

Procedimento De Ajuste Direto Para Aquisição De Equipamento Informático -Sistema de Firewall, proteção avançada contra ameaças e Consola de Gestão

Capítulo I
Disposições gerais

Cláusula 1ª

Objeto

- 1- O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento de Ajuste Direto para a **Aquisição De Equipamento Informático -Sistema de Firewall, proteção avançada contra ameaças e Consola de Gestão.**
- 2- O objeto do presente contrato consiste no fornecimento e configuração de equipamento informático, nomeadamente: uma appliance firewall, 120 terminais de proteção avançada contra ameaças para postos de trabalho e servidores com uma consola de gestão, de acordo com as características técnicas mínimas exigidas e descritas na Parte II do Caderno de Encargos, com os recursos ativos por 3 anos.
- 3- De acordo com a nomenclatura da referência aplicável aos Contratos Públicos CPV (Vocabulário Comum para os Contratos Públicos) aprovado pelo Regulamento (CE) N°213/2008 de 28 de novembro, o objeto do presente procedimento tem a seguinte classificação: 30200000-1 Equipamento e Material Informático.

Cláusula 2ª

Local de prestação do serviço

O objeto do presente contrato será executado no IDC dos Serviços Técnicos do Município Vila Nova da Barquinha.

Cláusula 3ª

Contrato

- 1- O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
- 2- O contrato a celebrar integra ainda os seguintes elementos:
 - a. Os suprimimentos dos erros e das omissões do Caderno de Encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
 - b. Os esclarecimentos e as retificações relativos ao Caderno de Encargos;
 - c. O presente Caderno de Encargos;
 - d. A proposta adjudicada;
 - e. Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.
- 3- Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual aí são indicados.
- 4- Em caso de divergência entre os documentos referidos no nº2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99º do Código dos Contratos Públicos e aceites pelo adjudicatário nos termos do disposto no artigo 101º desse mesmo diploma legal.

Cláusula 4ª

Prazo

- 1- O contrato mantém-se em vigor desde a data da sua adjudicação e até à entrega da totalidade dos equipamentos a fornecer, de acordo com os respetivos termos e condições e o disposto na

lei, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do Contrato.

- 2- Os equipamentos objeto do presente Caderno de Encargos deverão ser entregues no Município de Vila Nova da Barquinha, no prazo máximo de 30 dias, contados da data da adjudicação.

Cláusula 5ª

Preço base e preço contratual

1. Pela aquisição dos equipamentos objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a Câmara Municipal de Vila Nova da Barquinha obriga-se a pagar ao adjudicatário o valor constante da proposta adjudicada, tendo estabelecido como preço base do presente procedimento o valor de 18.000,00 € (Dezoito mil euros), acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço referido no número um inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, (incluindo despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças).

Capítulo II – Obrigações contratuais

Secção I – Obrigações do Adjudicatário

Subsecção I – Disposições Gerais

Cláusula 6ª

Obrigações e deveres do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos, incluindo Especificações dos equipamentos a fornecer, ou nos artigos contratuais, da celebração do contrato decorrem para o adjudicatário as seguintes obrigações principais:
 - a) Fornecer os equipamentos à Câmara Municipal de Vila Nova da Barquinha, de acordo com as especificações e quantidades constantes na Parte II do presente caderno de encargos;
 - b) Os produtos são fornecidos com os cabos necessários ao seu funcionamento;
 - c) Fazer acompanhar os bens do material de apoio necessário à sua entrada em funcionamento ou utilização;
 - d) Executar os testes que sejam requeridos nas especificações técnicas do presente Caderno de Encargos;
 - e) Disponibilizar, simultaneamente, com a entrega dos bens objeto do contrato, todos os documentos, designadamente relativos à utilização e manutenção, em língua portuguesa;
 - f) Prestar garantia aos bens, mesmo em caso de descontinuidade de fabrico, no mínimo, pelo prazo de dois anos a contar da data de assinatura do auto de receção ou da entrega dos bens, contra quaisquer defeitos ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos, correndo por sua conta os encargos inerentes à colocação do bem em boas condições de utilização;

- g) Os riscos na fase de transporte, acondicionamento, embalagem, carga e descarga da entrega, são da exclusiva responsabilidade do fornecedor;
 - h) Obrigação de prestar todos os esclarecimentos solicitados pela Entidade Adjudicante relacionados com o objeto do contrato;
 - i) A responsabilidade de todos os trabalhos incluídos no Contrato, seja qual for o agente executor, será sempre do Adjudicatário e só dele, não reconhecendo a Entidade Adjudicante a existência de quaisquer outros que trabalhem por conta ou em combinação com o Adjudicatário;
 - j) O Adjudicatário obriga-se a corrigir prontamente os erros e anomalias identificados durante as ações de verificação dos trabalhos, de acordo com as orientações ou esclarecimentos da Entidade Adjudicante, e dentro dos prazos por estes fixados;
 - k) Serão inteiramente de conta do Adjudicatário os encargos e responsabilidade decorrentes da utilização de elementos a que respeitem quaisquer marcas registadas, patentes registadas ou licenças;
2. A título acessório, o adjudicatário fica ainda obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à entrega dos bens contratados, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 7ª

Prazo de execução

1. O adjudicatário obriga-se a executar o contrato no prazo de **3 meses**, a contar a partir da data da adjudicação.
2. O prazo previsto no número anterior pode ser prorrogado por iniciativa da CMVNB ou a requerimento do adjudicatário devidamente fundamentado e aprovado pela CMVNB.

Cláusula 8ª

Receção dos elementos ao abrigo do contrato

1. No prazo de 5 (cinco) dias a contar da entrega dos equipamentos objeto do presente contrato, a CMVNB procede à respetiva análise, com vista a verificar se os mesmos reúnem as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos e na proposta adjudicada, bem como outros requisitos exigidos por lei.
2. Com vista à análise a que se refere o número anterior, o adjudicatário deve cooperar com a CMVNB fornecendo-lhe todos os esclarecimentos necessários.
3. No caso de a CMVNB verificar na análise a que se refere o n.º 1, a desconformidade dos elementos entregues com as exigências legais, ou no caso de existirem discrepâncias com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos, a CMVNB deve de isso informar, por escrito, o adjudicatário.
4. No caso previsto no número anterior, o adjudicatário deve proceder, à sua custa e no prazo razoável que for determinado pela CMVNB às alterações e complementos necessários para garantir o cumprimento das exigências legais e das características, especificações e requisitos técnicos exigidos.

