Nimi: _____ Päivämäärä: _____ Pisteet: _____

Virustorjuntaohjelmisto ja päätelaitteet Suojausopas

Allekirjoitustunnistus, heuristiikka, käyttäytymisen seuranta, hiekkalaatikointi, päivitykset

VIRUSTORJUNTAOHJELMISTO: OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: virustorjuntaohjelmistot ja päätelaitteiden suojaus. Tutustut allekirjoitustietokantoihin, heuristisiin skannereihin, käyttäytymisen valvontaan, hiekkalaatikon virtuaalitiedostoihin ja virheellisten hälytysten vähentämiseen.

TEHTÄVÄMONISTEEN TARKISTUSPISTEET

- [ ] **Osat 1–4: Hallitse kyberturvallisuus ja uhkien ehkäisy.**
- [ ] **Osat 5–7: Ratkaise ristisanatehtäviä ja sanahakuja.**
- [ ] **Osat 8–9: Ratkaise tapaustutkimuksia ja salakirjoitushaaste.**
- [ ] **Osa 10: Tarkista perus- ja jatkotason UKK-sivut.**
- [ ] **Osa 11: Tutustu 10 mielenkiintoiseen tosielämän faktaan.**
- [ ] **Bonus: Nopeat vastaukset -haaste.**

Avaa VPN.comin kyberturvallisuusopas

URL: https://www.vpn.com/fi/kyberturvallisuus/virustorjunta/

Oppimispolkusi: virustorjuntastrategia

- Erota toisistaan allekirjoituspohjainen ja heuristinen haittaohjelmien tunnistus.
- Ymmärrä käyttäytymisen valvonta ja hiekkalaatikkoeristyksen protokollat.
- Arvioi reaaliaikaisten skannausten vaikutuksia järjestelmän suorituskykyyn ja päätelaitteisiin.
- Vähennä vääriä positiivisia luokituksia digitaalisten varmenteiden tarkistuksella.
- Hallitse päivittäisten määritelmäpäivitysten jakelua yrityksen päätelaitteille.

VIRUSTORJUNTAOPAS: OHJEET

Vastaa monivalinta- ja tosi/epätosi-kysymyksiin, täydennä aukkolauseet sanapankin avulla, yhdistä määritelmät sekä ratkaise ristisanatehtävä ja sanahaku. Sovella osaamistasi näihin aiheisiin: päätelaitteiden virustorjunta. Lopuksi bonustehtävä Nopeat vastaukset.

VIRUSTORJUNTA JA ALLEKIRJOITUSSKANNAUS (JOHDANTO)

Virustorjuntaohjelmisto suojaa päätelaitteita tunnistamalla, eristämällä ja poistamalla haittaohjelmia. Nykyaikaiset järjestelmät yhdistävät allekirjoitustietokannat (tunnettujen uhkien tiivisteiden vertailu), heuristiikan (tiedostorakenteen analysointi) ja toiminnan seurannan nollapäivähaavoittuvuuksien havaitsemiseksi.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on allekirjoituspohjaisen tunnistuksen rajoite?

- A. Se ei pysty tunnistamaan tuntemattomia tai muokattuja haittaohjelmia
- B. Se tuottaa paljon vääriä hälytyksiä
- C. Se vaatii paljon suoritinkapasiteettia
- D. Se toimii vain internetiin yhdistettynä

2. Miten heuristiset skannerit havaitsevat uusia haittaohjelmavariantteja?

- A. Tunnistamalla epäilyttäviä kaavoja ja koodirakenteita
- B. Vertaamalla tiedostojen tiivisteitä uhkien tietokantaan
- C. Poistamalla automaattisesti kaikki allekirjoittamattomat suoritustiedostot
- D. Lataamalla jokaisen tiedoston julkiseen pilvikansioon

3. Mikä on virustentorjunnan hiekkalaatikkosuorituksen tarkoitus?

- A. Tiedostojen eristäminen ja analysointi suojatussa virtuaalisessa holvissa
- B. Paikallisen tiedostojärjestelmän varmuuskopiosiirron nopeuttaminen
- C. Paikallisen käyttöjärjestelmän tietoturvakorjausten päivittäminen
- D. Suurten asiakirjatiedostojen pakkaaminen tallennustilan säästämiseksi

4. Mikä tunnistusmenetelmä merkitsee uhkakäyttäytymisen reaaliajassa?

- A. Käyttäytymisanalyysi, joka valvoo ohjelmiston toimia
- B. Yöllä tehtävä historiallisten lokien tarkastus
- C. Käyttäjän manuaalinen ilmoitus hitaista sovelluksista
- D. Asennettujen ohjelmien viikoittaiset manuaaliset tarkastukset

