CONSULTA PRELIMINAR AO MERCADO DAG/DPDO – UCS n.º 14/2024

Implementação de Solução XDR

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 XDR (*Extended Detection and Response*) e os respetivos serviços de implementação e manutenção, pelo que com vista à preparação do respetivo

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

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 XDR 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 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 XDR

1. Requisitos gerais da plataforma XDR

A solução XDR a adquirir deve:

1. Ser robusta para defender a infraestrutura de TI corporativa contra ciberameaças, incluindo aquelas que não podem ser detetadas pelas aplicações EPP (*endpoint protection platform*).
2. Ser capaz de correlacionar dados provenientes de múltiplas fontes, incluindo *endpoints*, servidores, redes, e-mails e serviços em nuvem, para identificar padrões e comportamentos anómalos que possam indicar uma ameaça.
3. Utilizar técnicas de *machine learning* e inteligência artificial para detetar ameaças avançadas e persistentes (APTs), que podem não ser identificadas por métodos tradicionais de assinatura.
4. Fornecer monitorização contínua das atividades de rede e *endpoints* para detetar e responder rapidamente a atividades suspeitas, garantindo uma vigilância constante contra ameaças potenciais.
5. Ser capaz de executar automaticamente respostas pré-definidas (através de *playbooks*) para incidentes detetados, tais como aplicar processos de remediação tais como isolar dispositivos comprometidos, bloquear comunicações maliciosas, entre outros.

6. Fornecer um processo unificado de deteção e resposta através de componentes integrados e cenários holísticos em uma única interface que permite consultar informações, priorizar os eventos mais críticos, desenvolver respostas automatizadas, eliminar falsos positivos, entre outros.
7. Garantir que a interface do utilizador é intuitiva e fornece acesso rápido às funcionalidades mais críticas.
8. Permitir priorizar alertas com base em credibilidade, relevância e severidade do risco.
9. Ser capaz de receber indicadores personalizados de comprometimento (IOC) e indicadores de ataque (IOA) para classificar e analisar eventos.
10. Ter capacidade atualização tecnológica contínua, garantindo que novas ameaças e vulnerabilidades são constantemente abordadas.
11. Ser capaz de armazenar localmente assinaturas de ameaças, regras de deteção e algoritmos de *machine learning*.
12. Possuir capacidade de operação autónoma, executando deteção e resposta a ameaças sem a necessidade de comunicação constante com servidores remotos ou serviços em nuvem.
13. Ter capacidade suficiente de armazenamento e processamento para analisar *logs* e eventos localmente, sem depender de infraestrutura externa.
14. Garantir configuração de sensores com a capacidade de analisar pelo menos 1TB de tráfego de rede por mês.
15. Garantir a possibilidade de criar *parsers* para processamento de eventos não reconhecidos automaticamente.
16. Incluir recursos de autoavaliação da sua própria configuração, por exemplo, detetando regras para as quais não existe tráfego ou tráfego que não é usado por nenhuma regra existente.
17. Disponibilizar informações detalhadas sobre incidentes de segurança nomeadamente para apoiar as análises forenses a realizar. Esta deve permitir a captura integral dos eventos dos *endpoints* de forma a ser possível realizar análises forenses de um evento e a análise deve ser capaz de usar todos os dados capturados por esse sensor de modo a reconstruir a linha temporal de acontecimentos associados ao evento.
18. Disponibilizar um módulo de *Vulnerability Assessment* e *Asset Inventory*.
19. Contemplar funcionalidades de *Information Exfiltration*, permitindo nomeadamente:
    a) Implementar políticas de segurança associadas à temática de exfiltração de informação ao nível do *endpoint* (agente).
    b) Detetar e impedir a exfiltração não autorizada de informação.
    c) Identificar e alertar (early warnings) sobre extração e movimentos anómalos de informação.

d) Alertar sobre ações em ficheiros que violem as políticas de segurança.
e) Bloquear automaticamente ações sobre ficheiros que violem as políticas de segurança.
f) Detetar comportamento anormal ou suspeito do utilizador recorrendo a mecanismos de *machine learning* para detetar ameaças internas.
g) Mitigar ataques de *ransomware,* detetando e bloqueando padrões típicos de acesso a ficheiros.
h) Monitorizar o acesso a todos os ficheiros confidenciais e registar dados granulares de uso, como utilizador, departamento, ficheiro acedido, tipo de ficheiro e tempo de resposta da operação.
i) Existência de consola para evidenciar as ações perante uma auditoria, ações de conformidade e investigação contendo relatórios sobre todas as operações sobre ficheiros.

