Nome: _____ Data: _____ Pontuação: _____

Software antivírus e proteção de Guia de proteção

Deteção por assinaturas, heurística, monitorização de comportamento, sandboxing, atualizações

VISÃO GERAL DE APRENDIZAGEM SOBRE SOFTWARE ANTIVÍRUS

PROTEGIDO
ENCRIPTAÇÃO DE DADOS
Norma AES de 256 bits

CONFORME
NORMAS GLOBAIS
Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST
POLÍTICA DE ACESSO
Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te por software antivírus e proteção de pontos de extremidade. Vais explorar bases de dados de assinaturas, analisadores heurísticos, monitorização comportamental, ficheiros virtuais em sandbox e mitigação de falsos positivos.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/ciberseguranca/antivirus/

O teu roteiro de aprendizagem sobre estratégia de antivírus

- Distingue a deteção de malware baseada em assinaturas da baseada em heurística.
- Compreender a monitorização de comportamento e os protocolos de isolamento em sandbox.
- Avalia o impacto das análises em tempo real no desempenho do sistema e dos terminais.
- Mitigar classificações de falsos positivos através da verificação de certificados digitais.
- Gerir a distribuição diária de atualizações de definições pelos terminais da empresa.

INSTRUÇÕES DO GUIA DE ANTIVÍRUS

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à segurança antivírus de endpoints. Termina com a atividade bónus Pensa rápido.

PROTEÇÃO ANTIVÍRUS E ANÁLISE DE ASSINATURAS (INTRODUÇÃO)

O software antivírus protege os endpoints identificando, colocando em quarentena e removendo software malicioso. Os sistemas modernos combinam bases de dados de assinaturas (que fazem a correspondência com hashes de ameaças conhecidas) com heurísticas (que analisam a estrutura dos ficheiros) e monitorização de comportamento para detetar explorações de dia zero.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA

Ponto de controlo 1: Desafio de escolha múltipla

1. Qual é uma limitação da deteção baseada em assinaturas?

- A. Não consegue identificar software malicioso desconhecido ou modificado
- B. Gera taxas elevadas de falsos positivos
- C. Requer elevada capacidade de processamento do CPU
- D. Só funciona quando está ligado à internet

2. Como detetam os scanners heurísticos novas variantes de software malicioso?

- A. Identificando padrões e estruturas de código suspeitos
- B. Fazendo corresponder hashes de ficheiros a uma base de dados de ameaças
- C. Eliminando automaticamente todos os executáveis não assinados
- D. Carregando todos os ficheiros para uma pasta pública na nuvem

3. Qual é o objetivo da execução em sandbox do antivírus?

- A. Isolar e analisar ficheiros num cofre virtual seguro
- B. Acelerar a transferência da cópia de segurança do sistema de ficheiros local
- C. Atualizar os patches de segurança do sistema operativo local
- D. Comprimir ficheiros de documentos grandes para poupar armazenamento

4. Que método de deteção assinala comportamentos de ameaça em tempo real?

- A. Análise comportamental que monitoriza as ações do software
- B. Inspeção do histórico de registos realizada durante a noite
- C. Intervenção manual do utilizador a comunicar aplicações lentas
- D. Revisões manuais semanais dos programas instalados

5. Porque são essenciais as atualizações regulares de definições para os analisadores?

- A. Alimentar os motores de assinaturas com identificadores de ameaças da base de dados
- B. Aumentar as frequências de relógio do CPU durante as operações
- C. Para modificar os tempos de cache globais dos servidores de nomes DNS
- D. Para autorizar as definições de cookies do navegador

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta (verdadeiro/falso) 6

6. A deteção por assinaturas compara hashes criptográficos de ficheiros com listas de bases de dados.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta (verdadeiro/falso) 7

7. Os scanners heurísticos podem gerar alertas de falsos positivos em ficheiros seguros.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta (verdadeiro/falso) 8

8. Uma sandbox permite que o software malicioso aceda a ficheiros de rede sem limites.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta (verdadeiro/falso) 9

9. A análise comportamental bloqueia ficheiros quando estes exibem ações maliciosas.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta (verdadeiro/falso) 10

10. O software antivírus padrão bloqueia por completo todos os ataques de dia zero.

- ◯ Verdadeiro
- ◯ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Um analisador tradicional baseia-se na correspondência de _____ para identificar malware conhecido.

