Nimi: _____ Päivämäärä: _____ Pisteet: _____

Zero Trust -arkkitehtuuri ja tietoturva

Jatkuva varmennus, verkon mikrosegmentointi, identiteetin ja pääsyn hallinta, vähimmäisoikeudet ja suojaustason tarkistukset.

ZERO TRUST -TIETOTURVAN OPPIMISKATSAUS

SUOJATTU
TIETOJEN SALAUS
256-bittinen AES-standardi

LAINMUKAINEN
GLOBAALIT STANDARDIT
GDPR- ja CCPA-säädökset

NOLLALUOTTAMUS
KÄYTTÖKÄYTÄNTÖ
Monivaiheinen tunnistautuminen

Tervetuloa! Tämä tehtäväpaketti käsittelee aihetta: Zero Trust -arkkitehtuuri ja tietoturva. Tutustut jatkuvaan varmennukseen, verkon mikrosegmentointiin, identiteetin ja käyttöoikeuksien hallintaan (IAM), vähimmän oikeuden periaatteeseen ja istuntojen auditointiin.

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/nollaluottamus-kyberturvallisuus/

Oppimispolkusi: Zero Trust -strategia

- Ymmärrä jatkuvan varmennuksen perusperiaate.
- Toteuta verkon mikrosegmentointi ja vähimpien oikeuksien periaatteen mukainen pääsy.
- Määritä laitteen suojaustason tarkistukset ja aktiivisten istuntojen auditointi.

ZERO TRUST -TIETOTURVAOPPAAN OHJEET

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

ZERO TRUST -ARKKITEHTUURI JA TIETOTURVA (JOHDANTO)

Zero Trust -tietoturva korvaa vanhat verkon ulkorajaan perustuvat mallit tiukalla "älä koskaan luota, varmenna aina" -periaatteella. Mikrosegmentointi, identiteetin- ja käyttöoikeuksien hallinta (IAM), vähimmän oikeuden periaate ja tilatarkistukset estävät uhkien liikkumisen sivusuunnassa.

LUE JOKAINEN TARKISTUSPISTE HUOLELLISESTI JA VALITSE TAI KIRJOITA OIKEA VASTAUS.

Tarkistuspiste 1: Monivalintahaaste

1. Mikä on Zero Trust -tietoturvamallin ydinperiaate?

- A. Älä koskaan luota, tarkista aina jokainen käyttöpyyntö lähteestä riippumatta
- B. Oletus, että kaikki yrityksen palomuurin sisäpuolinen liikenne on turvallista
- C. Tietokantatiedostojen tallentaminen salaamattomina nopeuden parantamiseksi
- D. Sähköpostin todennuksen pakottaminen vain SPF-tietueilla

2. Mitä on verkon mikrosegmentointi?

- A. Verkkojen jakaminen pieniin, eristettyihin vyöhykkeisiin sivuttaisliikkeen rajoittamiseksi
- B. Verkkokorttien salaaminen datan siirron aikana
- C. Kaikkien paikallisten palvelimien yhdistäminen yhteen julkiseen IP-osoitteeseen
- D. Käyttäjien näppäinpainallusten valvonta selainistunnoissa

3. Mikä on vähimmän oikeuden periaate?

- A. Käyttäjien käyttöoikeuksien rajoittaminen vain siihen, mitä heidän työnsä vaatii
- B. Kaikkien järjestelmäoikeuksien antaminen jokaiselle käyttäjälle oletuksena
- C. Anonyymien kirjautumisten salliminen yrityksen tietokantapalvelimille
- D. Julkisten Wi-Fi-reitittimien määrittäminen ilman salasanoja

4. Mitä on identiteetin ja käyttöoikeuksien hallinta (IAM)?

- A. Kehykset, jotka hallitsevat digitaalisia identiteettejä ja valvovat järjestelmäoikeuksia
- B. Virustorjuntatyökalut, jotka tarkistavat paikalliset tiedostohakemistot
- C. Varmuuskopiointijärjestelmä, joka käyttää verkosta erotettua tallennusmediaa
- D. Sähköpostin yhdyskäytäväprotokolla, joka hylkää väärennetyt verkkotunnukset

5. Mitä jatkuva todennus tarkoittaa?

- A. Käyttäjän henkilöllisyyden ja laitteen tilan toistuva varmentaminen aktiivisen istunnon aikana
- B. Pääsalasanan vaihtaminen 10 minuutin välein
- C. Tietokantatietueiden tiivistäminen useilla algoritmeilla
- D. Verkon siirtopakettien salaus TLS-avaimilla