2. Requisitos de arquitetura e integrações da plataforma XDR

A solução deve:

1. Suportar uma arquitetura em alta disponibilidade para um serviço 24x7x365.
2. Contemplar uma arquitetura escalável e modular, permitindo a expansão sem necessidade de reconfiguração.
3. Ter uma arquitetura explicitamente *on-premise* com arquitetura baseada em micro-servicos locais, com possibilidade de publicar um *gateway* de conexão para dar cobertura aos dispositivos fora da rede interna.
4. Garantir na sua arquitetura que a comunicação dos *endpoints* seja feita de forma segura e cifrada com portas/protocolos bem definidos com a possibilidade de utilizar um *gateway* de conexão para os dispositivos fora da rede interna.
5. Ser *multi-tenant* com modelo RBAC (*Role-based access control*), preservando a anonimização dos dados pessoais conforme normas locais e internacionais, bem como se manter atualizada e a conformidade mediante atualizações de tais normas.
6. Disponibilizar software para instalação nos *endpoints* via Microsoft SCCM (Microsoft *System Center Configuration Manager*) e ANSIBLE.
7. Obter e carregar dados da/na plataforma via API.
8. Permitir a operação e gestão através de uma API, ou seja, permitindo executar as mesmas operações que estão disponíveis via a interface gráfica, bem como as respostas desenvolvidas nesta.
9. Ser capaz de integrar-se com terceiros via ICAP (*Internet Content Adaptation Protocol*) para realizar *scanning* de objetos.
10. Ter capacidade de integração com sistemas externos para atualizações de componentes, assinaturas e regras e inclusão de *feeds* de reputação.

11. Ter capacidade de integração com sistemas externos para automatizar processos de consciencialização (*awareness*).
12. Permitir a correlação cruzada para conectar soluções de terceiros, gestão de *logs* e *data lake*.
13. Permitir a integração com SIEMs (*Security information and event management*).
14. Ter capacidade de integrar com sistemas de *ticketing.*
15. Garantir integração com plataformas SOAR (*security orchestration, automation and response*)
16. Integrar com soluções CMDB (*Configuration Management DB*).
17. Suportar mecanismos de *Disaster Recovery* e endereçamento IPv6.
18. Permitir a inclusão de *feeds* sobre reputação de endereços IP e domínios.
19. Suportar análise comportamental (UEBA - *User and entity behavior analytics*) e integração com ferramentas de *Identity & Access Management* (IAM) e *Privileged Access Management* (PAM).
20. Garantir o suporte para envio de alarmística por correio eletrónico e por *trap* SNMPv3.
21. Ser capaz de suportar a integração no modo de monitorização SPAN (*Switched Port Analyzer*).
22. Garantir suporte para envio e recebimento de dados em diversos formatos, incluindo JSON e XML.
23. Exportar *logs* em formato *syslog* para qualquer solução de gestão de *logs*.

3. Requisitos de autenticação e perfis da plataforma XDR

1. A autenticação na solução deve ser feita com protocolos seguros (TLS v1.2 e superior) e incluir múltiplo fator de autenticação (MFA) e mecanismos contra *bruteforce authentication* (captcha).
2. A autenticação dos utilizadores das consolas do XDR deve ser feita através de um diretório central LDAPS (e.g., Microsoft Active Directory).
3. A solução deve permitir acessos utilizando SAML (*Security Assertion Markup Language*), OAUTH2 (*Open Authorization*), API *keys* e/ou *tokens* JWT (JSON *Web Tokens*).
4. A solução deve definir acessos baseados em perfis (RBAC - *Role-Based Access Control*) a várias áreas funcionais da solução.
5. As atividades de administração e dos utilizadores devem ser registadas.
6. As ações dos utilizadores do sistema devem ser registadas tanto no log de atividade local quanto remotamente.
7. Devem ser cumpridos os requisitos de *security event logging*, permitindo responder para qualquer acesso efetuado, quem, o quê, onde, quando, porquê e como.
8. A solução deve utilizar um canal seguro para a comunicação entre a consola e o administrador, nomeadamente com a importação do certificado digital usado para proteger o canal de comunicação.

