

PROGRAMA DO PROCEDIMENTO

CONCURSO PÚBLICO SEM PUBLICAÇÃO DE ANÚNCIO NO JOUE Nº NCP20220081

**AQUISIÇÃO DE FIREWALL INTERNA E PLATAFORMA PARA SEGURANÇA
INFORMÁTICA**

ÍNDICE

SECÇÃO I- DISPOSIÇÕES GERAIS

- Cláusula 1.^a Identificação do concurso
- Cláusula 2.^a Entidade pública contratante
- Cláusula 3.^a Órgão que tomou a decisão de contratar
- Cláusula 4.^a Concorrentes
- Cláusula 5.^a Agrupamentos
- Cláusula 6.^a Critério de adjudicação
- Cláusula 7.^a Preço base

SECÇÃO II PROPOSTAS

- Cláusula 8.^a Apresentação das propostas
- Cláusula 9.^a Fornecimento das peças do procedimento
- Cláusula 10.^a Esclarecimentos
- Cláusula 11.^a Proposta
- Cláusula 12.^a Propostas variantes
- Cláusula 13.^a Prazo de manutenção das propostas

SECÇÃO III ANÁLISE DAS PROPOSTAS

- Cláusula 14.^a Análise das propostas
- Cláusula 15.^a Esclarecimentos sobre as propostas

SECÇÃO IV ADJUDICAÇÃO

- Cláusula 16.^a Notificação da decisão de adjudicação
- Cláusula 17.^a Documentos de habilitação
- Cláusula 18.^a Causas de não adjudicação

SECÇÃO V CAUÇÃO

- Cláusula 19.^a Caução

SECÇÃO VI CONTRATO

- Cláusula 20.^a Aceitação da minuta do contrato
- Cláusula 21.^a Notificação de ajustamento ao contrato
- Cláusula 22.^a Outorga do contrato

SECÇÃO VII DISPOSIÇÕES FINAIS

Cláusula 23.^a Prazos

Cláusula 24.^a Encargos

Cláusula 25.^a Legislação aplicável

SECÇÃO I

DISPOSIÇÕES GERAIS

Cláusula 1.^a

Identificação do concurso

O presente Concurso Público sem publicação no Jornal Oficial da União Europeia, aberto ao abrigo do disposto na alínea b), do n.º 1 do artigo 20.º do Código dos Contratos Públicos, visa a **aquisição de firewall interna e plataforma para segurança informática**, nos termos descritos na memória descritiva, em anexo ao presente programa do procedimento e do qual faz parte integrante, nos termos e condições estipuladas no caderno de encargos.

Cláusula 2.^a

Entidade pública contratante

A entidade pública contratante é o Serviço de Saúde da Região Autónoma da Madeira, EPERAM (SESARAM, EPERAM), com sede à Av. Luís de Camões, n.º 57, Edifício do Núcleo de Apoio ao Hospital Dr. Nélcio Mendonça, freguesia de São Pedro, 9004-514 Funchal, com o telefone 291 705 610, o fax 291 742 545, o endereço eletrónico www.sesaram.pt/aprovisionamento e o correio eletrónico aprovisionamento@sesaram.pt relativo ao Núcleo de Aprovisionamento, responsável pelo presente procedimento.

Cláusula 3.^a

Órgão que tomou a decisão de contratar

A decisão de contratar foi tomada por deliberação de 21 de outubro de 2022 do Conselho de Administração do Serviço de Saúde da Região Autónoma da Madeira, EPERAM, nomeado pelas Resoluções do Conselho de Governo n.º 848/2019, de 14 de novembro, n.º 567/2020, de 30 de julho e n.º 921/2022, de 29 de setembro, no uso das suas competências atribuídas por força dos Estatutos do SESARAM, EPERAM, aprovados pelo Decreto Legislativo Regional n.º 13/2019/M, de 22 de agosto, alterados pelo Decreto Legislativo Regional n.º 1-A/2020/M, de 31 de janeiro, na sua redação atual e pelo Decreto Legislativo Regional n.º 8/2020/M, de 13 de julho, mediante autorização prévia do Exmo. Sr. Secretário Regional das Finanças e parecer prévio da Direção Regional de Informática datados, respetivamente, de 19 e 18 de outubro de 2022, em conformidade com o disposto na alínea a) do n.º 1 do artigo 20.º do Decreto Regulamentar Regional n.º 12/2022/M, de 29 de agosto.

Cláusula 4.^a

Concorrentes

Podem apresentar propostas as entidades que não se encontrem em nenhuma das situações previstas no artigo 55.º do Código dos Contratos Públicos, e que, quando legalmente exigido, cumpram as obrigações fiscais declarativas referidas no nº 2 do artigo 7º do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na sua redação atual.

Cláusula 5.^a

Agrupamentos

1. Podem ser concorrentes, agrupamentos de pessoas singulares ou coletivas, sem que entre as mesmas exista qualquer modalidade jurídica de associação.
2. Os membros de um agrupamento concorrente não podem ser concorrentes no mesmo procedimento, nem integrar outro agrupamento concorrente.
3. Todos os membros de um agrupamento concorrente são solidariamente responsáveis, perante a entidade adjudicante, pela manutenção da proposta.
4. Em caso de adjudicação, todos os membros do agrupamento concorrente, e apenas estes, devem associar-se, antes da celebração do contrato, na modalidade jurídica de consórcio externo.

Cláusula 6.^a

Critério de adjudicação

1. O critério de adjudicação é o da proposta economicamente mais vantajosa, na modalidade multifator, composto pelos seguintes fatores:

Fator 1 - Preço – 80%, avaliado da seguinte forma:

$$\frac{P_B - P_A}{P_B} \times 80\%$$

Em que:

P_B – preço base

P_A – preço em análise

Fator 2 – Prazo de garantia – 20%, avaliado da seguinte forma:

$$\frac{P_{G.P.} - P_{G.Min.}}{P_{G.Min.}} \times 20\%$$

Sendo que:

$P_{G.P.}$ – Prazo de Garantia proposto

$P_{G.Min.}$ – Prazo de Garantia Mínimo

Nota: Prazo mínimo de garantia admissível, sob pena de exclusão da proposta, é de 3 anos.

O valor máximo será: 100%

2. A classificação final de cada proposta será obtida através do somatório das pontuações parciais de cada um dos fatores de ponderação que integram o critério de adjudicação, da seguinte forma:

Soma do Fator 1x80% + Fator 2x20%

3. Em caso de empate dar-se-á preferência à proposta que, pela seguinte ordem, apresente maior pontuação no fator 1 e no fator 2.

4. Se, ainda assim, subsistir a igualdade, proceder-se-á ao desempate através da realização de sorteio a decorrer nos seguintes termos:

- a) O sorteio será presencial e realizar-se-á na presença de um ou mais elementos do Júri, após o termo do prazo de audiência prévia ao relatório preliminar, no Núcleo de Aprovisionamento do Serviço de Saúde da Região Autónoma da Madeira, EPERAM (SESARAM, EPERAM), em dia e hora a comunicar aos concorrentes;
- b) Os concorrentes que queiram comparecer ao sorteio devem fazer-se acompanhar da respetiva credencial que lhes confira os necessários poderes de representação, sob pena de se considerarem como ausentes.
- c) Será utilizado o sistema de “bolas”, sendo a ordenação a seguinte:
 - A bola branca corresponde ao primeiro lugar
 - A bola preta corresponde ao segundo lugar
 - A bola vermelha corresponde ao terceiro lugar
 - A bola verde corresponde ao quarto lugar.
- d) A seriação dos concorrentes para efeitos de retirar a bola será determinada pela maior pontuação obtida através de um lance de dados.
- e) O(s) concorrente(s) que não possam comparecer ao sorteio podem solicitar a sua representação por uma testemunha a designar pelo Coordenador do Núcleo de Aprovisionamento, devendo, para o efeito, remeter ao Núcleo de Aprovisionamento uma declaração nesse sentido, até às 17h00 da véspera do dia do sorteio.
- f) Os concorrentes que não compareçam nem queiram fazer-se representar nos termos da alínea precedente, ficarão posicionados nos seguintes termos:

- Tratando-se de empate entre duas propostas, em que compareça apenas um dos concorrentes, este ficará imediatamente posicionado em primeiro lugar, ficando o concorrente que não compareceu posicionado em segundo lugar;
- Tratando-se de empate entre três ou mais propostas, em que compareçam apenas alguns dos concorrentes, estes ficarão posicionados nos lugares que resultarem do sorteio a realizar de acordo com o estipulado nas alíneas b) e c) supra, sendo os concorrentes ausentes representados por testemunha(s) a designar pelo Coordenador do Núcleo de Aprovisionamento;
- Caso não compareçam quaisquer concorrentes, os mesmos ficarão posicionados nos lugares que resultarem do sorteio a decorrer de acordo com o estipulado nas alíneas c) e d) supra, a realizar por testemunha (s) a designar pelo Coordenador do Núcleo de Aprovisionamento.

g) Deste ato será lavrada ata que será assinada por todos os presentes.

Cláusula 7.^a

Preço base

1. O preço base é de **EUR 175.000,00 (cento e setenta e cinco mil euros)**, acrescido de IVA à taxa legal em vigor.
2. O preço base fixado no ponto precedente resultou dos preços obtidos em resultado da consulta preliminar ao mercado realizada nos termos previstos no artigo 35.º-A do CCP. A informação pertinente poderá ser disponibilizada aos futuros concorrentes, caso seja solicitada, em conformidade com a Orientação Técnica do IMPIC n.º 04/CCP/2019.

SECÇÃO II PROPOSTAS

Cláusula 8.^a

Apresentação das propostas

1. As propostas devem ser apresentadas até às **17H00 do 9.º dia a contar da data do envio do anúncio para o Diário da República**, na plataforma eletrónica usada pelo Serviço de Saúde da Região Autónoma da Madeira, EPERAM, www.acinGov.pt, devendo ser respeitado o disposto no Código dos Contratos Públicos e na Lei nº 96/2015, de 17 de agosto.

O computador utilizado pelos concorrentes deverá estar preparado com os requisitos mínimos disponíveis na plataforma eletrónica usada pelo Serviço de Saúde da Região Autónoma da Madeira, EPERAM, www.acinGov.pt, sob pena de exclusão da proposta por não observação das formalidades de apresentação das mesmas, nos termos do disposto na alínea I) do n.º 2 do artigo 146º do CCP.

2. Quando, pela sua natureza, qualquer documento dos que constituem a proposta não possa ser apresentado nos termos do disposto no n.º 1, deve ser encerrado em invólucro opaco e fechado:

- a) No rosto do qual se deve indicar a designação do procedimento e da entidade adjudicante;
- b) Que deve ser entregue diretamente ou enviado por correio registado à entidade adjudicante, devendo, em qualquer caso, a respetiva receção ocorrer dentro do prazo fixado para a apresentação das propostas;
- c) Cujas receções deve ser registada por referência à respetiva data e hora.

3. A proposta e os documentos/ficheiros que lhes associarem devem ser assinados eletronicamente mediante a utilização de certificados de assinatura eletrónica qualificada, previamente ao seu carregamento na plataforma, nos termos dos artigos 54.º e 68º da Lei n.º 96/2015, de 17 de agosto conjugado com o n.º 2 do artigo 3.º do Decreto Lei n.º 12/2021, de 9 de fevereiro.

ATENÇÃO: Os documentos que integram as pastas compactadas, têm de ser individualmente assinados, nos moldes atrás referidos.

Cláusula 9.ª

Fornecimento das peças do procedimento

O programa do procedimento, o caderno de encargos e as informações sobre o presente concurso estão disponíveis na plataforma eletrónica indicada na cláusula anterior, para consulta dos interessados, desde o dia da publicação do anúncio no Diário da República, até ao termo do prazo fixado para a apresentação das propostas.

