Namn: _____ **Datum:** _____ **Poäng:** _____

Antivirusprogram och slutpunkter Skyddsguide

Signaturbaserad upptäckt, heuristik, beteendeövervakning, sandlådekörning, uppdateringar

ÖVERSIKT: LÄR DIG OM ANTIVIRUSPROGRAM

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom antivirusprogram och slutpunktsskydd. Du utforskar signaturdatabaser, heuristiska skannrar, beteendeövervakning, virtuella sandlådefiler och hur man minskar falska positiva.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska cybersäkerhet och hothantering.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s guide om cybersäkerhet

URL: https://www.vpn.com/sv/cybersakerhet/antivirusprogram/

Din inlärningsplan för antivirusstrategi

- Skilj mellan signaturbaserad och heuristisk identifiering av skadlig kod.
- Förstå beteendeövervakning och protokoll för sandlådeisolering.
- Utvärdera effekterna av realtidsskanning på systemprestanda och slutpunkter.
- Minska felaktiga klassificeringar (falska positiva) med hjälp av verifiering av digitala certifikat.
- Hantera den dagliga distributionen av definitionsuppdateringar över företagets slutpunkter.

INSTRUKTIONER FÖR ANTIVIRUS

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om antivirusskydd för slutpunkter. Avsluta med bonusaktiviteten Tänk snabbt.

ANTIVIRUSSKYDD OCH SIGNATURSKANNING (INLEDNING)

Antivirusprogram skyddar slutpunkter genom att identifiera, sätta i karantän och ta bort skadlig kod. Moderna system kombinerar signaturdatabaser (som matchar hashvärden för kända hot) med heuristik (som analyserar filstruktur) och beteendeövervakning för att upptäcka nolldagsangrepp.

LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA

Kontrollpunkt 1: Utmaning med flerval

1. Vad är en begränsning med signaturbaserad detektering?

- A. Den kan inte identifiera okänd eller modifierad skadlig kod
- B. Den ger många falska positiva träffar
- C. Den kräver hög CPU-kraft
- D. Den fungerar bara när den är ansluten till internet

2. Hur upptäcker heuristiska skannrar nya varianter av skadlig kod?

- A. Genom att identifiera misstänkta mönster och kodstrukturer
- B. Genom att matcha filers hashvärden mot en databas över hot
- C. Genom att automatiskt radera alla osignerade körbara filer
- D. Genom att ladda upp varje fil till en offentlig molnmapp

3. Vad är syftet med att köra antivirus i sandbox?

- A. Att isolera och analysera filer i ett säkert virtuellt valv
- B. Att snabba upp överföringen av lokal säkerhetskopiering av filsystemet
- C. Att uppdatera det lokala operativsystemets säkerhetsuppdateringar
- D. Att komprimera stora dokumentfiler för att spara lagringsutrymme

4. Vilken detekteringsmetod flaggar hotbeteende i realtid?

- A. Beteendeanalys som övervakar programmens åtgärder
- B. Inspektion av historiska loggar som utförs över natten
- C. Manuell användarrapportering om långsamma appar
- D. Veckovisa manuella genomgångar av installerade program

5. Varför är regelbundna uppdateringar av definitioner avgörande för skannrar?

- A. Att mata signaturmotorers databaser med hotidentifierare
- B. För att öka CPU:ns klockfrekvens under drift
- C. Att ändra cachetider för globala DNS-namnservrar
- D. För att godkänna webbläsarens cookieinställningar

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga sant/falskt 6

6. Signaturbaserad upptäckt jämför kryptografiska filhashar med databaslistor.

- ( ) Sant
- ( ) Falskt

7 Fråga sant/falskt 7

7. Heuristiska skannrar kan ge falska positiva larm på säkra filer.

- ( ) Sant
- ( ) Falskt

8 Fråga sant/falskt 8

8. En sandlåda låter skadlig kod komma åt nätverksfiler utan begränsningar.

- ( ) Sant
- ( ) Falskt

9 Fråga sant/falskt 9

9. Beteendeskanning blockerar filer när de uppvisar skadliga handlingar.

- ( ) Sant
- ( ) Falskt

10 Fråga sant/falskt 10

10. Vanlig antivirusprogramvara stoppar helt alla zero day-attacker.

- ( ) Sant
- ( ) Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. En traditionell skanner identifierar känd skadlig kod genom matchning mot _____ .
2. Att analysera filers kodmönster kallas _____ .
3. Antivirusprogram isolerar misstänkta filer i en _____ .
4. Övervakning i realtid följer programmens _____ för att hitta misstänkt aktivitet.
5. Skannrar laddar ner dagliga _____ av databasen för att känna igen nya hot.
6. Säkra program som flaggas som skadlig kod utlöser så kallade _____ .