2. A análise dos padrões de código dos ficheiros chama-se análise _____ .

3. Os antivírus isolam os ficheiros suspeitos num ambiente de _____ .

4. A monitorização em tempo real vigia o _____ dos programas à procura de atividades suspeitas.

5. Os analisadores descarregam todos os dias as _____ da base de dados para reconhecer novas ameaças.

6. Os programas seguros assinalados como malware geram alertas de _____ .

BANCO DE PALAVRAS DE VOCABULÁRIO

ANTIVÍRUS ASSINATURA HASH ATUALIZAÇÕES COMPORTAMENTO
FALSO POSITIVO FIREWALL HEURÍSTICA SANDBOX

Escreve aqui as tuas respostas:

1.
2.
3.
4.
5.
6.

Ponto de controlo 4: Associação de conceitos de segurança

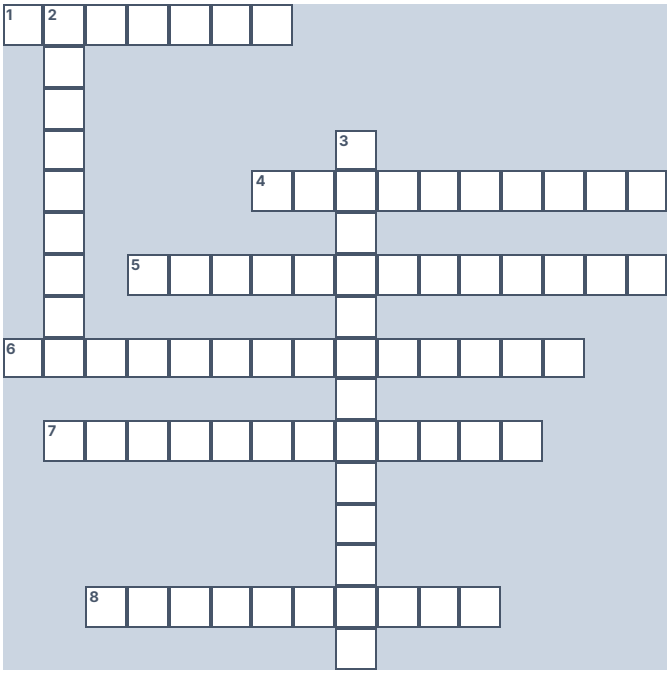
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. Assinatura hash	A	Confinar ficheiros suspeitos para evitar a exposição do sistema local.
☐	2. Heurística de código	B	Conjunto de software que analisa e protege terminais contra exploits.
☐	3. Sandbox de ficheiros	C	Monitorização das ações do software em execução à procura de padrões de operação maliciosos.
☐	4. Análise de comportamento	D	Impressão digital criptográfica única de base de dados, usada para identificar ameaças conhecidas.
☐	5. Atualizações diárias	E	Ambiente de teste virtual seguro que executa código não fiável em segurança.
☐	6. Falso positivo	F	Transferências regulares de definições que alimentam a base de dados de ameaças.
☐	7. Isolamento de ameaças	G	Análise baseada em regras que sinaliza ficheiros com estruturas de código suspeitas.
☐	8. Ferramenta antivírus	H	Alerta de segurança que classifica incorretamente software seguro como software malicioso.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

1. Ambiente virtual de testes seguro que executa código não confiável sem riscos (7)

4. Confinamento de ficheiros suspeitos para evitar a exposição do sistema local (10)

5. Alerta de segurança que classifica erradamente software seguro como malware (13)

6. Impressão digital criptográfica única, guardada numa base de dados, usada para identificar ameaças conhecidas (14)

7. Descargas regulares de definições que alimentam a base de dados de ameaças (12)

8. Análise baseada em regras que assinala ficheiros com estruturas de código suspeitas (10)

VERTICAIS

2. Conjunto de software que analisa e protege os dispositivos finais contra exploits (9)

3. Monitorização das ações do software em execução à procura de padrões de funcionamento malicioso (13)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo. HORIZONTAIS VERTICAIS

