Navn: _____ Dato: _____ Poeng: _____

Antivirusprogramvare og endepunkt Veiledning om beskyttelse

Signaturdeteksjon, heuristikk, atferdsovervåking, sandboxing, oppdateringer

LÆRINGSOVERSIKT OM ANTIVIRUSPROGRAMVARE

SIKRET

DATAKRYPTERING

256-bits AES-standard

I SAMSVAR

GLOBALE STANDARDER

Rammeverk for GDPR og CCPA

ZERO TRUST

TILGANGSPOLICY

Flerfaktorautentisering

Velkommen! Dette aktivitetsheftet veileder deg gjennom antivirusprogramvare og endepunktbeskyttelse. Du utforsker signaturdatabaser, heuristiske skannere, atferdsovervåking, virtuelle sandkassefiler og reduksjon av falske positiver.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk cybersikkerhet og forebygging av trusler.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om cybersikkerhet

URL: https://www.vpn.com/no/cybersikkerhet/antivirus/

Din læringsveiledning for antivirusstrategi

- Skill mellom signaturbasert og heuristikkbasert oppdagelse av skadevare.
- Forstå overvåking av atferd og protokoller for sandkasseisolasjon.
- Vurder hvordan sanntidsskanning påvirker ytelsen til system og endepunkter.
- Redusere falske positive klassifiseringer ved hjelp av verifisering av digitale sertifikater.
- Administrere daglig distribusjon av definisjonsoppdateringer til bedriftens endepunkter.

VEILEDNING FOR ANTIVIRUS

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på antivirussikkerhet for endepunkter. Avslutt med bonusaktiviteten Tenk raskt.

ANTIVIRUSBESKYTTELSE OG SIGNATURSKANNING (INNLEDNING)

Antivirusprogramvare beskytter endepunkter ved å identifisere, sette i karantene og fjerne skadevare. Moderne systemer kombinerer signaturdatabaser (som matcher hasher for kjente trusler) med heuristikk (som analyserer filstruktur) og atferdsovervåking for å oppdage nulldagsangrep.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er en begrensning ved signaturbasert deteksjon?

- A. Den kan ikke identifisere ukjent eller modifisert skadevare
- B. Den gir mange falske positiver
- C. Den krever høy CPU-kraft
- D. Den fungerer bare når du er koblet til internett

2. Hvordan oppdager heuristiske skannere nye varianter av skadevare?

- A. Ved å identifisere mistenkelige mønstre og kodestrukturer
- B. Ved å sammenligne filhasher med en database over trusler
- C. Ved automatisk å slette alle usignerte kjørbare filer
- D. Ved å laste opp hver fil til en offentlig skymappe

3. Hva er formålet med kjøring av antivirus i sandkasse?

- A. Å isolere og analysere filer i et sikkert virtuelt hvelv
- B. Å øke hastigheten på overføring av sikkerhetskopier av det lokale filsystemet
- C. Å oppdatere sikkerhetsoppdateringene i det lokale operativsystemet
- D. Å komprimere store dokumentfiler for å spare lagringsplass

4. Hvilken deteksjonsmetode flagger trusselatferd i sanntid?

- A. Atferdsanalyse som overvåker programvarens handlinger
- B. Gjennomgang av historiske logger som utføres over natten
- C. Manuell brukerrapportering av trege apper
- D. Ukentlige manuelle gjennomganger av installerte programmer

5. Hvorfor er jevnlige oppdateringer av definisjoner avgjørende for skannere?

- A. Å mate signaturmotorer med trusselidentifikatorer fra databasen
- B. Å øke CPU-klokkehastigheten under drift
- C. For å endre mellomlagringstidene for globale DNS-navneservere
- D. For å autorisere innstillinger for informasjonskapsler i nettleseren

