

CADERNO DE ENCARGOS

Aquisição de Solução de Segurança de Endpoint

ARTIGO 1.º

OBJETO

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar entre a Fundação para a Ciência e a Tecnologia, I.P. e adjudicatário na sequência da adjudicação no âmbito da consulta para aquisição de “Aquisição de Solução de Segurança de Endpoint”.
2. O **CONTRATO** a celebrar integra, para além do clausulado contratual:
 - a) os suprimientos dos erros ou 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, nos termos do artigo 50º do Código dos Contratos Públicos;
 - b) os esclarecimentos e retificações relativos ao caderno de encargos que sejam emitidos ao abrigo do artigo 50º do Código dos Contratos Públicos;
 - c) o 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 nas diferentes alíneas do número anterior, a prevalência obedece à ordem por que vêm enunciados nas suas diferentes alíneas.
4. Em caso de divergência entre os documentos referidos nas diferentes alíneas do nº 2 e o clausulado contratual, 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 do mesmo diploma.

ARTIGO 2.º

OBRIGAÇÕES DO ADJUDICATÁRIO

1. O adjudicatário obriga-se a executar o Contrato em termos que se conformem com o estabelecido no Caderno de Encargos, nos anexos que dele fazem parte integrante e na legislação aplicável.
2. Para além de outras obrigações previstas na lei ou no presente caderno de encargos, o adjudicatário obriga-se a:
 - a) Assegurar que o objeto da prestação obedece às especificações técnicas exigidas;
 - b) Assegurar a manutenção;
 - c) Cumprir os prazos estabelecidos, designadamente, para a execução das prestações a que se obriga;
 - d) Prestar informação;
 - e) Assegurar o sigilo.

ARTIGO 3.º

ESPECIFICAÇÕES TÉCNICAS

O adjudicatário obriga-se a assegurar que o objeto de aquisição obedece às especificações técnicas que constam do Anexo I ao presente Caderno de Encargos, do qual faz parte integrante.

ARTIGO 4.º

PRAZOS

O adjudicatário obriga-se ao pontual cumprimento de todos os prazos de execução das prestações objeto do contrato, os quais são os que constam do clausulado deste ou de outros documentos referidos no nº 2 do artigo 1º.

ARTIGO 5.º

ENTREGA

1. O bem objeto de adjudicação considera-se entregue após a respetiva aceitação por parte da FCT, I.P, a qual será comunicada por escrito ao adjudicatário.

2. O adjudicante poderá promover a realização de testes de aceitação, destinados à verificação da conformidade dos bens objeto de adjudicação com os requisitos técnicos constantes do presente Caderno de Encargos.

3. Os testes referidos no número anterior devem ocorrer no prazo de 3 dias corridos após a receção de todos os bens objeto do contrato a qual deve ocorrer nas instalações da unidade FCCN da FCT, I.P., sitas na Av. do Brasil, 101, em Lisboa no prazo máximo de 5 dias corridos contados a partir da entrada em vigor do contrato

4. Os bens consideram-se aceites na data em que a FCT, I.P. disso expressamente notificar, por escrito, o adjudicatário ou, na ausência de notificação, no dia subsequente ao fixado no número anterior como limite para a realização de testes de aceitação.

5. Se nos termos dos testes de aceitação a FCT, I.P. constatar que os bens não cumprem os requisitos técnicos constantes do presente Caderno de Encargos, disso dará conhecimento ao adjudicatário, abrindo-se um prazo de 5 dias corridos para que este desenvolva as diligências necessárias a que aqueles requisitos sejam cumpridos, e o equipamento seja de novo submetido a testes.

6. Se, estes testes de aceitação, não forem concluídos com êxito, persistindo a desadequação aos requisitos técnicos exigidos, a FCT, I.P. poderá conceder novo prazo de 5 dias corridos para que o adjudicatário desenvolva as diligências necessárias para que sejam cumpridos os requisitos constante do presente Caderno de Encargos, aplicando-se, com as devidas adaptações, o estabelecido nos números 2 e seguintes ou, em alternativa, considerar incumprida a obrigação de fornecimento e rescindir o Contrato.