Cláusula 10.ª

Esclarecimentos e erros e omissões das peças

1. Os esclarecimentos necessários à boa compreensão e interpretação das peças do concurso são da competência do júri do concurso.

2. Os interessados podem solicitar esclarecimentos relativos à boa compreensão e interpretação dos elementos expostos durante o primeiro terço do prazo fixado na cláusula 8ª do presente programa do procedimento.
3. Os pedidos de esclarecimentos devem ser solicitados por escrito ao júri do concurso na plataforma eletrónica www.acinGov.pt, utilizada pelo Serviço de Saúde da Região Autónoma da Madeira, EPERAM.
4. Os esclarecimentos devem ser prestados pelo júri, por escrito na plataforma eletrónica www.acinGov.pt, até ao fim do segundo terço do prazo fixado na cláusula 8ª.
5. No prazo referido no número 2, os interessados devem apresentar uma lista na qual identifiquem, expressa e inequivocamente, os erros e as omissões das peças do procedimento por si detetados, nos termos do artigo 50.º do Código dos Contratos Públicos.
6. Os esclarecimentos prestados serão disponibilizados na plataforma eletrónica www.acinGov.pt, utilizada pelo Serviço de Saúde da Região Autónoma da Madeira, EPERAM.

Cláusula 11.^a

Proposta

1. Na proposta o concorrente manifesta à entidade adjudicante a sua vontade de contratar e o modo pelo qual se dispõe a fazê-lo.
2. O concorrente deve apresentar proposta para a totalidade dos artigos que constituem o único lote a concurso.
3. Na proposta, o concorrente deve ainda indicar os seguintes elementos:
 - a) Referência do concurso;
 - b) Nome do concorrente;
 - c) **Documento que comprove os poderes de representação de quem assina a proposta;**
 - d) Declaração do concorrente de aceitação do conteúdo do caderno de encargos, elaborada em conformidade com o modelo constante do anexo I-M ao presente programa de procedimento, do qual faz parte integrante;
 - e) Documentos que contenham os atributos da proposta, de acordo com os quais o concorrente se dispõe a contratar:

- i. Preço total em algarismos, e preferencialmente por extenso, mencionando que a este acresce o IVA, indicando o respetivo valor e a taxa legal aplicável, entendendo-se, na falta daquela menção, que o preço apresentado não inclui aquele imposto. **No preço indicado consideram-se, incluídos todos os serviços descritos na Memória Descritiva.**
- ii. Preço unitário, em algarismos, e preferencialmente por extenso, mencionando que a este acresce o IVA, indicando o respetivo valor e a taxa legal aplicável, entendendo-se, na falta daquela menção, que o preço apresentado não inclui aquele imposto;
- iii. Prazo de garantia.

4.O concorrente deve indicar/apresentar ainda:

- i. **Catálogos e/ou fichas técnicas (datasheets)**, onde constem as características técnicas dos artigos com que concorre, de modo a aferir o cumprimento dos requisitos e especificações exigidos (em português ou inglês).
- ii. De modo a comprovar o cumprimento dos requisitos técnicos exigidos, o concorrente deverá preencher na íntegra e apresentar os anexos I e II junto ao presente programa do procedimento, dele fazendo parte integrante, **sob pena de exclusão da proposta;**
- iii. O prazo de entrega, que não poderá ser superior a 90 (noventa) dias úteis, a contar da receção da nota de encomenda, sob pena de exclusão da proposta;
- iv. Plano de formação, de acordo com o exigido na memória descritiva;
- v. Declaração do fabricante fazendo prova que o mesmo tem conhecimento da proposta apresentada pelo concorrente, certificando que este possui as competências necessárias para implementação e suporte da solução.

5. Integram também a proposta quaisquer outros documentos que o concorrente considere relevantes para a apreciação da mesma.

6. À exceção dos catálogos e fichas técnicas, que podem ser apresentados em português, e/ou inglês, todos os documentos solicitados na presente cláusula devem ser redigidos em língua portuguesa, sem emendas ou rasuras, ou, não o sendo, devem ser acompanhados de tradução devidamente legalizada e em relação à qual o concorrente declara aceitar a sua prevalência, para todos os efeitos, sobre os respectivos originais.

Cláusula 12.^a

Propostas variantes

1. Não é permitida a apresentação de propostas com variantes.
2. Não é permitida a apresentação de propostas com alterações às cláusulas do caderno de encargos.

Cláusula 13.^a

Prazo de manutenção das propostas

O prazo obrigatório de manutenção das propostas é de 66 (sessenta e seis) dias, não prorrogáveis, contados da data do termo do prazo fixado para apresentação das mesmas.

SECÇÃO III

ANÁLISE DAS PROPOSTAS

Cláusula 14.^a

Análise das propostas

1. As propostas são analisadas considerando o critério de adjudicação.
2. As propostas serão excluídas nos termos do disposto no n.º 2 do artigo 146.º do Código dos Contratos Públicos.
3. É aplicável o disposto no n.º 6 do artigo 70.º do Código dos Contratos Públicos, na redacção que lhe foi dada pela Lei 30/2021, de 21 de maio.

Cláusula 15.^a

Esclarecimentos sobre as propostas

1. O júri do procedimento pode pedir aos concorrentes quaisquer esclarecimentos sobre as propostas apresentadas que considere necessários para efeito da análise e da avaliação das mesmas.
2. Os esclarecimentos prestados pelos respetivos concorrentes fazem parte integrante das mesmas, desde que não contrariem os elementos constantes dos documentos que as constituem, não alterem ou completem os respetivos atributos, nem visem suprir omissões que determinam a sua exclusão nos termos do disposto na alínea a) do n.º 2 do artigo 70.º do Código dos Contratos Públicos.
3. Os esclarecimentos referidos no número anterior serão disponibilizados em plataforma eletrónica www.acinGov.pt, sendo todos os concorrentes notificados desse facto.

SECÇÃO IV

ADJUDICAÇÃO

Cláusula 16^a

Notificação da decisão de adjudicação

1. A decisão de adjudicação será notificada, em simultâneo, a todos os concorrentes.
2. Juntamente com a notificação da decisão de adjudicação, o órgão competente para a decisão de contratar notificará o adjudicatário para:
 - a. Apresentar os documentos de habilitação exigidos nos termos do disposto na cláusula que se segue;
 - b. Pronunciar-se sobre a minuta do contrato, quando este for reduzido a escrito.
3. As notificações referidas nos números anteriores serão acompanhadas do relatório final de análise das propostas.

Cláusula 17. ^a

Documentos de habilitação

1. Ao adjudicatário ser-lhe-á exigida a apresentação, no prazo de 5 (cinco) dias contados da receção da notificação da decisão de adjudicação, da apresentação dos documentos a seguir mencionados, nos termos do artigo 83.º do Código dos Contratos Públicos:
 - a) Declaração emitida conforme modelo constante do anexo II M ao presente programa e do qual faz parte integrante;
 - b) Documentos comprovativos de que não se encontra nas situações previstas nas alíneas **b), d), e) e h)** do artigo 55.º do Código dos Contratos Públicos;
 - c) Documentos exigidos no n.º 2 do artigo 7.º do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na sua redação atual (**Apenas para entidades com rendimentos gerados no território da RAM**):
 - I. Última declaração de rendimentos modelo 3 ou modelo 22, este último acompanhado do Anexo C, caso o adjudicatário tenha exercido nesse período atividade na Região Autónoma da Madeira, bem como enquanto se mantiver em vigor o respetivo contrato;
 - II. Última declaração de rendimentos e retenções de residentes (modelo 10) e DMR;
 - III. Anexo Q da última informação empresarial simplificada (IES);
 - IV. Anexo R do IVA da última declaração periódica do IVA.

- d) **Os adjudicatários que considerem não preencher as condições legais relativas ao cumprimento das obrigações declarativas referidas na alínea precedente, devem apresentar declaração sob compromisso de honra (anexo III-modelo 3), subscrita por quem os obriga, referindo expressamente essa situação.**
- e) Cópia da Certidão do Registo Comercial e de procuração, caso o contrato seja assinado por procurador.
2. Caso os documentos apresentados ao abrigo do ponto anterior contenham irregularidades que possam determinar a caducidade da adjudicação nos termos do disposto no artigo 86º do Código dos Contratos Públicos, será concedido o prazo não superior a 3 (três) dias úteis para a supressão das mesmas.
3. Os documentos de habilitação devem ser redigidos em língua portuguesa e ser assinados pelas entidades que os emitem.
4. Quando, pela sua própria natureza ou origem, os documentos de habilitação estiverem redigidos em língua estrangeira, deve o adjudicatário fazê-los acompanhar de tradução devidamente legalizada.
5. Os documentos de habilitação devem ser apresentados através da plataforma eletrónica www.acinGov.pt, utilizada pelo Serviço de Saúde da Região Autónoma da Madeira, EPERAM.
6. O adjudicatário não tem de apresentar os documentos previstos na alínea b) do artigo 81.º do CPCP se estiver registado no Portal Nacional de Fornecedores do Estado.

Cláusula 18.ª

Causas de não adjudicação

1. Não há lugar a adjudicação nos termos do artigo 79.º do Código dos Contratos Públicos.
2. A decisão de não adjudicação, bem como os respetivos fundamentos, caso ocorra, será notificada a todos os concorrentes.

SECÇÃO V

CAUÇÃO

Cláusula 19.ª

Caução

No presente procedimento não haverá lugar a prestação de caução.

SECÇÃO VI

CONTRATO

Cláusula 20.ª

Aceitação da minuta do contrato

1. A minuta do contrato é enviada, para aceitação, ao adjudicatário.
2. A minuta considera-se aceite pelo adjudicatário quando haja aceitação expressa ou quando não haja reclamação nos 5 (cinco) dias subsequentes à respetiva notificação.
3. As reclamações da minuta do contrato a celebrar só podem ter por fundamento a previsão de obrigações que contrariem ou que não constem dos documentos que integram o contrato ou ainda a recusa dos ajustamentos propostos.

Cláusula 21.ª

Notificação de ajustamento ao contrato

Caso se procedam a ajustamentos ao contrato e estes sejam aceites pelo adjudicatário, todos os concorrentes cujas propostas não tenham sido excluídas serão notificados desse facto.

Cláusula 22.ª

Outorga do contrato

O órgão competente para a decisão de contratar comunicará ao adjudicatário, com a antecedência mínima de 5 (cinco) dias, a hora e o local em que ocorrerá a outorga do contrato.

SECÇÃO VII

DISPOSIÇÕES FINAIS

Cláusula 23.ª

Prazos

Todos os prazos indicados no presente programa cumprem o disposto no artigo 470.º do Código dos Contratos Públicos.

Cláusula 24.ª

Encargos

Constituem encargos do concorrente o pagamento de todas as despesas inerentes à elaboração da proposta no âmbito do presente concurso e do adjudicatário as relativas à celebração do contrato, designadamente a prestação de caução.

Cláusula 25.ª

Legislação aplicável

A tudo o que não esteja especialmente previsto no presente programa aplica-se o regime previsto no Código dos Contratos Públicos.

ANEXOS

ANEXO I/M

Modelo de declaração

[a que se refere a alínea a) do n.º 1 do artigo 57.º ou a subalínea i) da alínea b) e alínea c) do n.º 3 do artigo 256.º -A, conforme aplicável do Código dos Contratos Públicos e o artigo 6.º do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto.]

1 — ... (nome, número de documento de identificação e morada), na qualidade de representante legal de (1) ... (firma, número de identificação fiscal e sede ou, no caso de agrupamento concorrente, firmas, números de identificação fiscal e sedes), tendo tomado inteiro e perfeito conhecimento do caderno de encargos relativo à execução do contrato a celebrar na sequência do procedimento de ... (designação ou referência ao procedimento em causa), e, se for o caso, do caderno de encargos do acordo -quadro aplicável ao procedimento, declara, sob compromisso de honra, que a sua representada (2) se obriga a executar o referido contrato em conformidade com o conteúdo do mencionado caderno de encargos, relativamente ao qual declara aceitar, sem reservas, todas as suas cláusulas.