ORDBANK

BETEENDE FALSKA POSITIVA HEURISTISK SKANNING ISOLERING SANDLÅDA SIGNATURER UPPDATERINGAR VIRUSSKYDD

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

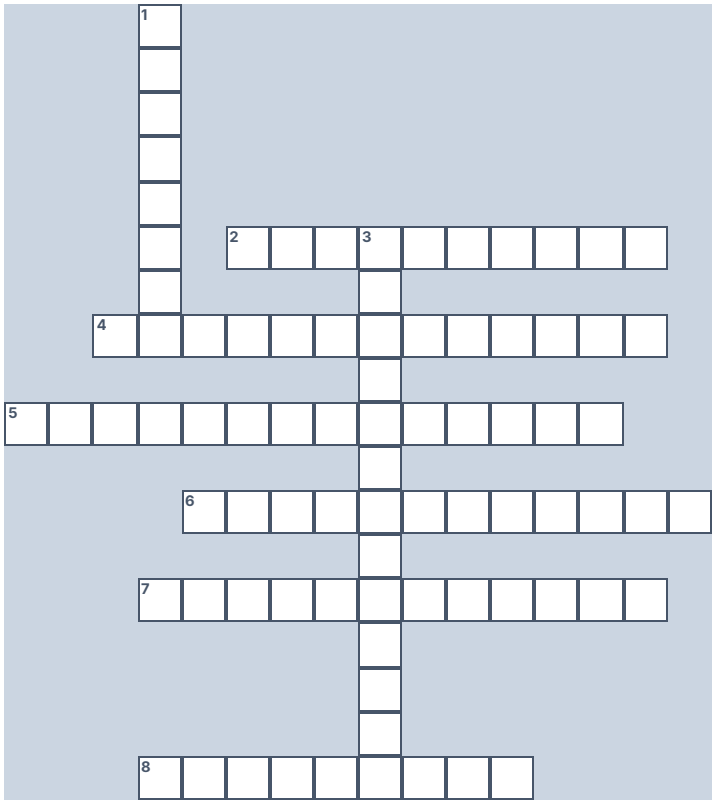
MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

☐	1. Hashsignatur	A	Att isolera misstänkta filer för att förhindra att det lokala systemet exponeras.
☐	2. Kodheuristik	B	Programsvit som skannar och skyddar slutpunkter mot exploateringar.
☐	3. Filsandlåda	C	Övervakning av vad körande programvara gör för att hitta skadliga aktivitetsmönster.
☐	4. Beteendeskanning	D	Unikt kryptografiskt databasavtryck som används för att identifiera kända hot.
☐	5. Dagliga uppdateringar	E	Säker virtuell testmiljö som kör obetrodd kod på ett tryggt sätt.
☐	6. Falskt positivt	F	Regelbundna nedladdningar av definitioner som matar hotdatabasen.
☐	7. Hotisolering	G	Regelbaserad analys som flaggar filer med misstänkta kodstrukturer.
☐	8. Antivirusverktyg	H	Säkerhetsvarning som felaktigt klassar säker programvara som skadlig kod.

Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.



VÅGRÄTT

2. Programpaket som skannar och skyddar slutenheter mot sårbarhetsutnyttjande (10)

4. Säkerhetslarm som felaktigt klassar ofarlig programvara som skadlig kod (13)

5. Övervakning av vad körande programvara gör för att hitta skadliga mönster (14)

6. Regelbaserad analys som flaggar filer med misstänkt kodstruktur (12)

7. Unikt kryptografiskt databasfotavtryck som används för att identifiera kända hot (12)

8. Att låsa in misstänkta filer så att det lokala systemet inte utsätts (9)

LODRÄTT

1. Säker virtuell testmiljö där ej betrodd kod körs riskfritt (8)

3. Regelbundna nedladdningar av definitioner som matar hotdatabasen (13)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.
HORISONTELLA LEDTRÅDAR VERTIKALA LEDTRÅDAR

VÅGRÄTT

2 vågrätt: Programpaket som skannar och skyddar slutenheter mot sårbarhetsutnyttjande (10 bokstäver):