5. Miksi säännölliset tunnistetietojen päivitykset ovat ratkaisevan tärkeitä haittaohjelmatarkistimille?

- A. Syöttää allekirjoitusmoottoreille tietokannan uhkatunnisteet
- B. Nostaa suorittimen kellotaajuuksia toimintojen aikana
- C. Maailmanlaajuisten DNS-nimipalvelinten välimuistiaikojen muuttaminen
- D. Selaimen evästeasetusten valtuuttaminen

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys tf 6

6. Allekirjoituspohjainen tunnistus vertaa kryptografisia tiedostotiivisteitä tietokantalistoihin.

○ Tosi ○ Epätosi

7 Kysymys tf 7

7. Heuristiset skannerit voivat laukaista vääriä positiivisia hälytyksiä turvallisista tiedostoista.

○ Tosi ○ Epätosi

8 Kysymys tf 8

8. Hiekkalaatikko sallii haittaohjelman käyttää verkkotiedostoja rajoituksetta.

○ Tosi ○ Epätosi

9 Kysymys tf 9

9. Toimintaan perustuva tarkistus estää tiedostot, kun ne osoittavat haitallista toimintaa.

○ Tosi ○ Epätosi

10 Kysymys tf 10

10. Tavallinen virustorjuntaohjelmisto pysäyttää kaikki nollapäivähyökkäykset täysin.

○ Tosi ○ Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

Lue jokainen alla oleva lause ja täytä aukko oikealla termillä sanapankista.

1. Perinteinen skanneri tunnistaa tunnetut haittaohjelmat _____ -vertailun avulla.
2. Tiedostojen koodimallien analysointia kutsutaan _____ -skannaukseksi.
3. Virustorjuntaohjelmat eristävät epäilyttävät tiedostot _____ -ympäristöön.
4. Reaaliaikainen _____ seuraa ohjelmien toimintaa epäilyttävien toimien varalta.
5. Skannerit lataavat tietokantaan päivittäin uusia määrityksiä uusien uhkien tunnistamiseksi; ne ovat _____ .
6. Kun turvallinen ohjelma merkitään haittaohjelmaksi, kyseessä on _____ .

SANASTON SANAPANKKI

ERISTÄMINEN HEURISTIIKKA HIEKKALAATIKKO KÄYTÖSVALVONTA
LUNNASOHJELMA PÄIVITYKSET VIRUSTUNNISTE VÄÄRÄHÄLYTYS

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

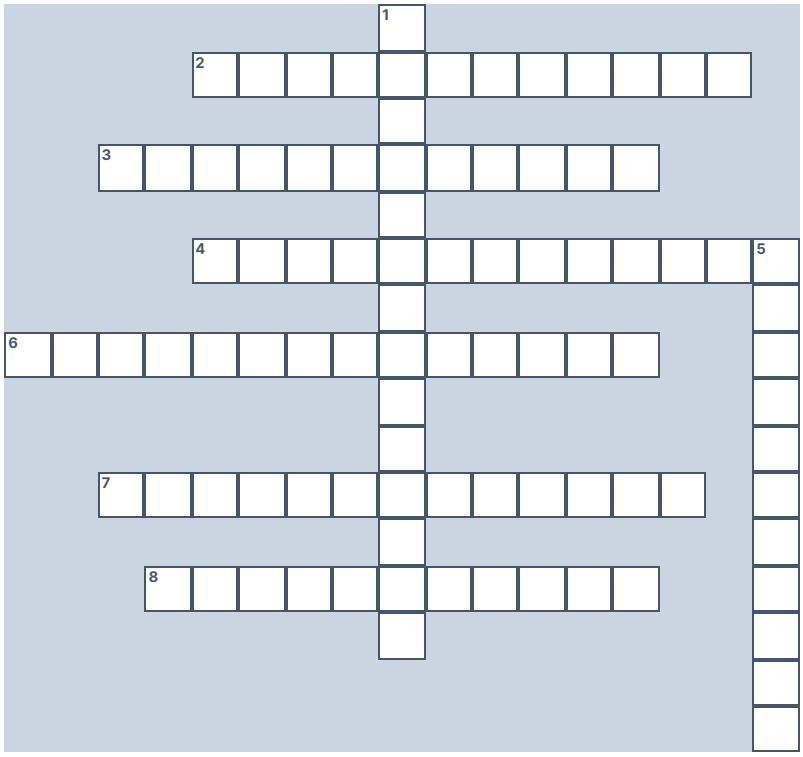
MÄÄRITELMIEN YHDISTÄMINEN

Yhdistä kukin vasemman puolen sanastotermi oikean puolen oikeaan määritelmään kirjoittamalla vastaava kirjain (A–H) täytettävään kenttään.

