

Navn: _____

Dato: _____

Point: _____

Antivirus og beskyttelse af endepunkter

Signaturer, heuristik, adfærdsovervågning, sandkasser, opdateringer

OVERBLIK OVER LÆRING OM ANTIVIRUSPROGRAMMER

SIKRET

DATAKRYPTERING

256-bit AES-standard

OVERHOLDER KRAV

GLOBALE STANDARDER

GDPR- og CCPA-rammer

ZERO-TRUST

ADGANGSPOLITIK

Multifaktorgodkendelse

Velkommen! Dette opgavehæfte guider dig gennem antivirusprogrammer og beskyttelse af endepunkter. Du vil udforske signatordatabaser, heuristiske scannere, adfærdsovervågning, virtuelle sandkasser og håndtering af falske alarmer.

OPGAVEARKETS KONTROLPUNKTER

- ☐ Del 1-4: Lær cybersikkerhed og trusselsforebyggelse.
- ☐ Del 5-7: Løs kryds og tværs samt ordjagt.
- ☐ Del 8-9: Løs casestudier og chifferudfordring.
- ☐ Del 10: Gennemgå grundlæggende og avanceret FAQ.
- ☐ Del 11: Udforsk 10 interessante fakta fra virkeligheden.

Åbn VPN.com's guide til cybersikkerhed

URL: <https://www.vpn.com/cybersecurity/antivirus/>

Din læringsplan for antivirusstrategi

- Skeln mellem signaturbaseret og heuristisk genkendelse af malware.
- Forstå adfærdsovervågning og isolering i sandkasser.
- Vurdér, hvordan scanning i realtid påvirker ydelsen og endepunkterne.
- Begræns falske alarmer ved at kontrollere digitale certifikater.
- Styr de daglige opdateringer af definitioner til virksomhedens endepunkter.

VEJLEDNING TIL GUIDEN OM ANTIVIRUS

Besvar multiple choice- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden om antivirus på endepunkter.

ANTIVIRUSBESKYTTELSE OG SIGNATURSCANNING (INTRODUKTION)

Antivirus beskytter endepunkter ved at finde, sætte i karantæne og fjerne malware. Moderne systemer kombinerer signaturdatabaser (kendte hashes), heuristik (analyse af filers opbygning) og adfærdsovervågning for at opdage zero-day-angreb.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE

Kontrolpunkt 1: Multiple choice-udfordring

1 1. Hvad er en begrænsning ved signaturbaseret genkendelse?

- ☐ A. Den kan ikke genkende ukendt eller ændret malware
- ☐ B. Den giver mange falske alarmer
- ☐ C. Den kræver meget processorkraft
- ☐ D. Den virker kun med forbindelse til internettet

2 2. Hvordan finder heuristiske scannere nye varianter af malware?

- ☐ A. Ved at genkende mistænkelige mønstre og kodestrukturer
- ☐ B. Ved at sammenligne filhashes med en trusselsdatabase
- ☐ C. Ved automatisk at slette alle usignede programmer
- ☐ D. Ved at sende mistænkelige pakker til en VPN

3 3. Hvad er formålet med at køre filer i en sandkasse?

- ☐ A. At isolere og analysere filer i et sikkert virtuelt rum
- ☐ B. At gøre lokal sikkerhedskopiering hurtigere
- ☐ C. At installere sikkerhedsrettelser til styresystemet
- ☐ D. At komprimere store dokumenter for at spare plads

4 4. Hvilken metode opdager truende adfærd i realtid?

- ☐ A. Adfærdsanalyse, der overvåger programmers handlinger
- ☐ B. Gennemgang af gamle logfiler om natten
- ☐ C. Brugere, der selv melder langsomme apps
- ☐ D. Søgning på nøgleord i ICANN's register

5 5. Hvorfor er jævnlige opdateringer af definitioner vigtige?