4. Requisitos de Backups e Armazenamento da plataforma XDR

A Solução deve:

1. Ter capacidade de *backup* completo diário de todos os componentes XDR.
2. Ter capacidade de realizar *backups* locais e centralizados regularmente.
3. Permitir uma gestão de um tempo de retenção online de no mínimo 90 dias e offline de 365 dias, sendo preferencialmente ilimitada (limitada apenas pelo tamanho de armazenamento disponível).
4. Ter capacidade de gerir alterações nos termos de retenção.
5. Armazenar todos os *logs* capturados no seu formato original e geração de *hash* (e.g., SHA2).
6. Ter capacidade de cifrar os *hash* com HMAC (*Hash-based message authentication code*).
7. Possuir armazenamento complementar de *logs* com índices e propriedades extraídas.
8. Suportar a tecnologia de *bufferização* de consultas.

5. Requisitos de deteção e proteção da plataforma XDR

A solução deve:

1. Permitir a deteção avançada de ameaças e correlação cruzada em tempo real de eventos de diferentes fontes utilizando inteligência artificial e automação. São requisitos mínimos da utilização da inteligência artificial na deteção e correlação de eventos:
   a) Análise Comportamental: A IA deverá ser utilizada para analisar padrões de comportamento dos utilizadores e sistemas, identificando atividades anómalas que podem indicar a presença de ameaças. Algoritmos de *machine learning* deverão ser aplicados para estabelecer perfis de comportamento normal e detetar desvios que possam representar riscos de segurança.
   b) Deteção de Anomalias: A IA deverá aplicar técnicas de deteção de anomalias para identificar atividades fora do padrão, como acesso não autorizado, transferência de dados incomuns ou alterações inesperadas nos sistemas.
   c) Correlação de Eventos: A IA deverá correlacionar eventos de segurança provenientes de diversas fontes (*endpoints*, rede, nuvem, etc.) em tempo real. Isso permite a identificação de padrões complexos e multifacetados de ataque que seriam difíceis de detetar manualmente. A IA pode correlacionar dados de *logs*, alertas e outras fontes para construir uma visão abrangente de um possível incidente.
   d) Automatização de Respostas: Utilizando IA, o XDR deverá automatizar respostas a incidentes, aplicando *playbooks* predefinidos com base na análise de ameaças. Isso inclui isolamento

automático de dispositivos comprometidos, bloqueio de tráfego malicioso e execução de scripts de remediação.

e) Aprendizagem Contínua: Algoritmos de *machine learning* devem ser treinados continuamente com novos dados e incidentes para melhorar a precisão da deteção e reduzir falsos positivos. A IA deve adapta-se a novas ameaças e técnicas de ataque, aprimorando sua eficácia ao longo do tempo.

2. Usar algoritmos pré-programados para a deteção de comportamentos anómalos na rede.
3. Utilizar *Machine Learning* para análise de ficheiros APK (*Android Application Pack*).
4. Fornecer alertas com base em anomalias observadas e mudanças comportamentais nos *endpoints* e demais fontes de alerta.
5. Permitir definir padrões de comportamento normal nos dispositivos sob análise e permitir a criação de alertas, em tempo real, caso essas políticas não sejam cumpridas.
6. Suportar a análise de objetos comprimidos em múltiplos níveis.
7. Prevenir contra *exploits*, incluindo vulnerabilidades do tipo *Zero-Day*, com atualização da base de dados de inteligência de ameaças em tempo real.
8. Prevenir contra a execução de *malware*, sem requerer qualquer conhecimento prévio.
9. Conseguir prevenir de forma efetiva *exploits* e *malware*, mesmo quando não existe conectividade ou atualizações do servidor de gestão e/ou acesso a recursos da nuvem.
10. Ter capacidade de detetar e reportar ameaças de segurança nos *endpoints* ligados à rede da SPMS (incluindo com equipamentos externos à SPMS, permitindo uma Política de BYOD).
11. Permitir definir a complexidade e *aging* das passwords dos utilizadores, de forma a cumprir com as Políticas de Segurança da organização.
12. Suportar todos os sistemas operativos em uso na SPMS.
13. Proteger contra *ransomware*.
14. Deter capacidade de restringir a execução de determinados ficheiros.
15. Controlar dispositivos USB.
16. Permitir a gestão e proteção de dispositivos móveis.
17. Permitir a gestão de *Disk Encryption* via *BitLocker*.
18. Disponibilizar *Host Firewall*.
19. Definir regras de correlação de eventos em linguagem semelhante à natural.
20. Utilizar regras YARA personalizáveis, garantindo que as estas poderão ser atualizadas automaticamente a partir de fontes confiáveis de *Threat Intelligence*.
21. Permitir a análise automática de objetos suspeitos na *Sandbox*.