☐	1. Tiivistetunniste	A	Epäilyttävien tiedostojen rajaaminen eristykseen paikallisen järjestelmän altistumisen estämiseksi.
☐	2. Koodin heuristiikka	B	Ohjelmistopaketti, joka skannaa päätelaitteita ja suojaa niitä haavoittuvuuksien hyväksikäytöltä.
☐	3. Tiedostojen hiekkalaatikko	C	Käynnissä olevien ohjelmistotoimintojen seuranta haitallisten toimintamallien varalta.
☐	4. Käyttäytymisskannaus	D	Yksilöllinen kryptografinen tietokantajälki, jolla tunnistetaan tunnetut uhat.
☐	5. Päivittäiset päivitykset	E	Suojattu virtuaalinen testiympäristö, jossa epäluotettavaa koodia ajetaan turvallisesti.
☐	6. Väärä positiivinen	F	Säännölliset määrittelylataukset, jotka syöttävät uhkatietokantaa.
☐	7. Uhkien eristäminen	G	Sääntöpohjainen analyysi, joka merkitsee tiedostot, joiden koodirakenne on epäilyttävä.
☐	8. Virustorjuntatyökalu	H	Tietoturvahälytys, joka luokittelee turvallisen ohjelmiston virheellisesti haittaohjelmaksi.

Tarkistuspiste 5: Ristikko

Ratkaise ristikko kirjoittamalla kirjaimia aktiivisiin valkoisiin ruutuihin. Numerot vastaavat alla olevia vihjeitä.



VAAKASUORAAN

2. Tietoturvailmoitus, joka luokittelee turvallisen ohjelmiston virheellisesti haittaohjelmaksi (12)

3. Sääntöpohjainen analyysi, joka merkitsee tiedostot, joiden koodirakenne on epäilyttävä (12)

4. Yksilöllinen kryptografinen tietokantajälki, jolla tunnetut uhat tunnistetaan (13)

6. Suojattu virtuaalinen testiympäristö, jossa epäluotettavaa koodia ajetaan turvallisesti (14)

7. Ohjelmistokokonaisuus, joka skannaa ja suojaa päätelaitteita hyökkäyksiltä (13)

8. Säännöllisesti ladattavat määritykset, jotka syöttävät uhkatietokantaa (11)

PYSTYSUORAAN

1. Käynnissä olevan ohjelmiston toimien seuranta haitallisten toimintamallien varalta (14)

5. Epäilyttävien tiedostojen rajaaminen erilleen, jotta paikallinen järjestelmä ei altistu (11)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

Näytönlukijan ja näppäimistön käyttäjät voivat kirjoittaa ristikon vastaukset suoraan alla oleviin tekstikenttiin. VAAKAVIHJEET PYSTYVIHJEET

VAAKASUORAAN

2 vaakasuoraan: Tietoturvailmoitus, joka luokittelee turvallisen ohjelmiston virheellisesti haittaohjelmaksi (12 kirjainta):

3 vaakasuoraan: Sääntöpohjainen analyysi, joka merkitsee tiedostot, joiden koodirakenne on epäilyttävä (12 kirjainta):

4 vaakasuoraan: Yksilöllinen kryptografinen tietokantajälki, jolla tunnetut uhat tunnistetaan (13 kirjainta):

6 vaakasuoraan: Suojattu virtuaalinen testiympäristö, jossa epäluotettavaa koodia ajetaan turvallisesti (14 kirjainta):

7 vaakasuoraan: Ohjelmistokokonaisuus, joka skannaa ja suojaa päätelaitteita hyökkäyksiltä (13 kirjainta):

8 vaakasuoraan: Säännöllisesti ladattavat määritykset, jotka syöttävät uhkatietokantaa (11 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Käynnissä olevan ohjelmiston toimien seuranta haitallisten toimintamallien varalta (14 kirjainta):

5 pystysuoraan: Epäilyttävien tiedostojen rajaaminen erilleen, jotta paikallinen järjestelmä ei altistu (11 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

Etsi ruudukosta 8 piilotettua keskeistä sanastotermiä. Sanat voivat olla vaaka-, pysty- tai vinosuunnassa.