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål (sant/usant) 6

6. Signaturdeteksjon sammenligner kryptografiske filhasher med databaselister.

- ◯ Sant
- ◯ Usant

7 Spørsmål (sant/usant) 7

7. Heuristiske skannere kan utløse falske positive varsler på trygge filer.

- ◯ Sant
- ◯ Usant

8 Spørsmål (sant/usant) 8

8. En sandkasse lar skadevare få tilgang til nettverksfiler uten begrensninger.

- ◯ Sant
- ◯ Usant

9 Spørsmål (sant/usant) 9

9. Atferdsskanning blokkerer filer når de viser ondsinnede handlinger.

- ◯ Sant
- ◯ Usant

10 Spørsmål (sant/usant) 10

10. Standard antivirusprogramvare stopper alle zero-day-angrep fullstendig.

- ◯ Sant
- ◯ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. En tradisjonell skanner baserer seg på sammenligning med kjente _____ for å identifisere kjent skadevare.

2. Å analysere kodemønstre i filer kalles skanning med _____ .

3. Antivirusverktøy isolerer mistenkelige filer i et miljø kalt _____ .

4. Sanntidsovervåking holder øye med programmenes _____ for å oppdage mistenkelig aktivitet.

5. Skannere laster ned _____ av databasen hver dag for å gjenkjenne nye trusler.

6. Trygge programmer som blir merket som skadevare, utløser varsler av typen _____ .

ORDBANK

ATFERD BRANNMUR FALSK POSITIV HEURISTIKK LØSEPENGEVIRUS OPPDATERINGER SANDKASSE SIGNATUR

Skriv svarene dine her:

1.

2.

3.

4.

5.

6.

Kontrollpunkt 4: Koble sikkerhetsbegreper

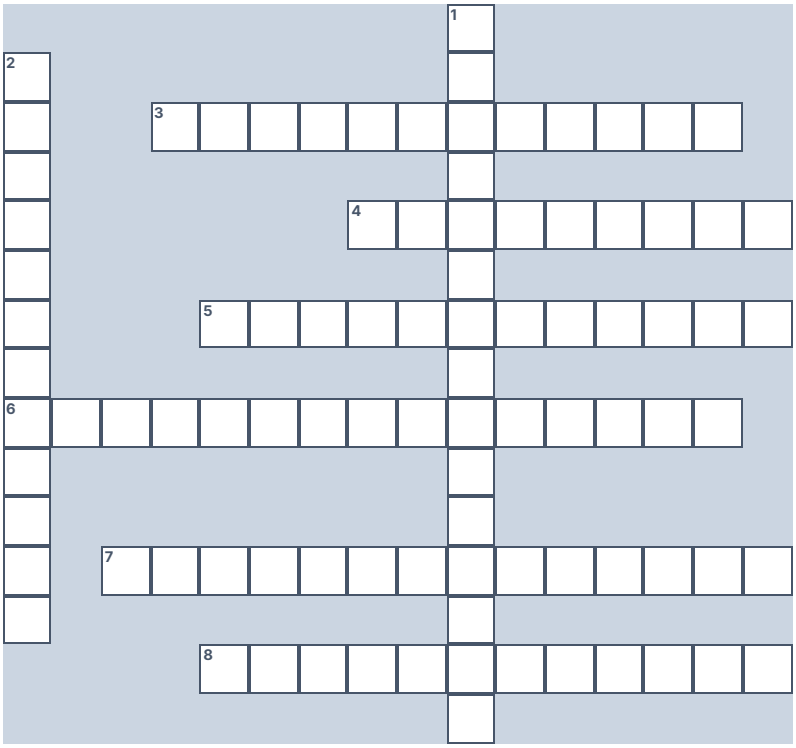
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. Hash-signatur	A	Å isolere mistenkelige filer for å hindre eksponering av det lokale systemet.
☐	2. Kodeheuristikk	B	Programvarepakke som skanner og beskytter endepunkter mot sårbarhetsutnyttelse.
☐	3. FIL-SANDKASSE	C	Overvåking av handlinger som kjøres av programvare, for å finne ondsinnede mønstre.
☐	4. Atferdsskanning	D	Unikt kryptografisk databasefingeravtrykk som brukes til å identifisere kjente trusler.
☐	5. Daglige oppdateringer	E	Sikkert virtuelt testmiljø som kjører upålitelig kode trygt.
☐	6. Falsk positiv	F	Regelmessige nedlastinger av definisjoner som mater trusseldatabasen.
☐	7. Trusselisolering	G	Regelbasert analyse som flagger filer med mistenkelig kodeoppbygging.
☐	8. Antivirusverktøy	H	Sikkerhetsvarsel som feilaktig klassifiserer trygg programvare som skadevare.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