- ☐ A. For at give signatormotoren nye kendetegn for trusler
- ☐ B. For at øge processorens hastighed
- ☐ C. For at ændre DNS-servernes cachetider
- ☐ D. For at godkende browserens cookieindstillinger

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål tf 6

6. Signaturgenkendelse sammenligner kryptografiske filhashes med lister i en database.

☐ Sandt ☐ Falsk

7 Spørgsmål tf 7

7. Heuristiske scannere kan give falske alarmer på sikre filer.

☐ Sandt ☐ Falsk

8 Spørgsmål tf 8

8. En sandkasse giver malware fri adgang til filer på netværket.

☐ Sandt ☐ Falsk

9 Spørgsmål tf 9

9. Adfærdsscanning blokerer filer, når de udfører skadelige handlinger.

☐ Sandt ☐ Falsk

10 Spørgsmål tf 10

10. Almindelige antivirusprogrammer stopper alle zero-day-angreb fuldstændigt.

☐ Sandt ☐ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. En traditionel scanner bygger på _____ for at genkende kendt malware.
2. Når en scanner analyserer kodemønstre, bruger den _____ til scanningen.
3. Antivirus isolerer mistænkelige filer i en _____ (et isoleret miljø).
4. Overvågning i realtid holder øje med programmers _____ og leder efter mistænkelige handlinger.
5. Scannere henter _____ af databasen dagligt for at genkende nye trusler.
6. Sikre programmer, der udpeges som malware, udløser en _____ (falsk positiv).

ORDBANK MED FAGUDTRYK

ADFAERD

FALSKALARM

HEURISTIK

KARANTAENE

OPDATERINGER

SANDKASSE

SCANNER

SIGNATUR

Skriv dine svar her:

1.

2.

3.

4.

5.

6.

Kontrolpunkt 4: Match sikkerhedsbegreber

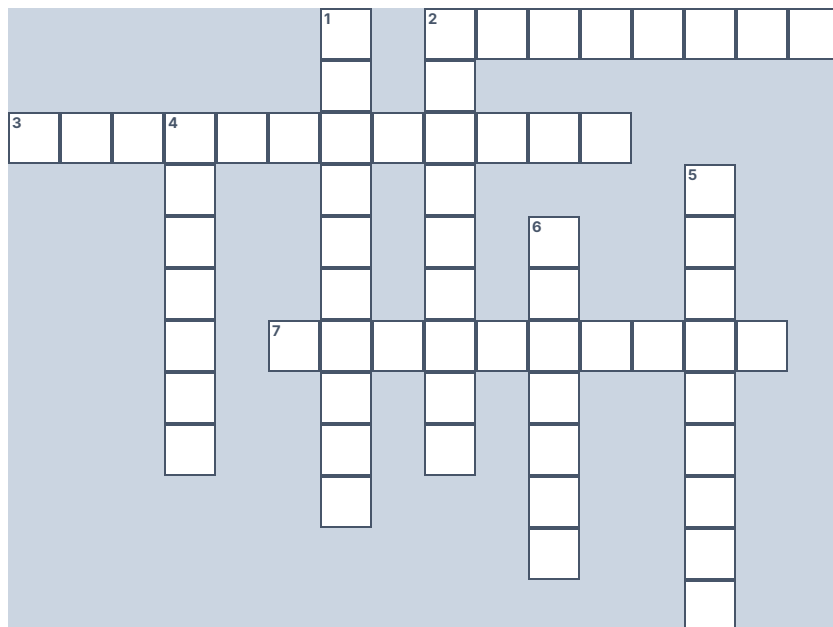
MATCH DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

- | | | |
|--|----------|---|
| <input type="text"/> 1. Hash-signatur | A | Entydigt kryptografisk aftryk, der bruges til at genkende kendte trusler. |
| <input type="text"/> 2. Kodeheuristik | B | Regelbaseret analyse, der markerer filer med mistænkelig kode. |
| <input type="text"/> 3. Sandkasse til filer | C | Sikkert virtuelt testmiljø, hvor ukendt kode kan køre ufarligt. |
| <input type="text"/> 4. Adfærdsscanning | D | Overvågning af kørende programmer for skadelige mønstre. |
| <input type="text"/> 5. Daglige opdateringer | E | Jævnlige hentninger af definitioner til trusselsdatabasen. |
| <input type="text"/> 6. Falsk alarm | F | Alarm, der fejlagtigt udpeger sikkert software som malware. |
| <input type="text"/> 7. Isolering af trusler | G | Afspærring af mistænkelige filer, så systemet ikke udsættes for dem. |
| <input type="text"/> 8. Antivirusværktøj | H | Program, der scanner og beskytter endepunkter mod angreb. |