ARTIGO 6.º

OBRIGAÇÃO DE MANUTENÇÃO

Caso se verifique qualquer anomalia no bem objeto de adjudicação que impeça ou prejudique o desempenho da sua função, o adjudicatário obriga-se a proceder às operações necessárias à reposição deste nas mesmas condições que deram origem à aceitação nos termos e condições referidas no Anexo I ao presente Caderno de Encargos.

ARTIGO 7.º

OBRIGAÇÃO DE PRESTAÇÃO DE INFORMAÇÃO

O adjudicatário obriga-se a prestar à FCT, I.P., por escrito, toda a informação que lhe for solicitada relativa ao objeto da adjudicação ou à sua atuação em cumprimento das obrigações que para si decorrem do contrato.

ARTIGO 8.º

OBRIGAÇÃO DE SIGILO

O adjudicatário obriga-se a não divulgar informações que obtenha em virtude da execução do CONTRATO durante a vigência deste e por um período de dois anos contados a partir da data da sua cessação.

ARTIGO 9.º

PREÇO E CONDIÇÕES DE PAGAMENTO

1. O preço base da aquisição a que se refere o presente caderno de encargos, entendido como o preço máximo que a FCT, I.P. se dispõe a pagar pela execução de todas as prestações que constituem o seu objeto é de 52.600,00 € (cinquenta e dois mil e seiscentos euros)
2. Pela aquisição do bem objeto da presente aquisição, a FCT, I.P. pagará ao adjudicatário a quantia de ____ € [*valor indicado na proposta*], acrescida de IVA à taxa legal em vigor nos termos do número seguinte.
3. A quantia prevista no número anterior deve ser satisfeita através do pagamento de três faturas, emitidas anualmente, após a entrega do bem ou serviço nos termos a que se refere o artigo 5º.
4. As faturas a emitir pelo adjudicatário assumem a forma de faturas eletrónicas, com os requisitos legais, nomeadamente os resultantes do artigo 299º-B do CCP.
5. A fatura referida no número anterior será paga no prazo máximo de trinta dias a contar da sua receção.

6. A entidade adjudicante utiliza a solução EDI e faturação eletrónica ilink (acessível em <https://www.ilink.pt>), de registo gratuito, devendo todas as faturas emitidas pelo adjudicatário no âmbito do presente contrato ser enviadas por esta via¹.

ARTIGO 10.º

VIGÊNCIA DO CONTRATO

1. O contrato inicia a sua vigência na data da respetiva assinatura.
2. O contrato cessa vigência no prazo de 3 anos.
3. O artigo 8º cessa vigência na data em que cesse o prazo nele previsto.

ARTIGO 12.º

RESPONSABILIDADE DO ADJUDICATÁRIO

1. O adjudicatário responde pelos danos que causar à **FCT, I.P.** em razão do incumprimento culposo das obrigações que sobre ele impendam, nos termos das normas gerais de direito e do presente artigo.
2. O adjudicatário responde ainda perante a **FCT, I.P.** pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do **CONTRATO**, como se tais atos ou omissões fossem praticados por aquele.
3. O adjudicatário responde, independentemente de culpa, pelos danos causados à **FCT, I.P.** pela execução deficiente do **CONTRATO**.
4. Nenhuma das partes responde por danos causados à outra parte em virtude de incumprimento de obrigações emergentes do **CONTRATO** decorrente de caso fortuito ou força maior.
5. A parte que pretenda beneficiar-se do regime acolhido no número anterior deve, para o efeito, informar a outra parte da verificação de uma situação de incumprimento decorrente de caso fortuito ou de força maior, fazendo menção dos factos que, em seu entender, permitem atribuir esta origem ao incumprimento e, ainda, do prazo que estima necessário para cumprir a obrigação em causa.

¹ Para qualquer questão de carregamento de faturas ou ligação/integração de sistema e de faturação deve ser contactada a iLink através do email apoio@ilink.pt ou pelo telefone 707 451 451.

ARTIGO 13.º

CLÁUSULA PENAL

Pelo incumprimento, sob a forma de mora, de obrigações emergentes do contrato, a **FCT, I.P.** pode, sem prejuízo do n.º 4 do artigo anterior, exigir do adjudicatário o pagamento de uma pena pecuniária nos seguintes termos:

1% do valor do contrato, por cada período de indisponibilidade consecutivo em 72 horas da plataforma, até ao limite máximo permitido pela Lei.