3. Unikt kryptografisk fingeravtrykk i en database som brukes til å identifisere kjente trusler (12)

4. Å holde mistenkelige filer avgrenset slik at det lokale systemet ikke utsettes (9)

5. Sikkerhetsvarsel som feilaktig klassifiserer trygg programvare som skadevare (12)

6. Overvåking av hva kjørende programvare gjør, for å finne mønstre som tyder på skadelig drift (15)

7. Regelbasert analyse som flagger filer med mistenkelig kodeoppbygning (14)

8. Sikkert virtuelt testmiljø som kjører ikke-klarert kode på en trygg måte (12)

LODDRETT

1. Jevnlige nedlastinger av definisjoner som mater trusseldatabasen (15)

2. Programvarepakke som skanner og beskytter endepunkter mot utnyttelse av sårbarheter (12)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.
HORISONTALE HINT VERTIKALE HINT

VANNRETT

3 vannrett: Unikt kryptografisk fingeravtrykk i en database som brukes til å identifisere kjente trusler (12 bokstaver):

4 vannrett: Å holde mistenkelige filer avgrenset slik at det lokale systemet ikke utsettes (9 bokstaver):

5 vannrett: Sikkerhetsvarsel som feilaktig klassifiserer trygg programvare som skadevare (12 bokstaver):

6 vannrett: Overvåking av hva kjørende programvare gjør, for å finne mønstre som tyder på skadelig drift (15 bokstaver):

7 vannrett: Regelbasert analyse som flagger filer med mistenkelig kodeoppbygning (14 bokstaver):

8 vannrett: Sikkert virtuelt testmiljø som kjører ikke-klarert kode på en trygg måte (12 bokstaver):

LODDRETT

1 loddrett: Jevnlige nedlastinger av definisjoner som mater trusseldatabasen (15 bokstaver):

2 loddrett: Programvarepakke som skanner og beskytter endepunkter mot utnyttelse av sårbarheter (12 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

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

ORDLISTE

HASHSIGNATUR KODEHEURISTIKK FILSANDKASSE ATFERDSSKANNING
DAGSOPPDATERING FALSKPOSITIV ISOLERING VIRUSSKANNER

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER

- **A. HASHSIGNATUR**
- **B. KODEHEURISTIKK**
- **C. FILSANDKASSE**
- **D. ATFERDSSKANNING**
- **E. DAGSOPPDATERING**
- **F. FALSKPOSITIV**
- **G. ISOLERING**
- **H. VIRUSSKANNER**

DEFINISJONER OG TILHØRENDE FELT

1. Overvåking av hva kjørende programvare gjør, for å finne mønstre som tyder på skadelig drift.
2. Programvarepakke som skanner og beskytter endepunkter mot utnyttelse av sårbarheter.
3. Jevnlige nedlastinger av definisjoner som mater trusseldatabasen.
4. Regelbasert analyse som flagger filer med mistenkelig kodeoppbygning.
5. Å holde mistenkelige filer avgrenset slik at det lokale systemet ikke utsettes.
6. Unikt kryptografisk fingeravtrykk i en database som brukes til å identifisere kjente trusler.
7. Sikkert virtuelt testmiljø som kjører ikke-klarert kode på en trygg måte.
8. Sikkerhetsvarsel som feilaktig klassifiserer trygg programvare som skadevare.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. AINSAGTHUSRH
2. EIANFSSLKADS
3. DGTANPAERSDGPIO
4. EGNLIRISO
5. SDIORIHKETUKKE
6. NSIFDSANGNATKER
7. SIKFAOVTILPS
8. ARSNKRVSIENU