HORIZONTAIS

1 horizontal: Ambiente virtual de testes seguro que executa código não confiável sem riscos (7 letras):

4 horizontal: Confinamento de ficheiros suspeitos para evitar a exposição do sistema local (10 letras):

5 horizontal: Alerta de segurança que classifica erradamente software seguro como malware (13 letras):

6 horizontal: Impressão digital criptográfica única, guardada numa base de dados, usada para identificar ameaças conhecidas (14 letras):

7 horizontal: Descargas regulares de definições que alimentam a base de dados de ameaças (12 letras):

8 horizontal: Análise baseada em regras que assinala ficheiros com estruturas de código suspeitas (10 letras):

VERTICAIS

2 vertical: Conjunto de software que analisa e protege os dispositivos finais contra exploits (9 letras):

3 vertical: Monitorização das ações do software em execução à procura de padrões de funcionamento malicioso (13 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

O Y J K V J Y W Y P J I Z I J

T N A E I A S A J F W E K Z K

N E K Q H E U R I S T I C A N

E J A F O K N D N C D H I B A

M P R L P W T I Y F Y S G X W

A H F R T N U K R D T S L P L

T M S H K P H Y P L W U N Y Q

R Q S E O C A Z I L A U T A B

O A L P M B L I F I N Y B Z Z

P Y B N V X M X O B D N A S C

M A S S I N A T U R A H A S H

O F P I S O L A M E N T O W Q

C Q F A L S O P O S I T I V O

X H E Y C W L F G H Z W C O R

S U R I V I T N A J X X R K Z

LISTA DE PALAVRAS DE VOCABULÁRIO

ASSINATURAHASH HEURISTICA SANDBOX COMPORTAMENTO ATUALIZACOES
FALSOPOSITIVO ISOLAMENTO ANTIVIRUS

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO

- **A. ASSINATURAHASH**
- **B. HEURISTICA**
- **C. SANDBOX**
- **D. COMPORTAMENTO**
- **E. ATUALIZACOES**
- **F. FALSOPOSITIVO**
- **G. ISOLAMENTO**
- **H. ANTIVIRUS**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Monitorização das ações do software em execução à procura de padrões de funcionamento malicioso.

_____ 2. Conjunto de software que analisa e protege os dispositivos finais contra exploits.

_____ 3. Descargas regulares de definições que alimentam a base de dados de ameaças.

_____ 4. Análise baseada em regras que assinala ficheiros com estruturas de código suspeitas.

_____ 5. Confinamento de ficheiros suspeitos para evitar a exposição do sistema local.

_____ 6. Impressão digital criptográfica única, guardada numa base de dados, usada para identificar ameaças conhecidas.

_____ 7. Ambiente virtual de testes seguro que executa código não confiável sem riscos.

_____ 8. Alerta de segurança que classifica erradamente software seguro como malware.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. HAUATSSRAA SHNI
2. SNXOBDA
3. ATAZECUISLO A
4. MTAOLNEISO
5. ISAERTIHCU
6. OETRNMTMC OAOP
7. TISPFAIOOVL OS
8. SVUAINIRT

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Razões para atualizar o software			
2	Pessoas a quem podes pedir ajuda de TI			
3	Coisas a fazer quando o antivírus encontra algo			
4	Sinais de um vírus informático			
5	Coisas que vão para quarentena			
6	Locais onde os vírus se escondem			
7	Informações que nunca deves partilhar			
8	Tipos de software malicioso			
9	Ferramentas de segurança que conheces			
10	Coisas que um antivírus analisa			
11	Coisas de que fazes cópia de segurança			
12	Dispositivos que podem ser hackeados			
13	Programas antivírus que conheces			
14	Razões para falsos alarmes			
15	Hábitos seguros que podes começar hoje			

Ponto de controlo 8: Estudos de caso de cibersegurança

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

ESTUDO DE CASO 1: ANÁLISE POR ASSINATURA VS. HEURÍSTICA



Cenário: Um colaborador transfere um utilitário personalizado criado internamente por outra equipa. O analisador de assinaturas aprova-o, mas o analisador heurístico assinala-o como suspeito.