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

SANASTOLISTA

VIRUSTUNNISTE
HEURISTIIKKA
VÄÄRÄHÄLYTYS
HIEKKALAATIKKO
ERISTÄMINEN
KÄYTÖSVALVONTA
VIRUSTORJUNTA
PÄIVITYKSET

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

Yhdistä kukin sanahaun 8 sanastotermistä sen oikeaan määritelmään kirjoittamalla kirjain (A–H) tyhjään kohtaan.

SANASTOTERMIT

- **A. VIRUSTUNNISTE**
- **B. HEURISTIIKKA**
- **C. HIEKKALAATIKKO**
- **D. KÄYTÖSVALVONTA**
- **E. PÄIVITYKSET**
- **F. VÄÄRÄHÄLYTYS**
- **G. ERISTÄMINEN**
- **H. VIRUSTORJUNTA**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Käynnissä olevan ohjelmiston toimien seuranta haitallisten toimintamallien varalta.
2. Ohjelmistokokonaisuus, joka skannaa ja suojaa päätelaitteita hyökkäyksiltä.
3. Säännöllisesti ladattavat määritykset, jotka syöttävät uhkatietokantaa.
4. Sääntöpohjainen analyysi, joka merkitsee tiedostot, joiden koodirakenne on epäilyttävä.
5. Epäilyttävien tiedostojen rajaaminen erilleen, jotta paikallinen järjestelmä ei altistu.
6. Yksilöllinen kryptografinen tietokantajälki, jolla tunnetut uhat tunnistetaan.
7. Suojattu virtuaalinen testiympäristö, jossa epäluotettavaa koodia ajetaan turvallisesti.
8. Tietoturvailmoitus, joka luokittelee turvallisen ohjelmiston virheellisesti haittaohjelmaksi.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

Selvitä alla olevat kirjaimet paljastaaksesi keskeisiä kyberturvallisuuden käsitteitä ja termejä. Kirjoita vastauksesi annettuihin syöttökenttiin.

1. URNTTINIVSESU
2. KIAELKHKAOTIAK
3. PYTKIÄETISV
4. MENÄITNIERS
5. EKITAUIISHKR
6. SVOÖYNATVKÄLAT
7. LYÄVÄÄSTYÄHR
8. JRSTNRAVOITUU

Bonustehtävä: Nopeat vastaukset

3 VASTAUSTA JOKAISEEN LUOKKAAN. VOITTAJA ON SE, JOKA TÄYTTÄÄ LISTAN ENSIMMÄISENÄ.

1	Syitä päivittää ohjelmistot			
2	Ihmisiä, joilta voit pyytää IT-apua			
3	Asioita, joita teet, kun virustorjunta löytää jotain			
4	Tietokonevirusten merkkejä			
5	Asioita, jotka joutuvat karanteeniin			
6	Paikkoja, joihin virukset piiloutuvat			
7	Tietoja, joita sinun ei pitäisi koskaan jakaa			
8	Haittaohjelmatyyppejä			
9	Tietoturvatyökaluja, jotka tunnet			
10	Asioita, joita virustorjunta tarkistaa			
11	Asioita, joista otat varmuuskopion			
12	Laitteita, jotka voidaan hakkeroida			
13	Virustorjuntaohjelmia, jotka tunnet			
14	Syitä vääriin hälytyksiin			
15	Turvallisia tapoja, joita voit aloittaa tänään			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: ALLEKIRJOITUS- JA HEURISTINEN SKANNAUS



Tilanne: Työntekijä lataa toisen tiimin sisäisesti rakentaman mukautetun apuohjelman. Allekirjoitusskanneri päästää sen läpi, mutta heuristinen skanneri merkitsee sen epäilyttäväksi.

Keskustelukysymys: Selitä, miksi näin kävi ja miten voidaan varmistaa, onko tiedosto turvallinen.

TAPAUSTUTKIMUS 2: VÄÄRIEN HÄLYTYSTEN KÄSITTELY



Tilanne: Ohjelmistokehittäjä kääntää sovelluksensa. Järjestelmän virustorjunta merkitsee uuden suoritettavan tiedoston haittaohjelmaksi ja asettaa sen karanteeniin.

Keskustelukysymys: Kuvaa sallittujen luetteloon lisäämisen riskit ja selitä oikea ratkaisutapa.

Tarkistuspiste 9: Salakirjoituksen purkaminen

Kyberturvallisuuden ammattilainen suojaa verkon resursseja verkkohyökkääjiltä. Käytä alla olevaa kirjain–numero-avainta purkaaksesi viestin kirjoittamalla vastaavat kirjaimet tyhjiin kohtiin.