ARTIGO 14.º

RESCISÃO

1. A **FCT, I.P.** pode rescindir o **CONTRATO**:

a) quando, estando o adjudicatário em mora, este não realize a prestação no prazo que lhe haja razoavelmente sido fixado pela **FCT, I.P.**;

b) com fundamento em incumprimento das obrigações previstas no artigo 2º que determine a perda objetiva de interesse nas prestações que constituam o seu objeto;

2. A rescisão do **CONTRATO** ao abrigo do disposto no número anterior determina a perda da caução prestada pelo adjudicatário, caso esta tenha sido prestada nos termos da lei e a extinção dos créditos de que este seja titular em virtude do referido **CONTRATO**.

3. A perda da caução ao abrigo do número anterior não extingue o direito da **FCT, I.P.** de ser ressarcida da totalidade dos danos que lhe hajam sido causados pela conduta do adjudicatário que haja fundamentado a rescisão.

ARTIGO 15.º

DESPESAS

Correm por conta do adjudicatário todas as despesas em que este haja de incorrer em virtude do cumprimento de obrigações emergentes do **CONTRATO**.

ARTIGO 16.º

LEI APLICÁVEL

O **CONTRATO** rege-se pela lei portuguesa.

ARTIGO 17.º

INTERPRETAÇÃO DO CONTRATO

1. Em caso de dúvida sobre a interpretação das regras aplicáveis à execução do **CONTRATO**, o adjudicatário deve solicitar por escrito um esclarecimento à **FCT, I.P.**.
2. O adjudicatário obriga-se a ter em conta as orientações que lhe forem transmitidas por escrito pela **FCT, I.P.**, na medida em que as mesmas não colidam com as regras aplicáveis à execução do **CONTRATO**.

ARTIGO 19.º

COMUNICAÇÕES

1. Para efeitos de comunicações relativas à fase de execução do contrato, as partes podem recorrer aos seguintes meios de comunicação:
 - a) correio postal, através de carta registada ou de carta registada com aviso de receção;
 - b) correio eletrónico;
 - c) outro meio de transmissão eletrónica de dados.
2. Todas as comunicações devem ser escritas e redigidas em língua portuguesa.
3. Para efeitos de estabelecimento das comunicações a que se refere o presente artigo, as partes identificam os seguintes contactos, através dos quais as mesmas se devem concretizar:

a) Pela FCT, I.P.:

Nome do representante:

Endereço postal: Av. do Brasil, 101 1700-066 Lisboa

Endereço electrónico:

b) Pelo adjudicatário:

Nome do representante:

Endereço postal:

Endereço electrónico:

ARTIGO 20.º

GESTOR DO CONTRATO

Para o exercício das funções de acompanhamento da execução do contrato nos termos regulados pelo artigo 290º-A do Código dos Contratos Públicos é designado Artur Gaspar.

ARTIGO 21.º

CESSÃO DA POSIÇÃO CONTRATUAL

1. A cessão da posição contratual do adjudicatário é possível nos termos do artigo 318º do Código dos Contratos Públicos.
2. Em caso de incumprimento contratual pelo adjudicatário que seja suscetível de conduzir à resolução do contrato, a sua posição contratual pode ser cedida aos concorrentes do procedimento pré-contratual classificados nas posições subsequentes à do adjudicatário, nos termos do estabelecido no artigo 318º-A do Código dos Contratos Públicos.

ARTIGO 21.º

DADOS PESSOAIS

1. No tratamento de dados pessoais por conta do adjudicante, o adjudicatário obriga-se ao escrupuloso cumprimento do Regulamento Geral sobre a Proteção de Dados (Regulamento 2016/679) e demais legislação aplicável.
2. O tratamento referido no número anterior é apenas o necessário à execução do contrato e feito durante a sua vigência, aplicando-se, em especial, o estabelecido no nº 3 do artigo 28º do Regulamento Geral sobre a Proteção de Dados.

ANEXO I

(ANEXO TÉCNICO)

A solução de Endpoint a fornecer tem de cumprir as seguintes especificações,

Requisitos Gerais

- A instalação de, pelo menos, 500 postos de trabalho/servidores (*endpoints*) com 3 anos de suporte;
- 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*;
- Capacidades de *Endpoint Detection and Response* (EDR).