5. Após a realização das alterações e complementos necessários pelo adjudicatário, no prazo respectivo, a CMVNB procede a nova análise, nos termos do **n.º 1**.
6. Caso a análise da CMVNB a que se refere o **n.º 1** comprove a conformidade dos elementos entregues pelo adjudicatário com as exigências legais, e neles não sejam detetadas quaisquer discrepâncias com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos, deve ser emitida, no prazo máximo de 2 (dois) dias a contar do termo dessa análise, declaração de aceitação.
7. No caso de persistirem desconformidades dos elementos entregues com as exigências legais, ou no caso de existirem discrepâncias com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos, repetir-se-á o procedimento descrito no **n.º 3** da presente cláusula.
8. A emissão da declaração a que se refere o número anterior não implica a aceitação de eventuais discrepâncias com as exigências legais ou com as características, especificações e requisitos técnicos previstos no Caderno de Encargos.

Cláusula 9ª

Transferência de propriedade

Com a declaração de aceitação a que se refere o n.º 6 da cláusula anterior, ocorre a transferência da posse e propriedade para a CMVNB, de todos os direitos inerentes aos equipamentos a fornecer ao abrigo do contrato.

Cláusula 10ª

Responsabilidade

1. O adjudicatário assume integral responsabilidade pelos bens contratados, sendo o único responsável perante a CMVNB pela boa prestação e fornecimento dos mesmos.
2. O adjudicatário responde nomeadamente por quaisquer erros, deficiências ou omissões no fornecimento de bens, qualquer que seja a sua origem e qualquer que seja o momento em que forem detetados.
3. Em qualquer altura e logo que solicitado pela CMVNB, o adjudicatário obriga-se a corrigir os erros, as deficiências ou omissões no prazo razoável que lhe vier a ser fixado, sob pena de esta mandar executá-los por conta do adjudicatário, sempre que a responsabilidade dos mesmos lhe seja imputável.

Subseção II – Dever de sigilo

Cláusula 11ª

Objeto do dever de sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa à CMVNB, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.

3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 12ª

Prazo do dever de Sigilo

O dever de sigilo mantém-se em vigor até ao termo do prazo de 5 (cinco) anos a contar do cumprimento ou cessação, por qualquer causa, do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Secção II – Obrigações da CMVNB

Cláusula 13ª

Preço contratual

1. Pelo cumprimento das obrigações constantes do presente Caderno de Encargos, a CMVNB deve pagar ao adjudicatário o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, nomeadamente quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.

Cláusula 14ª

Condições de pagamento

1. A quantia devida pela CMVNB, nos termos da cláusula anterior, deve ser paga num prazo de 30 (trinta) dias após a receção pela CMVNB da respetiva fatura.
2. Em caso de discordância por parte da CMVNB, quanto aos valores indicados nas faturas, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o adjudicatário obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.

Capítulo III – Penalidades contratuais e resolução

Cláusula 15ª

Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a CMVNB pode exigir do adjudicatário o pagamento de uma pena pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
 - a) Pelo incumprimento das datas e prazos de entrega dos elementos referentes ao contrato, até 1% (um por cento) do valor do contrato;
2. Em caso de resolução do contrato por incumprimento do adjudicatário, a CMVNB pode exigir-lhe uma pena pecuniária de até 10% (dez por cento) do valor do contrato.

3. Na determinação da gravidade do incumprimento, a CMVNB tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.
4. A CMVNB pode compensar os pagamentos devidos ao abrigo do contrato com as penas pecuniárias devidas nos termos da presente cláusula.
5. As penas pecuniárias previstas na presente cláusula não obstam a que CMVNB exija uma indemnização pelo dano excedente.

Cláusula 16ª

Força maior

1. Não podem ser impostas penalidades ao adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;
 - e) Incêndios ou inundações com origem nas instalações do adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do adjudicatário não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 17ª

Resolução por parte do contraente público

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a CMVNB pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem, designadamente nos seguintes casos:
 - a) Pelo atraso na entrega dos elementos referentes ao contrato superior a 3 (três) meses ou declaração escrita do adjudicatário de que o atraso respetivo excederá esse prazo;
2. O direito de resolução referido no número anterior exerce-se mediante declaração enviada ao adjudicatário.

Cláusula 18ª

Resolução por parte do adjudicatário

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, o adjudicatário pode resolver o contrato quando:
 - a) Qualquer montante que lhe seja devido esteja em dívida há mais de 90 (noventa) dias ou o montante em dívida exceda 20% (vinte por cento) do preço contratual, excluindo juros;
2. O direito de resolução pode ser exercido mediante declaração enviada à CMVNB que produz efeitos 30 (trinta) dias após a receção dessa declaração, salvo se este último cumprir as obrigações em atraso nesse prazo, acrescidas dos juros de mora a que houver lugar.

Capítulo IV – Resolução de litígios

Cláusula 19ª

Legislação aplicável e Foro competente

1. Em tudo o que o Contrato for omissos observar-se-á o disposto no Código dos Contratos Públicos e demais legislação aplicável e, em qualquer caso, sempre a Lei Portuguesa.
2. Para resolução de todos os litígios decorrentes do contrato fica estipulado o Tribunal Administrativo de Leiria, com expressa renúncia a qualquer outro.

Capítulo V – Disposições finais

Cláusula 20ª

Subcontratação e cessão da posição contratual

A subcontratação pelo adjudicatário e a cessão da posição contratual por qualquer das partes depende da autorização prévia e por escrito da outra, nos termos do Código dos Contratos Públicos.

Cláusula 21ª

Publicidade

O adjudicatário não poderá fazer ou consentir qualquer espécie de publicidade relacionada com o presente contrato, sem a prévia autorização da CMVNB.

Cláusula 22ª

Comunicações e Notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato.

2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 23ª

Contagem dos prazos

Aos prazos estabelecidos no presente caderno de encargos aplica-se o estipulado no artigo 471º do Código dos Contratos Públicos.

Cláusula 24ª

Legislação aplicável

A tudo o que não esteja especialmente previsto aplica-se o regime previsto no Decreto-Lei n.º 18/2008, de 29 de Janeiro, na redação que lhe foi dada pelo Decreto-Lei nº111-B/2017, de 31 de agosto e demais legislação aplicável.