KIRJAIN-NUMERO-SALAUSAVAIN

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

20	21	14	14	9	19	20	1		21	21	4	5	20

8	1	9	20	20	1	15	8	10	5	12	13	1	20

8	5	21	18	9	19	20	9	9	11	1	12	12	1

Purettu viesti:

VIHJE: JOKAINEN NUMERO VASTAA KIRJAIMEN PAIKKAA AAKKOSISSA (ESIM. 1 = A, 2 = B, 29 = Ö).

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa A)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q1: Miten virustorjuntaohjelmisto tunnistaa haittaohjelmia?

Se tunnistaa haittaohjelmat tietokannan tunnisteiden vertailulla, heuristisella koodirakenteen analyysillä ja reaaliaikaisella käyttäytymisen valvonnalla.

Q2: Mitä on allekirjoituspohjainen tunnistus?

Se on skannausmenetelmä, joka vertaa tiedostojen kryptografisia tiivisteitä tunnettujen haittaohjelmauhkien tietokantaluetteloihin.

Q3: Mikä on heuristinen tarkistin?

Heuristiikka analysoi tiedoston rakennetta ja koodikäskyjä ja merkitsee haittaohjelmavarianteille tyypilliset epäilyttävät kuviot.

Q4: Mitä tarkoittaa, kun tiedosto on karanteenissa?

Virustorjunta siirtää tiedoston suojattuun, eristettyyn kansioon ja estää sen suorittamisen käyttöjärjestelmän suojaamiseksi.

Q5: Mikä on virustorjunnan väärä positiivinen havainto?

Se on virhe, jossa skannausalgoritmit merkitsevät laillisen, turvallisen ohjelmiston virheellisesti haittaohjelmaksi.

Tarkistuspiste 10: Usein kysytyt kysymykset kyberturvallisuudesta, perustaso (Osa B)

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Miten käyttäytymisen seuranta suojaa järjestelmiä?

Se valvoo käynnissä olevaa ohjelmistoa reaaliajassa ja estää prosessit, jotka yrittävät epäilyttäviä muutoksia, kuten koodin injektointia.

Q7: Miksi hiekkalaatikkotestaus on tärkeää?

Hiekkalaatikkotestaus suorittaa epäluotettavia tiedostoja eristetyssä virtuaalikoneessa ja tarkkailee toimintaa turvallisesti ilman järjestelmän altistamista.

Q8: Kuinka usein virustorjunnan määritelmät pitäisi päivittää?

Tarkistimien tulisi päivittää määrittelyt päivittäin tai tunneittain tunnistaakseen uusia haittaohjelmakantoja.

Q9: Mikä on virustorjunnan ja EDR:n ero?

Virustorjunta keskittyy tiedostojen tarkistamiseen, kun taas Endpoint Detection and Response (EDR) seuraa ja eristää uhkia koko verkossa.

Q10: Voinko ajaa kahta virustorjuntaohjelmaa yhtä aikaa?

Ei. Kahden aktiivisen tarkistimen käyttö aiheuttaa järjestelmäristiriitoja, hidastaa suorituskykyä ja voi estää toistensa toimintoja.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa C)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q1: Miten heuristiset säännöt vähentävät uhkien ohitusta?

Heuristiikka analysoi yleisiä uhkakuvioita yksittäisten tunnisteiden sijaan ja havaitsee tunnettujen haittaohjelmaperheiden muunnellut variantit.

Q2: Mikä on polymorfinen virus?

Se on haittaohjelma, joka muuttaa tiedostorakennettaan ja salauksenpurkurutiiniaan jokaisella suorituskerralla, mikä tekee tunnisteskannauksista tehottomia.

Q3: Miten hiekkalaatikot havaitsevat virtuaalikoneen kiertämisen?

Nykyaikaiset hiekkalaatikot simuloivat hiiren napsautuksia ja järjestelmän käyttöaikaa ja huijaavat haittaohjelmia, jotka on suunniteltu piiloutumaan virtuaalikoneissa.

Q4: Mitä latausmuotoja allekirjoituspäivityksillä on?

Päivitykset ovat yleensä kevyitä inkrementaalisia binäärierotiedostoja, mikä minimoi asiakasverkon kaistanleveyden kulutuksen.

Q5: Miten päätelaiteagentit hallinnoivat paikallisia tarkistuksia?

Agentit suorittavat kevyitä taustatarkistuksia ja siirtävät syvät salaustiivisteiden haut pilvipohjaisiin uhkatietokantoihin.

Tarkistuspiste 10: Usein kysytyt kysymykset tietoturvasta, jatkotaso (Osa D)

Tutustu tietoturvaviitekehysten, haittaohjelma-analyysin ja tietojen vaatimustenmukaisuuden edistyneisiin teknisiin puoliin.