4 vågrätt: Säkerhetslarm som felaktigt klassar ofarlig programvara som skadlig kod (13 bokstäver):

5 vågrätt: Övervakning av vad körande programvara gör för att hitta skadliga mönster (14 bokstäver):

6 vågrätt: Regelbaserad analys som flaggar filer med misstänkt kodstruktur (12 bokstäver):

7 vågrätt: Unikt kryptografiskt databasfotavtryck som används för att identifiera kända hot (12 bokstäver):

8 vågrätt: Att låsa in misstänkta filer så att det lokala systemet inte utsätts (9 bokstäver):

LODRÄTT

1 lodrätt: Säker virtuell testmiljö där ej betrodd kod körs riskfritt (8 bokstäver):

3 lodrätt: Regelbundna nedladdningar av definitioner som matar hotdatabasen (13 bokstäver):

Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

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

ORDLISTA

HASHSIGNATUR, KODHEURISTIK, SANDLÅDA, BETEENDEANALYS, UPPDATERINGAR, FALSKTPOSITIV, ISOLERING, VIRUSSKYDD

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. HASHSIGNATUR**
- **B. KODHEURISTIK**
- **C. SANDLÅDA**
- **D. BETEENDEANALYS**
- **E. UPPDATERINGAR**
- **F. FALSKTPOSITIV**
- **G. ISOLERING**
- **H. VIRUSSKYDD**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Övervakning av vad körande programvara gör för att hitta skadliga mönster.
2. Programpaket som skannar och skyddar slutenheter mot sårbarhetsutnyttjande.
3. Regelbundna nedladdningar av definitioner som matar hotdatabasen.
4. Regelbaserad analys som flaggar filer med misstänkt kodstruktur.
5. Att låsa in misstänkta filer så att det lokala systemet inte utsätts.
6. Unikt kryptografiskt databasfotavtryck som används för att identifiera kända hot.
7. Säker virtuell testmiljö där ej betrodd kod körs riskfritt.
8. Säkerhetslarm som felaktigt klassar ofarlig programvara som skadlig kod.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp och termer inom cybersäkerhet. Skriv dina svar i rutorna.

1. AINSAGTHUSRH
2. DSAADÅLN
3. PURNIARPEATGD
4. EGNLIRISO
5. OTIRKDESUKIH
6. NDAETLEYNBEASE
7. ITOTFASKVILPS
8. DUSDVSIKYR

Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

1	Skäl till att uppdatera programvara			
2	Personer du kan fråga om IT-hjälp			
3	Saker att göra när antivirusprogrammet hittar något			
4	Tecken på ett datorvirus			
5	Saker som hamnar i karantän			
6	Platser där virus gömmer sig			
7	Information du aldrig bör dela			
8	Typer av skadlig programvara			
9	Säkerhetsverktyg du känner till			
10	Saker som ett antivirusprogram skannar			
11	Saker du säkerhetskopierar			
12	Enheter som kan hackas			
13	Antivirusprogram du känner till			
14	Skäl till falsklarm			
15	Säkra vanor du kan börja med i dag			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

FALLSTUDIE 1: SIGNATURSKANNING MOT HEURISTISK SKANNING



Scenario: En anställd laddar ner ett skräddarsytt verktyg som ett annat team har byggt internt. Signaturskannern släpper igenom det, men den heuristiska skannern flaggar det som misstänkt.

Diskussionsfråga: Förklara varför detta hände och hur du kan kontrollera om filen är säker.

FALLSTUDIE 2: HANTERA FALSKA POSITIVA



Scenario: En programvaruutvecklare kompilerar sin applikation. Systemets antivirusprogram flaggar den nya körbara filen som skadlig kod och placerar den i karantän.

Diskussionsfråga: Beskriv riskerna med att vitlista filen och redogör för den rätta lösningen.

Kontrollpunkt 9: Knäck chiffret

En cybersäkerhetsexpert skyddar nätverkstillgångar mot hotaktörer online. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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 Å=27 Ä=28 Ö=29

21 16 16 20 28 3 11 14 25 19 11 1 4 12 9 7

11 15 4 13 5 4 8 5 21 18 9 19 20 9 19 11

11 15 4 1 14 1 12 25 19

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del A)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q1: Hur identifierar antivirusprogram skadlig kod?

Den identifierar skadlig kod med hjälp av signaturmatchning mot databaser, heuristisk analys av kodlayout och beteendeövervakning i realtid.