Questão para debate: Explica por que razão isto aconteceu e como verificar se o ficheiro é seguro.

ESTUDO DE CASO 2: LIDAR COM FALSOS POSITIVOS



Cenário: Um programador de software compila a sua aplicação. O antivírus do sistema assinala o novo executável como malware e coloca-o em quarentena.

Questão para debate: Descreve os riscos de colocar na lista de exceções (whitelist) e indica o caminho de resolução correto.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

4 5 20 5 20 1 13 1 12 23 1 18 5 14 15 22 15

3 15 13 1 14 1 12 9 19 5

8 5 21 18 9 19 20 9 3 1

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: Como identifica o software antivírus o malware?

Identifica software malicioso através da correspondência de assinaturas em bases de dados, da análise heurística da estrutura do código e da monitorização comportamental em tempo real.

Q2: O que é a deteção baseada em assinaturas?

É um método de análise que compara hashes criptográficos de ficheiros com listas de bases de dados de ameaças de software malicioso conhecidas.

Q3: O que é um analisador heurístico?

A heurística analisa a estrutura de um ficheiro e as instruções de código, sinalizando padrões suspeitos comuns a variantes de software malicioso.

Q4: O que significa um ficheiro estar em quarentena?

O antivírus move o ficheiro para uma pasta segura e isolada, impedindo a sua execução para proteger o sistema operativo.

Q5: O que é um falso positivo de antivírus?

É um erro em que software legítimo e seguro é incorretamente sinalizado como software malicioso pelos algoritmos de análise.

Ponto de controlo 10: Perguntas frequentes básicas sobre cibersegurança (Parte B)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: Como protege a monitorização de comportamento os sistemas?

Monitoriza o software em execução em tempo real, bloqueando os processos que tentam alterações suspeitas, como a injeção de código.

Q7: Porque são importantes os testes em sandbox?

O sandboxing executa ficheiros não fiáveis numa máquina virtual isolada, observando as ações em segurança sem expor o sistema.

Q8: Com que frequência devem ser atualizadas as definições do antivírus?

Os analisadores devem atualizar as definições diária ou horariamente para reconhecer estirpes de software malicioso recém-descobertas.

Q9: Qual é a diferença entre antivírus e EDR?

O antivírus centra-se na análise de ficheiros, enquanto a Endpoint Detection and Response (EDR) oferece rastreamento e contenção de ameaças em toda a rede.

Q10: Posso executar dois programas antivírus em conjunto?

Não. Executar dois analisadores ativos causa conflitos no sistema, reduz o desempenho e pode bloquear as operações um do outro.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte C)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como é que as regras heurísticas minimizam o contorno de ameaças?

A heurística analisa padrões gerais de ameaças em vez de assinaturas específicas, detetando variantes modificadas de famílias conhecidas de software malicioso.

Q2: O que é um vírus polimórfico?

É software malicioso que altera a estrutura dos seus ficheiros e a rotina de desencriptação a cada execução, tornando ineficazes as análises por assinatura.

Q3: Como detetam as sandboxes a evasão de máquinas virtuais?

As sandboxes modernas simulam cliques do rato e o tempo de atividade do sistema, enganando o software malicioso concebido para se esconder quando é executado em máquinas virtuais.

Q4: Quais são os formatos de transferência das atualizações de assinaturas?

As atualizações são normalmente ficheiros leves de diferenças binárias incrementais, minimizando o consumo de largura de banda de rede do cliente.

Q5: Como gerem os agentes de terminal as análises locais?

Os agentes efetuam verificações leves em segundo plano, delegando as pesquisas profundas de hashes criptográficos em bases de dados de ameaças na nuvem.