Q6: Mitä rootkit-tunnistustarkistus on?

Se skannaa ytimen tason muistitaulukoita ohittaen käyttöjärjestelmän rajapinnat, joihin rootkitit kytkeytyvät piilottaakseen aktiiviset säikeensä.

Q7: Miten käyttäytymistarkistus estää kiristyshaittaohjelmat?

Se havaitsee automaattiset massatiedostojen salaussilmukat ja lopettaa isäntäprosessin ennen kuin järjestelmätietokannat lukitaan.

Q8: Mitä koodin allekirjoitusvarmenteen varmennus on?

Tarkistimet vertaavat koodin digitaalisia allekirjoituksia luotettuihin juurivarmenteiden myöntäjiin ja validoivat ohjelmistokehittäjän henkilöllisyyden.

Q9: Miten pakkaajat (packer) vaikuttavat tarkistusmoottoreihin?

Pakkaajat tiivistävät tai salaavat haittaohjelmien sisällön. Tarkistusohjelmien on purettava tiedosto muistissa ennen kuin allekirjoitusvertailut ajetaan.

Q10: Miten EDR-työkalut automatisoivat eristämisen?

EDR-agentit asettavat vaarantuneet päätelaitteet karanteeniin verkkotasolla, mikä estää sivuttaisliikkeen mutta sallii analyytikon pääsyn.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Allekirjoitustietokannat tallentavat tunnettujen haittaohjelmien tiivisteet, joten aivan uusia tai muunneltuja tiedostoja ei havaita ennen kuin määritykset päivitetään.

2. TURVALLISUUSOIVALLUS

Heuristiset moottorit voivat merkitä joitakin uusia haittaohjelmavariantteja ennen kuin tunnistetiedot ovat olemassa, mutta ne tuottavat enemmän vääriä positiivisia havaintoja.

3. TURVALLISUUSOIVALLUS

Virheelliset hälytykset maksavat IT-tiimeille aikaa, joka kuluu virheellisesti karanteeniin asetettujen tiedostojen todentamiseen ja palauttamiseen.

4. TURVALLISUUSOIVALLUS

Polymorfinen haittaohjelma muuttaa koodiaan jokaisessa kopiossa, joten puolustajat yhdistävät allekirjoitukset heuristisiin ja käyttäytymistarkastuksiin.

6. TURVALLISUUSOIVALLUS

Haittaohjelmien tekijät kirjoittavat mukautettua koodia, joka tunnistaa hiekkalaatikkoympäristöt ja viivästyttää suoritusta ohittaakseen ajastimet.

5. TURVALLISUUSOIVALLUS

Pilvipohjaiset virustorjuntamoottorit tarkistavat epäilyttävien tiedostojen tiivisteet suurista verkkopohjaisista uhkatietokannoista lähes reaaliajassa.

7. TIETOTURVATIETOA

Toimittajat työntävät määrityspäivityksiä päätelaitteisiin säännöllisesti, jotta skannerit tunnistavat uudet vahvistetut uhat.

8. TIETOTURVATIETOA

Kiristyshaittaohjelmien käyttäytymisvalvonta kohdistuu tiettyihin Win32 API -kutsuihin, jotka liittyvät tiedostojen salaamiseen ja varjokopioiden poistoon.

9. TIETOTURVATIETOA

Kelvolliset koodiallekirjoitukset voivat pienentää väärien positiivisten tulosten riskiä, mutta allekirjoitetut tiedostot skannataan silti, koska haittaohjelmatkin voivat olla allekirjoitettuja.

10. TURVALLISUUSOIVALLUS

Rootkitit muokkaavat järjestelmän ytimen rakenteita, minkä vuoksi niiden havaitseminen ja poistaminen vaatii erikoistuneita käynnistysaikaisia tarkistimia.

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista NIST-, OWASP- ja tietosuojavaatimustenmukaisuusstandardeista. TIETEELLISET JA ALAN LÄHTEET

TIETEELLISET JA ALAN VIITTEET

[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

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

ALLEKIRJOITUKSET

Oikea vastaus: A

OPETTAJALLE

Allekirjoitusskannaus perustuu tunnettuihin tietokannan tiivisteisiin, eikä se havaitse tuntemattomia tai muokattuja haittaohjelmia. Lähde: OWASP Secure Configuration.