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

- 2. Entydigt kryptografisk aftryk, der bruges til at genkende kendte trusler (8)
- 3. Jævnligte hentninger af nye definitioner til trusselsdatabasen (12)
- 7. Advarsel, der fejlagtigt udpeger sikkert software som malware (10)

LODRETTE NØGLER

- 1. Isoleret mappe, hvor mistænkelige filer spærres inde (10)
- 2. Sikkert virtuelt testmiljø, hvor ukendt kode kan køre ufarligt (9)
- 4. Det, som overvågningen holder øje med, når programmer kører (7)
- 5. Regelbaseret analyse, der markerer filer med mistænkelig kode (9)
- 6. Programdelen, der gennem søger filer og endepunkter for trusler (7)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.
VANDRETTE NØGLER LODRETTE NØGLER

VANDRETTE NØGLER

2 vandret: Entydigt kryptografisk aftryk, der bruges til at genkende kendte trusler (8 bogstaver):

3 vandret: Jævnlig hentninger af nye definitioner til trusselsdatabasen (12 bogstaver):

7 vandret: Advarsel, der fejlagtigt udpeger sikkert software som malware (10 bogstaver):

LODRETTE NØGLER

1 lodret: Isoleret mappe, hvor mistænkelige filer spærres inde (10 bogstaver):

2 lodret: Sikkert virtuelt testmiljø, hvor ukendt kode kan køre ufarligt (9 bogstaver):

4 lodret: Det, som overvågningen holder øje med, når programmer kører (7 bogstaver):

5 lodret: Regelbaseret analyse, der markerer filer med mistænkelig kode (9 bogstaver):

6 lodret: Programdelen, der gennem søger filer og endepunkter for trusler (7 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

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

ORDLISTE MED FAGUDTRYK

SIGNATUR

HEURISTIK

SANDKASSE

ADFAERD

OPDATERINGER

KARANTAENE

FALSKALARM

SCANNER

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK

- A. SIGNATUR
- B. HEURISTIK
- C. SANDKASSE
- D. ADFAERD
- E. OPDATERINGER
- F. FALSKALARM
- G. KARANTAENE
- H. SCANNER

DEFINITIONER OG MATCHFELTER

- ☐ 1. Entydigt kryptografisk aftryk, der bruges til at genkende kendte trusler.
- ☐ 2. Regelbaseret analyse, der markerer filer med mistænkelig kode.
- ☐ 3. Sikkert virtuelt testmiljø, hvor ukendt kode kan køre ufarligt.
- ☐ 4. Overvågning af kørende programmer for skadelige mønstre.
- ☐ 5. Jævnlig hentninger af definitioner til trusselsdatabasen.
- ☐ 6. Alarm, der fejlagtigt udpeger sikkert software som malware.
- ☐ 7. Afspærring af mistænkelige filer, så systemet ikke udsættes for dem.
- ☐ 8. Program, der scanner og beskytter endepunkter mod angreb.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige cybersikkerhedsbegreber. Skriv dine svar i indtastningsfelterne.

1. **UNASTIRG**

5. **TIEKSRHIU**

2. **ESSDAASKN**

6. **RFEAADD**

3. **OPIRENDERTG
A**

7. **AAKATENENR**

4. **ARKMSALFAL**

8. **CNRSENA**

Kontrolpunkt 8: Casestudier om cybersikkerhed

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

CASESTUDIE 1: SIGNATUR MOD HEURISTIK



Scenarie: En medarbejder henter et værktøj, som et andet team har lavet internt. Signaturscanneren godkender det, men den heuristiske scanner markerer det som mistænkeligt.