Q2: Vad är signaturbaserad detektering?

Det är en skanningsmetod som matchar kryptografiska filhashar mot databaslistor över kända hot från skadlig kod.

Q3: Vad är en heuristisk skanner?

Heuristik analyserar en fils struktur och kodinstruktioner och flaggar misstänkta mönster som är vanliga i varianter av skadlig kod.

Q4: Vad betyder det när en fil sätts i karantän?

Antiviruset flyttar filen till en säker, isolerad mapp och blockerar körning för att skydda operativsystemet.

Q5: Vad är ett falsklarm i antivirusprogram?

Det är ett fel där legitim, säker programvara felaktigt flaggas som skadlig kod av skanningsalgoritmer.

Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del B)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

Q6: Hur skyddar beteendeövervakning system?

Den övervakar program som körs i realtid och blockerar processer som försöker göra misstänkta ändringar, som att injicera kod.

Q7: Varför är testning i sandlåda viktig?

Sandlådekörning kör opålitliga filer i en isolerad virtuell maskin och observerar åtgärderna säkert utan att systemet exponeras.

Q8: Hur ofta bör antivirusdefinitioner uppdateras?

Skannrar bör uppdatera definitioner dagligen eller varje timme för att känna igen nyupptäckta typer av skadlig kod.

Q9: Vad är skillnaden mellan antivirus och EDR?

Antivirus fokuserar på filskanning, medan Endpoint Detection and Response (EDR) ger nätverksövergripande hotspårning och isolering.

Q10: Kan jag köra två antivirusprogram samtidigt?

Nej. Att köra två aktiva skannrar orsakar systemkonflikter, sänker prestandan och kan blockera varandras funktioner.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del C)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q1: Hur minimerar heuristiska regler att hot slinker förbi?

Heuristik analyserar allmänna hotmönster snarare än specifika signaturer och fångar upp modifierade varianter av kända familjer av skadlig kod.

Q2: Vad är ett polymorft virus?

Det är skadlig kod som ändrar sin fillayout och sin dekrypteringsrutin vid varje körning, vilket gör signaturskanningar verkningslösa.

Q3: Hur upptäcker sandlådor att skadlig kod försöker undvika virtuella maskiner?

Moderna sandlådor simulerar musklick och systemets drifttid och lurar skadlig kod som är utformad för att gömma sig när den körs i virtuella maskiner.

Q4: Vilka nedladdningsformat har signaturuppdateringar?

Uppdateringar är oftast lätta inkrementella binära diff-filer, vilket minimerar klientens bandbreddsförbrukning.

Q5: Hur hanterar slutpunktsagenter lokala skanningar?

Agenter utför lätta bakgrundskontroller och lägger över djupa kryptografiska hashuppslag på molnbaserade hotdatabaser.

Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del D)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

Q6: Vad är skanning för att upptäcka rootkits?

Den skannar minnestabeller på kärnnivå och kringgår operativsystemets API:er som rootkits kopplar in sig i för att dölja sina aktiva trådar.

Q7: Hur blockerar beteendeskanning ransomware?

Den upptäcker automatiserade massfilskrypteringsloopar och avslutar värdprocessen innan systemdatabaser låses.

Q8: Vad är verifiering av certifikat för kodsignering?

Skannrar kontrollerar kodens digitala signaturer mot betrodda rotcertifikatutfärdare och validerar programvaruutvecklarens identitet.

Q9: Hur påverkar packare skanningsmotorer?

Packare komprimerar eller krypterar skadliga nyttolaster. Skannrar måste packa upp filen i minnet innan signaturmatchningar körs.

Q10: Hur automatiserar EDR-verktyg isolering?

EDR-agenter sätter kompromitterade slutpunkter i karantän på nätverksnivå, vilket blockerar lateral rörelse samtidigt som analytiker behåller åtkomst.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

Signaturdatabaser lagrar hashar av känd skadlig kod, så helt nya eller ändrade filer missas tills definitionerna uppdateras.

2. SÄKERHETSINSIKT

Heuristiska motorer kan flagga vissa nya varianter av skadlig kod innan signaturer finns, till priset av fler falska positiva.

3. SÄKERHETSINSIKT

Falska positiva larm kostar IT-team tid för att verifiera och återställa filer som felaktigt satts i karantän.

4. SÄKERHETSINSIKT

Polymorf skadlig kod ändrar sin kod för varje kopia, så försvarare kombinerar signaturer med heuristiska kontroller och beteendekontroller.

