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 signaturdatabaser, 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.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

Åbn VPN.com's guide til cybersikkerhed

URL: https://www.vpn.com/da/cybersikkerhed/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 flervalgs- 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. Slut af med bonusaktiviteten Tænk hurtigt.

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: Flervalgsopgave

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. 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 usignerede programmer
- D. Ved at uploade alle filer til en offentlig cloudmappe

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. 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. Ugentlige manuelle gennemgange af installerede programmer

5. Hvorfor er jævnlige opdateringer af definitioner vigtige?

- A. For at give signaturmotoren 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

ADFÆRD | FALSK ALARM | HEURISTIK | KARANTÆNE | OPDATERINGER | SANDKASSE | SCANNER | SIGNATUR

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

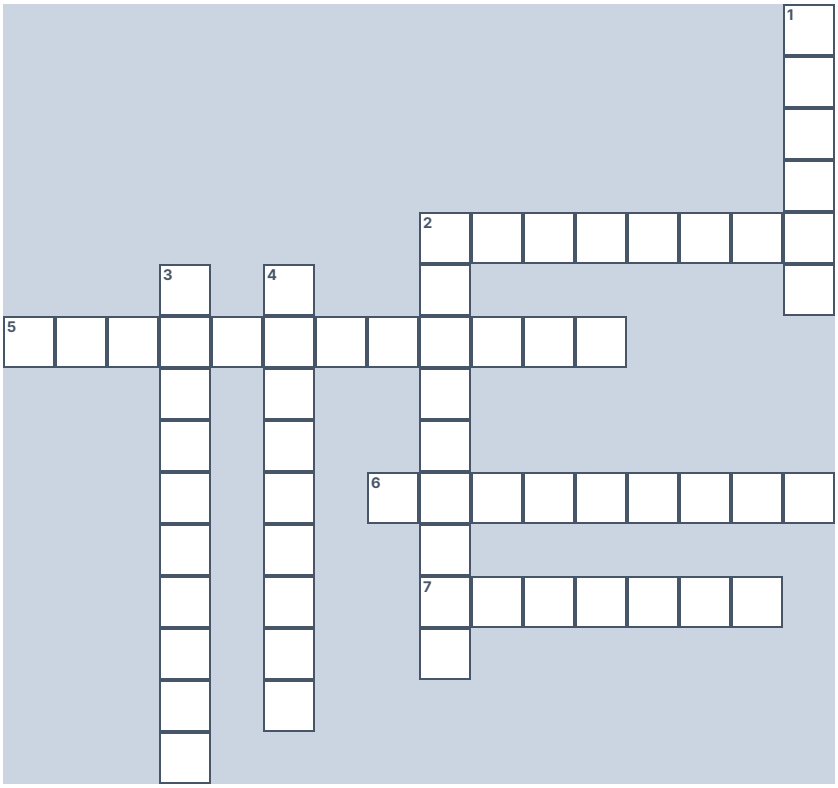
MATCH BEGREBER OG DEFINITIONER

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

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

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)

5. Jævnlige hentninger af nye definitioner til trusselsdatabasen (12)

6. Isoleret mappe, hvor mistænkelige filer spærres inde (9)

7. Programdelen, der gennemsøger filer og endepunkter for trusler (7)

LODRETTE NØGLER

1. Det, som overvågningen holder øje med, når programmer kører (6)

2. Sikkert virtuelt testmiljø, hvor ukendt kode kan køre ufarligt (9)

3. Advarsel, der fejlagtigt udpeger sikkert software som malware (10)

4. Regelbaseret analyse, der markerer filer med mistænkelig kode (9)

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):

5 vandret: Jævnlige hentninger af nye definitioner til trusselsdatabasen (12 bogstaver):

6 vandret: Isoleret mappe, hvor mistænkelige filer spærres inde (9 bogstaver):

7 vandret: Programdelen, der gennemsøger filer og endepunkter for trusler (7 bogstaver):

LODRETTE NØGLER

1 lodret: Det, som overvågningen holder øje med, når programmer kører (6 bogstaver):

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

3 lodret: Advarsel, der fejlagtigt udpeger sikkert software som malware (10 bogstaver):

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

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

SIGNATUR HEURISTIK SANDKASSE ADFÆRD OPDATERINGER KARANTÆNE 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. ADFÆRD
E. OPDATERINGER
F. KARANTÆNE
G. FALSKALARM
H. SCANNER