Tarkistuspiste 2: Tosi vai epätosi -haaste

6 Kysymys 6

6. Zero Trust olettaa, että kaikki yrityksen palomuurin sisäpuolella oleva liikenne on turvallista.

- ( ) Tosi
- ( ) Epätosi

7 Kysymys 7

7. Mikrosegmentointi rajoittaa hyökkääjien mahdollisuutta liikkua sivusuunnassa sisäisten palvelinten välillä.

- ( ) Tosi
- ( ) Epätosi

8 Kysymys 8

8. Vähimpien oikeuksien periaate antaa oletuksena pääsyn kaikkiin tietokantatiedostoihin.

- ( ) Tosi
- ( ) Epätosi

9 Kysymys 9

9. Jatkuva varmennus validoi laitteen terveyden ja käyttötunnukset koko kirjautumisistunnon ajan.

- ( ) Tosi
- ( ) Epätosi

10 Kysymys 10

10. Zero Trustin käyttöönotto pienentää vaarantuneiden yrityskirjautumisten vaikutusta.

- ( ) Tosi
- ( ) Epätosi

Tarkistuspiste 3: Avainkäsitteiden täyttö

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

1. Tunnistetietojen vaatiminen jokaisessa pääsypisteessä on jatkuva _____ .
2. Yritysverkon jakaminen pieniin vyöhykkeisiin on nimeltään _____ .
3. Digitaalisten identiteettien ja pääsynhallinnan määrittämiseen käytetään ratkaisua, jonka nimi on _____ .
4. Käyttäjien oikeuksien rajoittaminen perustuu periaatteeseen, jossa kullekin annetaan vain pienin tarvittava _____ .
5. Yhdistettyjen laitteiden kunnon arvioinnissa tarkistetaan laitteen _____ .
6. Lokitettujen aktiivisten istuntojen kirjaaminen ja tarkastelu on tietoturvan _____ .

SANASTON SANAPANKKI

IAM-JÄRJESTELMÄ KÄYTTÖOIKEUS LAITEKUNTO MIKROSEGMENTOINTI
PALOMUURI REITITIN TARKASTUS TODENNUS

Kirjoita vastauksesi tähän:

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

Tarkistuspiste 4: Tietoturvakäsitteiden yhdistäminen

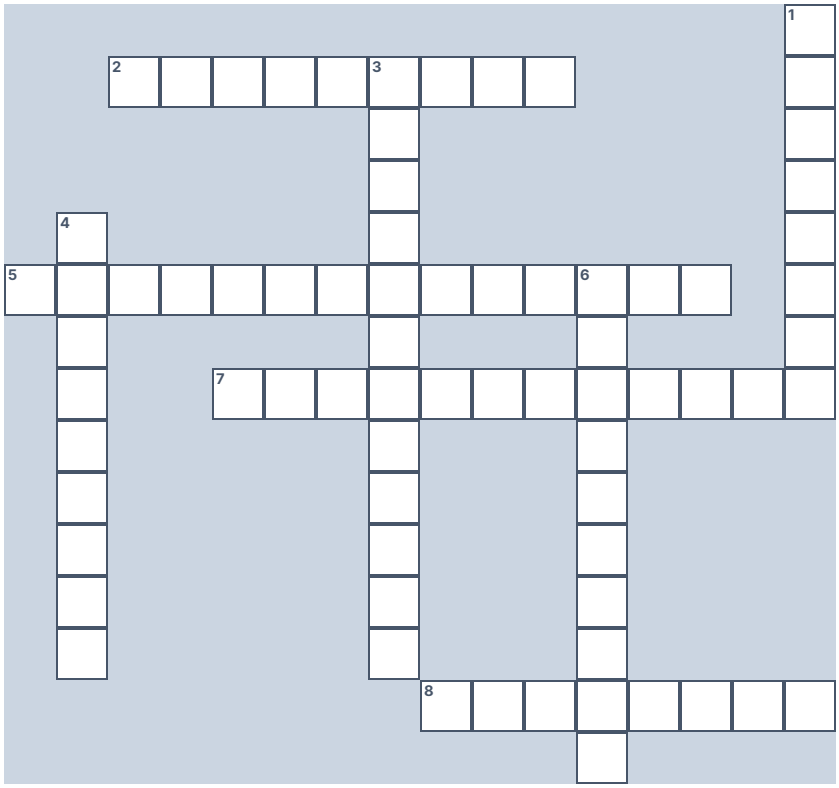
MÄÄRITELMIEN YHDISTÄMINEN

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

☐	1. TARKISTUS	A	Käyttäjätunnusten käyttöoikeuksien hallinta.
☐	2. SEGMENTOINTI	B	Vähimpien käyttöoikeuksien periaate.
☐	3. IAM	C	Verkkopakettiliikenteen reititys.
☐	4. OIKEUS	D	Ulkoisen verkon rajasuojaus.
☐	5. LAITETILA	E	Kirjattujen käyttöistuntojen tarkastelu.
☐	6. AUDITOINTI	F	Sisäisten verkkovyöhykkeiden jakaminen.
☐	7. PALOMUURI	G	Käyttäjän tunnistetietojen jatkuva tarkistus.
☐	8. REITITIN	H	Laitteen kuntotilan arviointi.

Tarkistuspiste 5: Ristikko

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



VAAKASUORAAN

2. Kirjattujen pääsyistuntojen läpikäynti. (9)

5. Käyttäjien tunnistetietojen ja käyttöoikeuksien hallinta. (14)

7. Vähimpien käyttöoikeuksien periaate. (12)

8. Verkkopakettiliikenteen reititys. (8)

PYSTYSUORAAN

1. Käyttäjien tunnistetietojen jatkuva tarkistaminen. (8)

3. Sisäisten verkkovyöhykkeiden jakaminen. (12)

4. Ulkoisen verkon rajasuojaus. (9)

6. Laitteen terveydentilan arviointi. (10)

Tarkistuspiste 5, vaihtoehto: Saavutettavat ristikon vihjeet

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

VAAKASUORAAN

2 vaakasuoraan: Kirjattujen pääsyistuntojen läpikäynti. (9 kirjainta):

5 vaakasuoraan: Käyttäjien tunnistetietojen ja käyttöoikeuksien hallinta. (14 kirjainta):

7 vaakasuoraan: Vähimpien käyttöoikeuksien periaate. (12 kirjainta):

8 vaakasuoraan: Verkkopakettiliikenteen reititys. (8 kirjainta):

PYSTYSUORAAN

1 pystysuoraan: Käyttäjien tunnistetietojen jatkuva tarkistaminen. (8 kirjainta):

3 pystysuoraan: Sisäisten verkkovyöhykkeiden jakaminen. (12 kirjainta):

4 pystysuoraan: Ulkoisen verkon rajasuojaus. (9 kirjainta):

6 pystysuoraan: Laitteen terveydentilan arviointi. (10 kirjainta):

Tarkistuspiste 6: Piilotettujen sanojen haku

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

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

SANASTOLISTA

TODENNUS SEGMENTOINTI IAMJÄRJESTELMÄ KÄYTTÖOIKEUS LAITEKUNTO
TARKASTUS PALOMUURI REITITIN

Tarkistuspiste 6, vaihtoehto: Saavutettava sanaston yhdistäminen

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

SANASTOTERMIT

- **A. TODENNUS**
- **B. SEGMENTOINTI**
- **C. IAMJÄRJESTELMÄ**
- **D. KÄYTTÖOIKEUS**
- **E. LAITEKUNTO**
- **F. TARKASTUS**
- **G. PALOMUURI**
- **H. REITITIN**

MÄÄRITELMÄT JA YHDISTETTÄVÄT KENTÄT

1. Ulkoisen verkon rajasuojaus.
2. Kirjattujen pääsyistuntojen läpikäynti.
3. Vähimpien käyttöoikeuksien periaate.
4. Sisäisten verkkovyöhykkeiden jakaminen.
5. Verkkopakettiliikenteen reititys.
6. Laitteen terveydentilan arviointi.
7. Käyttäjien tunnistetietojen ja käyttöoikeuksien hallinta.
8. Käyttäjien tunnistetietojen jatkuva tarkistaminen.