Gestão

- A solução fornecida deve ser gerida através de uma interface gráfica *web*;
- A solução fornecida deve poder exportar os seus *logs* em formato *syslog* para qualquer solução de gestão de *log*;
- A solução deve vir de base já configurada com as *best practices* do fabricante de forma a simplificar o *deployment* da mesma;
- A solução fornecida deve possuir um modelo de licenciamento por *endpoint* e não por outros parâmetros como por exemplo número de utilizadores, CPUs, etc.;
- A solução fornecida deve suportar a atualização de *software* dos agentes de *endpoint* diretamente a partir da *cloud* ou de servidores *on-prem*.

Prevenção de Exploits

- A solução fornecida deve suportar a proteção dos 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 fornecida 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 fornecida 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 fornecida previna ou bloqueie 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 fornecida 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 fornecida 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 fornecida 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 fornecida deve conseguir proteger o *endpoint* contra “*Kernel privilege escalation*”;
- A solução fornecida deve também conseguir proteger contra *exploits* para MacOS e Linux, como por exemplo “*local privilege escalation*”.

Prevenção de Malware

- A solução fornecida deve suportar proteção contra a execução de executáveis maliciosos;
- A solução fornecida 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 fornecida 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 fornecida 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 fornecida 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 fornecida deve ser capaz de prevenir a execução de malware através da análise de comportamentos desencadeados pelo *malware*;
- A solução fornecida deve garantir a possibilidade de configurar *whitelists* globais para permitir a execução de certos ficheiros executáveis;
- A solução fornecida deve ser capaz de criar regras de exclusão das capacidades de proteção para *endpoints* específicos;
- A solução fornecida 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 fornecida deve ter a opção de integrar com soluções de *Advanced Persistent Threat* (APT) na *cloud* ou localmente, 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* (ou localmente) deve ser do mesmo fabricante da solução proposta para garantir uma maior integração;
- A solução fornecida deve conseguir perguntar aos serviços APT por valores de *hash* para verificar se determinado ficheiro é malicioso ou benigno;

- 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 fornecida deve ter a capacidade de submeter aos serviços APT ficheiros potencialmente malicioso;
- A solução fornecida deve conseguir visualizar na plataforma de gestão centralizada os relatórios de análise do *malware*;
- A solução fornecida não deve analisar ficheiros que já tenham sido anteriormente submetidos aos serviços APT;
- A solução fornecida deve conseguir prevenir *malware* desconhecido utilizando tecnologia APT *sandbox* e fornecer um relatório com o veredicto e análise do ficheiro submetido. A solução de APT *sandbox* deve ser do mesmo fabricante da solução proposta para garantir uma maior integração;
- A solução fornecida deve ter a capacidade de modificar manualmente a decisão tomada pelos serviços APT para uma *hash* em particular;
- A solução fornecida deve ter a capacidade de prevenir a execução de um ficheiro no caso da sua hash ser desconhecida dos serviços APT;
- A solução fornecida deve ter a capacidade de prevenir a execução de um ficheiro no caso do *endpoint* não conseguir contactar os serviços APT e o valor da *hash* do ficheiro não ser localmente conhecido;
- A solução fornecida deve garantir a capacidade de efetuar análises estáticas (*machine learning*) em modo *offline* para Windows, Linux e macOS;
- A solução fornecida 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 fornecida 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 fornecida deve conseguir prevenir ataques que tirem partido do *kernel* para carregar e correr código "shell" malicioso;
- A solução fornecida deve conseguir que o módulo de análise de comportamentos de *ransomware* opere em modo de notificação ou de prevenção;
- A solução fornecida 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 fornecida 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, 18 e 20

- macOS 10.x, 11.x e 12.x
- 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;
- Quando diferentes alertas estão relacionados, a solução deve ser capaz de os agregar automaticamente num 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 do fabricante assim como de ferramentas *OpenSource* (ex: *VirusTotal*);
- A solução deve mapear os diferentes alertas para a Framework Mitre ATT&CK;
- 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.

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 detetar 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.

ARTUR JOSÉ DE
SOUSA GASPAR

Digitally signed by ARTUR JOSÉ DE
SOUSA GASPAR
Date: 2022.10.20 11:02:15 +01'00'