22. Permitir deteção e bloqueio de ações em serviços na nuvem.
23. Ser capaz de processar e analisar anexos em mensagens de e-mail, incluindo ficheiros documentos do Office e protegidos por senha.
24. Detetar tráfego de rede potencialmente malicioso, como consultas DNS para *Botnet* C2 e outras comunicações.
25. Permitir criar regras de deteção de rede pelos administradores da solução no formato *Snort* ou *Suricata*.
26. Disponibilizar funcionalidades aos administradores da solução para colocar regras de deteção de rede em *whitelist*, se necessário.
27. Permitir descarregar uma cópia do tráfego de rede que causou a deteção no formato PCAP (*Packet Capture*).
28. Ser capaz de gravar tráfego de rede bruto para investigação posterior.
29. Ser capaz de operar em modo de monitorização (fora de banda), sem interferir na comunicação de entrada/saída e sem interromper os processos de negócios.
30. Ser capaz de reexaminar inteligentemente eventos e objetos passados usando a inteligência mais recente adquirida para descobrir possíveis ameaças anteriores.
31. Contemplar um subsistema de análise automática de *malware* da solução que, por sua vez, deve:
    a) usar múltiplos sistemas operacionais virtuais de cliente das arquiteturas x64 e x86. A lista deve conter pelo menos o seguinte: Windows 10, Windows 7 64 bits, Windows XP 32 bits, CentOS 7.8.
    b) fornecer a capacidade de preparar e usar imagens de VM personalizadas para análise dinâmica de malware.
    c) permitir definir regras de *scanning* que condicionem quais objetos a scanear ou não scanear em uma VM específica.
    d) fornecer visualização para o analista que inclua, pelo menos, uma representação gráfica da árvore de processos, dados sobre tráfego web e comunicação DNS.
    e) ser capaz de trabalhar com vários centros de análise simultaneamente.
    f) ter a opção de usar uma conexão dedicada à Internet para permitir a análise das comunicações de saída e download de módulos extras.
    g) ser capaz de simular ações do utilizador final para forçar a execução de *malware* que dependem de ações do utilizador final.
    h) ser capaz de se ocultar de *malwares* que tentam evadir a *sandbox* durante a análise dos objetos.
    i) ser capaz de processar objetos submetidos manualmente via interface de gestão da solução.

6. Requisitos de resposta da plataforma XDR

A solução deve:

1. Permitir isolar automaticamente da rede máquinas infetadas com *malware*, porém garantindo que o administrador do sistema, possa aceder remotamente ao equipamento.
2. Permitir ações de resposta manual. São exemplos de comandos, sem se limitar aos mesmos:
   - PowerShell: Get-Process, Stop-Process, Get-Service, Restart-Service, Get-EventLog, Set-ExecutionPolicy
   - Bash: ps aux, kill -9 <PID>, systemctl restart <service>, netstat -tuln, tail -f /var/log/syslog
   - Firewall Rules: iptables -A INPUT -s <malicious_ip> -j DROP, firewalld-cmd --zone=public --add-port=80/tcp
   - Antivirus Commands: mpcmdrun.exe -Scan -ScanType 3, clamscan -r /home
3. Ter capacidade de reverter automaticamente alterações feitas na máquina por determinado *malware*.
4. Fornecer orientações acionáveis sobre como responder de maneira relevante a alertas registados.
5. Contemplar manuais predefinidos e criados pelo utilizador para automatizar operações de resposta.
6. Permitir ações de resposta de produtos de terceiros e cenários de resposta entre produtos.
7. Poder enriquecer os seus *playbooks* e informações com *Threat Intelligence*.
8. Ter capacidade de terminar processos remotamente, mover dispositivos para grupos de gestão distintos, executar análises de *malware*, e mover dispositivos para quarentena.
9. Ter capacidade de bloquear contas no *Active Directory*, adicionar ou remover utilizadores de grupos de segurança.
10. Implementar medidas corretivas e preventivas em *EndPoints* comprometidos.
11. Permitir a execução de um *Playbook* em modo manual e automático. São considerados como principais critérios para a execução de *playbooks* automáticos:
    - Classificação e Severidade do Incidente:
      - Nível de Severidade: Incidentes classificados como críticos ou de alta severidade devem acionar *playbooks* automáticos para mitigar rapidamente as ameaças.
      - Tipo de Ameaça: *Playbooks* automáticos podem ser desencadeados por tipos específicos de ameaças, como *ransomware*, *malware* conhecido, ou atividades suspeitas de exfiltração de dados.
    - Confiabilidade dos Alertas:
      - Precisão do Alerta: Apenas alertas com alta confiança e baixa taxa de falsos positivos devem acionar *playbooks* automáticos.