2 — Declara também que executará o referido contrato nos termos previstos nos seguintes documentos, que junta em anexo (3):

a)

b)

3 — Declara ainda que renuncia a foro especial e se submete, em tudo o que respeitar à execução do referido contrato, ao disposto na legislação portuguesa aplicável.

4 — Mais declara, sob compromisso de honra, que não se encontra em nenhuma das situações previstas no n.º 1 do artigo 55.º do Código dos Contratos Públicos e artigo 5.º do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na sua atual redação.

5 — O declarante tem pleno conhecimento de que a prestação de falsas declarações implica, consoante o caso, a exclusão da proposta apresentada ou a caducidade da adjudicação que eventualmente sobre ela recaia e constitui contraordenação muito grave, nos termos do artigo 456.º do Código dos Contratos Públicos, a qual pode determinar a aplicação da sanção acessória de privação do direito de participar, como candidato, como concorrente ou como membro de agrupamento candidato ou concorrente, em qualquer procedimento adotado para a formação de contratos públicos, sem prejuízo da participação à entidade competente para efeitos de procedimento criminal.

6 — Quando a entidade adjudicante o solicitar, o concorrente obriga -se, nos termos do disposto no artigo 81.º do Código dos Contratos Públicos, a apresentar a declaração que

constitui o anexo II -M do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na sua atual redação, bem como os documentos comprovativos de que se encontra nas situações previstas nas alíneas *b)*, *d)*, *e)* e *h)* do n.º 1 do artigo 55.º do referido Código e artigo 5.º do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto, na sua atual redação.

7 — O declarante tem ainda pleno conhecimento de que a não apresentação dos documentos solicitados nos termos do número anterior, por motivo que lhe seja imputável, determina a caducidade da adjudicação que eventualmente recaia sobre a proposta apresentada e constitui contraordenação muito grave, nos termos do artigo 456.º do Código dos Contratos Públicos, a qual pode determinar a aplicação da sanção acessória de privação do direito de participar, como candidato, como concorrente ou como membro de agrupamento candidato ou concorrente, em qualquer procedimento adotado para a formação de contratos públicos, sem prejuízo da participação à entidade competente para efeitos de procedimento criminal.

... (local), ... (data), ... [assinatura (4)].

(1) Aplicável apenas a concorrentes que sejam pessoas coletivas.

(2) No caso de o concorrente ser uma pessoa singular, suprimir a expressão «a sua representada».

(3) Enumerar todos os documentos que constituem a proposta, para além desta declaração, nos termos do disposto nas alíneas *b)*, *c)* e *d)* do n.º 1 e nos n.os 2 e 3 do artigo 57.º

(4) Nos termos do disposto nos n.os 4 e 5 do artigo 57.º

ANEXO II - M

Modelo de declaração

[a que se refere a alínea a) do n.º 1 do artigo 81.º do Código dos Contratos Públicos e o n.º 1 do artigo 7.º do Decreto Legislativo Regional n.º 34/2008/M, de 14 de agosto]

1 — ... (nome, número de documento de identificação e morada), na qualidade de representante legal de (1) ... (firma, número de identificação fiscal e sede ou, no caso de agrupamento concorrente, firmas, números de identificação fiscal e sedes), adjudicatário(a) no procedimento de ... (designação ou referência ao procedimento em causa), declara, sob compromisso de honra, que a sua representada (2) não se encontra em nenhuma das situações previstas no n.º 1 do artigo 55.º do Código dos Contratos Públicos.

2 — O declarante junta em anexo [ou indica... como endereço do sítio da Internet onde podem ser consultados (3)] os documentos comprovativos de que a sua representada (4) não se encontra nas situações previstas nas alíneas b), d), e) e h) do artigo 55.º do Código dos Contratos Públicos e (quando aplicável) os documentos comprovativos de que cumpriu as obrigações fiscais declarativas cujo conteúdo assume interesse específico para a Região Autónoma da Madeira referidos no n.º 2 do artigo 7.º do Decreto Legislativo Regional n.º 34/2008/M.

3 — O declarante tem pleno conhecimento de que a prestação de falsas declarações implica a caducidade da adjudicação e constitui contraordenação muito grave, nos termos do artigo 456.º do Código dos Contratos Públicos, a qual pode determinar a aplicação da sanção acessória de privação do direito de participar, como candidato, como concorrente ou como membro de agrupamento candidato ou concorrente, em qualquer procedimento adotado para a formação de contratos públicos, sem prejuízo da participação à entidade competente para efeitos de procedimento criminal.

... (local), ... (data), ... [assinatura (5)].

(1) Aplicável apenas a concorrentes que sejam pessoas coletivas.

(2) No caso de o concorrente ser uma pessoa singular, suprimir a expressão «a sua representada».

(3) Acrescentar as informações necessárias à consulta, se for o caso.

(4) No caso de o concorrente ser uma pessoa singular, suprimir a expressão «a sua representada».

(5) Nos termos do disposto nos n.os 4 e 5 do artigo 57.º

ANEXO III

Modelo 3

“xxx, titular do CC n.º xxx, com morada xxx, na qualidade de gerente/representante da xxxxx com sede em xxx, capital social xxx, NIF xxx, matriculada na conservatória do registo comercial de xxx, declara que o adjudicatário do Concurso N.º NCPxxxxxx, não preenche os pressupostos de incidência, previstos nos artigos 23º, 25º e 26º da Lei de Finanças das Regiões Autónomas, aprovada pela Lei Orgânica nº 2/2013, de 2 de Setembro.

Data

assinatura

MEMÓRIA DESCRITIVA

Serve a presente Memória Descritiva para instalação de uma plataforma de segurança informática com a aquisição de duas firewalls internas redundantes e uma solução de proteção de dispositivos, para controlo e segurança do tráfego interno gerado pelas várias redes do Hospital Dr. Nélio Mendonça do SESARAM, EPERAM.

A solução a fornecer deverá ter os seguintes componentes integrados numa solução única do mesmo fabricante:

1. Firewalls internas:

Duas firewalls (Next Generation Firewall) com as seguintes características:

Hardware (obrigatório dentro do mesmo equipamento):

- Número de portas 1G/2.5G/5G/10Gbit/s RJ45 ≥ 12
- Número de portas Gigabit SFP+ 10Gbit/s ≥ 10
- Número de portas Gigabit SFP28 25Gbit/s ≥ 4
- Número de portas Gigabit QSFP/QSFP28 40G/100Gbit/s ≥ 2
- Porta de gestão dedicada "Out of Band"
- Número de portas de alta disponibilidade 1Gbit/s ≥ 2
- Número de portas de alta disponibilidade 10 Gbit/s SFP+ ≥ 1
- Porta USB
- Disco rígido SSD $\geq 480GB$
- Arquitetura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção
- Deverá estar garantido que a appliance de Firewall quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afete de forma alguma a performance dos serviços de gestão e vice-versa
- Fontes de alimentação redundantes.

Performance:

- Performance da appliance com a funcionalidade de firewall com identificação e controlo de aplicações (inspeção L7 de todo o tráfego - valores de produção) $\geq 20,5$ Gbps
- Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware (valores de produção) $\geq 10,5$ Gbps
- Performance da appliance com a funcionalidade de VPN IPSec $\geq 12,2$ Gbps
- Número de novas sessões por segundo $\geq 240\,000$
- Número máximo de sessões $\geq 2\,500\,000$

Gestão:

- Gestão e administração da própria appliance através de interface web, linha de comandos e API XML
- Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio
- Deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy
- Possibilidade de editar configurações pendentes que ainda não foram aplicadas
- Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas
- Possibilidade de descartar alterações à configuração realizadas
- Possibilidade de armazenar diferentes versões da configuração
- Capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda a infraestrutura instalada

- Deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos.
- Deve existir um ponto centralizado para efetuar upgrades e atualizações de versões e assinaturas
- Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão
- Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas
- Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds públicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud.
- Análise da utilização das regras para reduzir a superfície de exposição e melhorar postura de segurança.
- Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento
- Possibilidade de envio seletivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça
- Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade

Networking:

- As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3
- Suporte de IEEE 802.1Q
- Suporte de IEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo
- Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP
- Suporte de routing estático
- Suporte de DHCP, NAT e PAT
- Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas
- Capacidade de realizar policy based routing através do IP ou rede de origem
- Capacidade de realizar policy based routing através do utilizador ou grupo
- Capacidade de realizar policy based routing através do tipo de aplicação
- Suporte de arquiteturas de alta disponibilidade do tipo ativo/passivo e ativo/ativo
- Permitir a criação de clusters de alta disponibilidade até 6 membros
- Suporte para TLS 1.3 e capacidade de descriptar este tráfego

Identificação de Utilizadores:

- Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP
- Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory
- Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores
- Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores
- Possibilidade de gerir utilizadores através de API XML
- Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local
- Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing

Funcionalidades Gerais de Segurança:

- Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança
- Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança
- Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino
- Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas
- Capacidade de identificação de subfunções dentro de uma aplicação
- Capacidade de aplicar e/ou excecionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7
- Possibilidade de agrupar aplicações por categorias de forma que as políticas de segurança sejam aplicadas por categorias de aplicações
- Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP
- Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP
- Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL
- Capacidade de decifrar tráfego SSH e detetar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling)
- Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego
- Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança
- Capacidade de forçar o uso de MFA para acesso a aplicações internas.
- Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes

IDS/IPS:

- Capacidade de aplicar políticas de prevenção ou de deteção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1ms para não penalizar a experiência do utilizador, efetuando a análise numa única passagem do tráfego para todas as ameaças
- Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas
- Possibilidade de escolher proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos
- As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma que a aplicação de perfis de proteção se possa realizar com base nestas categorias
- Deve ser possível identificar as proteções pela identificação CVE das vulnerabilidades
- Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da seleção de perfis
- Deve ser possível converter assinaturas snort e suricata para dentro da plataforma

Antivirus & Anti-Malware:

- Detetar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C
- Capacidade de habilitar mecanismos de DNS sinkholing que permitam intercetar pedidos de resolução de nomes para domínios comprometidos com malware
- Capacidade de definir políticas de antivírus, de forma que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso
- Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a ação a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs)
- Possibilidade de enviar o ficheiro para serviços de inspeção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possam tomar uma ação no caso de um ficheiro malicioso

- Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com determinada direção e a determinadas aplicações
- Capacidade de identificar ficheiros não através das suas extensões, mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros
- Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente
- Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro
- Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do ponto de vista de ameaça de segurança
- Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados
- Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing.
- Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.

Sandboxing e protecção Zero Day:

- Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)
- Perante uma análise por parte do serviço de Sandboxing na cloud que categoriza a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)
- O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios
- A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP
- A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.
- Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux
- O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida.
- Em termos de suporte de sistemas operativos Windows emulados deve suportar: Windows XP, Windows 7 e Windows 10
- Deve ser garantido suporte para os seguintes ficheiros executáveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS),
- Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)
- Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.
- Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.

Relatórios & Logs:

- A appliance deve ter a capacidade gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais
- Deve ser possível gerar relatórios de atividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas
- Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatórios num único documento em formato pdf
- Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detetadas e relatórios sobre a análise do comportamento do tráfego observado que permita detetar equipamentos comprometidos que participem em botnets
- Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende
- Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento
- Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objetivo de manter os logs a longo prazo
- Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema
- Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detetadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detetados, informação enviado ao serviço de sandboxing e equipamentos internos comprometidos
- Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma que a partir dos logs criados se possa obter informações de alto nível

IOT Security:

- A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT.
- A firewall deve colecionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede.
- A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses.
- O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilância), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo
- Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também.
- Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo, mas bloqueie qualquer ligação anormal.
- A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas.

- Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos, etc.
- O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associadas ao uso/configuração incorreta dos mesmos. Exemplo: uso de credenciais default.
- Deve existir a possibilidade de o Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB (Cloud Access Security Broker).
- O repositório de dados deve ter capacidade de armazenamento de logs de 1 TB.

Network Packet Broker

- O equipamento deve ter capacidades de Network Packet Broker de forma a permitir filtrar e encaminhar tráfego para uma cadeia externa de dispositivos de segurança de terceiros para uma análise estendida
- Capacidade para usar um ou mais dispositivos de segurança de terceiros (Security Chain) como parte do conjunto geral de segurança
- Capacidade de definir o tráfego encaminhado com base em aplicações, utilizadores, zonas, dispositivos e endereços de IP
- Capacidade para encaminhar tráfego TLS (Decryption Broker) descriptado e sem ser descriptado
- Capacidade para assegurar que o caminho para a cadeia de segurança está íntegro e que tenha opções para lidar com o tráfego se a cadeia não estiver operacional
- Capacidade para suportar tráfego unidirecional e bidirecional na cadeia (Client-to-server e Server-to-client) no mesmo par de interfaces (broker interfaces)
- Capacidade de definir múltiplos perfis e associar o perfil a uma regra/política
- As regras/políticas devem definir o tráfego a ser encaminhado para a cadeia de segurança e o perfil deve definir como encaminhar esse tráfego, incluindo as interfaces para encaminhamento, monitorização da integridade da cadeia, distribuição de sessão entre várias cadeias e escolha da forma como é encaminhada Routing (Layer 3) ou Transparente Bridge (Layer 1).

Outras Funcionalidades:

- Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade.
- Possibilidade de decifrar tráfego SSL e SSH de forma que se possa estabelecer políticas de descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados.
- Capacidade de criar exceções à descriptação para determinado tipo de tráfego.
- Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC).
- Possibilidade de enviar tráfego após descriptação para uma interface de port mirror para análise de terceiras partes.
- Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego.
- Capacidade de capturar tráfego em formato pcap exclusivamente quando se deteta um vírus ou um ataque em qualquer um dos motores de proteção.

Mapa de Quantidades de equipamentos e licenças

Descrição	Quantidade
Appliance de Segurança em alta disponibilidade (HA)	2(1 cluster)
Licenciamento, em HA, com subscrição por 36 meses:	1 Cluster
• Firewall Aplicacional (Layer7)	
• Controlo de utilizadores	
• Threat Prevention	
• IDS/IPS	
• Antivirus & Anti-Malware	
• AntiSpyware	
• Sandboxing	
• IoT Security	
• Analise de eventos	
• Reporting	

- 4x SFP de 10G para interligação com a infraestrutura existente
- Suporte e subscrições de 3 anos

2. Plataforma de proteção de dispositivos

A solução de Endpoint Security tem de cumprir as seguintes especificações:

Requisitos Gerais

- A instalação de, pelo menos, 2500 postos de trabalho/servidores (endpoints).
- Suporte e subscrição incluída para um mínimo de 3 anos.
- Prevenção contra exploits, incluindo aqueles que utilizam vulnerabilidades do tipo Zero-Day.
- Prevenção contra a execução de malware, sem requerer qualquer conhecimento prévio.
- Garantir uma análise forense detalhada dos ataques prevenidos.
- Capacidade de restringir a execução de determinados ficheiros.
- Proteger contra ransomware.
- Conseguir prevenir de forma efetiva Exploits e Malwares quando não existe conectividade ou atualizações do servidor de gestão e/ou acesso a recursos da cloud.
- Controlar dispositivos USB
- Disk Encryption
- Host Firewall
- Permitir isolar automaticamente da rede máquinas infetadas com malware
- Módulo de Endpoint Detection and Response (EDR)
- Configuração de sensores com a capacidade de analisar pelo menos 1 TBs de tráfego de rede por mês

Gestão

- A solução proposta deve ser gerida através de uma interface gráfica web.
- A solução proposta deve poder exportar os seus logs em formato syslog para qualquer solução de gestão de logs.
- A solução proposta deve ter uma gestão centralizada baseada em cloud.
- A solução deve vir de base já configurada com as best practices do fabricante de forma a simplificar o deployment da mesma.
- A solução deve permitir que seja utilizado um serviço de logging na cloud para alojar tanto os logs de firewalls como de endpoints para depois poder integrar com vários outros fabricantes através de uma Framework e APIs.
- A solução proposta deve possuir um modelo de licenciamento por endpoint e/ou largura de banda e não por outros parâmetros como por exemplo número de utilizadores, CPUs, etc.
- A solução proposta deve suportar a atualização de software dos agentes de endpoint diretamente a partir da cloud.

Prevenção de Exploits

- A solução proposta deve suportar proteger processos do sistema operativo e aplicações, com a capacidade de adicionar à lista de aplicações protegidas, aplicações proprietárias, de terceiras partes ou customizadas.
- A solução proposta deve ser capaz de fornecer prevenção em tempo real contra exploits de qualquer vulnerabilidade aplicacional (incluindo do tipo zero-day ou desconhecidos) através do bloqueio de técnicas de exploits como “Software Logic Flaws”, “Memory Corruptions”, “DLL Hijacking”, “heap spray”, “JIT”, “ROP”, “SEH”, etc.
- A solução proposta deve ser capaz de efetuar prevenção de exploits através do bloqueio de técnicas de exploits sem requerer conectividade com o servidor de gestão e/ou serviço da cloud e sem utilizar assinaturas.
- Assim que a solução proposta previne ou bloqueia uma técnica de exploit deve parar imediatamente o processo relacionado, coletar informação forense (nome do processo, ficheiro de origem e o caminho, data e hora, dump da memória, versão do sistema operativo, identificação do utilizador, identificação e versão da aplicação vulnerável, etc.) e terminar apenas este processo.
- A solução proposta deve utilizar módulos de técnicas de exploit para prevenir ou bloquear exploits. Não deve basear a prevenção ou bloqueio de exploits em assinaturas, reputação e heurísticas dos ficheiros.
- A solução proposta não deve utilizar de forma intensiva os recursos do endpoint ou utilizar técnicas de análise baseada em hardware específico como sandbox local baseado em virtualização de software ou containers. A solução proposta deve ter impacto mínimo no desempenho através da utilização de um agente leve e não intrusivo que pode ser totalmente invisível para o utilizador.
- A solução proposta deve proteger de forma simultânea todas as aplicações e processos do endpoint contra técnicas de exploit.
- A solução proposta deve permitir a configuração granular de políticas de prevenção e bloqueio de exploits por utilizador, grupos ou máquina (endpoint) e ter políticas pré-configuradas para os processos mais comuns do sistema Microsoft Windows.
- A solução proposta deve conseguir proteger o endpoint contra “Kernel privilege escalation”.
- A solução proposta deve também conseguir proteger contra exploits para MacOS e Linux, como por exemplo “local privilege escalation”

Prevenção de Malware

- A solução proposta deve suportar proteção contra a execução de executáveis maliciosos.
- A solução proposta deve garantir a funcionalidade de monitorização ou aprendizagem do ambiente onde está instalado (i.e., processos e aplicações instaladas e a correr nos endpoints). Esta deverá ser utilizada na fase inicial de instalação e configuração.
- A solução proposta deve ter a capacidade de controlar o que pode ser executado no endpoint, a partir de onde pode ser executado e com que parâmetros.
- A solução proposta deve prevenir um processo de lançar qualquer processo legítimo que possa ser utilizado para fins maliciosos. Esta técnica é muitas vezes utilizada em ransomware e outros malwares para fazer bypass à segurança do endpoint.
- A solução proposta deve ser capaz de bloquear processos filhos iniciados por um determinado processo através de whitelist (bloquear todos exceto os listados) e blacklist (bloquear apenas os listados).
- A solução proposta deve ser capaz de prevenir a execução de malware através da análise de comportamentos desencadeados pelo malware.
- A solução proposta deve garantir a possibilidade de configurar whitelists globais para permitir a execução de certos ficheiros executáveis.
- A solução proposta deve ser capaz de criar regras de exclusão das capacidades de proteção para endpoints específicos.
- A solução proposta deve detetar e bloquear malware através do uso de machine learning e não deve utilizar assinaturas locais independentemente do sistema operativo
- A solução deve ser capaz de analisar ficheiros do tipo mach-o, ELF e APK.

- A solução proposta deve ter a opção de integrar com soluções de Advanced Persistent Threat (APT) na cloud, tendo a capacidade de fornecer uma prevenção efetiva mesmo quando não possui ligação à cloud ou ao serviço de gestão centralizado. A solução de APT na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração.
- A solução proposta deve conseguir perguntar aos serviços APT na cloud por valores de hash para verificar se determinado ficheiro é malicioso ou benigno.
- A solução deve utilizar técnicas locais de machine learning para detetar malware desconhecido
- A solução deve monitorizar os diferentes processos bem como as suas relações e origens (Parent processes) de forma a ser capaz de bloquear processos com comportamento malicioso.

Requisitos técnicos obrigatórios

- A solução proposta deve ter a capacidade de submeter aos serviços APT na cloud ficheiros potencialmente maliciosos.
- A solução proposta deve conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do malware.
- A solução proposta não deve analisar ficheiros que já tenham sido anteriormente submetidos aos serviços APT na cloud.
- A solução proposta deve conseguir prevenir malware desconhecido utilizando tecnologia APT sandbox na cloud e fornecer um relatório com o veredicto e análise do ficheiro submetido. A solução de APT sandbox na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração.
- A solução proposta deve ter a capacidade de modificar manualmente a decisão tomada pelos serviços APT na cloud para uma hash em particular.
- A solução proposta deve ter a capacidade de prevenir a execução de um ficheiro no caso da sua hash ser desconhecida dos serviços APT na cloud.
- A solução proposta deve ter a capacidade de prevenir a execução de um ficheiro no caso do endpoint não conseguir contactar os serviços APT na cloud e o valor da hash do ficheiro não ser localmente conhecido.
- A solução proposta deve garantir a capacidade de efetuar análises estáticas (machine learning) em modo offline para Windows, Linux e macOS.
- A solução proposta deve prevenir processos que corram no endpoint de fazer o carregamento de DLL's maliciosos. A solução proposta deve examinar os DLL's e criar um veredicto sobre se deve ou não ser executado o carregamento de determinado DLL.
- A solução proposta deve conseguir analisar comportamentos de ransomware antes da execução do mesmo e deve conseguir parar ataques baseados em encriptação através da análise em tempo real de atividades de encriptação.
- A solução proposta deve conseguir prevenir ataques que tirem partido do kernel para carregar e correr código "shell" malicioso.
- A solução proposta deve conseguir que o módulo de análise de comportamentos de ransomware opere em modo de notificação ou de prevenção.
- A solução proposta deve possuir um módulo de análise de comportamentos de ransomware que suporte os seguintes sistemas de ficheiros: NTFS, FAT, exFAT.
- A solução deve poder bloquear qualquer dispositivo USB externo que se conecte a um endpoint monitorizado pela solução. Deve ser possível bloquear determinado tipo de dispositivo USB, mas permitir apenas dispositivos de um vendedor específico ou com um Serial Number específico. Deverá ser possível criar políticas apenas temporárias.
- A solução proposta deve ter a capacidade de automaticamente criar uma regra de exclusão e um hash de exclusão a partir do relatório de ameaças detetadas, para garantir que determinado processo possa ser executado num endpoint em particular.
- A solução deve suportar os seguintes sistemas operativos:
 - Android 5, 6, 7, 8, 9 e 10
 - Debian 8 e 9
 - CentOS 6 e 7
 - Oracle 6 e 7
 - Red Hat 6 e 7

- SUSE 12
- Ubuntu 12, 14, 16 e 18
- macOS 10.11, 10.12, 10.13, 10.14 e 10.15
- Windows 7, 8 e 10
- Windows Server 2008R2, 2012, 2016 e 2019
- A solução deve suportar ainda os seguintes ambientes virtuais: Citrix XenApp, Citrix App layering, VMware AppVolumes, VMware ThinApp.