DEFINITIONER OG MATCHFELTER	
	1. Det, som overvågningen holder øje med, når programmer kører.
	2. Programdelen, der gennemsøger filer og endepunkter for trusler.
	3. Jævnlige hentninger af nye definitioner til trusselsdatabasen.
	4. Regelbaseret analyse, der markerer filer med mistænkelig kode.
	5. Advarsel, der fejlagtigt udpeger sikkert software som malware.
	6. Entydigt kryptografisk aftryk, der bruges til at genkende kendte trusler.
	7. Sikkert virtuelt testmiljø, hvor ukendt kode kan køre ufarligt.
	8. Isoleret mappe, hvor mistænkelige filer spærres inde.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. **U N A S T I R G** _____
2. **E S S D A A S K N** _____
3. **O P I R E N D E R T G A** _____
4. **A R K M S A L F A L** _____
5. **T I E K S R H I U** _____
6. **R Æ A F D D** _____
7. **T K N E Æ A A N R** _____
8. **C N R S E N A** _____

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Grunde til at opdatere software			
2	Personer, du kan spørge om it-hjælp			
3	Ting, du gør, når antivirus finder noget			
4	Tegn på en computervirus			
5	Ting, der kommer i karantæne			
6	Steder, hvor virus gemmer sig			
7	Oplysninger, du aldrig bør dele			
8	Typer af skadelig software			
9	Sikkerhedsværktøjer, du kender			
10	Ting, et antivirus scanner			
11	Ting, du tager backup af			
12	Enheder, der kan blive hacket			
13	Antivirusprogrammer, du kender			
14	Grunde til falske alarmer			
15	Sikkerhedsvaner, du kan starte i dag			

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.

Kontrolpunkt 9: 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.

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 Æ=27 Ø=28 Å=29

6	9	14	4		14	25		13	1	12	23	1	18	5		13	5	4

8	5	21	18	9	19	20	9	11

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

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 10: Avanceret FAQ om sikkerhed (del C)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

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 oppetid og snyder malware, der skjuler sig i virtuelle maskiner.

Q4: I hvilket format hentes signaturopdateringer?

Som regel små trinvise 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 10: Avanceret FAQ om sikkerhed (del D)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

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

Signaturdatabaser gemmer hashværdier af kendt malware, så helt nye eller ændrede filer overses, indtil definitionerne opdateres.

2. SIKKERHEDSINDSIGT

Heuristiske motorer kan markere nogle nye malwarevarianter, før der findes signaturer, men på bekostning af flere falske alarmer.

3. SIKKERHEDSINDSIGT

Falske alarmer koster IT-teams tid på at kontrollere og gendanne filer, der fejlagtigt er sat i karantæne.

4. SIKKERHEDSINDSIGT

Polymorf malware ændrer sin kode for hver kopi, så forsvarere kombinerer signaturer med heuristiske og adfærdsbaserede kontroller.

6. SIKKERHEDSINDSIGT

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

5. SIKKERHEDSINDSIGT

Skybaserede antivirusmotorer tjekker mistænkelige filers hashværdier mod store onlinetrusselsdatabaser næsten i realtid.

7. SIKKERHEDSINDSIGT

Leverandører sender jævnligt definitionsopdateringer ud til enhederne, så scannere kan genkende nyligt bekræftede trusler.

8. SIKKERHEDSINDSIGT

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

9. SIKKERHEDSINDSIGT

Gyldige kodesignaturer kan mindske risikoen for falske alarmer, men signerede filer scannes stadig, da malware også kan være signeret.

10. SIKKERHEDSINDSIGT

Rootkits ændrer kernens strukturer 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] 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

Facitliste: Kontrolpunkt 1 – Flervalg

1 **Spørgsmål 1** SIGNATURER **Rigtigt svar: A**

UNDERVISNINGSNOTE

Signaturscanning bygger på kendte hashes og opdager ikke ukendt eller ændret malware.

2 **Spørgsmål 2** HEURISTIK **Rigtigt svar: A**

UNDERVISNINGSNOTE

Heuristik analyserer kodens opbygning og kommandoer for at finde mistænkelige træk ved nye trusler.

3 **Spørgsmål 3** SANDKASSE **Rigtigt svar: A**

UNDERVISNINGSNOTE

En sandkasse kører mistænkelige filer i en isoleret virtuel maskine, så adfærden kan iagttages sikkert.