Diskussion: Forklar, hvorfor det skete, og hvordan man kontrollerer, om filen er sikker.

CASESTUDIE 2: HÅNDTERING AF FALSKE ALARMER



Scenarie: En udvikler kompilerer sit program, og antivirus udpeger den nye fil som malware og sætter den i karantæne.

Diskussion: Beskriv risikoen ved undtagelser, og forklar den rigtige løsning.

Sidste udfordring: Afkod chifferet

En cybersikkerhedsekspert beskytter netværkets aktiver mod trusselsaktører online. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter. Afkodet cybersikkerhedsbesked:

BOGSTAV-TIL-TAL-NØGLE

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

<u>6</u>	<u>9</u>	<u>14</u>	<u>4</u>	<u>14</u>	<u>25</u>	<u>13</u>	<u>1</u>	<u>12</u>	<u>23</u>	<u>1</u>	<u>18</u>	<u>5</u>	<u>13</u>	<u>5</u>	<u>4</u>
				<u>8</u>	<u>5</u>	<u>21</u>	<u>18</u>	<u>9</u>	<u>19</u>	<u>20</u>	<u>9</u>	<u>11</u>			

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del A)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q1: Hvordan genkender antivirus malware?

Ved at sammenligne med signaturer i en database, analysere koden heuristisk og overvåge adfærd i realtid.

Q2: Hvad er signaturbaseret genkendelse?

En scanning, der sammenligner kryptografiske filhashes med lister over kendt malware.

Q3: Hvad er en heuristisk scanner?

Heuristik analyserer filens opbygning og kode og markerer mønstre, der er typiske for malware.

Q4: Hvad betyder det, at en fil sættes i karantæne?

Antivirus flytter filen til en sikker, isoleret mappe og forhindrer, at den køres.

Q5: Hvad er en falsk alarm?

En fejl, hvor lovligt og sikkert software fejlagtigt udpeges som malware.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvordan beskytter adfærdsovervågning systemet?

Den overvåger kørende programmer i realtid og stopper processer, der forsøger mistænkelige ændringer som at indsprøjte kode.

Q7: Hvorfor er test i sandkasse vigtig?

Ukendte filer køres i en isoleret virtuel maskine, så deres handlinger kan iagttages uden risiko.

Q8: Hvor ofte bør definitionerne opdateres?

Dagligt eller hver time, så ny malware bliver genkendt.

Q9: Hvad er forskellen på antivirus og EDR?

Antivirus scanner filer, mens Endpoint Detection and Response (EDR) sporer og inddæmmer trusler i hele netværket.

Q10: Kan jeg køre to antivirusprogrammer samtidig?

Nej. To aktive scannere giver konflikter, gør systemet langsomt og kan blokere hinanden.

Kontrolpunkt 11: Avanceret FAQ om sikkerhed (del A)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og datacompliance.

Q1: Hvordan gør heuristiske regler det sværere at slippe forbi?

Heuristik ser på generelle mønstre frem for bestemte signaturer og fanger ændrede varianter af kendt malware.

Q2: Hvad er en polymorf virus?

Malware, der ændrer sin opbygning og dekryptering hver gang, den køres, så signaturer ikke virker.

Q3: Hvordan opdager sandkasser forsøg på at undgå virtuelle maskiner?

Moderne sandkasser efterligner museklik og opetid og snyder malware, der skjuler sig i virtuelle maskiner.

Q4: I hvilket format hentes signaturopdateringer?

Som regel små trinvis differencefiler, der sparer båndbredde.

Q5: Hvordan håndterer agenter lokale scanninger?

Agenterne laver lette tjek i baggrunden og overlader tunge opslag af hashes til trusselsdatabaser i skyen.

Kontrolpunkt 11: Avanceret FAQ om sikkerhed (del B)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og datacompliance.

Q6: Hvad er scanning efter rootkits?