Ponto de controlo 10: Perguntas frequentes avançadas sobre segurança (Parte D)

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: O que é a análise de deteção de rootkits?

Analisa as tabelas de memória ao nível do kernel, contornando as API do sistema operativo que os rootkits intercetam para esconder os seus threads ativos.

Q7: Como bloqueia a análise de comportamento o ransomware?

Deteta ciclos de encriptação em massa de ficheiros automatizados, terminando o processo do anfitrião antes de as bases de dados do sistema serem bloqueadas.

Q8: O que é a verificação de certificados de assinatura de código?

Os analisadores verificam as assinaturas digitais do código face a autoridades de certificação de raiz fiáveis, validando a identidade do programador do software.

Q9: Como afetam os packers os motores de análise?

Os packers comprimem ou encriptam as cargas úteis do malware. Os scanners têm de descompactar o ficheiro em memória antes de as correspondências de assinaturas serem executadas.

Q10: Como é que as ferramentas EDR automatizam o isolamento?

Os agentes EDR põem em quarentena os terminais comprometidos ao nível da rede, bloqueando o movimento lateral e permitindo o acesso do analista.

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

As bases de dados de assinaturas guardam hashes de software malicioso conhecido, pelo que ficheiros totalmente novos ou alterados passam despercebidos até as definições serem atualizadas.

2. PERSPETIVA SOBRE SEGURANÇA

Os motores heurísticos podem sinalizar algumas variantes novas de software malicioso antes de existirem assinaturas, ao custo de mais falsos positivos.

3. PERSPETIVA SOBRE SEGURANÇA

Os alertas de falsos positivos custam às equipas de TI tempo gasto a verificar e a restaurar ficheiros que foram postos em quarentena por engano.

4. PERSPETIVA SOBRE SEGURANÇA

O malware polimórfico altera o seu código a cada cópia, pelo que os defensores combinam assinaturas com verificações heurísticas e comportamentais.

6. PERSPETIVA SOBRE SEGURANÇA

Os autores de software malicioso escrevem código personalizado para verificar ambientes de sandbox, atrasando a execução para contornar os temporizadores.

5. PERSPETIVA SOBRE SEGURANÇA

Os motores antivírus baseados na nuvem comparam os hashes de ficheiros suspeitos com grandes bases de dados de ameaças online quase em tempo real.

7. PERSPETIVA SOBRE SEGURANÇA

Os fornecedores enviam regularmente atualizações de definições para os dispositivos terminais, para que os analisadores reconheçam ameaças recém-confirmadas.

8. PERSPETIVA SOBRE SEGURANÇA

Os monitores comportamentais de ransomware visam chamadas específicas à API Win32 associadas à encriptação de ficheiros e à eliminação de cópias de sombra.

9. PERSPETIVA SOBRE SEGURANÇA

Assinaturas de código válidas podem reduzir o risco de falsos positivos, mas os ficheiros assinados continuam a ser analisados, pois o malware também pode estar assinado.

10. PERSPETIVA SOBRE SEGURANÇA

Os rootkits modificam as estruturas do kernel do sistema, exigindo analisadores especializados no arranque para os detetar e limpar.

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados. REFERÊNCIAS ACADÉMICAS E DO SETOR

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.

https://csrc.nist.gov/pubs/sp/800/61/r3/final

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

ASSINATURAS

Resposta correta: A

NOTA PARA O PROFESSOR

A análise por assinaturas baseia-se em hashes conhecidos de bases de dados, pelo que não deteta malware desconhecido ou modificado. Citação: OWASP Secure Configuration.

2 Pergunta 2

HEURÍSTICA

Resposta correta: A

NOTA PARA O PROFESSOR

A heurística analisa a estrutura do código e os comandos para identificar características suspeitas de novas variantes de ameaças. Citação: Center for Internet Security (CIS).

3 Pergunta 3

SANDBOXING

Resposta correta: A

NOTA PARA O PROFESSOR

Uma sandbox executa ficheiros suspeitos numa máquina virtual isolada para observar em segurança o comportamento de execução. Citação: NIST Digital Identity.