4 **Spørgsmål 4** ADFÆRD **Rigtigt svar: A**

UNDERVISNINGSNOTE

Adfærdsscanning overvåger kørende programmer i realtid og stopper uautoriserede ændringer.

5 **Spørgsmål 5** OPDATERINGER **Rigtigt svar: A**

UNDERVISNINGSNOTE

Scannere henter daglige trinvise opdateringer for at følge med trusselsbilledet.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Spørgsmål 6** SIGNATURER — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Signaturværktøjer beregner kryptografiske hashes og sammenligner dem med en database over kendte trusler.

7 **Spørgsmål 7** HEURISTIK — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Heuristiske motorer bruger regler, der kan udpege lovlige, sikre filer som mistænkelige.

8 **Spørgsmål 8** SANDKASSE — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

En sandkasse kører kode i en virtuel beholder og blokerer adgang til delte netværksmapper.

9 **Spørgsmål 9** ADFÆRD — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Overvågning i realtid markerer processer, der forsøger ulovlig skrivning eller låsning af filer.

10 **Spørgsmål 10** — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Intet antivirusprogram stopper alle zero-day-angreb; ukendte trusler kan undgå signaturer og heuristik.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt parring (8 point i alt) og hvert korrekt kontekstbegreb (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

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

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 SIGNATUR	2 HEURISTIK	3 SANDKASSE	4 ADFÆRD
5 OPDATERINGER	6 FALSK ALARM		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 D – ADFÆRD	2 H – SCANNER	3 E – OPDATERINGER	4 B – HEURISTIK
5 G – FALSKALARM	6 A – SIGNATUR	7 C – SANDKASSE	8 F – KARANTÆNE

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare Hash-signatur, Kodeheuristik og Sandkasse til filer med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

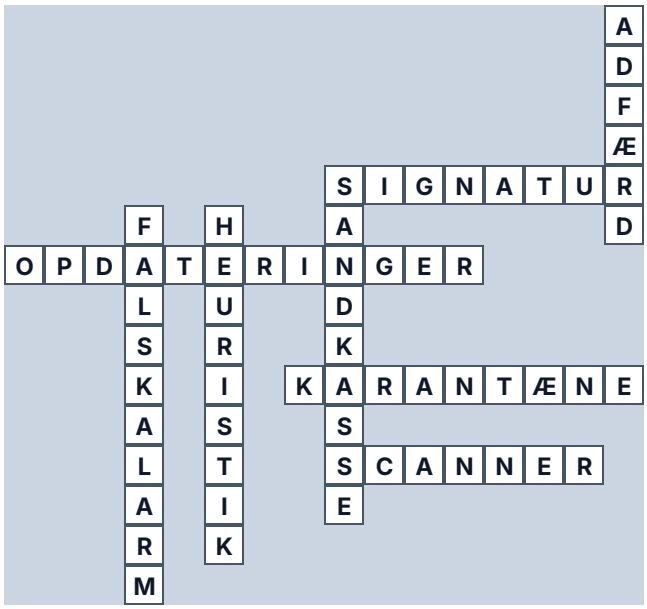
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



VANDRETTE NØGLER

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

5 vandret: OPDATERINGER Jævnlige hentninger af nye definitioner til trusselsdatabasen (12 bogstaver)

6 vandret: KARANTÆNE Isoleret mappe, hvor mistænkelige filer spærres inde (9 bogstaver)

7 vandret: SCANNER Programdelen, der gennemsøger filer og endepunkter for trusler (7 bogstaver)

LODRETTE NØGLER

1 lodret: ADFÆRD Det, som overvågningen holder øje med, når programmer kører (6 bogstaver)

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

3 lodret: FALSKALARM Advarsel, der fejlagtigt udpeger sikkert software som malware (10 bogstaver)

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

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. U N A S T I R G — **SIGNATUR**
2. E S S D A A S K N — **SANDKASSE**
3. O P I R E N D E R T G A — **OPDATERINGER**
4. A R K M S A L F A L — **FALSKALARM**
5. T I E K S R H I U — **HEURISTIK**
6. R Æ A F D D — **ADFÆRD**
7. T K N E Æ A A N R — **KARANTÆNE**
8. C N R S E N A — **SCANNER**

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"FIND NY MALWARE MED HEURISTIK"

Facit til casestudier

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.