Den scanner kernens hukommelsestabeller uden om de systemkald, som rootkits kaprer for at skjule sig.

Q7: Hvordan stopper adfærdsscanning ransomware?

Den opdager automatisk massekryptering af filer og stopper processen, før data bliver låst.

Q8: Hvad er kontrol af kodesigneringscertifikater?

Scannere kontrollerer kodens digitale signatur mod betroede certifikatudstedere og bekræfter udviklerens identitet.

Q9: Hvordan påvirker pakkeprogrammer scanningen?

De komprimerer eller krypterer malware, så scanneren skal pakke filen ud i hukommelsen, før signaturer kan sammenlignes.

Q10: Hvordan isolerer EDR automatisk?

EDR sætter kompromitterede endepunkter i karantæne på netværket, så angriberen ikke kan bevæge sig videre, men analytikere stadig har adgang.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Traditionelle signaturdatabaser rummer over 1 milliard unikke hashes for malware verden over.

2. SIKKERHEDSINDSIGT

Heuristiske scannere fanger op til 80 % af nye varianter, før der findes signaturer til dem.

3. SIKKERHEDSINDSIGT

Falske alarmer koster virksomheder tusindvis af timer om året til kontrol og gendannelse af filer.

4. SIKKERHEDSINDSIGT

Polymorf malware står for over 90 % af nutidens trusler og kræver heuristik og adfærdsforsvar.

6. SIKKERHEDSINDSIGT

Malwareforfattere skriver kode, der tjekker for sandkasser og venter med at køre for at snyde tidsgrænser.

5. SIKKERHEDSINDSIGT

Antivirus i skyen tjekker mistænkelige hashes mod globale databaser på under 10 millisekunder.

7. SIKKERHEDSINDSIGT

Opdateringer sendes ud til endepunkter verden over få minutter efter, at en ny trussel er bekræftet.

8. SIKKERHEDSINDSIGT

Adfærdsovervågning mod ransomware holder øje med bestemte Win32-kald til kryptering af filer og sletning af skyggekopier.

9. SIKKERHEDSINDSIGT

Generel heuristik springer software med gyldige kodecertifikater over for at undgå falske alarmer.

10. SIKKERHEDSINDSIGT

Rootkits ændrer kernens struktur og kræver særlige scannere ved opstart for at blive fundet og fjernet.

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale standarder fra NIST, OWASP og regler om databeskyttelse. VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[1] CISA. (2025). Cybersikkerhedsvarsler og -vejledninger.

<https://www.cisa.gov/news-events/>

[3] NIST. (2024). Special Publication 800-53: Sikkerheds- og privatlivskontroller.

[https://\[3\]csrc.nist.gov/publications/detail/sp/800-53/rev-5/final](https://[3]csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)

[5] NIST. (2023). Special Publication 800-88: Retningslinjer for sikker sletning af medier.

[https://\[5\]csrc.nist.gov/publications/detail/sp/800-88/rev-1/final](https://[5]csrc.nist.gov/publications/detail/sp/800-88/rev-1/final)

[7] IETF. (2022). RFC 7519: Specifikation af JSON Web Token (JWT).

<https://datatracker.ietf.org/>

[9] OWASP. (2024). Top 10 over sikkerhedsrisici i webapplikationer.

<https://owasp.org/www-project->

[2] [1] cybersecurity-advisories [2] GDPR. (2024).

Databeskyttelsesforordningen (GDPR), officiel tekst.

<https://gdpr-info.eu/>

[4] [4] NIST. (2023). Special Publication 800-61: Vejledning i håndtering af sikkerhedshændelser.

<https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

[6] IETF. (2021). RFC 8446: Specifikation af Transport Layer Security (TLS) 1.3.

[https://\[6\]datatracker.ietf.org/doc/rfc8446/](https://[6]datatracker.ietf.org/doc/rfc8446/)

[8] [7] doc/rfc7519/ Center for Internet Security (CIS). (2024). Kritiske sikkerhedskontroller.