Endpoint Detection and Response

- A solução deve monitorizar todos os endpoints, nomeadamente informação relativa a: processos, ficheiros, tráfego de rede, registry e memória. Qualquer atividade relacionada com estes pontos deve ser guardada no mínimo para os últimos 30 dias. Deverá ser possível prolongar esta retenção indefinidamente.
- Com base na informação disponível para os últimos 30 dias, a solução deve ser capaz de detetar máquinas comprometidas, seja com base em análise de processos, ficheiros, registry, e tráfego de rede nas máquinas ou com base na análise do comportamento do utilizador ligado na máquina.
- A solução deve permitir ao analista definir regras e pesquisar por padrões relacionados com toda a informação que é retida para os endpoints. Por exemplo, deve ser possível pesquisar por endpoints onde determinada registry key foi modificada. Isto sem ser necessário utilizar ou aprender uma nova query language.
- Quando diferentes alertas estão relacionados, a solução deve ser capaz de os agregar automaticamente em um único incidente.
- Deve ser possível agregar diferentes incidentes num único.
- Quando é identificado um novo incidente, a solução deve ser capaz de automaticamente identificar a root cause do incidente e mostrar toda a sequência de eventos que causou o incidente, assim como todas as alterações introduzidas por estes eventos. Para cada evento deve ser possível visualizar o processo associado, o tráfego de rede gerado por esse processo, os ficheiros acedidos alterados ou criados, qualquer modificação no registry, assim como todos os módulos/DLLs carregados por este processo em memória.
- Para cada incidente, a solução deve indicar: todos os alertas associados a este incidente, todos os artefactos relevantes para a investigação, as máquinas e os utilizadores envolvidos. Cada incidente deve ter uma funcionalidade de chat e de notas para os analistas poderem colaborar entre si.
- Para cada artefacto deve existir informação sobre se há assinaturas válidas para estes, assim como um veredicto sobre o artefacto da própria cloud do fabricante assim como de ferramentas OpenSource (ex: VirusTotal)
- A solução deve mapear os diferentes alertas para a Framework Mitre ATT&CK
- Através de licenciamento adicional, a solução deve ser capaz de ingerir dados da rede do cliente (on-prem e cloud) de forma a ter visibilidade de todo o tráfego de rede e efetuar deteção comportamental sobre a rede, endpoint e cloud numa única solução e interface gráfica. Para recolher o tráfego de rede a solução deve ser capaz de integrar com pelo menos 4 fabricantes de Firewalls.
- Através de licenciamento adicional deve ser possível ingerir logs de identity providers, nomeadamente: AzureAD, Okta e PingID de forma a detetar anomalias nos padrões de autenticação dos utilizadores.
- Deve existir uma funcionalidade de “search&destroy” que permite pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo
- A solução deve aprender o comportamento de cada máquina e criar perfis de forma a ser capaz de identificar comportamentos anômalos
- Com base na aprendizagem comportamental para cada máquina e utilizador a solução deverá ser capaz de gerar alarmística para estes cenários:
 - Sessão rara de SSH
 - Uso de comandos fora do comum (arp -a, ipconfig, etc)
 - processos raros a comunicar com máquinas fora da organização

- processos a comunicar com máquinas externas que não são normalmente acedidas pelas máquinas da organização
- scripts a comunicar com hosts externos
- listagem de utilizadores do domínio
- comando de powershell anormal
- volume de conexões entre máquinas elevado
- Capacidade de reverter automaticamente alterações feitas na máquina por determinado malware. A solução deve listar as alterações feitas por qualquer processo malicioso e permitir reverter essas alterações.

NTA&UEBA

- A solução deve ser capaz de ingerir dados da rede do cliente (on-prem e cloud) de forma a ter visibilidade de todo o tráfego de rede e efetuar deteção comportamental sobre a rede, endpoint e cloud numa única solução e interface gráfica.
- A solução deve poder utilizar como sensores na rede, Firewalls de pelo menos 4 fabricantes distintos.
- Deve ser possível colocar sensores em ambientes de cloud, nomeadamente: AWS, Azure, GCP e Alibaba.
- A solução proposta deve fazer stitching dos logs provenientes dos sensores na rede com os logs dos endpoints de forma a permitir a unificação dos mesmos e simplificar o processo de deteção e investigação de ameaças.
- A solução proposta deverá utilizar Machine Learning para criar perfis das diferentes máquinas e utilizadores na rede de forma a detetar comportamentos anómalos que sejam indicadores de ataques.
- A solução deverá ser capaz de detetar o seguinte tipo de eventos:
 - Malware a ser transmitido na rede;
 - Máquina a enviar SPAM;
 - Máquina com um número anormal de conexões falhadas para outros endpoints;
 - Elevado número de conexões para um determinado porto que não corresponde ao perfil;
 - Port Scan;
 - Conexões consecutivas entre 2 endpoints que não são normais;
 - Novo tipo de comportamento administrativo;
 - Execução remota de comandos;
 - Reverse Shell;
 - Tráfego SMB/KRB através de um protocolo inesperado;
 - DNS Tunneling;
 - Número anormal de resoluções de DNS falhados;
 - DGA (Domain Generated Algorithm);
 - Command and Control através da análise de pedidos de DNS, URLs e ligações diretas a IPs;
 - Tunneling;
 - Volume anormal de dados a ser transferidos;
- No caso de ser identificado um comportamento malicioso na rede, deve ser possível obter informação sobre os processos da máquina afetada mesmo que esta não tenha nenhum agente instalado.

Visibilidade sobre as máquinas

A solução deve incluir um módulo de visibilidade com as seguintes características:

- Capacidade de identificar:
 - Utilizadores e grupos configurados em cada máquina
 - Serviços a correr nas máquinas
 - Drivers instalados nas máquinas
 - Processos, drivers, serviços que são automaticamente inicializados sempre que o utilizador liga as máquinas.

- Shares de rede configurados nas máquinas
- Discos existentes nas máquinas
- Funcionalidade de “search&destroy” que permite pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo
- Identificar vulnerabilidades e respetiva criticidade para ambientes Windows e Linux
- Identificar as aplicações a correr em cada equipamento

Resposta a incidentes

- A solução proposta deve permitir iniciar scans de malware à máquina infetada.
- Deve ser possível efetuar blacklists e whitelists a hashes.
- Deve ser possível fazer quarentena a determinados processos.
- Durante a investigação de um incidente, a solução deve permitir isolar da rede máquinas infetadas.
- A solução deve permitir reverter automaticamente alterações que tenham sido efetuadas por um processo malicioso. Exemplo: Alterar uma registry key para o valor anterior ao comprometimento da máquina.
- Deve existir uma funcionalidade de Live Terminal, onde o analista possa aceder remotamente às máquinas de forma a: gerir os processos e ficheiros, correr scripts Python, correr comandos de Powershell e aceder à linha de comandos da máquina.
- Deve ser possível correr scripts em python sobre todo o parque de máquinas instalado em simultâneo. A solução deve disponibilizar scripts para os use cases mais comuns e permitir a criação de novos scripts.
- Capacidade de criar regras de correlação personalizadas que permitem detectar ataques retroativamente.
- A solução deve incluir uma linguagem de consulta avançada que suporte wildcards, expressões regulares, JSON, agregação de dados, manipulação de campos e valores, agregação de dados de fontes diferentes e visualização de dados.

Toda a plataforma a fornecer tem de cumprir todas as especificações indicadas e para comprovar as especificações deverá ser preenchido o Anexo I e II (anexos ao programa do procedimento) onde se deve indicar o cumprimento do requisito e respetivo documento público do fabricante a fazer prova desse requisito (catálogos e/ou fichas técnicas).

É necessário entregar uma declaração do fabricante a fazer prova que o mesmo tem conhecimento da proposta apresentada pelo concorrente, certificando que a empresa possui as competências necessárias para implementação e suporte da solução.

3. Serviços de implementação:

3.1. Instalação e configuração dos equipamentos fornecidos:

- Integração na infraestrutura existente
- Configuração de interfaces, políticas de segurança e outras configurações relevantes

3.2. Documentação:

- Documentos do fabricante dos produtos propostos que garanta a capacidade do concorrente para o seu fornecimento, de acordo com especificação técnica do caderno de encargos.
- Documento que comprove a compra dos serviços de suporte ao fabricante, após a adjudicação;

- Documento do fabricante que comprove que o mesmo tem conhecimento do projeto e que o parceiro é registado e autorizado;

3.3. Formação on-job sobre a solução proposta

4. Formação

- Inclusão de formação de 4 dias para 6 pessoas com os seguintes conteúdos:

- Portfolio and Architecture of Firewalls
- Connect to the Management Network
- Manage Firewall Configurations
- Manage Firewall Administrator Accounts
- Connect to Production Networks
- Block Threats Using Security and NAT Policies

- Block Packet and Protocol-Based Attacks
- Block Threats from Known Bad Sources
- Block Threats by Identifying Applications
- Maintain Application-Based Policies
- Block Threats Using Custom Applications
- Block Threats by Identifying Users

- Block Unknown Threats
- Block Threats in Encrypted Traffic
- Prevent Use of Stolen Credentials
- Block Threats Using Security Profiles
- View Threat and Traffic Information

- Initial Configuration
- Adding Firewalls
- Templates
- Device Groups
- Log Collection and Forwarding
- Using Logs on Firewalls
- Vendor Administrative Accounts
- Reporting
- Troubleshooting

5. Garantia e manutenção

- 5.1. Garantia no mínimo de 3 anos
- 5.2. Suporte e subscrições no mínimo de 3 anos
- 5.3. Todos os equipamentos deverão ser originais e do mesmo fabricante, não sendo aceite equipamentos recondicionados.
- 5.4. Em caso de suporte deverá haver uma resposta com SLA de 24x7x8h suporte remoto e SLA de 8x5xNBD para peças.

- 5.5. Todos os equipamentos propostos deverão ser totalmente suportados pelo fabricante, e deverá ser possível abrir cases diretamente no fabricante para a totalidade dos equipamentos propostos.

Anexo I - Tabela de conformidades

Funcionalidades Obrigatórias das Firewalls				
Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se Cumpre (sim ou não)			
	SIM	NÃO	Nome do Documento do fabricante	Nº da Pagina
Número de portas 1G/2.5G/5G/10 Gbit/s RJ45 >= 12				
Número de portas Gigabit SFP+ 10 Gbit/s >= 10				
Número de portas Gigabit SFP28 25 Gbit/s >= 4				
Número de portas Gigabit QSFP+/QSFP28 40/100 Gbit/s >= 2				
Porta de gestão dedicada "Out of Band"				
Número de portas de alta disponibilidade 1Gbit/s >= 2				
Número de portas de alta disponibilidade 10 Gbit/s SFP+ >= 1				
Porta USB				
Disco rígido SSD >= 480GB				
A appliance de FW deverá ter uma arquitectura com recursos de hardware dedicados e independentes entre os serviços de gestão e os serviços de inspeção.				
Deverá estar garantido que a appliance de FW quando gerida localmente e perante uma sobrecarga dos serviços de inspeção de tráfego não afecte de forma alguma a performance dos serviços de gestão e vice versa.				
Fontes de alimentação redundantes.				
Performance				
Performance da appliance com a funcionalidade de firewall com identificação e controle de aplicações (inspeção L7 de todo o tráfego) >= 20,5 Gbps				
Performance da appliance com as funcionalidades IDS/IPS, Antivírus e Anti-Spyware, URL Filtering e Sandboxing >= 10,5 Gbps				
Performance da appliance com a funcionalidade de VPN IPSec >= 12,2 Gbps				
Número de novas sessões por segundo >= 240 000				
Número máximo de sessões >= 2 500 000				

Gestão				
Gestão e administração da própria appliance através de interface web, linha de comandos e API XML				
Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio				
Deve ser possível criar perfis de administração que permita segmentar a gestão em diferentes tenants (Por Firewall, por número de firewalls) - Multi-tenancy				
Possibilidade de criar diferentes perfis e cargos de administração para a gestão da appliance, com diferentes níveis de privilégio;				
Possibilidade de editar configurações pendentes que ainda não foram aplicadas				
Possibilidade de visualizar e validar alterações à configuração antes de estas alterações serem aplicadas				
Possibilidade de descartar alterações à configuração realizadas				
Possibilidade de armazenar diferentes versões da configuração				
Capacidade de criar hierarquização da política de segurança para permitir ter políticas globais para toda infraestrutura instalada				
Deve existir a capacidade de stacks de templates com configurações reutilizáveis para múltiplos equipamentos.				
Deve existir um ponto centralizado para efectuar upgrades e atualizações de versões e assinaturas				
Capacidade de transformar políticas de layer4 em layer7 com machine learning e aprendizagem embebida na plataforma de gestão				
Na gestão centralizada deve existir a capacidade de "zero touch provisioning" para simplificar o deployment de firewalls remotas				
Deve existir a capacidade de correr a Gestão centralizada sobre hardware dedicado assim como numa Máquina Virtual em VMware ESXi™, KVM e Microsoft Hyper-V, ou então em clouds públicas incluindo Google Cloud Platform (GCP™), Amazon Web Services (AWS®), AWS GovCloud, Microsoft Azure e Azure GovCloud.				