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Grunner til å oppdatere programvare			
2	Personer du kan spørre om IT-hjelp			
3	Ting å gjøre når antivirusprogrammet finner noe			
4	Tegn på et datavirus			
5	Ting som settes i karantene			
6	Steder der virus skjuler seg			
7	Informasjon du aldri bør dele			
8	Typer skadelig programvare			
9	Sikkerhetsverktøy du kjenner til			
10	Ting et antivirusprogram skanner			
11	Ting du tar sikkerhetskopi av			
12	Enheter som kan hackes			
13	Antivirusprogrammer du kjenner til			
14	Grunner til falske alarmer			
15	Trygge vaner du kan begynne med i dag			

Kontrollpunkt 8: Casestudier om cybersikkerhet

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: SIGNATURSKANNING MOT HEURISTISK SKANNING



Scenario: En ansatt laster ned et tilpasset verktøy som et annet team har utviklet internt. Signaturskanneren godkjenner det, men den heuristiske skanneren markerer det som mistenkelig.

Diskusjonsspørsmål: Forklar hvorfor dette skjedde, og hvordan man kan kontrollere om filen er trygg.

CASESTUDIE 2: HÅNDTERE FALSKE POSITIVE



Scenario: En programvareutvikler kompilerer applikasjonen sin. Systemets antivirusprogram markerer den nye kjørbare filen som skadevare og setter den i karantene.

Diskusjonsspørsmål: Gjør rede for risikoene ved hvitelisting, og beskriv riktig løsningsmetode.

Kontrollpunkt 9: Knekk chifferet

En cybersikkerhetsekspert beskytter nettverksressurser mot trusselaktører på nettet. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

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

15	16	16	4	1	7		14	25		19	11	1	4	5	22	1	18	5
13	5	4		8	5	21	18	9	19	20	9	19	11					
11	15	4	5	1	14	1	12	25	19	5								

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del A)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q1: Hvordan identifiserer antivirusprogramvare skadevare?

Den identifiserer skadevare ved hjelp av signaturmatching mot database, heuristisk analyse av kodeoppbygging og overvåking av atferd i sanntid.

Q2: Hva er signaturbasert gjenkjenning?

Det er en skannemetode som sammenligner kryptografiske filhasher med databaselister over kjente skadevaretrusler.

Q3: Hva er en heuristisk skanner?

Heuristikk analyserer en fils struktur og kodeinstruksjoner og flagger mistenkelige mønstre som er vanlige i varianter av skadevare.

Q4: Hva betyr det at en fil er satt i karantene?

Antivirusprogrammet flytter filen til en sikker, isolert mappe og blokkerer kjøring for å beskytte operativsystemet.

Q5: Hva er en falsk positiv i antivirus?

Det er en feil der legitim, trygg programvare feilaktig flagges som skadevare av skannealgoritmer.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del B)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q6: Hvordan beskytter atferdsovervåking systemer?

Den overvåker programvare som kjører i sanntid og blokkerer prosesser som forsøker mistenkelige endringer, som å injisere kode.

Q7: Hvorfor er testing i sandkasse (sandbox) viktig?

Sandkassekjøring kjører ikke-pålitelige filer i en isolert virtuell maskin og observerer handlingene trygt uten eksponering av systemet.

Q8: Hvor ofte bør antivirusdefinisjoner oppdateres?

Skannere bør oppdatere definisjoner daglig eller hver time for å gjenkjenne nylig oppdagede skadevarestammer.

Q9: Hva er forskjellen mellom antivirus og EDR?

Antivirus fokuserer på filskanning, mens Endpoint Detection and Response (EDR) gir sporing og inneslutning av trusler i hele nettverket.