4 Pergunta 4

COMPORTAMENTAL

Resposta correta: A

NOTA PARA O PROFESSOR

A análise comportamental monitoriza os programas em execução em tempo real para bloquear alterações não autorizadas ao sistema. Citação: Center for Internet Security (CIS).

5 Pergunta 5

ATUALIZAÇÕES

Resposta correta: A

NOTA PARA O PROFESSOR

Os analisadores transferem atualizações incrementais diárias de definições para se manterem sincronizados com o panorama das ameaças. Citação: OWASP Secure Configuration.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Pergunta 6** ASSINATURAS **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

As ferramentas de assinaturas calculam hashes criptográficos e comparam-nos com uma base de dados de hashes de ameaças conhecidas. Citação: OWASP Secure Configuration.

7 **Pergunta 7** HEURÍSTICA **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os motores heurísticos executam esquemas baseados em regras que podem assinalar ficheiros legítimos e seguros como suspeitos. Citação: Center for Internet Security (CIS).

8 **Pergunta 8** SANDBOXING **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Uma sandbox executa o código num contentor virtual, bloqueando estritamente o acesso a partilhas de rede. Citação: NIST Digital Identity.

9 **Pergunta 9** COMPORTAMENTAL **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

A monitorização em tempo real assinala processos em execução que tentam escritas ilegais ou bloqueio de ficheiros. Citação: Center for Internet Security (CIS).

10 **Pergunta 10** **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Nenhum antivírus pára todos os ataques de dia zero; as ameaças desconhecidas podem escapar às assinaturas e à heurística.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

D 1. Assinatura hash	G 2. Heurística de código	E 3. Sandbox de ficheiros	C 4. Análise de comportamento
F 5. Atualizações diárias	H 6. Falso positivo	A 7. Isolamento de ameaças	B 8. Ferramenta antivírus

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 ASSINATURA HASH	2 HEURÍSTICA	3 SANDBOX	4 COMPORTAMENTO
5 ATUALIZAÇÕES	6 FALSO POSITIVO		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 D – COMPORTAMENTO	2 H – ANTIVIRUS	3 E – ATUALIZACOES	4 B – HEURISTICA
5 G – ISOLAMENTO	6 A – ASSINATURAHASH	7 C – SANDBOX	8 F – FALSOPOSITIVO

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar Assinatura hash, Heurística de código e Sandbox de ficheiros por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

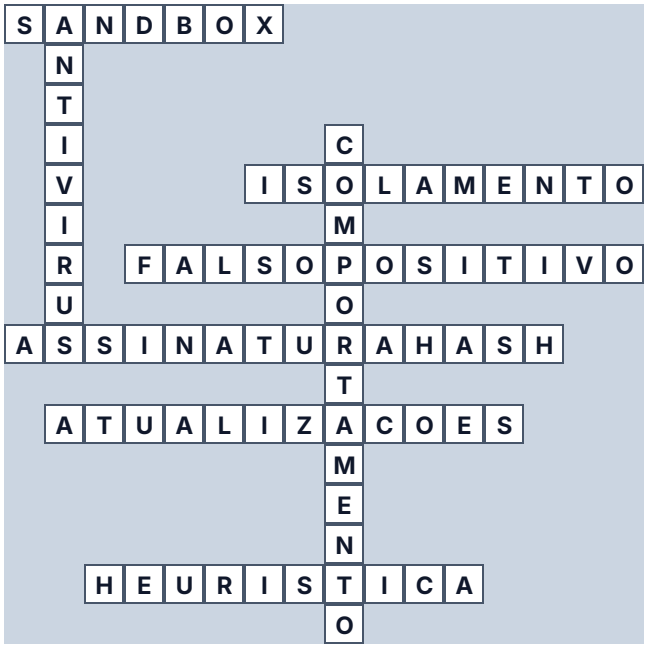
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