6. SÄKERHETSINSIKT

Skapare av skadlig kod skriver anpassad kod som kontrollerar sandlådemiljöer och fördröjer körningen för att kringgå tidsgränser.

5. SÄKERHETSINSIKT

Molnbaserade antivirusmotorer kontrollerar hashvärden för misstänkta filer mot stora onlinedatabaser över hot i nära realtid.

7. SÄKERHETSINSIKT

Leverantörer skickar regelbundet ut definitionsuppdateringar till slutpunkter så att skannrar kan känna igen nyligen bekräftade hot.

8. SÄKERHETSINSIKT

Beteendeövervakare mot ransomware inriktar sig på specifika Win32 API-anrop som hör ihop med filkryptering och radering av skuggkopior.

9. SÄKERHETSINSIKT

Giltiga kodsignaturer kan minska risken för falska positiva, men signerade filer skannas ändå eftersom skadlig kod också kan vara signerad.

10. SÄKERHETSINSIKT

Rootkits ändrar systemkärnans strukturer, vilket kräver specialiserade skannrar vid uppstart för att upptäckas och rensas.

Tekniska referenser och källor

Studieguiden och de interaktiva pusslen är sammanställda utifrån globala standarder från NIST och OWASP samt standarder för efterlevnad av dataskydd. VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[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

Facit: Kontrollpunkt 1 – Flerval

1 **Fråga 1** SIGNATURER **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Signaturskanning bygger på kända hashvärden i databaser och upptäcker därför inte okänd eller modifierad skadlig kod. Källa: OWASP Secure Configuration.

2 **Fråga 2** HEURISTIK **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Heuristik analyserar kodens uppbyggnad och kommandon för att identifiera misstänkta drag hos nya hotvarianter. Källa: Center for Internet Security (CIS).

3 **Fråga 3** SANDLÅDEKÖRNING **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

En sandbox kör misstänkta filer i en isolerad virtuell maskin för att säkert observera körbeteendet. Källa: NIST Digital Identity.

4 **Fråga 4** BETEENDEBASERAD **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Beteendeskanning övervakar program som körs i realtid för att blockera obehöriga systemändringar. Källa: Center for Internet Security (CIS).

5 **Fråga 5** UPPDATERINGAR **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Skannrar laddar ned dagliga inkrementella definitionsuppdateringar för att hålla sig synkroniserade med hotbilden. Källa: OWASP Secure Configuration.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Fråga 6** SIGNATURER **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Signaturverktyg beräknar kryptografiska hashvärden och matchar dem mot en databas med kända hothashar. Källa: OWASP Secure Configuration.

7 **Fråga 7** HEURISTIK **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Heuristiska motorer kör regelbaserade mönster som kan flagga legitima, säkra filer som misstänkta. Källa: Center for Internet Security (CIS).

8 **Fråga 8** SANDLÅDEKÖRNING **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

En sandbox kör kod i en virtuell container och blockerar strikt åtkomst till nätverksresurser. Källa: NIST Digital Identity.

9 **Fråga 9** BETEENDEBASERAD **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Realtidsövervakning flaggar processer som körs och försöker göra otillåtna skrivningar eller fillåsning. Källa: Center for Internet Security (CIS).

10 **Fråga 10** **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Inget antivirusprogram stoppar alla zero-day-attacker; okända hot kan undvika signaturer och heuristik.

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

D 1. Hashsignatur	G 2. Kodheuristik	E 3. Filsandlåda	C 4. Beteendeskanning
F 5. Dagliga uppdateringar	H 6. Falskt positivt	A 7. Hotisolering	B 8. Antivirusverktyg

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 SIGNATURER	2 HEURISTISK SKANNING	3 SANDLÅDA	4 BETEENDE
5 UPPDATERINGAR	6 FALSKA POSITIVA		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 D – BETEENDEANALYS	2 H – VIRUSSKYDD	3 E – UPPDATERINGAR	4 B – KODHEURISTIK
5 G – ISOLERING	6 A – HASHSIGNATUR	7 C – SANDLÅDA	8 F – FALSKTPOSITIV

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara Hashsignatur, Kodheuristik och Filsandlåda med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