[https://\[8\]www.cisecurity.org/controls/cis-controls-list](https://[8]www.cisecurity.org/controls/cis-controls-list)

[10] [9] top-ten/ OWASP. (2025). Standard for verifikation af applikationssikkerhed (ASVS).

<https://owasp.org/www->

Facitliste: Kontrolpunkt 1 – Multiple choice

1

SIGNATURER

UNDERVISNINGSNOTE

Rigtigt svar: A Signaturscanning bygger på kendte hashes og opdager ikke ukendt eller ændret malware. Kilde: OWASP Secure Configuration [Ref 10].

Rigtigt svar: A

2

HEURISTIK

UNDERVISNINGSNOTE

Rigtigt svar: A Heuristik analyserer kodens opbygning og kommandoer for at finde mistænkelige træk ved nye trusler. Kilde: Center for Internet Security (CIS) [Ref 8].

Rigtigt svar: A

3

SANDKASSE

UNDERVISNINGSNOTE

Rigtigt svar: A En sandkasse kører mistænkelige filer i en isoleret virtuel maskine, så adfærden kan iagttages sikkert. Kilde: NIST Digital Identity [Ref 9].

Rigtigt svar: A

4

ADFÆRD

UNDERVISNINGSNOTE

Rigtigt svar: A Adfærdsscanning overvåger kørende programmer i realtid og stopper uautoriserede ændringer. Kilde: Center for Internet Security (CIS) [Ref 8].

Rigtigt svar: A

5

OPDATERINGER

UNDERVISNINGSNOTE

Rigtigt svar: A Scannere henter daglige trinvis opdateringer for at følge med trusselsbilledet. Kilde: OWASP Secure Configuration [Ref 10].

Rigtigt svar: A

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6

SIGNATURER

UNDERVISNINGSNOTE

Rigtigt svar: Sandt Signaturværktøjer beregner kryptografiske hashes og sammenligner dem med en database over kendte trusler. Kilde: OWASP Secure Configuration [Ref 10].

Rigtigt svar: Sandt

7

HEURISTIK

UNDERVISNINGSNOTE

Rigtigt svar: Sandt Heuristiske motorer bruger regler, der kan udpege lovlige, sikre filer som mistænkelige. Kilde: Center for Internet Security (CIS) [Ref 8].

Rigtigt svar: Sandt

8

SANDKASSE

UNDERVISNINGSNOTE

Rigtigt svar: Falsk En sandkasse kører kode i en virtuel beholder og blokerer adgang til delte netværksmapper. Kilde: NIST Digital Identity [Ref 9].

Rigtigt svar: Falsk

9

ADFÆRD

UNDERVISNINGSNOTE

Rigtigt svar: Sandt Overvågning i realtid markerer processer, der forsøger ulovlig skrivning eller låsning af filer. Kilde: Center for Internet Security (CIS) [Ref 8].

Rigtigt svar: Sandt

10

FORSVAR

UNDERVISNINGSNOTE

Rigtigt svar: Falsk Almindelig signaturbaseret antivirus kan ikke stoppe zero-day-angreb uden heuristik. Kilde: OWASP Secure Configuration [Ref 10].

Rigtigt svar: Falsk

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

- | | | | |
|----------------------------------|---------------------------|----------------------------------|------------------------------|
| A 1. Hash-signatur | B 2. Kodeheuristik | C 3. Sandkasse til filer | D 4. Adfærdsscanning |
| E 5. Daglige opdateringer | F 6. Falsk alarm | G 7. Isolering af trusler | H 8. Antivirusværktøj |

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

- | | | | |
|-----------------------|---------------------|--------------------|-----------------|
| 1 SIGNATUR | 2 HEURISTIK | 3 SANDKASSE | 4 ADFÆRD |
| 5 OPDATERINGER | 6 FALSKALARM | | |

DISKUSSIONSNOTER TIL UNDERVISERE

Trusselsbilledet:

Kontrollér, at eleverne forstår, hvordan malware, phishing og zero-day-angreb rammer og bryder netværkets forsvar.