2 Kysymys 2

HEURISTIIKKA

Oikea vastaus: A

OPETTAJALLE

Heuristiikat analysoivat koodin rakennetta ja komentoja tunnistaakseen uusien uhkaversioiden epäilyttäviä piirteitä. Lähde: Center for Internet Security (CIS).

3 Kysymys 3

HIEKKALAATIKKOTESTAUS

Oikea vastaus: A

OPETTAJALLE

Hiekkalaatikko ajaa epäilyttävät tiedostot eristetyssä virtuaalikoneessa, jotta suoritustoimintaa voi tarkkailla turvallisesti. Lähde: NIST Digital Identity.

4 Kysymys 4

TOIMINTAPERUSTEINEN

Oikea vastaus: A

OPETTAJALLE

Käyttäytymisskannaus valvoo käynnissä olevia ohjelmia reaaliajassa luvattomien järjestelmämuutosten estämiseksi. Lähde: Center for Internet Security (CIS).

5 Kysymys 5

PÄIVITYKSET

Oikea vastaus: A

OPETTAJALLE

Skannerit lataavat päivittäisiä inkrementaalisia tunnistepäivityksiä pysyäkseen synkronoituina uhkamaiseman kanssa. Lähde: OWASP Secure Configuration.

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** ALLEKIRJOITUKSET **Oikea vastaus: Tosi**

OPETTAJALLE

Allekirjoitustyökalut laskevat kryptografisia tiivisteitä ja vertaavat niitä tunnettujen uhkien tiivisteiden tietokantaan. Lähde: OWASP Secure Configuration.

7 **Kysymys 7** HEURISTIIKKA **Oikea vastaus: Tosi**

OPETTAJALLE

Heuristiset moottorit ajavat sääntöpohjaisia rakenteita, jotka voivat merkitä laillisia, turvallisia tiedostoja epäilyttäviksi. Lähde: Center for Internet Security (CIS).

8 **Kysymys 8** HIEKKALAATIKKOTESTAUS **Oikea vastaus: Epätosi**

OPETTAJALLE

Hiekkalaatikko ajaa koodia virtuaalisessa kontissa ja estää tiukasti pääsyn verkkojakoihin. Lähde: NIST Digital Identity.

9 **Kysymys 9** TOIMINTAPERUSTEINEN **Oikea vastaus: Tosi**

OPETTAJALLE

Reaaliaikainen valvonta merkitsee käynnissä olevat prosessit, jotka yrittävät laittomia kirjoituksia tai tiedostojen lukitusta. Lähde: Center for Internet Security (CIS).

10 **Kysymys 10** **Oikea vastaus: Epätosi**

OPETTAJALLE

Mikään virustorjunta ei pysäytä jokaista nollapäivähyökkäystä; tuntemattomat uhat voivat väistää allekirjoitukset ja heuristiikat.

Sanastoavaimet ja arviointikriteerit

Opettajan arviointikriteeri: Anna 1 piste jokaisesta oikeasta yhdistämisestä (yhteensä 8 pistettä) ja asiayhteystermistä (yhteensä 6 pistettä).

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

D 1. Tiivistetunniste	G 2. Koodin heuristiikka	E 3. Tiedostojen hiekkalaatikko	C 4. Käyttäytymisskannaus
F 5. Päivittäiset päivitykset	H 6. Väärä positiivinen	A 7. Uhkien eristäminen	B 8. Virustorjuntatyökalu

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 VIRUSTUNNISTE	2 HEURISTIIKKA	3 HIEKKALAATIKKO	4 KÄYTÖSVALVONTA
5 PÄIVITYKSET	6 VÄÄRÄHÄLYTYS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 D – KÄYTÖSVALVONTA	2 H – VIRUSTORJUNTA	3 E – PÄIVITYKSET	4 B – HEURISTIIKKA
5 G – ERISTÄMINEN	6 A – VIRUSTUNNISTE	7 C – HIEKKALAATIKKO	8 F – VÄÄRÄHÄLYTYS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit Tiivistetunniste, Koodin heuristiikka ja Tiedostojen hiekkalaatikko omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