Vila Nova da Barquinha, __ de _____ de 2022

O Presidente da Câmara Municipal

FERNANDO
MANUEL DOS
SANTOS FREIRE

Assinado de forma digital
por FERNANDO MANUEL
DOS SANTOS FREIRE
Dados: 2022.08.31 09:35:01
+01'00'

Fernando Manuel dos Santos Freire

PARTE II

CARACTERÍSTICAS E ESPECIFICAÇÕES TÉCNICAS DO EQUIPAMENTO

Firewall

Pretende-se o fornecimento de uma firewall e que incorpore uma plataforma de gestão capaz de gerir e monitorizar outros equipamentos instalados local ou geograficamente dispersos. Toda a componente de reporting da solução a adquirir no âmbito deste procedimento deverá ser parte integrante da solução. O equipamento a propor deverá cumprir os seguintes requisitos:

- O fabricante deverá ter no mínimo 20 anos de experiência no mercado da segurança, e desenvolver em exclusivo, apenas soluções de segurança;
- O fabricante deverá comprovar a sua liderança em soluções de segurança (UTM, Firewall e prevenção de intrusões) ano após ano, em análises/relatórios de entidades independentes;
- O fabricante deverá endereçar todos os requisitos de um equipamento de segurança (Firewall), tais como processamento de largura de banda, número de ligações, capacidade de securização de aplicações de nova geração em todas as vertentes da rede (escritório, centro de dados) num único equipamento;
- O fabricante deverá disponibilizar as mesmas funcionalidades de inspeção avançada (Firewall, intrusion prevention, application control, URL filtering, Anti-Bot, Anti-Virus, Sandboxing) geridas localmente ou por uma única consola central;
- A solução proposta, deverá endereçar todas as funcionalidades que se seguem, de forma unificada, suportadas e desenvolvidas somente pelo mesmo fabricante (single vendor):
 - ✓ Statefull Inspection Firewall - A gateway deverá inspecionar end-to-end (não apenas “half-way” ou “header”) todos os fluxos de comunicação desde o estabelecimento da sessão (3-way handshake TCP), durante a transferência de informação (payload), até que esta seja terminada;
 - ✓ Intrusion Prevention System;
 - ✓ User Identity Acquisition
 - ✓ Application Control and URL filtering
 - ✓ Anti – Bot / Anti – Virus
 - ✓ Anti – Spam and Email Security
 - ✓ IPSec VPN

- ✓ Remote Access VPN (Mobile Access)
- ✓ Logging and Status
- ✓ Event Correlation and Reporting
- A solução proposta, não poderá em momento algum “sacrificar” a segurança em detrimento da performance (desabilitar inspeção end-to-end em cenários de “carga” na plataforma);
- A solução proposta deverá conter uma plataforma de gestão dedicada com:
 - ✓ Centralização de políticas, logs, reports;
 - ✓ Sem limite de storage com base em requisitos de licenciamento;
- A solução proposta, não poderá em momento algum “sacrificar” a segurança em detrimento da performance (desabilitar inspeção end-to-end em cenários de “carga” na plataforma);
- A solução proposta deverá conter uma plataforma de gestão dedicada com:
 - Centralização de políticas, logs, reports;
 - Sem limite de storage com base em requisitos de licenciamento;
 - O servidor de gestão deverá ter a capacidade de obter detalhes de configuração diretamente da gateway de firewall (fetch de informação de routing, interfaces, etc.) de forma “automática”, e não apenas se estas forem instanciadas previamente via template, a partir do servidor de gestão;

Requisitos Mínimos de Performance

- | | |
|-------------------------------|---------------|
| • Threat Prevention | >=2.0 Gbps |
| • NextGen Firewall | >=5.0 Gbps |
| • Intrusion Prevention System | >= 5.5 Gbps |
| • VPN Throughput | >= 4.0 Gbps |
| • Firewall Throughput | >= 17.00 Gbps |
| • Connections per second | >=66k |
| • Concurrent Connections | >=2.4 M |

Requisitos físicos

- Disco SSD de 256 GB com slot para cartões Micro-SD de 32 e 64 GB;
- Interfaces;
 - ✓ WAN:
 - 2x1GE UTP;
 - 2x1GE SFP;
 - ✓ DMZ:
 - 1x10GE UTP;
 - 1x10GE SFP+;
 - ✓ LAN:
 - 2x2.5GE UTP plus;
 - 16x1GE UTP;
- Fontes de alimentação (PSU) redundantes: 110-240VAC:
 - ✓ Potência de 150 W;
 - ✓ Consumo máx. 93.6 W;
- Dimensões:
 - ✓ Largura x Altura x Profundidade (mm): 430 x 300 x 44.2
 - ✓ Peso (kg): 6.76

Requisitos - Funcionalidades de rede

- Suporte para interfaces vlan;
- Suporte para protocolos de agregação de links (LACP 802.3ad);
- Suporte para funcionamento em modo L2 (bridging) e L3 (routing);
- Suporte de NAT
 - ✓ Static, Hide, PAT;
 - ✓ NAT44, NAT46, NAT64, NAT66;
- Suporte para routing estático;
- Suporte para Policy Based Routing (PBR);
- Suporte para protocolos de routing dinâmico:
 - ✓ BGP, OSPF, RIP;
 - ✓ Suporte para multicast;

- Routing Multicast;
 - ✓ L2 (IGMP);
 - ✓ L3 (PIM-SM, PIM-SSM, PIM-DM);

Requisitos de alta disponibilidade

- Activo/Passivo ou Activo/Standby:
 - ✓ Failover:
 - Falhas de routing;
 - Falhas de dispositivo;
 - Falhas de link;
 - ✓ Sincronização de sessões entre membros do cluster;

Requisitos técnicos/lógicos

- O equipamento de segurança, deve utilizar a tecnologia de Stateful Inspection, para construir e manter a tabela de sessões (fluxos de comunicação).
- O Equipamento de segurança deve ser capaz de suportar o debito, número de novas ligações e manutenção das mesmas de acordo com as necessidades do cliente.
- A solução deve identificar/controlar o acesso de pelo menos 150 serviços/protocolos.
- A solução tem de suportar que se apliquem regras em intervalos de tempo, para que seja possível definir o tempo útil das mesmas.
- A Firewall tem de suportar métodos de autenticação por sessão, utilizadores e clientes.
- A solução tem de ter base de dados de utilizadores local, para permitir a autenticação e autorização dos mesmos sem recurso a um dispositivo externo;
- A solução tem de suportar as funções de DHCP server e Relay;
- A solução tem de ter capacidade de trabalhar em modo transparente/Bridge (L2);

Sistema de prevenção de intrusões (IPS)

- O fabricante deve fornecer evidências da sua posição de liderança, ano após ano, no Quadrante Mágico do Gartner para:
 - ✓ Soluções de Prevenção de Intrusão
 - ✓ Soluções de Firewall Enterprise