Forsvarskontroller:

Understreg brugen af netværksfirewalls, sandkasseafvikling, adfærdsscannere og multifaktorgodkendelse (MFA).

Overholdelse af lovgivning:

Fremhæv brugersamtykke, dataminimering, kryptering under lagring og transport samt globale rammer som GDPR og CCPA.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

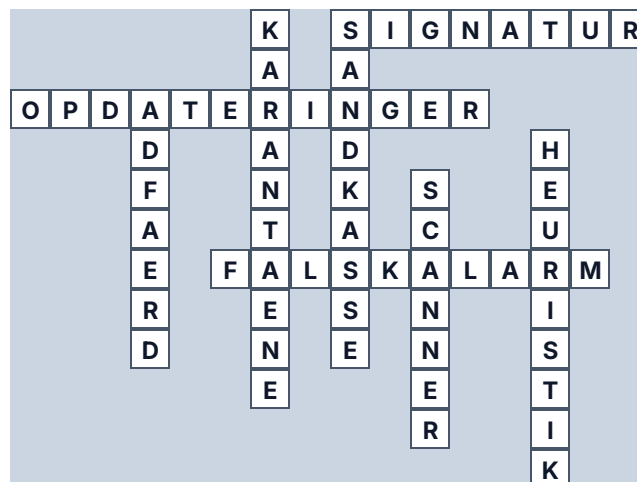
VANDRETTE NØGLER

2 vandret: SIGNATUR Entydigt kryptografisk aftryk, der bruges til at genkende kendte trusler (7,11)

3 vandret: OPDATERINGER Jævnlig hentninger af nye definitioner til trusselsdatabasen (9,3)

7 vandret: FALSKALARM Advarsel, der fejlagtigt udpeger sikkert software som malware (13,8)

LØSNING PÅ KRYDS OG TVÆRS



LODRETTE NØGLER

1 lodret: KARANTAENE Isoleret mappe, hvor mistænkelige filer spærres inde (7,9)

2 lodret: SANDKASSE Sikkert virtuelt testmiljø, hvor ukendt kode kan køre ufarligt (7,11)

4 lodret: ADFAERD Det, som overvågningen holder øje med, når programmer kører (9,6)

5 lodret: HEURISTIK Regelbaseret analyse, der markerer filer med mistænkelig kode (10,16)

6 lodret: SCANNER Programdelen, der gennem søger filer og endepunkter for trusler (11,13)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. UNASTIRG	SIGNATUR	5. TIEKSRHIU	HEURISTIK
2. ESSDAASKN	SANDKASSE	6. RFEAADD	ADFAERD
3. OPIRENDERTGA	OPDATERINGER	7. AAKATENENR	KARANTAENE
4. ARKMSALFAL	FALSKALARM	8. CNRSENA	SCANNER

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"FIND NY MALWARE MED HEURISTIK"

Facit til casestudier om domænemægling

A Casestudie 1: Signatur mod heuristik

[Underviserens løsning](#)

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En medarbejder henter et værktøj, som et andet team har lavet internt. Signaturscanneren godkender det, men den heuristiske scanner markerer det som mistænkeligt.
- Anbefalet strategi og løsning: Årsag: Signaturscanning tjekker hashes, og et internt værktøj findes ikke i databasen. Heuristikken så på opbygningen og markerede mistænkelige handlinger (f.eks. skrivning i registreringsdatabasen). Kontrol: Kør filen i en sandkasse, tjek den digitale signatur, og indsend hashen til portaler med trusselsdata.

B Casestudie 2: Håndtering af falske alarmer

[Underviserens løsning](#)

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En udvikler kompilerer sit program. Antivirus udpeger den nye fil som malware og sætter den i karantæne.
- Anbefalet strategi og løsning: Risiko ved undtagelser: Hvis scanneren omgås, kan ægte inficeret kode køre. Løsning: Send filen til antivirusleverandøren til analyse, signér koden med et certifikat fra en udsteder, og opret midlertidige undtagelser for bestemte mapper i stedet for at slå antivirus fra.