- Correlações de Eventos: Alertas que resultam da correlação de múltiplos eventos e fontes de dados confiáveis devem ter maior probabilidade de desencadear ações automáticas.

- Contexto do Ativo:
  - Importância do Ativo: Ativos críticos, como servidores de produção ou bancos de dados, podem ter *playbooks* automáticos configurados para respostas rápidas.
  - Localização do Ativo: Considerar a localização física ou lógica do ativo (e.g., dentro da rede corporativa ou em um ambiente de nuvem).
- Histórico de Ameaças:
  - Reputação da Origem: Se a origem do ataque é conhecida por ser maliciosa com base em histórico de ameaças.
  - Padrões de Comportamento: Atividades que correspondem a padrões de comportamento maliciosos previamente identificados.
- Políticas de Segurança:
  - Políticas Corporativas: Adesão a políticas de segurança corporativa que especificam quando e como os *playbooks* automáticos devem ser acionados.
  - Regulamentações e Conformidade: Considerar requisitos de conformidade regulamentar que exigem respostas automáticas para determinados tipos de incidentes.
- Disponibilidade de Ações de Remediação:
  - Capacidade de Remediação: Ações que podem ser realizadas de forma segura e eficaz sem intervenção manual.
  - Automatização Completa: *Playbooks* que incluem todas as etapas necessárias para resolver um incidente sem necessidade de validação adicional.

7. Requisitos de gestão de ativos da plataforma XDR

A solução deve:

1. Implementar agentes nos ativos da SPMS.
2. Permitir a realização remota de tarefas de *scanning* e atualização.
3. Identificar automaticamente ativos e máquinas na rede.
4. Deter mecanismo para descobrir e classificar ativos por tipo de dispositivo.
5. Manter uma base de dados dos ativos existentes de forma automática e dinâmica.

6. Ter uma classificação automática dos ativos baseada no tráfego de rede e no comportamento de utilizadores.
7. Ter capacidade de inventário de software instalado, vulnerabilidades detetadas tanto de sistema operativo como de aplicações de terceiros fabricantes.
8. Obter informações detalhadas sobre a rede, *software e hardware*. Devem ser consideradas as seguintes informações (sem se limitar aos mesmos):
    - Topologia da Rede (Mapeamento e Segmentação);
    - Lista de dispositivos na rede e suas respetivas configurações (incluindo listas de controle de acesso- ACL's, tradução de endereços de Rede -NAT, e políticas de qualidade de serviço – QoS);
    - Monitorização de tráfego de rede, incluindo *logs* e análise de protocolos;
    - Segurança de Rede, incluindo: Regras de firewall, assinaturas de deteção, alertas e *logs* de intrusões detetadas/prevenidas e configurações de VPN (tipos de criptografia utilizados, e políticas de acesso remoto).
9. Configurar todos os componentes de segurança da solução.
10. Gerir os ativos de forma centralizada a partir de uma interface gráfica web.
11. Permitir inserir informações sobre redes IP, máquinas, servidores, e serviços para análises geográficas e de serviços.

8. Requisitos de *reporting* e relatórios da plataforma XDR

A solução deve:

1. Ter a capacidade de produzir relatórios situacionais e *dashboards*.
2. Ter a capacidade de produzir relatórios com dados de histórico.
3. Contemplar gráficos de investigação para visualizar e facilitar a investigação de um incidente e identificar as causas fundamentais do alerta.
4. Permitir ter alertas e eventos associados às técnicas da Matriz MITRE ATT&CK (*Adversary Tactics, Techniques and Common Knowledge*), incluindo a necessidade de correlação automática de alertas com indicadores de comprometimento (IOCs) e indicadores de ataque (IOAs);
5. Permitir agrupar alertas por incidentes.
6. Disponibilizar *dashboards* que permitem monitorizar as tendências de segurança no ecossistema da SPMS.
7. Contemplar relatórios pré-definidos e permitir a extração de relatórios em formatos PDF, DOC, CSV e HTML.
8. Ter a capacidade de elaborar relatórios de alto nível e relatórios técnicos com maior granularidade.