Tarkistuspiste 7: Sekoitettujen sanojen haaste

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

1. UENTNOSD
2. ÄARMJMILEÄ TESJ
3. LKTUAEOTNI
4. MIROUUPAL
5. ENOTIGEINST M
6. STKEÖUIKÄO YT
7. STUSTKAAR
8. TEINRITI

Bonustehtävä: Nopeat vastaukset

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

1	Tietoja, joita sinun ei pitäisi koskaan jakaa			
2	Turvallisia tapoja, joita voit aloittaa tänään			
3	Asioita, joita laitteesta tarkistetaan			
4	Asioita, jotka kirjataan lokiin			
5	Kyberturvallisuuteen liittyviä sanoja			
6	Asioita, joita Zero Trust tarkistaa			
7	Paikkoja, joissa näytät henkilöllisyystodistuksen arjessa			
8	Tapoja todistaa, että se oikeasti olet sinä			
9	Asioita, joita teet tietovuodon jälkeen			
10	Merkkejä siitä, että tietokone on saanut tartunnan			
11	Syitä päivittää ohjelmistot			
12	Käyttöoikeustasoja yrityksessä			
13	Tietoturvatyökaluja, jotka tunnet			
14	Vyöhykkeitä, joihin verkko voidaan jakaa			
15	Sananlaskuja luottamuksesta			

Tarkistuspiste 8: Kyberturvallisuuden tapaustutkimukset

Hyödynnä oppimiasi käsitteitä ratkaistessasi alla olevat tosielämän tilanteet.

TAPAUSTUTKIMUS 1: SIIRTYMINEN ZERO TRUST -VERKKOARKKITEHTUURIIN

👷

Tilanne: Suuri yritys käyttää tällä hetkellä litteää sisäverkkoa, jossa mikä tahansa paikallisverkon laite voi käyttää kaikkia yrityksen palvelimia ja tietokantoja.

Keskustelukysymys: Suunnittele verkon mikrosegmentointistrategia sivuttaisliikkeen rajoittamiseksi.

TAPAUSTUTKIMUS 2: VÄHIMMÄISOIKEUKSIEN PERIAATTEEN MUKAISTEN PÄÄSYNHALLINTOJEN KÄYTTÖÖNOTTO

👷

Tilanne: Tarkastuslokit paljastavat, että tilapäiset tietokantakäyttäjät ja matalan tason työntekijät omaavat yleiset luku- ja kirjoitusoikeudet kriittisiin kirjanpitotietokantoihin.

Keskustelukysymys: Tarkasta ja rajoita tietokannan IAM-oikeudet vähimmän oikeuden periaatteen toteuttamiseksi.

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

22	1	18	13	9	19	20	1		1	9	14	1				
14	15	12	12	1	12	21	15	20	20	1	13	21	11	19	5	14
1	18	11	11	9	20	5	8	20	21	21	18	9	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: Mikä on Zero Trust?

Zero Trust on tietoturvakehys, joka olettaa uhkien olevan sekä verkon rajan ulkopuolella että sen sisäpuolella, minkä vuoksi jokainen pyyntö on varmennettava. [1]

Q2: Mikä on Zero Trustin ydinsääntö?

Älä luota koskaan, varmista aina.

Q3: Mitä mikrosegmentointi on?

Verkon jakaminen pieniin, suojattuihin loogisiin segmentteihin liikenteen hallitsemiseksi ja tietomurtojen rajaamiseksi.

Q4: Mitä vähimpien oikeuksien periaate on?

Käyttäjille annetaan vain vähimmäiskäyttöoikeudet, jotka tarvitaan heidän tiettyjen työtehtäviensä suorittamiseen. [2]

Q5: Mitä IAM tarkoittaa?

Identiteetin- ja käyttöoikeuksien hallinta.

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

Tutustu yleisiin kysymyksiin ja vastauksiin verkkouhkien torjunnasta.

Q6: Miten laitteen tilatarkistus auttaa?

Se varmistaa, että laite on päivitetty, siinä on aktiivinen virustorjunta ja että se on turvallinen, ennen kuin pääsy sallitaan.

Q7: Mitä sivuttaisliike on?

Prosessi, jolla hyökkääjät etenevät verkossa ensimmäisestä vallatusta solmusta arvokkaampiin järjestelmiin.

Q8: Korvaako Zero Trust palomuurit?

Ei, se vahvistaa niitä lisäämällä identiteettikeskeisiä tarkistuksia ja sisäisiä segmentointipalomuureja.

Q9: Mitä jatkuva todennus on?

Käyttäjän henkilöllisyyden jatkuva varmistaminen koko kirjautumisistunnon ajan, ei vain ensimmäisen kirjautumisen yhteydessä.