- O IPS deve ser baseado nos seguintes mecanismos de detecção:
 - ✓ Assinaturas
 - ✓ Anomalias no protocolo
 - ✓ Controlo Aplicacional
 - ✓ Analise de comportamento
- Os Módulos de IPS e firewall devem estar integrados na mesma plataforma.
- O administrador deve ter a possibilidade de configurar a inspeção para proteção apenas da rede interna.
- O IPS deve ter opções para criar perfis com base em assinaturas para proteção de Clientes ou servidores. Também deve ser possível criar um perfil para proteção de ambos.
- O IPS deve fornecer pelo menos dois perfis/políticas predefinidas que podem ser utilizados no deployment da solução.
- O IPS deve ter um mecanismo fail-open baseado em software, ajustável com base em limites do gateway, CPU ou utilização de memória.
- O IPS deve ter mecanismo automático para ativar ou gerir as novas assinaturas após atualizações.
- O IPS deve suportar exceções com base em origem, destino, protocolo, ou uma combinação dos três.
- O IPS deve permitir mudar para o modo de detecção, sem alterar parâmetros individuais, por forma a facilitar as ações de troubleshooting.
- O IPS deve possuir uma solução centralizada de relatório de eventos.
- O administrador deve poder ativar de forma automática novas proteções, com base em parâmetros configuráveis:
 - ✓ Impacto no desempenho;
 - ✓ Grau de severidade da ameaça;
 - ✓ Nível de confiança;
 - ✓ Proteções do cliente;
 - ✓ Proteções do servidor;
- O IPS deve ser capaz de detetar e prevenir os seguintes tipos de ameaça:
 - ✓ Uso indevido de protocolo;
 - ✓ Comunicações de malware;
 - ✓ Tentativas de uso de protocolos de tunneling;

- ✓ Tipos genéricos de ataque sem assinaturas predefinidas;
- Para cada proteção, a solução deve incluir o tipo de proteção (relativamente a servidor ou cliente)
 - ✓ Gravidade da ameaça;
 - ✓ Impacto no desempenho;
 - ✓ Nível de confiança;
 - ✓ Referência - (ie CVE);
- O IPS deve ser capaz de detetar e bloquear ataques nas layers de network e application layer, protegendo pelo menos os seguintes tipos de serviços:
 - ✓ Serviços de email;
 - ✓ DNS;
 - ✓ FTP;
 - ✓ Serviços do Windows (Microsoft Networking);
- O fornecedor deve fornecer evidências de liderança na proteção de vulnerabilidades Microsoft.
- O IPS e/ou o Application Control deve incluir a capacidade de detetar e bloquear aplicações P2P e evasivas (Anonymizers).
- O administrador deve poder definir exclusões a plataforma de IPS, baseadas em redes ou hosts.
- A solução deve proteger DNS Cache Poisoning e impedir o acesso dos utilizadores a endereços de domínio bloqueados.
- Solução deve fornecer proteções para protocolos VOIP.
- O IPS e/ou o Application Control devem detetar e bloquear aplicações que permitam controlo remotos, incluindo as que são capazes de realizar tunneling sobre o tráfego HTTP.
- IPS deve ter proteções SCADA.
- IPS deve possibilitar a conversão de assinaturas SNORT.
- A solução deve permitir ao administrador bloquear de forma fácil o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os intervalos de IP correspondentes ao país.

Aquisição de identidade de utilizadores (User ID Acquisition)

- Deve ser capaz de adquirir a identidade dos utilizadores, com base na consulta dos eventos de segurança da Microsoft Active Directory.

- Deve ser possível a autenticação através de uma browser, numa base de dados local, para utilizadores ou dispositivos que não pertençam ao domínio.
- A solução deve integrar-se perfeitamente com Microsoft Active Directory.
- O impacto do uso da solução de aquisição de identidade no CPU das AD, deve ser inferior a 3%.
- A solução deve permitir a identificação de utilizadores que acedem através de um proxy (exemplo: X-forwarded headers).
- Deve ser capaz de adquirir a identidade de um utilizador presente numa Microsoft Active Directory sem qualquer tipo de agente instalado no controlador de domínio.

Filtragem de URL e Controlo de Aplicações

- A solução deve reconhecer e controlar mais de 6000 aplicações conhecidas.
- A base de dados da solução deve conter mais de 200 milhões de URL's categorizados, abrangendo mais de 85% da Alexa's top 1M sites.
- A solução deve permitir criar uma regra de filtragem de conteúdos com várias categorias.
- A solução deve permitir filtrar conteúdos de URL's baseada em HTTPS sem efetuar inspeção de SSL.
- A solução deve ser capaz de filtrar um único site sendo este identificado em várias categorias.
- A solução deve permitir criar regras de segurança por utilizador ou grupo de utilizadores.
- A solução, após 4 semanas de produção, deve ter em cache cerca de 99% das solicitações de categorização.
- A solução deve ter uma interface fácil de pesquisa de aplicações e URL's.
- A solução deve categorizar aplicações e URL's por fator de risco
- A política de URLF e Application Control deve poder ser definida por identidade do utilizador.
- A base de dados de URLF e Application Control devem ser atualizados por um serviço Cloud.
- A solução deve ter o controlo de aplicações e URLF unificado na mesma política.
- A solução deve ter mecanismos para informar ou perguntar ao utilizador em tempo real, para os educar ou para confirmarem as suas ações com base na política de segurança.
- A solução deve ter mecanismo que permita limitar o uso de aplicações com base no consumo de largura de banda.
- A solução deve permitir exceções com base em objetos de rede previamente definidos.

- A solução deve fornecer a opção de modificar a página de Bloqueio e redirecionar o utilizador para uma página de remediação.
- A solução deve incluir um mecanismo de Black e White List, para permitir que se negue ou permita URL's específicos, independentemente da categoria.
- A solução deve fornecer um mecanismo de substituição na categorização de URL.