O	Y	J	K	V	J	Y	W	Y	P	J	I	Z	I	J
T	N	A	E	I	A	S	A	J	F	W	E	K	Z	K
N	E	K	Q	H	E	U	R	I	S	T	I	C	A	N
E	J	A	F	O	K	N	D	N	C	D	H	I	B	A
M	P	R	L	P	W	T	I	Y	F	Y	S	G	X	W
A	H	F	R	T	N	U	K	R	D	T	S	L	P	L
T	M	S	H	K	P	H	Y	P	L	W	U	N	Y	Q
R	Q	S	E	O	C	A	Z	I	L	A	U	T	A	B
O	A	L	P	M	B	L	I	F	I	N	Y	B	Z	Z
P	Y	B	N	V	X	M	X	O	B	D	N	A	S	C
M	A	S	S	I	N	A	T	U	R	A	H	A	S	H
O	F	P	I	S	O	L	A	M	E	N	T	O	W	Q
C	Q	F	A	L	S	O	P	O	S	I	T	I	V	O
X	H	E	Y	C	W	L	F	G	H	Z	W	C	O	R
S	U	R	I	V	I	T	N	A	J	X	X	R	K	Z

SOLUÇÃO DAS PALAVRAS CRUZADAS



HORIZONTAIS

1 horizontal: SANDBOX Ambiente virtual de testes seguro que executa código não confiável sem riscos (7 letras)

4 horizontal: ISOLAMENTO Confinamento de ficheiros suspeitos para evitar a exposição do sistema local (10 letras)

5 horizontal: FALSOPOSITIVO Alerta de segurança que classifica erradamente software seguro como malware (13 letras)

6 horizontal: ASSINATURAHASH Impressão digital criptográfica única, guardada numa base de dados, usada para identificar ameaças conhecidas (14 letras)

7 horizontal: ATUALIZACOES Descargas regulares de definições que alimentam a base de dados de ameaças (12 letras)

8 horizontal: HEURISTICA Análise baseada em regras que assinala ficheiros com estruturas de código suspeitas (10 letras)

VERTICAIS

2 vertical: ANTIVIRUS Conjunto de software que analisa e protege os dispositivos finais contra exploits (9 letras)

3 vertical: COMPORTAMENTO Monitorização das ações do software em execução à procura de padrões de funcionamento malicioso (13 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. HAUATSSRAASHNI — **ASSINATURAHASH**
2. SNXOBDA — **SANDBOX**
3. ATAZECUISLOA — **ATUALIZACOES**
4. MTAOLNEISO — **ISOLAMENTO**
5. ISAERTIHCU — **HEURISTICA**
6. OETRNMTMCOAOP — **COMPORTAMENTO**
7. TISPFAIOOVLOS — **FALSOPOSITIVO**
8. SVUAINIRT — **ANTIVIRUS**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"DETETA MALWARE NOVO COM ANALISE HEURISTICA"

Soluções dos estudos de caso

A Estudo de caso 1: Análise por assinatura vs. heurística

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um funcionário transfere um utilitário personalizado criado internamente por outra equipa. O analisador de assinaturas aprova-o, mas o analisador heurístico sinaliza-o como suspeito.
- Estratégia e solução recomendadas: Porque aconteceu: A análise por assinaturas verifica os hashes dos ficheiros; como é personalizado, não consta da base de dados de ameaças. A heurística analisa a estrutura e sinalizou ações suspeitas (por exemplo, gravações no registo). Verificação: Executar o ficheiro numa sandbox para observar as ações, verificar as assinaturas digitais e submeter o hash a portais de informações sobre ameaças.

B Estudo de caso 2: Lidar com falsos positivos

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um programador compila a sua aplicação. O antivírus do sistema sinaliza o novo executável como software malicioso e coloca-o em quarentena.
- Estratégia e solução recomendadas: Riscos da lista de permissões: Contornar os analisadores pode permitir a execução de código real infetado. Caminho de resolução: Submeter o ficheiro ao fornecedor do antivírus para análise, assinar digitalmente o código através de autoridades de certificação e configurar temporariamente exceções para pastas específicas em vez de desligar o antivírus.