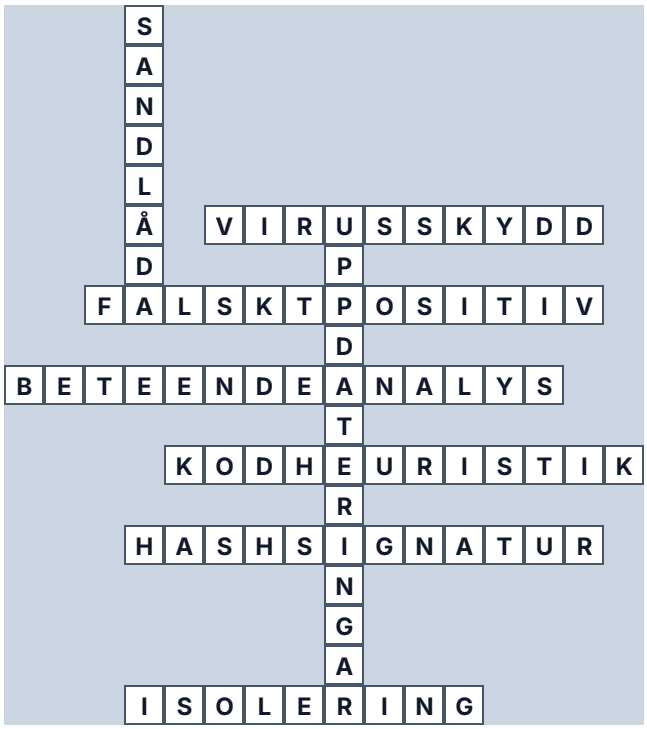
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



VÅGRÄTT

2 vågrätt: VIRUSSKYDD Programpaket som skannar och skyddar slutenheter mot sårbarhetsutnyttjande (10 bokstäver)

4 vågrätt: FALSKTPOSITIV Säkerhetslarm som felaktigt klassar ofarlig programvara som skadlig kod (13 bokstäver)

5 vågrätt: BETEENDEANALYS Övervakning av vad körande programvara gör för att hitta skadliga mönster (14 bokstäver)

6 vågrätt: KODHEURISTIK Regelbaserad analys som flaggar filer med misstänkt kodstruktur (12 bokstäver)

7 vågrätt: HASHSIGNATUR Unikt kryptografiskt databasfotavtryck som används för att identifiera kända hot (12 bokstäver)

8 vågrätt: ISOLERING Att låsa in misstänkta filer så att det lokala systemet inte utsätts (9 bokstäver)

LODRÄTT

1 lodrätt: SANDLÅDA Säker virtuell testmiljö där ej betrodd kod körs riskfritt (8 bokstäver)

3 lodrätt: UPPDATERINGAR Regelbundna nedladdningar av definitioner som matar hotdatabasen (13 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. AINSAGTHUSRH — **HASHSIGNATUR**
2. DSAADÅLN — **SANDLÅDA**
3. PURNIARPEATGD — **UPPDATERINGAR**
4. EGNLIRISO — **ISOLERING**
5. OTIRKDESUKIH — **KODHEURISTIK**
6. NDAETLEYNBEASE — **BETEENDEANALYS**
7. ITOTFASKVILPS — **FALSKTPOSITIV**
8. DUSDVSIKYR — **VIRUSSKYDD**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"UPPTÄCK NY SKADLIG KOD MED HEURISTISK KODANALYS"

Facit till fallstudierna

A Fallstudie 1: Signaturskanning mot heuristisk skanning

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En anställd laddar ned ett anpassat verktyg som byggts internt av ett annat team. Signaturskannern släpper igenom det, men den heuristiska skannern flaggar det som misstänkt.
- Rekommenderad strategi och lösning: Varför det hände: Signaturskanning kontrollerar filers hashvärden; eftersom filen är egentillverkad finns den inte i hotdatabasen. Heuristik analyserar strukturen och flaggade misstänkta åtgärder (t.ex. skrivningar till registret). Verifiering: Kör filen i en sandlåda för att observera åtgärderna, kontrollera digitala signaturer och skicka hashvärdet till portaler för hotunderrättelser.

B Fallstudie 2: Hantera falska positiva

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En programvaruutvecklare kompilerar sin applikation. Systemets antivirusprogram flaggar den nya körbara filen som skadlig kod och sätter den i karantän.
- Rekommenderad strategi och lösning: Risker med vitlistning: Att kringgå skannrar kan låta verklig, infekterad kod köras. Lösning: Skicka filen till antivirusleverantören för analys, signera koden digitalt via certifikatutfärdare och konfigurera tillfälligt specifika mappundantag i stället för att stänga av antivirusprogrammet.