Anti-bot e Anti-Virus

- O fornecedor deve ter solução de Anti-Bot e Anti-Virus integrado na firewall.
- A Solução de Anti-Bot deve ser capaz de detetar e parar comportamentos de rede suspeitos.
- O aplicativo Anti-Bot deve usar um mecanismo de detecção baseado em varias pontos. Reputação de endereços IP, URLs e DNS e detectar padrões de comunicação de bots.
- A proteção Anti-Bot deve ter capacidade de efetuar Scan a ações de bot.
- A solução deve apoiar a detecção e prevenção de vírus e variantes de Cryptors & ransomware (por exemplo, Wannacry, Cryptlocker, CryptoWall ...) através do uso de análise estática e/ou dinâmica.
- A solução deve ter suporte para proteção contra-ataques de spear phishing
- DNS based attacks - A solução deve ter recursos de detecção e prevenção para C&C DNS hideouts:
 - ✓ Pesquisa de padrões de tráfego de C & C, não apenas no destino de DNS
 - ✓ Reverse engineer do Malware para descobrir seu DGA (Domain Name Generation)
 - ✓ DNS Trap, como parte da política de ameaças, interceta e analisa tentativas de comunicações do endpoint com C&C.
 - ✓ A solução deve detetar e prevenir ataques de DNS tunneling.
- A política de Anti-Bot e Anti-Virus deve ser gerida a partir de uma consola central.
- A solução de Anti-Bot e Anti-Virus deve ter um mecanismo centralizado de relatório de eventos.
- A solução de antivírus deve ser capaz de impedir o acesso a sites maliciosos.
- A solução de antivírus deve poder inspecionar o tráfego SSL.
- O Anti-Bot e o Anti-Virus devem ter atualizações em tempo real na cloud.
- O Antivírus deve ser capaz de impedir a entrada de arquivos maliciosos.
- O Antivírus deve ser capaz de analisar arquivos compactados.

- Políticas antivírus e Anti-Bot devem ser geridas centralmente e ser possível a parametrização das mesmas.
- O Antivírus deve suportar a análise de links dentro de emails.
- O antivírus deve analisar os ficheiros que estão a passar no protocolo CIFS.

Anti-Spam & Email Security

- A solução deverá ser agnóstica em relação ao conteúdo, e ter a capacidade de classificar ameaças em tempo real, protegendo a infraestrutura com base em padrões comportamentais, e não com base em conteúdo;
- A solução proposta deverá incluir mecanismos de proteção com base em serviços online de IP reputation, de forma a evitar falsos positivos;
- A solução deverá incluir mecanismos de proteção imediata (zero-hour) para novos vírus propagados por email e spam.

IPsec VPN

- A solução deverá suportar implementações de VPN (domain based, e route based com protocolos de routing dinâmico e virtual tunnel interfaces), com utilização de Internal Certificate Authority ou External 3rd party Certificate Authority;
- A solução deverá suportar criptografia 3DES e AES-256 para IKE Phase 1 e 2.
- A solução deverá suportar criptografia IKEv2 plus "Suite-B-GCM-128" e "Suite-B-GCM-256" for IKE Phase 2;
- A solução deverá suportar os seguintes grupos Diffie-Hellman: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20;
- A solução deverá suportar os seguintes tipos de mecanismos de integridade de dados: md5, sha1, SHA-256, SHA-384 and AES-XCBC;
- A solução proposta deverá suportar as funcionalidades de VPN Site-to-Site.
- Suporte para 500 VPN's de acesso remoto "clientless" e "client based";
- Suporte para aplicação de políticas de segurança específicas, para controlo de tráfego associado à comunidade VPN;

Deteção de atividades em sistema

- A solução deve ter a capacidade de detetar atividades fora de “padrão de utilização/protocolo”:
 - ✓ Chamadas de API
 - ✓ Alterações no sistema de arquivos
 - ✓ Alterações de Registo
 - ✓ Ligações de rede
 - ✓ Em Processos do sistema Operativo
 - ✓ Criar e eliminar arquivos
 - ✓ Modificação de arquivos
 - ✓ Adição de código ao kernel
 - ✓ Detetar tentativas de elevação de privilégios
 - ✓ Alterações no kernel (Alterações de memória realizadas pelo código do kernel, não o fato de que um driver ser carregado - isso é controlado pelo item acima)
 - ✓ Analise de comportamento do kernel (analisar a atividade do código, não as alterações efetuadas pelo utilizador)
 - ✓ Contornar UAC (user access control)

Mecanismos Anti-evasão

- A solução proposta deverá ter capacidade de deteção de técnicas de evasão (emulação/sandboxing) para posterior reação e mitigação de ameaças;
- A solução deverá ser resiliente e identificar casos onde a execução de código malicioso (malware/shell-code) não ocorra mediante a deteção de um ambiente virtualizado (técnica de evasão para contornar mecanismos de deteção por sandboxing);
- A solução deverá ser resiliente e detetar delays implementados na execução de código malicioso (malware/shell-code);
- A solução deverá ser resiliente a situações em que a execução de código malicioso (malware/shell-code) apenas ocorre após um restart/shutdown da workstation/endpoint infetado;

Logging e Monitorização

- A solução de logging, deverá estar integrada na componente de gestão centralizada, e possibilitar a visualização de logs afetos a políticas, sem ser necessário recorrer a uma nova janela, ou aplicação;
- A solução deverá poder ser integrada na componente de gestão centralizada, ou numa appliance/máquina virtual dedicada;
- A solução deverá ter a capacidade de produzir logs de todas as políticas;
- A solução deverá ter a capacidade de consolidar os logs de todas as componentes de segurança que se encontrem ativas na plataforma: IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, User Identity, Mobile Access;
- A solução deverá implementar um mecanismo seguro de forwarding de logs, com autenticação e encriptação, para evitar potenciais ataques (ex. Eavesdropping);
 - ✓ Os logs deverão ser transferidos de forma segura entre a FW gateway, o log server, e o utilizador final;
- A solução deverá disponibilizar detalhes sobre o estado de todos os túneis IPSEC, site-to-site e remote access (client-to-site);
- A solução deverá possibilitar a customização de valores de threshold, para execução de ações, uma vez atingido/ultrapassado esse threshold: log, alert, snmp-trap, email notification;

Reporting

- A solução deverá ter uma parte de reporting e correlação de eventos com a sua componente de gestão;
- A solução deverá ter a capacidade de correlacionar eventos de todas as funcionalidades ativas nas demais gateways (FW, IPS, URL-F, etc.);
- A solução deverá disponibilizar um mecanismo para assignar os filtros criados a diferentes tipos de gráficos, a serem atualizados periodicamente, apresentando todos os eventos que igualem o filtro aplicado, permitindo ao operador focar-se nos eventos mais importantes;
- A solução deverá incluir relatórios horários, diários, semanais e mensais predefinidos, incluindo pelo menos: Top Events, Top Sources, Top Destinations, Top Services, etc.;
- A solução de reporting deverá disponibilizar informação consolidada sobre:

- ✓ Top de origens bloqueadas, e os destinos e serviços respetivos;
- ✓ Top de regras mais utilizadas na política de segurança;
- ✓ Top de ataques detetados no perímetro, com informação das origens e destinos associados;
- ✓ Atividade web por user, com top de web users e websites mais utilizados;

SSL Inspection (inbound / outbound)

- A solução deverá suportar inspeção SSL (inspection/decryption) com performance comprovada em todas as tecnologias de mitigação;
- A solução deverá suportar Perfect Forward Secrecy (PFS , ECDHE cipher suites);
- A solução deverá suportar AES-NI,AES-GCM for improved throughput;
- A solução deverá suportar a integração das tecnologias de emulação/sandboxing com inspeção SSL;
- A solução deverá permitir a reutilização da base de dados de URL Filtering, para criação de políticas de inspeção de SSL granulares;

Suporte e Manutenção

O suporte e manutenção, deve ser assegurado diretamente pelo fabricante. A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluído peças e mão-de-obra.