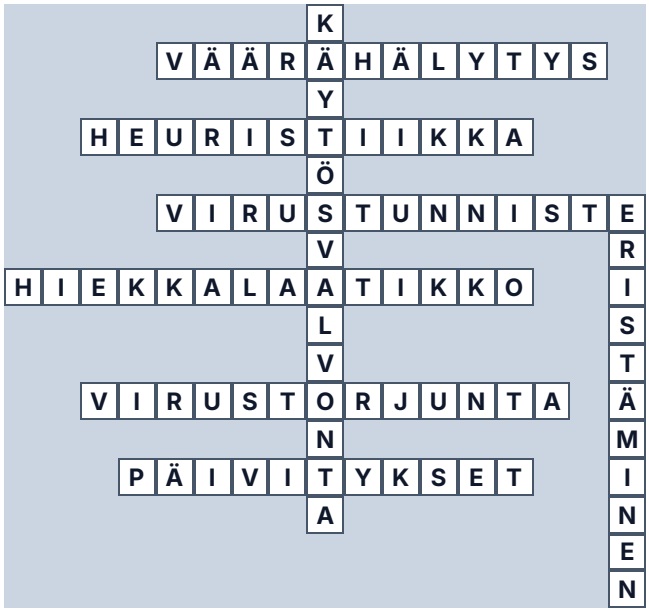
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



VAAKASUORAAN

2 vaakasuoraan: VÄÄRÄHÄLYTYS Tietoturvailmoitus, joka luokittelee turvallisen ohjelmiston virheellisesti haittaohjelmaksi (12 kirjainta)

3 vaakasuoraan: HEURISTIIKKA Sääntöpohjainen analyysi, joka merkitsee tiedostot, joiden koodirakenne on epäilyttävä (12 kirjainta)

4 vaakasuoraan: VIRUSTUNNISTE Yksilöllinen kryptografinen tietokantajälki, jolla tunnetut uhat tunnistetaan (13 kirjainta)

6 vaakasuoraan: HIEKKALAATIKKO Suojattu virtuaalinen testiympäristö, jossa epäluotettavaa koodia ajetaan turvallisesti (14 kirjainta)

7 vaakasuoraan: VIRUSTORJUNTA Ohjelmistokokonaisuus, joka skannaa ja suojaa päätelaitteita hyökkäyksiltä (13 kirjainta)

8 vaakasuoraan: PÄIVITYKSET Säännöllisesti ladattavat määritykset, jotka syöttävät uhkatietokantaa (11 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: KÄYTÖSVALVONTA Käynnissä olevan ohjelmiston toimien seuranta haitallisten toimintamallien varalta (14 kirjainta)

5 pystysuoraan: ERISTÄMINEN Epäilyttävien tiedostojen rajaaminen erilleen, jotta paikallinen järjestelmä ei altistu (11 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. URNTTINIVSESU — **VIRUSTUNNISTE**
2. KIAELKHKAOTIAK — **HIEKKALAATIKKO**
3. PYTKIÄETISV — **PÄIVITYKSET**
4. MENÄITNIERS — **ERISTÄMINEN**
5. EKITAUIISHKR — **HEURISTIIKKA**
6. SVOÖYNATVKÄLAT — **KÄYTÖSVALVONTA**
7. LYÄVÄÄSTYÄHR — **VÄÄRÄHÄLYTYS**
8. JRSTNRAVOITUU — **VIRUSTORJUNTA**

SALAKIRJOITUSHAASTEEN AVAIN

"TUNNISTA UUDET HAITTAOHJELMAT HEURISTIIKALLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Allekirjoitus- ja heuristinen skannaus

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Työntekijä lataa toisen tiimin sisäisesti rakentaman mukautetun apuohjelman. Allekirjoitustarkistin päästää sen läpi, mutta heuristinen tarkistin merkitsee sen epäilyttäväksi.
- Suositeltu strategia ja ratkaisu: Miksi näin kävi: Allekirjoitusskannaus tarkistaa tiedostojen tiivisteet; koska tiedosto on räätälöity, sitä ei ole uhkatietokannassa. Heuristiikka analysoi rakennetta ja merkitsi epäilyttäviä toimintoja (esim. rekisterikirjoitukset). Varmennus: Suorita tiedosto hiekkalaatikossa toiminnan havainnoimiseksi, tarkista digitaaliset allekirjoitukset ja lähetä tiiviste uhkatietoportaaleihin.

B Tapaustutkimus 2: Väärien hälytysten käsittely

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Ohjelmistokehittäjä kääntää sovelluksensa. Järjestelmän virustorjunta merkitsee uuden suoritettavan tiedoston haittaohjelmaksi ja asettaa sen karanteeniin.
- Suositeltu strategia ja ratkaisu: Sallittujen listan riskit: Tarkistimien ohittaminen voi antaa todellisen, tartunnan saaneen koodin suorittua. Ratkaisupolku: Lähetä tiedosto virustorjuntatoimittajalle analysoitavaksi, allekirjoita koodi digitaalisesti varmenteiden myöntäjien avulla ja määritä tilapäisesti tietyt kansioiden poikkeukset sen sijaan, että sammuttaisit virustorjunnan.