9. Ter a capacidade de criar relatórios imediatos, diários, semanais e mensais:
   a) Relatórios de Incidentes de Segurança Imediatos: Relatórios gerados automaticamente e enviados para a equipe de segurança ou partes interessadas logo após a Deteção de um incidente crítico. Este é o padrão para eventos graves que requerem ação urgente.
   b) Relatórios Diários: Relatórios diários que resumem todos os incidentes detetados, incluindo tentativas de intrusão, deteções de *malware*, e eventos anômalos.
   c) Relatórios Semanais: Relatórios que analisam tendências de segurança ao longo da semana, identificando padrões e possíveis ameaças emergentes. Além disso, devem detalhar vulnerabilidades descobertas, estados de remediação e novas ameaças.
   d) Relatórios Mensais: Relatórios mensais abrangentes que fornecem uma visão geral de todas as atividades de segurança, incluindo métricas de desempenho e eficácia das estratégias de mitigação. Além disso, devem detalhar um *status* de conformidade com políticas de segurança e *patches* aplicados.
10. Para cada ameaça gerar um relatório automaticamente com o respetivo sumário.
11. Ter a capacidade de *reporting* em formatos *standard* e permitir a inclusão de formatos pré-definidos com base na informação pretendida.
12. Permitir categorizar e incluir de forma personalizada informações nos relatórios, como alarmes, incidentes, estatísticas de rede e de eventos, informações sobre sistemas/equipamentos, atividades por endereço IP e/ou utilizador, e conformidade.
13. A solução deve ter capacidade de reporte de conformidade ao nível das normas ISO2700X e normativos legais RGPD e RJSC.

    A solução deve permitir a configuração do envio dos relatórios por e-mail e o download dos mesmos.

9. Outros requisitos

1. As licenças adquiridas devem ser perpétuas, com a opção de renovação de manutenção após três anos.
2. Deverá ter como capacidade e cobertura:
   a) **Hosts de Virtualização (300 unidades):**
      i. Compatibilidade com plataformas de virtualização como VMware ESXi, Microsoft Hyper-V, Citrix XenServer.
      ii. Proteção em tempo real contra ameaças e vulnerabilidades.
   b) 2.2. **Servidores Virtuais (3500 unidades):**
      i. Proteção contínua e em tempo real.

ii. Suporte para sistemas operativos Windows Server, Linux (todas as principais distribuições).

iii. Capacidade de isolamento de incidentes para minimizar impacto.

c) **Postos de Trabalho Tradicionais (1800 unidades):**

i. Suporte para sistemas operativos Windows, macOS e Linux.

ii. Funcionalidades EDR (Endpoint Detection and Response) com capacidade de deteção e resposta automática a ameaças.

iii. Monitorização contínua e análise de comportamento.

d) **Dispositivos Móveis (1800 Android e iOS):**

i. Suporte para gestão de dispositivos móveis (MDM) e proteção contra ameaças móveis.

ii. Funcionalidades de deteção de malware, verificação de segurança de aplicações, e proteção de rede.

iii. Capacidade de localização e controlo remoto em caso de perda ou roubo.

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 considerar uma análise inicial do ecossistema da SPMS, de forma a facilitar os processos de integração e configuração inicial e reduzir o tempo de implementação, assim como a complexidade técnica associada;
3. Os serviços de implementação devem incluir, no mínimo, as seguintes atividades macro:
   a) Atividades de definição de âmbito e pré-requisitos
   b) Instalação e configuração necessária ao funcionamento da solução proposta:
      i. Identificação e integração de várias fontes de dados;
      ii. Definição e configuração de políticas de segurança (regras) e as metodologias usadas para a sua definição;
      iii. Configuração de casos de uso, através da adaptação de casos de uso já fornecidos pelo fabricante (*out-of-the-box*);

iv. Definição e configuração de novos casos de uso associados ao ecossistema da SPMS através de parsers personalizados (pelo menos 10 tipos) para fontes de dados não suportadas pela solução *out-of-the-box*;

v. Definição e configuração de *dashboards*, relatórios e alertas (em diversas plataformas);

vi. Relatórios de gestão, relatórios administrativos e de manutenção da plataforma;

vii. 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".

4. 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.

5. A formação do ponto 3-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 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 XDR 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.

Tendo em conta a prossecução destes princípios, a informação da consulta preliminar é publicitada no portal Internet público da SPMS, da qual faz parte integrante o presente documento, em: http://www.spms.min-saude.pt e no respetivo LinkedIn.

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 16 de agosto de 2024, devendo os interessados indicar claramente no assunto do email a referência **"Consulta Preliminar n.º 14/2024 - Implementação de Solução XDR".**

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 XDR pretendida;
   b) O custo para os serviços de implementação e suporte;
   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) 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 **16/08/2024.**