Q10: Miksi tasainen verkko on vaarallinen?

Tasaisissa verkoissa yksi vaarantunut solmu antaa hyökkääjille helpon pääsyn mihin tahansa verkon tietokantaan.

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

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

Q1: Miten Zero Trust vastaa perimetrimalliin?

Se korvaa vanhentuneen "linna ja vallihauta" -mallin siirtämällä puolustuksen rajaverkoista tiettyihin käyttäjäidentiteetteihin ja resursseihin.

Q2: Mikä on käytäntöpäätöspiste (PDP)?

Järjestelmän osa, joka arvioi valtuutuspyynnöt tietoturvasääntöjä vasten päättääkseen, myönnetäänkö pääsy.

Q3: Mikä on käytännön täytäntöönpanopiste (PEP)?

Järjestelmäsolmu (kuten yhdyskäytävä tai välityspalvelin), joka fyysisesti sallii tai estää yhteyspyynnöt PDP-päätöksen perusteella.

Q4: Miten roolipohjainen käyttöoikeuksien hallinta (RBAC) tukee Zero Trustia?

RBAC ryhmittelee käyttöoikeudet tiettyihin rooleihin, mikä auttaa estämään käyttäjiä perimästä liiallisia ylläpito-oikeuksia.

Q5: Mitä kontekstipohjainen pääsynhallinta on?

Kirjautumispyyntöjen arviointi toissijaisten vihjeiden, kuten maantieteellisen sijainnin, laitteen tilan ja kirjautumisajan, perusteella riskin arvioimiseksi.

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

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

Q6: Miten mikrosegmentointi eroaa tavallisista VLAN-verkoista?

VLAN-verkot jakavat verkot laajoihin loogisiin segmentteihin kerroksella 2, kun taas mikrosegmentointi eristää yksittäiset työkuormat ohjelmistopohjaisella käytännöllä.

Q7: Mitä just-in-time (JIT) -pääsy on?

Korotettujen hallinnointioikeuksien myöntäminen väliaikaisesti ja niiden automaattinen peruuttaminen tehtävän valmistuttua.

Q8: Miten API:t suojataan Zero Trust -viitekehyksessä?

Vaatimalla kryptografisesti allekirjoitetut OAuth-tunnisteet ja auditoimalla pyyntöjen allekirjoitukset jokaisessa API-yhdyskäytävässä.

Q9: Mikä on Zero Trust -verkkopääsyn (ZTNA) asiakasohjelma?

Ohjelmistoagentti, joka muodostaa suojattuja, salattuja lähteviä yhteyksiä tiettyihin sovelluksiin raakojen aliverkkojen sijaan.

Q10: Miten lokien tarkastus auttaa Zero Trustia?

Jatkuva lokitus mahdollistaa sen, että automaattiset tietoturva-analytiikkatyökalut havaitsevat poikkeamia ja keskeyttävät luvattomat kirjautumiset välittömästi.

Osa 11: 10 tosielämän kyberturvallisuusfaktaa ja havaintoa

Tutustu todellisiin tosiasioihin tietoturvaloukkauksista, puolustusmekanismeista ja vaatimustenmukaisuusstandardeista.

1. TURVALLISUUSOIVALLUS

Zero Trust -arkkitehtuurit korvaavat vanhan linna ja vallihauta -mallin identiteettikeskeisillä varmennussäännöillä.

2. TURVALLISUUSOIVALLUS

Verkon mikrosegmentointi pienentää aluetta, jonne haittaohjelma pääsee, eristämällä työkuormat pieniin suojattuihin vyöhykkeisiin.

3. TURVALLISUUSOIVALLUS

Zero Trust keskittyy suojaamaan resursseja, kuten omaisuutta, palveluja ja tilejä, verkon segmenttien sijaan. [1]

4. TURVALLISUUSOIVALLUS

Vähimpien oikeuksien käyttöpolitiikat pienentävät riskiä, että sisäpiiriläinen vie tietoja ydintietokannoista.

5. TURVALLISUUSOIVALLUS

Laitteen tilan validointi tarkistaa käyttöjärjestelmän päivitystason ja aktiivisen virustorjunnan tilan reaaliajassa.

6. TURVALLISUUSOIVALLUS

Zero Trust Network Access (ZTNA) -välittäjät voivat korvata yritysten VPN-ratkaisut tai täydentää niitä rajoittamalla käyttäjien pääsyn laajuutta.