Análise da utilização das regras para reduzir a superfície de exposição e melhorar postura de segurança.				
Envio de logs via SYSLOG, FTP, SCP e TFTP para retenção e posterior tratamento				
Possibilidade de envio selectivo de logs, de acordo com o nível de severidade ou outros atributos como por exemplo o tipo de ameaça				
Suporte de SNMP, incluindo a possibilidade de obter estatísticas relacionadas com o processamento de logs e com as funcionalidades de alta disponibilidade				
Networking				
As interfaces de rede da appliance deverão suportar os seguintes modos de funcionamento: TAP, Layer 2, Layer 3				
Suporte de IEEE 802.1Q				
Suporte de IEEE 802.1AX, suportando até 8 grupos de agregação com 8 interfaces por cada grupo				
Suporte de protocolos dinâmicos de routing: RIP, OSPF, BGP				
Suporte de routing estático				
Suporte de DHCP, NAT e PAT				
Capacidade de deteção de falhas bidirecionais entre a appliance e router para aplicar a protocolos de routing dinâmico ou rotas estáticas				
Capacidade de realizar policy based routing através do IP ou rede de origem				
Capacidade de realizar policy based routing através do utilizador ou grupo				
Capacidade de realizar policy based routing através do tipo de aplicação				
Suporte para TLS 1.3 e capacidade de descriptar este tráfego				
Suporte de arquiteturas de alta disponibilidade do tipo activo/passivo e activo/activo				
Suporte de arquiteturas de alta disponibilidade e escalar lateralmente até 6 membros dentro de um único cluster sem a necessidade de balanceadores externos				
Identificação de Utilizadores				
Possibilidade de aplicar políticas baseadas em utilizadores e grupos, em vez de por IP				

Integração com sistemas de diretórios para obtenção de utilizadores e grupos, incluindo Microsoft Active Directory, Novell eDirectory e Sun ONE Directory				
Possibilidade de integração de com sistemas multiutilizador como Citrix ou Microsoft Terminal Server para identificação de utilizadores				
Capacidade de analisar mensagens de SYSLOG com informação de LOGIN/LOGOUT para identificação de utilizadores				
Possibilidade de gerir utilizadores através de API XML				
Possibilidade de identificação de utilizadores através de portal de autenticação próprio, fazendo uso dos seguintes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente e autenticação local				
Capacidade de obter a identidade dos utilizadores a partir dos seguintes métodos: LDAP, Captive Portal, VPN, NACs (XML e API), Syslog, Terminal Services, XFF Headers, Server Monitoring, e client probing				
Funcionalidades Gerais de Segurança				
Possibilidade de agrupar interfaces da appliance em conjuntos independentes, formando diferentes zonas de segurança				
Possibilidade de definir a política de segurança por zonas de segurança, podendo incluir na mesma política várias zonas de origem e/ou destino para a análise de tráfego e processamento de regras de segurança				
Possibilidade de criar múltiplas regras de segurança entre zonas de origem e destino				
Capacidade de identificação de aplicações em L7 com um mínimo de 2400 aplicações identificadas				
Capacidade de identificação de subfunções dentro de uma aplicação				
Capacidade de aplicar e/ou excepcionar qualquer das funcionalidades de inspeção (IPS, Antivírus, etc) apenas ao tráfego de determinadas aplicações L7				
Possibilidade de agrupar aplicações por categorias de forma a que as políticas de segurança sejam aplicadas por categorias de aplicações				

Possibilidade de identificar as aplicações quando estas não utilizam os portos TCP/UDP por defeito em qualquer tipo de tráfego/protocolo e não somente HTTP				
Possibilidade de identificar aplicações proprietárias que usem os protocolos HTTP e TCP				
Possibilidade de identificar aplicações que sejam transportadas em túneis encriptados SSL				
Capacidade de decifrar tráfego SSH e detectar aplicações não legítimas que utilizem este protocolo para comunicar (SSH tunneling)				
Capacidade de criar regras de QoS segundo as aplicações utilizadas no tráfego				
Possibilidade de aplicar políticas de NAT de forma independente das restantes políticas de segurança				
Capacidade de forçar o uso de MFA para acesso a aplicações internas				
Deve existir uma versão da solução que possa ser instalada como um container dentro de um ambiente de docker/kubernetes				
IDS/IPS				
Capacidade de aplicar políticas de prevenção ou de detecção contra a exploração de vulnerabilidades, tanto no tráfego que vai para a Internet como no tráfego que vem da Internet, sem incorrer numa latência superior a 1 ms para não penalizar a experiência do utilizador, efectuando a análise numa única passagem do tráfego para todas as ameaças				
Possibilidade de aplicar diferentes perfis proteção contra exploração de vulnerabilidades de acordo com as aplicações identificadas				
Possibilidade de seleccionar proteções contra a exploração de vulnerabilidades que se apliquem apenas a clientes ou servidores ou a ambos				
As vulnerabilidades devem estar categorizadas por tipo e por nível de risco, de forma a que a aplicação de perfis de protecção se possam realizar com base nestas categorias				
Deve ser possível identificar as protecções pela identificação CVE das vulnerabilidades				
Capacidade de aplicar apenas as assinaturas necessárias para determinada aplicação identificada, através da selecção de perfis				
Deve ser possível converter e importar assinaturas snort e suricata para dentro da plataforma				

Antivírus & Anti-Malware				
Detectar equipamentos possivelmente comprometidos que tentem estabelecer comunicações com servidores de C&C				
Capacidade de habilitar mecanismos de DNS sinkholing que permitam interceptar pedidos de resolução de nomes para domínios comprometidos com malware				
Capacidade de definir políticas de antivírus, de forma a que a transferência de ficheiros realizada no sentido Internet para rede interna ou vice-versa, sejam inspecionados e bloqueados se o seu conteúdo for malicioso				
Capacidade de aplicar políticas que permitam aplicar o motor de antivírus sobre protocolos como ftp, http, imap, pop3, smb ou smtp, definindo para cada um destes protocolos a acção a realizar (permitir os ficheiros, descartar os ficheiros, desconectar a sessão ou registar mediante logs)				
Possibilidade de enviar o ficheiro para serviços de inspecção adicionais na cloud que permitam analisar e emitir um veredicto para que appliance possa tomar uma acção no caso de um ficheiro malicioso				
Capacidade de aplicar políticas de antivírus de forma granular, permitindo aplicar essas políticas utilizadores ou grupos, a determinados segmentos de rede com com determinada direcção e a determinadas aplicações				
Capacidade de identificar ficheiros não através das suas extensões mas sim através do tipo MIME do ficheiro, permitindo no mínimo a identificação de 100 tipos de ficheiros				
Deve-se poder aplicar políticas de bloqueio de ficheiros, de forma a poder bloquear a transferência de certo tipo de ficheiros ou que se permita após a confirmação por parte do utilizador e criando um log correspondente				
Capacidade de aplicar políticas de bloqueio de ficheiros atendendo a critérios como origem e destino do tráfego, utilizador ou grupo, tipo de aplicação ou de tráfego que inicia a transferência do ficheiro				

Possibilidade de bloquear a transferência de ficheiros quando utilizados URLs categorizados como perigosos do pondo de vista de ameaça de segurança				
Capacidade pesquisa de padrões sensíveis no tráfego, evitando a exfiltração de dados.				
Deve existir a capacidade de analisar ficheiros executáveis e scripts powershell com um motor de machine learning local que permita bloquear ficheiros maliciosos localmente em tempo real sem necessidade de estabelecer ligações externas. Este motor deve permitir bloquear malwares nunca antes observados e para os quais não existem assinaturas sem necessidade de recorrer a sandboxing.				
Deve existir a capacidade de receber updates em tempo real de forma a não ter que aguardar minutos/horas/dias por determinado update. Assim que um novo malware é detetado por qualquer cliente do fabricante essa informação deve ser propagada em tempo real a todos os clientes de forma a diminuir o tempo de exposição a ameaças.				
Sandboxing e protecção Zero day				
Possibilidade de disponibilizar um serviço na cloud capaz de analisar ficheiros do tipo desconhecido ou links recebidos em e-mails, de forma a que se permita o envio desta informação para análise atendendo aos critérios: Tipo de aplicação utilizada para transferir o ficheiro, tipo de ficheiro que está a ser transferido, direção da transferência (download ou upload)				
Perante uma análise por parte do serviço de Sandboxing na cloud que categorize a informação enviada como maliciosa, deverão ser criadas assinaturas num prazo máximo de 5 minutos que possam ser utilizadas nos motores de Antivírus e URLF e que as descargas posteriores do mesmo ficheiro ou links sejam imediatamente bloqueadas (desta forma o malware desconhecido é transformado em malware conhecido automaticamente)				
O serviço de sandboxing na cloud deverá permitir consultar a informação enviada e avaliada e gerar os respetivos relatórios				

A tecnologia de Sandboxing tem que ser capaz de inspecionar protocolos como HTTP, HTTPS, SMTP, FTP, POP3 e IMAP				
A análise de malware deve ser inteligente o suficiente para analisar comportamentos do tipo "Call back" e IOC's durante a análise de malware e automaticamente criar assinaturas que permitam a prevenção de ameaças e que possam ser utilizadas pelas restantes funcionalidades da solução.				
Os sistemas de análise de malware devem ser capazes de detetar malware direcionado a sistemas operativos de MacOS, Windows, Android e Linux				
O malware cada vez mais utiliza técnicas de Anti-VM para detetar que está a ser executado num ambiente virtual e prevenir que seja detonado, escondendo o seu comportamento malicioso. A análise "Bare Metal" é uma funcionalidade onde o malware é executado em hardware real, o que impede que o malware utilize qualquer técnica de Anti-VM. A solução deve ter esta funcionalidade embebida.				
Em termos de suporte de sistemas operativos windows emulados deve suportar: Windows XP, Windows 7 e Windows 10				
Deve ser garantido suporte para os seguintes ficheiros executaveis (EXE, DLL) e todos os tipos de ficheiros Microsoft Office, PDF, Flash, Java applets (JAR e CLASS),				
Android (ficheiros APK), macOS binaries (mach-O, DMG, PKG e application bundles) e Linux (ficheiros ELF)				
Incluir o suporte de ficheiros comprimidos (RAR, 7Zip) e conteúdo encriptado.				
Capacidade de descriptar malware (unpacker) para utilização na análise estática e machine learning.				
Relatórios & Logs				
Deve ser possível gerar relatórios tanto predefinidos ou personalizados, utilizando os logs criados pelo próprio equipamento sem necessidade de equipamentos externos adicionais				
Deve ser possível gerar relatórios de actividade por utilizador, incluindo aplicações utilizadas e páginas web visitadas				