Q10: Kan jeg kjøre to antivirusprogrammer sammen?

Nei. Å kjøre to aktive skannere fører til systemkonflikter, gjør ytelsen dårligere og kan hindre hverandres operasjoner.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del C)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q1: Hvordan minimerer heuristiske regler omgåelse av trusler?

Heuristikk analyserer generelle trusselmønstre i stedet for bestemte signaturer, og fanger dermed opp endrede varianter av kjente skadevarefamilier.

Q2: Hva er et polymorft virus?

Det er skadevare som endrer filoppsettet og dekrypteringsrutinen ved hver kjøring, noe som gjør signaturskanninger ineffektive.

Q3: Hvordan oppdager sandkasser (sandboxes) unngåelse av virtuelle maskiner?

Moderne sandkasser simulerer museklikk og oppetid for systemet og lurer skadevare som er laget for å skjule seg når den kjører i virtuelle maskiner.

Q4: Hva er nedlastingsformatene for signaturoppdateringer?

Oppdateringer er vanligvis lette inkrementelle binære differansefiler, som minimerer klientens bruk av nettverksbåndbredde.

Q5: Hvordan håndterer endepunktagenter lokale skanninger?

Agenter utfører lette bakgrunnskontroller og overlater dyptgående kryptografiske hash-oppslag til trusseldatabaser i skyen.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del D)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q6: Hva er skanning for å oppdage rootkits?

Den skanner minnetabeller på kjernenivå og omgår OS-API-er som rootkits kobler seg på for å skjule de aktive trådene sine.

Q7: Hvordan blokkerer atferdsskanning løsepengevirus?

Den oppdager automatiske løkker med massekryptering av filer og avslutter vertsprosessen før systemdatabasene låses.

Q8: Hva er verifisering av kodesigneringssertifikater?

Skannere kontrollerer digitale kodesignaturer mot pålitelige rotsertifikatutstedere og validerer programvareutviklerens identitet.

Q9: Hvordan påvirker pakkere (packers) skannemotorer?

Pakkere komprimerer eller krypterer nyttelasten i skadevare. Skannere må pakke ut filen i minnet før signaturene kan sjekkes.

Q10: Hvordan automatiserer EDR-verktøy isolering?

EDR-agenter setter kompromitterte endepunkter i karantene på nettverksnivå, blokkerer lateral bevegelse og gir samtidig analytikere tilgang.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Signaturdatabaser lagrer hasher av kjent skadevare, så helt nye eller endrede filer overses til definisjonene oppdateres.

2. SIKKERHETSINNSIKT

Heuristiske motorer kan flagge enkelte nye varianter av skadevare før det finnes signaturer, til prisen av flere falske positiver.

3. SIKKERHETSINNSIKT

Falske positive varsler koster IT-team tid brukt på å verifisere og gjenopprette filer som ble satt feilaktig i karantene.

4. SIKKERHETSINNSIKT

Polymorf skadevare endrer koden sin for hver kopi, så forsvarerne kombinerer signaturer med heuristiske kontroller og atferdskontroller.

6. SIKKERHETSINNSIKT

Skadevareforfattere skriver tilpasset kode som er laget for å sjekke sandkassemiljøer og utsetter kjøringen for å omgå tidtakere.

5. SIKKERHETSINNSIKT

Skybaserte antivirusmotorer sjekker hash-verdiene til mistenkelige filer mot store trusseldatabaser på nett nesten i sanntid.

7. SIKKERHETSINNSIKT

Leverandører sender jevnlig oppdateringer av definisjoner til endepunkter slik at skannere kan gjenkjenne nylig bekreftede trusler.

8. SIKKERHETSINNSIKT

Atferdsovervåkere for løsepengevirus retter seg mot bestemte Win32-API-kall som er knyttet til filkryptering og sletting av skyggekopier.

9. SIKKERHETSINNSIKT

Gyldige kodesignaturer kan redusere risikoen for falske positive, men signerte filer skannes likevel, siden skadevare også kan signeres.