- SLA 24x7 com tempo de resposta nas instalações no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria.

Proteção avançada contra ameaças

Pretende-se o fornecimento de uma solução de proteção avançada contra ameaças para 120 postos de trabalho e servidores. A solução a propor deverá cumprir os seguintes requisitos:

Requisitos Gerais

- A solução deverá ser capaz de detectar e impedir o malware no estágio de exploração, usando Sandboxing e Emulação em ambientes virtuais. Esta emulação deverá utilizar duas camadas de detecção de exploits:
 - ✓ Tecnologia ao nível do CPU - Permite a detecção de explorações antes do malware ser executado.
 - ✓ Camadas de detecção adicionais que detectam comportamentos maliciosos e anómalos ao nível do SO.
 - ✓ Ficheiros que contêm exploits são impedidos de fazer download para a máquina. Se os ficheiros já estiverem na máquina, os mesmos serão colocados em quarentena.
- A solução deverá ser capaz de executar o malware num ambiente seguro fornecendo uma forte proteção estática e dinâmica de primeira linha, usando assinaturas e análises comportamentais. Utilizando a emulação de ameaças, que inclui tecnologias de detecção para identificar malware desconhecido para o qual não existem assinaturas. Deverá também fornecer uma camada adicional de prevenção de malware e ameaças, com uma proteção proativa de ameaças desconhecidas e de zero-day. A solução deverá suportar dois mecanismos principais de limpeza de ficheiros:
 - ✓ Manter o tipo de ficheiro - entrega o ficheiro no seu formato original, removendo qualquer conteúdo ativo, como macros.
 - ✓ Converter em PDF - os arquivos entregues aos utilizadores devem ser convertidos para o formato PDF. O acesso ao ficheiro original deverá ser garantido apenas após emulação do mesmo num ambiente seguro.
- A solução deverá ser capaz de bloquear proativamente a comunicação de Centros de Comando e Controlo (C&C) com a máquina e interromper a exfiltração de dados. A comunicação com os C&C deverá ser identificada e bloqueada - evitando ações de malware, progresso de ataques e exfiltração de dados. Os processos que tentam comunicação com C&C devem ser encerrados e o executável colocado em quarentena. As máquinas identificadas como infectadas devem ser isoladas da rede - impedindo movimentos laterais, acesso a dados em servidores e comunicações C&C.
- A solução deverá ser capaz de remediar a infecção de pelo menos duas maneiras: correção automática e correção manual. A correção deve incluir várias opções:

- ✓ Quarentena de ficheiros maliciosos - a detecção pelos mecanismos de Anti-Bot, emulação de ameaças e Anti-Ransomware devem acionar a quarentena automática dos ficheiros maliciosos.
- ✓ Remoção automática de malware - recurso automatizado de análise forense, que identifica todos os elementos de um ataque. Com base nessa análise, uma ação automatizada pode ser executada para remover todos os processos não respeitáveis que fazem parte do ataque. Também deve encerrar processos confiáveis que são usados de maneira maliciosa.
- ✓ Remoção de malware baseado em script - recurso automatizado de análise forense, que identifica todos os elementos de um ataque. Com base nessa análise, o produto pode gerar um script de remoção que pode ser usado em todos os hosts infectados para remover uma infecção generalizada. O script executa as mesmas ações que a opção de remoção automática de malware.
- ✓ Análise forense automatizada fornecida pelo produto deve permitir a correção refinada com base no entendimento profundo do ataque que é entregue pelo produto.
- ✓ Análise forense automatizada, fornecida pelo produto, mostra o ponto exato de entrada. Ele deve permitir que o administrador reforce a segurança para impedir que o mesmo vetor seja bem-sucedido em ataques futuros.
- A solução deve ter a capacidade de alavancar a inteligência em tempo real de bases de dados de ameaças alojadas numa nuvem comercial e/ou governamental (hash, assinatura, endereço IP, DNS, certificado digital e outros serviços de reputação) para detectar e/ou bloquear atividade maliciosa nas máquinas. O produto deve suportar fontes de inteligência adicionais de fornecedores externos.
- A solução deve verificar as máquinas quanto ao estado no nível do patch ou atualizações/patches específicos. A componente de compliance deve ter a capacidade de verificar as configurações do registro na máquina local. Deve abranger atualizações e patches da Microsoft em várias versões do sistema operativo Windows.
- A "footprint" da solução deve ter os seguintes requisitos:
 - ✓ O aumento da carga da CPU no intervalo de 0% a 5%.
 - ✓ O consumo de memória de até 300 MB.
 - ✓ O uso do disco é feito com as configurações padrão de até 3 GB.
 - ✓ A solução deve suportar os seguintes sistemas operativos, versões e máquinas:
 - ✓ Windows 7 32/64bit

- ✓ Windows 8 32/64bit
- ✓ Windows 8.1 32/64bit
- ✓ Windows 10 32/64bit
- ✓ Windows 11 64bits
- ✓ Windows 2008 R2 e todas as versões posteriores dos servidores Windows
- ✓ MacOS Sierra 10.12
- ✓ MacOS High Sierra 10.13
- ✓ MacOS Mojave 10.14
- ✓ MacOS Catalina 10.15
- A solução deve ter logging que registre todas as ações de gestão. Por exemplo: alterações na gestão de políticas, provisionamento de utilizadores e máquinas, alterações de administradores, login/logout de administrador, etc. Todas as detecções e proteções das máquinas devem ser registadas. Por exemplo: detecção e prevenção de malware por emulação/extração de ameaças, Anti-Bot (incluindo relatório completo), relatório de análise de ataque forense, ações de remediação e quarentena, etc.
- A solução deve gerar alertas para administradores com base em eventos de log e fornecer granularidade total. Os alertas devem ter opção de ser configurados para serem enviados como notificação por email que pode gerar notificações de push, SMS, etc. O logging deve poder ser integrado com todos os principais produtos de SIEM, que fornecem sua própria camada de alerta e granularidade. O produto também deve fornecer alertas aos utilizadores finais sobre qualquer infecção detectada.
- A solução deve fornecer a capacidade de bloquear ligações de/para serviços, portas e endereços IP específicos numa base por processo ou função e fornecer as atividades ao servidor de gestão.
- A solução deve registrar e/ou controlar o acesso a máquinas removíveis com base num conjunto de regras especificadas e enviar as atividades ao servidor de gestão. Deve fornecer controlo granular para periféricos e máquinas de armazenamento. Todos os periféricos e acessos a máquina de armazenamento devem ser registados no sistema.