Deve ser possível gerar relatórios de forma automática assim como agrupar vários relatório num único documento em formato pdf				
Entre os relatórios disponíveis devem constar relatórios com a largura de banda consumida pelas diferentes aplicações, relatórios sobre as origens e destinos geográficos das ameaças detectadas e relatórios sobre a análise do comportamento do tráfego observado que permita detectar equipamentos comprometidos que participem em botnets				
Deve ser possível programar o momento em que se deseja a geração do relatório pretendido e o seu envio através de e-mail, assim como o intervalo temporal que se pretende				
Possibilidade de armazenar os logs localmente tendo por única restrição a capacidade do disco do próprio equipamento				
Possibilidade de enviar logs para uma plataforma externa de gestão e processamento especializado de logs com o objectivo de manter os logs a longo prazo				
Capacidade de dispor de um painel de instrumentos personalizável por utilizador de administração da appliance com pelo menos a seguinte informação: Aplicações mais utilizadas, Aplicações de alto risco, Informação geral do sistema, Estado das interfaces, Logs relativos às ameaças mais observadas, Logs de URLs filtrados, Recursos do sistema				
Capacidade de dispor de estatística gerada a partir de logs, personalizável por utilizador que permita fornecer informações como: utilizadores que mais geram tráfego, regras de segurança que mais utilizam, vulnerabilidades mais detectadas e bloqueadas, equipamentos que acederam a domínios maliciosos, vírus detectados, informação enviada ao serviço de sandboxing e equipamentos internos comprometidos				
Capacidade de utilizar um motor integrado de correlação de eventos dentro da própria appliance de forma a que a partir dos logs criados se possa obter informações de alto nível.				
IoT Security				
A plataforma deve disponibilizar um serviço cloud de segurança para dispositivos IOT.				

A firewall deve coleccionar metadados do tráfego de rede dos dispositivos IoT, gerar logs com estas informações e enviá-los para um Data Lake na Cloud. O Serviço de IOT deve ter capacidade de analisar estes metadados através de um motor patenteado baseado em algoritmos de inteligência artificial e machine learning para detetar e identificar os dispositivos IoT e OT na rede.				
A identificação de dispositivos não se deve basear em fingerprinting, como por exemplo identificação de MAC addresses.				
O motor de identificação deve possuir 3 níveis: identificação da categoria do dispositivo (ex: camara de vigilancia), identificação do seu perfil (ex: fabricante, modelo e versão) e identificação de cada instância do dispositivo.				
Após a identificação dos dispositivos, a solução deve criar um padrão de comportamento para cada um e detetar automaticamente comportamentos anormais que possam sugerir que o dispositivo está comprometido. Para este tipo de eventos, devem ser gerados alertas no dashboard da solução. Deve ser possível receber estes alertas via email e sms também.				
Quando é observado um comportamento anormal a solução deve sugerir automaticamente políticas de segurança a aplicar na firewall que permitam o correto funcionamento do dispositivo mas bloqueie qualquer ligação anormal.				
A firewall deve permitir a criação de regras baseadas em tipos de dispositivos que devem ser identificados através da marca, modelo e versão. Não sendo assim necessário criar regras com base em IPs ou zonas.				
Este serviço deve observar mais de 200 parâmetros nos metadados do tráfego de rede, incluindo parâmetros de DHCP (option 55), HTTP user agent IDs, protocolos, headers dos protocolos,etc.				

O serviço deve identificar vulnerabilidades presentes no software a correr nos respetivos dispositivos e diferenciar entre dispositivos vulneráveis e potencialmente vulneráveis. O serviço deve identificar vulnerabilidades de software assim como vulnerabilidades associados os uso/configuração incorrecta dos mesmos. Exemplo: uso de credenciais default.				
Deve existir a possibilidade do Data Lake ser utilizado para outro conjunto de use cases através de licenciamento adicional, nomeadamente: NTA (Network Traffic Analysis), UEBA (User Entity Behavior Analytics), shadow IT e integração com CASB(Cloud Access Security Broker).				
O repositório de dados deve ter capacidade de armazenamento de logs de 1 TB.				
Network Broker				
O equipamento deve ter capacidades de Network Packet Broker de forma a permitir filtrar e encaminhar tráfego para uma cadeia externa de dispositivos de segurança de terceiros para uma análise estendida				
Capacidade para usar um ou mais dispositivos de segurança de terceiros (Security Chain) como parte do conjunto geral de segurança				
Capacidade de definir o tráfego encaminhado com base em aplicações, utilizadores, zonas, dispositivos e endereços de IP				
Capacidade para encaminhar tráfego TLS (Decryption Broker) descriptado e sem ser descriptado				
Capacidade para assegurar que o caminho para a cadeia de segurança está íntegro e que tenha opções para lidar com o tráfego se a cadeia não estiver operacional				
Capacidade para suportar tráfego unidirecional e bidirecional na cadeia (Client-to-server e Server-to-client) no mesmo par de interfaces (broker interfaces)				
Capacidade de definir múltiplos perfis e associar o perfil a uma regra/política				

As regras/políticas devem definir o tráfego a ser encaminhado para a cadeia de segurança e o perfil deve definir como encaminhar esse tráfego, incluindo os interfaces para encaminhamento, monitorização da integridade da cadeia, distribuição de sessão entre várias cadeias e escolha da forma como é encaminhada Routing (Layer 3) ou Transparente Bridge (Layer 1)				
Outras Funcionalidades				
Possibilidade de definir aplicações e/ou vulnerabilidades customizadas mediante diferentes parâmetros como: Portos TCP/UDP que sejam usados na aplicação e combinação de padrões dentro dos "headers" dos pacotes ou mesmo no "payload" dos próprios pacotes que se devam cumprir para que se reconheça a aplicação e/ou vulnerabilidade				
Possibilidade de decifrar tráfego SSL e SSH de forma a que se possa estabelecer políticas de descriptação baseadas em: zonas por onde passa o tráfego, IP de origem ou destino, utilizadores geram esse tráfego, portos utilizados.				
Capacidade de criar excepções à descriptação para determinado tipo de tráfego.				
Capacidade de decifrar tráfego com destino a sites web que utilizam certificados de curva elíptica (ECC).				
Possibilidade de enviar tráfego após descriptação para uma interface de port mirror para análise de terceiras partes.				
Capacidade de capturar tráfego em formato pcap, podendo ser estabelecido como critérios de captura do tráfego, uma determinada aplicação independentemente da origem ou destino desse tráfego.				
Capacidade de capturar tráfego em formato pcap exclusivamente quando se detecta um vírus ou um ataque em qualquer um dos motores de protecção.				

AnexoII-Tabela de conformidades

Funcionalidades Obrigatórias da Solução de Endpoint Security

Requisito (obrigatório dentro do mesmo equipamento)	Assinalar se Cumpre (sim ou não)			
	SIM	NÃO	Nome do Documento do fabricante	Nº da Pagina
1. Requisitos Gerais				
A instalação de, pelo menos, 2500 postos de trabalho/servidores (endpoints).				
Prevenção contra exploits, incluindo aqueles que utilizam vulnerabilidades do tipo Zero-Day.				
Prevenção contra a execução de malware, sem requerer qualquer conhecimento prévio.				
Garantir uma análise forense detalhada dos ataques prevenidos.				
Capacidade de restringir a execução de determinados ficheiros.				
Proteger contra ransomware.				
Conseguir prevenir de forma efetiva Exploits e Malwares quando não existe conectividade ou atualizações do servidor de gestão e/ou acesso a recursos da cloud.				
Controlar dispositivos USB				
Disk Encryption				
Host Firewall				
Permitir isolar automaticamente da rede máquinas infectadas com malware				
Módulo de Endpoint Detection and Response (EDR)				
Configuração de sensores com a capacidade de analisar pelo menos 1 TBs de tráfego de rede por mês				
2. Gestão				
A solução proposta deve ser gerida através de uma interface gráfica web.				
A solução proposta deve poder exportar os seus logs em formato syslog para qualquer solução de gestão de logs.				

A solução proposta deve ter uma gestão centralizada baseada em cloud.				
A solução deve vir de base já configurada com as best practices do fabricante de forma a simplificar o deployment da mesma.				
A solução deve permitir que seja utilizado um serviço de logging na cloud para alojar tanto os logs de firewalls como de endpoints para depois poder integrar com vários outros fabricantes através de uma Framework e APIs.				
A solução proposta deve possuir um modelo de licenciamento por endpoint e/ou largura de banda e não por outros parâmetros como por exemplo número de utilizadores, CPUs, etc.				
A solução proposta deve suportar a atualização de software dos agentes de endpoint diretamente a partir da cloud.				
3. Prevenção de Exploits				
A solução proposta deve suportar proteger processos do sistema operativo e aplicações, com a capacidade de adicionar à lista de aplicações protegidas, aplicações proprietárias, de terceiras partes ou customizadas.				
A solução proposta deve ser capaz de fornecer prevenção em tempo real contra exploits de qualquer vulnerabilidade aplicacional (incluindo do tipo zero-day ou desconhecidos) através do bloqueio de técnicas de exploits como “Software Logic Flaws”, “Memory Corruptions”, “DLL Hijacking”, “heap spray”, “JIT”, “ROP”, “SEH”, etc.				
A solução proposta deve ser capaz de efetuar prevenção de exploits através do bloqueio de técnicas de exploits sem requerer conectividade com o servidor de gestão e/ou serviço da cloud e sem utilizar assinaturas.				
Assim que a solução proposta previne ou bloqueia uma técnica de exploit deve parar imediatamente o processo relacionado, coletar informação forense (nome do processo, ficheiro de origem e o caminho, data e hora, dump da memória, versão do sistema operativo, identificação do utilizador, identificação e versão da aplicação vulnerável, etc.) e terminar apenas este processo.				

A solução proposta deve utilizar módulos de técnicas de exploit para prevenir ou bloquear exploits. Não deve basear a prevenção ou bloqueio de exploits em assinaturas, reputação e heurísticas dos ficheiros.				
A solução proposta não deve utilizar de forma intensiva os recursos do endpoint ou utilizar técnicas de análise baseada em hardware específico como sandbox local baseado em virtualização de software ou containers. A solução proposta deve ter impacto mínimo no desempenho através da utilização de um agente leve e não intrusivo que pode ser totalmente invisível para o utilizador.				
A solução proposta deve proteger de forma simultânea todas as aplicações e processos do endpoint contra técnicas de exploit.				
A solução proposta deve permitir a configuração granular de políticas de prevenção e bloqueio de exploits por utilizador, grupos ou máquina (endpoint) e ter políticas pré-configuradas para os processos mais comuns do sistema Microsoft Windows.				
A solução proposta deve conseguir proteger o endpoint contra “Kernel privilege escalation”.				
A solução proposta deve também conseguir proteger contra exploits para MacOS e Linux como por exemplo “local privilege escalation”.				
4. Prevenção de Malware				
A solução proposta deve suportar proteção contra a execução de executáveis maliciosos.				
A solução proposta deve garantir a funcionalidade de monitorização ou aprendizagem do ambiente onde está instalado (i.e. processos e aplicações instaladas e a correr nos endpoints). Esta deverá ser utilizada na fase inicial de instalação e configuração.				
A solução proposta deve ter a capacidade de controlar o que pode ser executado no endpoint, a partir de onde pode ser executado e com que parâmetros.				
A solução proposta deve prevenir um processo de lançar qualquer processo legítimo que possa ser utilizado para fins maliciosos. Esta técnica é muitas vezes utilizada em ransomware e outros malwares para fazer bypass à segurança do endpoint.				