10. SIKKERHETSINNSIKT

Rootkits endrer systemets kjernestrukturer, og krever spesialiserte skannere ved oppstart for å oppdage og fjerne dem.

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale standarder fra NIST og OWASP og standarder for etterlevelse av personvern. FAGLIGE OG BRANSJEMESSIGE REFERANSER

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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

Fasit: Kontrollpunkt 1 – flervalg

1 **Spørsmål 1** SIGNATURER **Riktig svar: A**

MERKNAD TIL LÆREREN

Signaturskanning bygger på kjente hash-verdier i databaser og klarer derfor ikke å oppdage ukjent eller modifisert skadevare.

2 **Spørsmål 2** HEURISTIKK **Riktig svar: A**

MERKNAD TIL LÆREREN

Heuristikk analyserer kodens oppbygning og kommandoer for å identifisere mistenkelige trekk ved nye trusselvarianter.

3 **Spørsmål 3** SANDKASSEKJØRING **Riktig svar: A**

MERKNAD TIL LÆREREN

En sandkasse kjører mistenkelige filer i en isolert virtuell maskin for å observere kjøringsatferden på en trygg måte.

4 **Spørsmål 4** ATFERDSBASERT **Riktig svar: A**

MERKNAD TIL LÆREREN

Atferdsskanning overvåker kjørende programmer i sanntid for å blokkere uautoriserte systemendringer.

5 **Spørsmål 5** OPPDATERINGER **Riktig svar: A**

MERKNAD TIL LÆREREN

Skannere laster ned daglige inkrementelle definisjonsoppdateringer for å holde seg synkronisert med trusselbildet.

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Spørsmål 6** SIGNATURER **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Signaturverktøy beregner kryptografiske hash-verdier og sammenligner dem med en database over kjente trusselhash-verdier.

7 **Spørsmål 7** HEURISTIKK **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Heuristiske motorer bruker regelbaserte oppsett som kan merke legitime, trygge filer som mistenkelige.

8 **Spørsmål 8** SANDKASSEKJØRING **Riktig svar: Usant**

MERKNAD TIL LÆREREN

En sandkasse kjører kode i en virtuell container og blokkerer strengt tilgang til nettverksressurser.

9 **Spørsmål 9** ATFERDSBASERT **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Sanntidsovervåking flagger kjørende prosesser som forsøker ulovlig skriving eller fillåsing.

10 **Spørsmål 10** **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Ingen antivirusprogram stopper alle zero-day-angrep; ukjente trusler kan unngå signaturer og heuristikk.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

D 1. Hash-signatur	G 2. Kodeheuristikk	E 3. FIL-SANDKASSE	C 4. Atferdsskanning
F 5. Daglige oppdateringer	H 6. Falsk positiv	A 7. Trusselisolering	B 8. Antivirusverktøy

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 SIGNATUR	2 HEURISTIKK	3 SANDKASSE	4 ATFERD
5 OPPDATERINGER	6 FALSK POSITIV		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 D – ATFERDSSKANNING	2 H – VIRUSSKANNER	3 E – DAGSOPPDATERING	4 B – KODEHEURISTIKK
5 G – ISOLERING	6 A – HASHSIGNATUR	7 C – FILSANDKASSE	8 F – FALSKPOSITIV

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare Hash-signatur, Kodeheuristikk og FIL-SANDKASSE med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