Administração Remota

- A solução deve poder ser instalada e desinstalada manualmente. A instalação deve ser feita usando pacotes MSI. A desinstalação, deve ser protegida por autenticação de dois fatores (Token).

- A solução deve permitir a instalação automática (instalador próprio, SCCM, EPO, etc.). A solução deve ser facilmente integrada com as ferramentas de instalação de terceiros, como o SCCM. A instalação alternativa pode ser feita via cliente de instalação inicial, que deve permitir instalações adicionais de software de acordo com a política definida.
- A solução deve ter a opção de ser iniciada e parada remotamente. Os componentes de segurança relevantes devem ser removidos usando a opção de instalação de software ou desativados através da política.
- A solução deve transferir logs de/para as máquinas. Os logs devem poder ser extraídos usando a operação push. Essa funcionalidade deve ser controlada pela configuração da política.
- As atualizações da solução devem poder ser realizadas através da consola de gestão ou apenas por meio ferramentas de instalação de software para desktop (por exemplo, SCCM). As atualizações do cliente devem ser feitas utilizando os servidores de gestão ou usando pacotes de atualização com ferramentas de instalação de software, como o SCCM.
- A solução deve fornecer a capacidade de reverter para versões anteriores após correções e atualizações. A solução deve oferecer um mecanismo de gestão de patches do cliente que pode ser revertido a qualquer momento através de um processo autenticado.
- A solução deve ter proteção contra acessos e modificações não autorizadas/ mal-intencionadas, esta proteção deve ter tecnologia de autoproteção baseada em kernel incorporada.

Integração

- A solução deve fornecer integração com o Splunk, McAfee Nitro ou qualquer outro sistema SIEM (Security Information and Event Management). A exportação de dados para produtos externos deve ser feita via APIs OPSEC.
- A solução deve fornecer integração aos sistemas de suporte técnico e sistemas de gestão de incidentes (por exemplo, JIRA, Remedy, ServiceNow etc.). A solução proposta deve poder integrar sistemas de ticketing.
- A solução deve poder proteger downloads efetuados na Internet antes de serem descarregados para a máquina. A solução deve proteger proativamente os utilizadores em tempo real contra ataques de malware avançados descarregados por meio de navegadores da Web. A solução deve permitir descarregar o ficheiro para o utilizador e entregar o conteúdo reconstruído e seguro em segundos, ao mesmo tempo deve enviar o ficheiro original para a análise e se o ficheiro for

considerado seguro, o utilizador poderá fazer o download do ficheiro original sem a assistência do administrador ou do suporte técnico.

- A solução deve fornecer recursos anti-phishing e proteção de formulário da web. A solução deve poder bloquear o acesso a sites de phishing, bloqueando ataques de phishing desconhecidos e de zero-day, visando as credenciais do utilizador, verificando todos os campos do formulário e verificando a sua validade (isso deve ser feito em tempo real, com pouco ou nenhum efeito para a experiência do utilizador). A solução também deve alertar sobre a reutilização de senhas corporativas em sites externos.

Prevenção/Deteção de Malware & Exploit

- A solução deve proteger o sistema com as seguintes funcionalidades:
 - ✓ Utilização de sandboxing/emulação, que monitoriza todas as atividades de malware e detecta a instalação do mesmo como parte da análise de malware resistente à evasão.
 - ✓ O sistema de monitorização de ficheiros deve identificar um ficheiro gravado no sistema como parte da instalação do malware e deve envia-lo para emulação.
 - ✓ A instalação de malware geralmente inclui o download de malware adicional para comunicação com Centros de Comando e Controlo (C&C). Esta comunicação deve ser detectada e bloqueada pelo Anti-Bot.
 - ✓ Ficheiros maliciosos gravados durante o processo de instalação devem colocados em quarentena.
 - ✓ O recurso de análise forense automatizada deve identificar todas as etapas da instalação do malware, fornecendo um relatório destacando todos os elementos de malware instalados e adicionando um recurso para executar desinfecção precisa automaticamente.
 - ✓ Anti-Virus deve detectar o malware usando a análise comportamental estática e dinâmica, cobrindo a instalação do malware.
 - ✓ A entrega na forma de um documento deve ser higienizada com a Extração de ameaças - para que os utilizadores recebam ficheiros com o conteúdo enviado, mas sem os elementos maliciosos incorporados no conteúdo.
 - ✓ A entrega na forma de executáveis deve ser tratada pela proteção de Sandboxing/Emulação de Ameaças para detecção avançada de ataques que não são baseados em assinaturas.
 - ✓ Todos os elementos do ataque devem ser revelados após a análise forense automatizada.

- A solução deve ter uma detecção avançada baseada na emulação de ameaças, que deve utilizar vários métodos avançados de detecção que não são baseados em assinaturas. Algumas tecnologias devem incluir:
 - ✓ Tecnologia ao nível do CPU - monitoriza o fluxo de execução dos programas ao nível do CPU, permitindo a detecção de exploits de zero-day, antes que qualquer código malicioso possa ser executado e, portanto, antes que a evasão possa ser tentada.
 - ✓ Mecanismo de inteligência artificial - utilizado para análises estáticas e dinâmicas com base numa extensa plataforma de aprendizagem para detecção de malware zero-day.
 - ✓ Mecanismo comportamental avançado - monitoriza vários indicadores de SO durante o tempo de execução.
- A solução deve permitir uma extração de ameaças adotando uma abordagem proativa, fornecendo ficheiros higienizados aos utilizadores. Devem existir dois modos principais para esta abordagem:
 - ✓ Manter o formato do ficheiro - componentes ativos e potencialmente maliciosos, como macros, devem ser removidos do documento original. O ficheiro é reconstruído, simplificando a sua estrutura. A maioria dos ataques de zero-day devem poder ser evitados com essa abordagem.
 - ✓ Converter em PDF - nesse modo, todos os documentos são convertidos em PDF antes da entrega. A extração de ameaças deve ser uma proteção prática que permite a entrega rápida de ficheiros aos utilizadores. Os utilizadores devem ter acesso automático e simples ao ficheiro original, caso precisem, mas somente depois que ele passar pelos mecanismos de Sandboxing/Emulação e se mostrar limpo.
- A solução deve fornecer uma análise forense para analisar e revelar o ataque completo e as suas ameaças maliciosas ou interpretações suspeitas. Isso deve incluir a capacidade de rastrear os relacionamentos entre componentes de ataque, injeções de memória, etc. A análise deve ser realizada automaticamente ao longo de semanas e meses de atividade, abrangendo inicializações do sistema e rastreando processos de persistência de malware.
- A solução deve ter a capacidade de impedir que tipos de malware ransomware e cryptolocker possam criptografar o sistema de ficheiros de uma máquina. Deve detetar o comportamento deste tipo de ataque, como excluir cópias de sombra, processos elevados das pastas temporárias, alterações nos registros MBR etc., descobrir essas ações deve acionar o Anti-Ransomware para bloquear a criptografia antes de ela começar.