A solução proposta deve ser capaz de bloquear processos filhos iniciados por um determinado processo através de whitelist (bloquear todos exceto os listados) e blacklist (bloquear apenas os listados).				
A solução proposta deve ser capaz de prevenir a execução de malware através da análise de comportamentos desencadeados pelo malware.				
A solução proposta deve garantir a possibilidade de configurar whitelists globais para permitir a execução de certos ficheiros executáveis.				
A solução proposta deve ser capaz de criar regras de exclusão das capacidades de protecção para endpoints específicos.				
A solução proposta deve detectar e bloquear malware através do uso de machine learning e não deve utilizar assinaturas locais independentemente do sistema operativo				
A solução deve ser capaz de analisar ficheiros do tipo mach-o, ELF e APK.				
A solução proposta deve ter a opção de integrar com soluções de Advanced Persistent Threat (APT) na cloud, tendo a capacidade de fornecer uma prevenção efetiva mesmo quando não possui ligação à cloud ou ao serviço de gestão centralizado. A solução de APT na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração.				
A solução proposta deve conseguir perguntar aos serviços APT na cloud por valores de hash para verificar se determinado ficheiro é malicioso ou benigno.				
A solução deve utilizar técnicas locais de machine learning para detetar malware desconhecido				
A solução deve monitorizar os diferentes processos bem como as suas relações e origens (Parent processes) de forma a ser capaz de bloquear processos com comportamento malicioso.				
5. Requisitos Obrigatórios				
A solução proposta deve ter a capacidade de submeter aos serviços APT na cloud ficheiros potencialmente maliciosos.				
A solução proposta deve conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do malware.				

A solução proposta não deve analisar ficheiros que já tenham sido anteriormente submetidos aos serviços APT na cloud.				
A solução proposta deve conseguir prevenir malware desconhecido utilizando tecnologia APT sandbox na cloud e fornecer um relatório com o veredicto e análise do ficheiro submetido. A solução de APT sandbox na cloud deve ser do mesmo fabricante da solução proposta para garantir uma maior integração.				
A solução proposta deve ter a capacidade de modificar manualmente a decisão tomada pelos serviços APT na cloud para uma hash em particular.				
A solução proposta deve ter a capacidade de prevenir a execução de um ficheiro no caso da sua hash ser desconhecida dos serviços APT na cloud.				
A solução proposta deve ter a capacidade de prevenir a execução de um ficheiro no caso do endpoint não conseguir contactar os serviços APT na cloud e o valor da hash do ficheiro não ser localmente conhecido.				
A solução proposta deve garantir a capacidade de efetuar análises estáticas (machine learning) em modo offline para Windows, Linux e macOS.				
A solução proposta deve prevenir processos que corram no endpoint de fazer o carregamento de DLL's maliciosos. A solução proposta deve examinar os DLL's e criar um veredicto sobre se deve ou não ser executado o carregamento de determinado DLL.				
A solução proposta deve conseguir analisar comportamentos de ransomware antes da execução do mesmo e deve conseguir parar ataques baseados em encriptação através da análise em tempo real de atividades de encriptação.				
A solução proposta deve conseguir prevenir ataques que tirem partido do kernel para carregar e correr código "shell" malicioso.				
A solução proposta deve conseguir que o módulo de análise de comportamentos de ransomware opere em modo de notificação ou de prevenção.				
A solução proposta deve possuir um módulo de análise de comportamentos de ransomware que suporte os seguintes sistemas de ficheiros: NTFS, FAT, exFAT.				

A solução deve poder bloquear qualquer dispositivo USB externo que se conecte a um endpoint monitorizado pela solução. Deve ser possível bloquear determinado tipo de dispositivo USB, mas permitir apenas dispositivos de um vendedor específico ou com um Serial Number específico. Deverá ser possível criar políticas apenas temporárias.				
A solução proposta deve ter a capacidade de automaticamente criar uma regra de exclusão e um hash de exclusão a partir do relatório de ameaças detetadas, para garantir que determinado processo possa ser executado num endpoint em particular.				
A solução deve suportar os seguintes sistemas operativos:				
Android 5, 6, 7, 8, 9 e 10				
Debian 8 e 9				
CentOS 6 e 7				
Oracle 6 e 7				
Red Hat 6 e 7				
SUSE 12				
Ubuntu 12, 14, 16 e 18				
macOS 10.11, 10.12, 10.13, 10.14 e 10.15				
Windows 7, 8 e 10				
Windows Server 2008R2, 2012, 2016 e 2019				
A solução deve suportar ainda os seguintes ambientes virtuais: Citrix XenApp, Citrix App layering, VMware AppVolumes, VMware ThinApp				
6. Endpoint Detection and Response				
Capacidade de monitorizar todos os endpoints, nomeadamente informação relativa a: processos, ficheiros, tráfego de rede, registry e memória. Qualquer atividade relacionada com estes pontos deve ser guardada no mínimo para os últimos 30 dias. Deverá ser possível prolongar esta retenção indefinidamente.				
Com base na informação disponível para os últimos 30 dias, a solução deve ser capaz de detetar máquinas comprometidas, seja com base em análise de processos, ficheiros, registry, e tráfego de rede nas máquinas ou com base na análise do comportamento do utilizador ligado na máquina.				

Permitir ao analista definir regras e pesquisar por padrões relacionados com toda a informação que é retida para os endpoints. Por exemplo, deve ser possível pesquisar por endpoints onde determinada registry key foi modificada. Isto sem ser necessário utilizar ou aprender uma nova query language.				
Quando diferentes alertas estão relacionados, a solução deve ser capaz de os agregar automaticamente em um único incidente.				
Deve ser possível agregar diferentes incidentes num único.				
Quando é identificado um novo incidente, a solução deve ser capaz de automaticamente identificar a root cause do incidente e mostrar toda a sequência de eventos que causou o incidente, assim como todas as alterações introduzidas por estes eventos. Para cada evento deve ser possível visualizar o processo associado, o tráfego de rede gerado por esse processo, os ficheiros acedidos alterados ou criados, qualquer modificação no registry, assim como todos os módulos/DLLs carregados por este processo em memória.				
Para cada incidente, a solução deve indicar: todos os alertas associados a este incidente, todos os artefactos relevantes para a investigação, as máquinas e os utilizadores envolvidos. Cada incidente deve ter uma funcionalidade de chat e de notas para os analistas poderem colaborar entre si.				
Para cada artefacto deve existir informação sobre se há assinaturas válidas para estes, assim como um veredicto sobre o artefacto da própria cloud do fabricante assim como de ferramentas OpenSource (ex:VirusTotal)				
A solução deve mapear os diferentes alertas para a Framework Mitre ATT&CK				
Através de licenciamento adicional, a solução deve ser capaz de ingerir dados da rede do cliente (on-prem e cloud) de forma a ter visibilidade de todo o tráfego de rede e efetuar deteção comportamental sobre a rede, endpoint e cloud numa única solução e interface gráfica. Para recolher o tráfego de rede a solução deve ser capaz de integrar com pelo menos 4 fabricantes de Firewalls.				

Através de licenciamento adicional deve ser possível ingerir logs de identity providers, nomeadamente: AzureAD, Okta e PingID de forma a detetar anomalias nos padrões de autenticação dos utilizadores.				
Deve existir uma funcionalidade de “search&destroy” que permite pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo				
A solução deve aprender o comportamento de cada máquina e criar perfis de forma a ser capaz de identificar comportamentos anômalos				
Com base na aprendizagem comportamental para cada máquina e utilizador a solução deverá ser capaz de gerar alarmística para estes cenários:				
Sessão rara de SSH				
Uso de comandos fora do comum (arp -a, ipconfig, etc)				
processos raros a comunicar com máquinas fora da organização				
processos a comunicar com máquinas externas que não são normalmente acedidas pelas máquinas da organização				
scripts a comunicar com hosts externos				
listagem de utilizadores do domínio				
comando de powershell anormal				
volume de conexões entre máquinas elevado				
Capacidade de reverter automaticamente alterações feitas na máquina por determinado malware. A solução deve listar as alterações feitas por qualquer processo malicioso e permitir reverter essas alterações.				
4. NTA&UEBA				
A solução deve ser capaz de ingerir dados da rede do cliente (on-prem e cloud) de forma a ter visibilidade de todo o tráfego de rede e efetuar deteção comportamental sobre a rede, endpoint e cloud numa única solução e interface gráfica.				
A solução deve poder utilizar como sensores na rede, Firewalls de pelo menos 4 fabricantes distintos.				
Deve ser possível colocar sensores em ambientes de cloud, nomeadamente: AWS, Azure, GCP e Alibaba.				

A solução proposta deve fazer stitching dos logs provenientes dos sensores na rede com os logs dos endpoints de forma a permitir a unificação dos mesmos e simplificar o processo de deteção e investigação de ameaças.				
A solução proposta deverá utilizar Machine Learning para criar perfis das diferentes máquinas e utilizadores na rede de forma a detetar comportamentos anómalos que sejam indicadores de ataques.				
A solução deverá ser capaz de detetar o seguinte tipo de eventos:				
Malware a ser transmitido na rede				
Máquina a enviar SPAM				
Máquina com um número anormal de conexões falhadas para outros endpoints				
Elevado número de conexões para um determinado porto que não corresponde ao perfil				
Port Scan				
Conexões consecutivas entre 2 endpoints que não são normais				
Novo tipo de comportamento administrativo				
Execução remota de comandos				
Reverse Shell				
Tráfico SMB/KRB através de um protocolo inesperado				
DNS Tunneling				
Número anormal de resoluções de DNS falhados				
DGA (Domain Generated Algorithm)				
Command and Control através da análise de pedidos de DNS, URLs e ligações diretas a IPs				
Tunneling				
Volume anormal de dados a ser transferidos				
No caso de ser identificado um comportamento malicioso na rede, deve ser possível obter informação sobre os processos da máquina afetada mesmo que esta não tenha nenhum agente instalado.				
7. Visibilidade sobre as máquinas				
A solução deve incluir um módulo de visibilidade com as seguintes características:				
Capacidade de identificar:				
Utilizadores e grupos configurados em cada máquina				

Serviços a correr nas máquinas				
Drivers instalados nas máquinas				
Processos, drivers, serviços que são automaticamente inicializados sempre que o utilizador liga as máquinas.				
Shares de rede configurados nas máquinas				
Discos existentes nas máquinas				
Funcionalidade de “search&destroy” que permita pesquisar por qualquer documento existente nas máquinas e automaticamente apagar o mesmo				
Identificar vulnerabilidades e respetiva criticidade para ambientes Windows e Linux				
Identificar as aplicações a correr em cada equipamento				
8. Resposta a Incidentes				
A solução proposta deve permitir iniciar scans de malware à máquina infetada				
Deve ser possível efetuar blacklist e whitelists a hashes				
Deve ser possível fazer quarentena a determinados processos				
Durante a investigação de um incidente, a solução deve permitir isolar da rede máquinas infetadas				
A solução deve permitir reverter automaticamente alterações que tenham sido efetuadas por um processo malicioso. Exemplo: Alterar uma registry key para o valor anterior ao comprometimento da máquina.				
Deve existir uma funcionalidade de Live Terminal, onde o analista possa aceder remotamente às máquinas de forma a: gerir os processos e ficheiros, correr scripts Python, correr comandos de Powershell e aceder à linha de comandos da máquina.				
Deve ser possível correr scripts em python sobre todo o parque de máquinas instalado em simultâneo. A solução deve disponibilizar scripts para os use cases mais comuns e permitir a criação de novos scripts.				
Capacidade de criar regras de correlação personalizadas que permitem detectar ataques retroativamente.				

A solução deve incluir uma linguagem de consulta avançada que suporte wildcards, expressões regulares, JSON, agregação de dados, manipulação de campos e valores, agregação de dados de fontes diferentes e visualização de dados.				
--	--	--	--	--