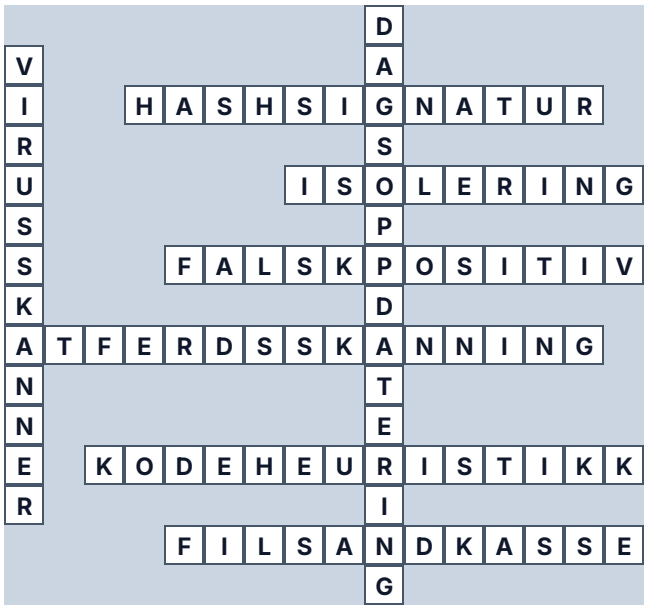
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



VANNRETT

3 vannrett: HASHSIGNATUR Unikt kryptografisk fingeravtrykk i en database som brukes til å identifisere kjente trusler (12 bokstaver)

4 vannrett: ISOLERING Å holde mistenkelige filer avgrenset slik at det lokale systemet ikke utsettes (9 bokstaver)

5 vannrett: FALSKPOSITIV Sikkerhetsvarsel som feilaktig klassifiserer trygg programvare som skadevare (12 bokstaver)

6 vannrett: ATFERDSSKANNING Overvåking av hva kjørende programvare gjør, for å finne mønstre som tyder på skadelig drift (15 bokstaver)

7 vannrett: KODEHEURISTIKK Regelbasert analyse som flagger filer med mistenkelig kodeoppbygning (14 bokstaver)

8 vannrett: FILSANDKASSE Sikkert virtuelt testmiljø som kjører ikke-klarert kode på en trygg måte (12 bokstaver)

LODDRETT

1 loddrett: DAGSOPPDATERING Jevnlige nedlastinger av definisjoner som mater trusseldatabasen (15 bokstaver)

2 loddrett: VIRUSSKANNER Programvarepakke som skanner og beskytter endepunkter mot utnyttelse av sårbarheter (12 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. AINSAGTHUSRH — **HASHSIGNATUR**
2. EIANFSSLKADS — **FILSANDKASSE**
3. DGTANPAERSDGPIO — **DAGSOPPDATERING**
4. EGNLIRISO — **ISOLERING**
5. SDIORIHKETUKKE — **KODEHEURISTIKK**
6. NSIFDSANGNATKER — **ATFERDSSKANNING**
7. SIKFAOVTILPS — **FALSKPOSITIV**
8. ARSNKRVSIENU — **VIRUSSKANNER**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"OPPDAG NY SKADEVARE MED HEURISTISK KODEANALYSE"

Fasit til casestudiene

A Casestudie 1: Signaturskanning mot heuristisk skanning

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En ansatt laster ned et egendefinert verktøy som er bygget internt av et annet team. Signaturskanneren godkjenner det, men heuristikkskanneren flagger det som mistenkelig.
- Anbefalt strategi og løsning: Hvorfor det skjedde: Signaturskanning sjekker filens hasher; fordi filen er egenutviklet, finnes den ikke i trusseldatabasen. Heuristikk analyserer strukturen og flagget mistenkelige handlinger (f.eks. skriving til registeret). Verifisering: Kjør filen i en sandkasse for å observere handlingene, kontroller digitale signaturer og send hashen til portaler for trusseletterretning.

B Casestudie 2: Håndtere falske positive

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En programvareutvikler kompilerer applikasjonen sin. Systemets antivirusprogram flagger den nye kjørbare filen som skadevare og setter den i karantene.
- Anbefalt strategi og løsning: Risiko ved hviteliste: Å omgå skannere kan la ekte, infisert kode kjøre. Løsningsvei: Send filen til antivirusleverandøren for analyse, signer koden digitalt med sertifiseringsinstanser og konfigurer midlertidige unntak for bestemte mapper i stedet for å slå av antivirusprogrammet.