- Caso um malware do tipo ransomware ou cryptolocker tenha sido detectado e bloqueado após o início da criptografia, a solução deve recuperar os ficheiros criptografados para o estado pré-criptografado. Deve manter uma cópia protegida pelo kernel dos ficheiros do utilizador. Os ficheiros devem ser mantidos numa pasta segura que o Ransomware não pode aceder.
- A solução deve ter a capacidade de proteger uma máquina sem uma ligação constante à Internet. As seguintes funcionalidades devem ser garantidas:
 - ✓ A análise forense deve funcionar em todos os ambientes, independentemente da ligação de internet.
 - ✓ Os recursos de detecção Anti-Bot baseados na inteligência devem poder funcionar em modo offline.
 - ✓ A emulação e a extração de ameaças devem poder ser executadas numa máquina offline.
 - ✓ A detecção, prevenção e restauração do Anti-Ransomware funciona deve funcionar em todos os ambientes, independentemente da ligação à Internet
 - ✓ Todas as ações de resposta (ficheiros de quarentena, bloqueio da máquina ...) podem ser executadas quando offline.

Mitigação/Remediação

- A solução deve ter a capacidade de enviar ou receber atualizações de segurança, patches, conjuntos de regras sem assinatura, assinaturas, políticas e outros dados de configuração. Os clientes devem receber todas as informações relacionadas por meio de políticas e operações push.
- A solução deve ter a capacidade de fornecer informações forenses relacionadas o malware detectado. A análise forense deve incluir os acessos a ficheiros, chaves de registro confidenciais, criação de processos, modificação de registro/ficheiros, todas as comunicações de rede, atividade de login do utilizador, elevação de permissões, monitorização de variáveis de ambiente, etc.
- A solução deve ter a capacidade de executar verificações agendadas ou sob demanda de malware ou atividade maliciosa com base em assinaturas comerciais e/ou governamentais. O administrador deve poder usar o recurso de pesquisa e realizar uma verificação por qualquer indicador. Esta verificação deve resultar em análises forenses, quarentena de ficheiros, quarentena da máquina, correção total da máquina, etc. Esta verificação não deve deixar nenhum rastro significativo na máquina.

- A solução deve ter a capacidade de colocar sistemas em quarentena automaticamente com base em regras personalizáveis (por exemplo, quando tipos de malware especificados são detectados). Devem ser utilizados os seguintes níveis:
 - ✓ Quarentena local na máquina - usando Firewall incorporado na máquina. Isso impedirá a máquina de comunicar e atacar outras máquinas ao seu redor.
 - ✓ Quarentena usando gateways. A solução pode interagir automaticamente com as Gateways para implementar automaticamente a imposição nas máquinas ofensivas. Além da quarentena da máquina, há também a opção de automaticamente colocar em quarentena apenas o processo malicioso ou todos os processos que a análise forense decidiu que fazem parte do ataque.
- A solução deve ter a capacidade de fornecer relatórios em tempo quase real de eventos específicos, com ações de resposta recomendadas para melhorar a segurança do host. Todos os incidentes de segurança devem ser totalmente analisados e o relatório resultante enviado quase em tempo real ao servidor de monitorização, incluindo informações altamente acionáveis, como análise do ponto de entrada, análise do impacto e todos os recursos maliciosos identificados na máquina com base na atividade forense. Este relatório deve incluir informações detalhadas sobre o ponto de entrada no sistema, permitindo que o administrador identificar os pontos fracos de entrada e melhorar a política de segurança de acordo.

Suporte e Manutenção

O suporte e manutenção, deve ser assegurado diretamente pelo fabricante. A manutenção pretendida é a seguinte:

Manutenção de 36 meses incluído peças e mão-de-obra.

- SLA 24x7 com tempo de resposta nas instalações no dia útil seguinte
- Prestação de assistência contínua até à solução da avaria.

Serviços de Instalação e Configuração

Para além dos pressupostos definido no Decreto-lei 65/2021, pretende-se que, as seguintes configurações e/ou implementações sejam efetuadas pelo adjudicatário:

Instalação da solução de Gestão

- Instalação da solução de Gestão
- Configuração da aplicação na rede e domínio, VPNs
- Criação dos acessos à aplicação
- Registo da Firewall
- Testes de acessos e funcionalidade da solução
- Passagem de conhecimento
- Formação On-Job.

Instalação Solução de Firewall

- Inicialização das aplicações na rede e domínio
- Instalação da última versão de software disponível à data
- Levantamento das regras na firewall existente
- Aplicação das regras na nova firewall
- Testes de funcionamento
- Go live
- Formação On-Job.

Implementação da Solução de Endpoint

- Instalação da Consola de Gestão
- Configuração de políticas de segurança
- Deploy de agente e políticas nos postos de trabalho/servidores
- Instalação da última versão de software disponível até a data
- Testes de funcionamento
- Passagem de conhecimentos
- Formação On-Job.

Validação, Transferência de Informação e Documentação

- Validação do correto funcionamento e enquadramento da legislação em vigor
- Formação on Job sobre solução
- Criação da Documentação

ANEXO I

Modelo de declaração de aceitação do conteúdo do caderno de encargos

[a que se referem a alínea a) do artigo 12.º do Programa do Procedimento e 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 CCP]

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 executa 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.

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 os documentos comprovativos de que não se encontra nas situações previstas nas alíneas b), d), e) e i) do n.º 1 do artigo 55.º do referido Código.

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