deverá ser ministrada por recursos certificados pelo fabricante e que participaram no projeto. Esta formação deverá ter uma duração mínima de 20 horas e ser realizada no prazo máximo de 2 meses a contar a partir da aceitação da solução.

7. No âmbito dos serviços de implementação, deve ser apresentado um plano temporal detalhado de implementação, com marcos específicos (*milestones*) e entregáveis definidos, bem como os responsáveis pelas diferentes ações.
8. A formação do ponto 2-e) deverá ser ministrada por recursos certificados pelo fabricante e que participaram no projeto. Esta formação deverá ter uma duração mínima de 20 horas e ser realizada na preparação para operação (em ambiente de teste) e em operação no prazo máximo de 2 meses a contar a partir da aceitação da solução.

Secção III - Serviços de manutenção e suporte

1. Nos serviços a prestar deverão estar incluídos o serviço de suporte e trabalhos de atualização de forma a garantir a total operacionalidade da solução com suporte 24x7;
2. O suporte técnico deverá ser em língua portuguesa;
3. A solução SOAR a implementar deve incluir suporte técnico do fabricante.
4. O suporte técnico deve oferecer a escolha de dois ou mais níveis de suporte diferentes.
5. O suporte técnico deve incluir:
    a) Conectividade remota entre o cliente e os especialistas de suporte do fabricante para resolução de problemas.
    b) Recomendações sobre otimização da solução.
    c) Atualizações de produtos.
    d) Um perfil de *Technical Account Manager*.

III. FORMA DA CONSULTA

É imperativo que a consulta preliminar ao mercado seja conduzida com transparência e não haja tratamento desigual de operadores económicos, conforme dispõe o artigo 35.º-A do Código dos Contratos Públicos.

Assim, a consulta preliminar ao mercado será publicitada no portal de internet público da SPMS, EPE, em http://www.spms.min-saude.pt, e no respetivo LinkedIn, devendo os operadores económicos interessados em apresentar contributos no âmbito da presente Consulta Preliminar, remeter email para consulta.preliminar@spms.min-saude.pt, até ao dia **29 de novembro de 2024**.

IV. PRESTAÇÃO DE INFORMAÇÃO PELOS OPERADORES ECONÓMICOS

A prestação voluntária de informação pelos operadores económicos, deverá ser efetuada para o correio eletrónico consulta.preliminar@spms.min-saude.pt até à data-limite de 29 de novembro de 2024, devendo os interessados indicar claramente no assunto do email a referência ***"Consulta Preliminar n.º 24/2024 - Implementação de Solução SOAR".***

V. INFORMAÇÃO PRETENDIDA

A informação a prestar voluntariamente pelos operadores económicos, considerada por eles como oportuna e relevante, é a seguinte:

1. Detalhes do operador económico: Nome, endereço, site, contacto telefónico e e-mail;
2. Áreas de especialidade e atuação, indicação do CAE;
3. Informação do equipamento, serviço ou do seu portefólio, com os detalhes que considerar relevante para o objeto da consulta preliminar;
4. Os operadores económicos deverão apresentar o ficheiro Excel em anexo à presente Consulta Preliminar, devidamente preenchido, com:
   a) O custo de aquisição da solução SOAR pretendida;
   b) O custo para os serviços de implementação;
   c) Prazo considerado necessário para a entrega da solução, bem como, o plano de implementação;
   d) O custo de manutenção a 3 e 10 anos;
   e) Informação sobre as características do Anexo Técnico;
   f) Arquitetura de referência e casos de sucesso (com dimensão significativa).

VI. PRAZO DA CONSULTA

A informação prestada pelos operadores económicos será aceite até à data de **29/11/2024.**