7. TIETOTURVATIETOA

Just-in-Time (JIT) -tyyppinen hallinnollisten oikeuksien delegointi pienentää tunnistetietojen varastamisen riskiä toimialueen ohjauskoneilla.

8. TIETOTURVATIETOA

Jatkuva validointi kirjaa ja auditoi istuntokäyttäytymistä ja keskeyttää käyttäjät, joiden komentosarjojen suoritus on poikkeavaa.

9. TIETOTURVATIETOA

Perinteiset kehäpuolustukset eivät estä sivuttaishyökkäyksiä, kun ylläpitäjän tunnistetiedot ovat vuotaneet.

10. TURVALLISUUSOIVALLUS

NIST Special Publication 800-207 (2020) antaa Zero Trust -arkkitehtuurille abstraktin määritelmän ja käyttöönottomalleja. [1]

Tekniset viitteet ja lähteet

Opiskeluopas ja interaktiiviset pulmat on koottu maailmanlaajuisista NIST-, OWASP- ja tietosuojavaatimustenmukaisuusstandardeista.

TIETEELLISET JA ALAN VIITTEET

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Vastausavain: Tarkistuspiste 1 – Monivalinta

1 Kysymys 1

Oikea vastaus: A

OPETTAJALLE

Mikä on Zero Trust -tietoturvamallin ydinperiaate? → Älä koskaan luota, tarkista aina jokainen käyttöpyyntö lähteestä riippumatta

2 Kysymys 2

Oikea vastaus: A

OPETTAJALLE

Mitä on verkon mikrosegmentointi? → Verkkojen jakaminen pieniin, eristettyihin vyöhykkeisiin sivuttaisliikkeen rajoittamiseksi

3 Kysymys 3

Oikea vastaus: A

OPETTAJALLE

Mikä on vähimmän oikeuden periaate? → Käyttäjien käyttöoikeuksien rajoittaminen vain siihen, mitä heidän työnsä vaatii

4 Kysymys 4

Oikea vastaus: A

OPETTAJALLE

Mitä on identiteetin ja käyttöoikeuksien hallinta (IAM)? → Kehykset, jotka hallitsevat digitaalisia identiteettejä ja valvovat järjestelmäoikeuksia

5 Kysymys 5

Oikea vastaus: A

OPETTAJALLE

Mitä jatkuva todennus tarkoittaa? → Käyttäjän henkilöllisyyden ja laitteen tilan toistuva varmentaminen aktiivisen istunnon aikana

Vastausavain: Tarkistuspiste 2 – Tosi vai epätosi

6 **Kysymys 6** **Oikea vastaus: Epätosi**

OPETTAJALLE

Epätosi: Zero Trust ei anna implisiittistä luottamusta verkon sijainnin perusteella, ei sisä-eikä ulkopuolella.

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

OPETTAJALLE

Tosi: pienet eristetyt vyöhykkeet rajoittavat sitä, kuinka pitkälle tunkeilija voi edetä palvelinten välillä.

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

OPETTAJALLE

Epätosi: vähimmän oikeuden periaate antaa vain kunkin roolin tarvitseman vähimmäiskäyttöoikeuden.

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

OPETTAJALLE

Jatkuva varmennus validoi laitteen terveyden ja käyttötunnukset koko kirjautumisistunnon ajan.

10 **Kysymys 10** **Oikea vastaus: Tosi**

OPETTAJALLE

Zero Trustin käyttöönotto pienentää vaarantuneiden yrityskirjautumisten vaikutusta.

Sanastoavaimet ja arviointikriteerit

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

TARKISTUSPISTE 4: VASTAUSAVAIN – KÄSITTEIDEN YHDISTÄMINEN

G 1. TARKISTUS	F 2. SEGMENTOINTI	A 3. IAM	B 4. OIKEUS
H 5. LAITETILA	E 6. AUDITOINTI	D 7. PALOMUURI	C 8. REITITIN

TARKISTUSPISTE 3: VASTAUSAVAIN – AVAINTERMIT

1 TODENNUS	2 MIKROSEGMENTOINTI	3 IAM-JÄRJESTELMÄ	4 KÄYTTÖOIKEUS
5 LAITEKUNTO	6 TARKASTUS		

TARKISTUSPISTE 6, VAIHTOEHTO: VASTAUSAVAIN – SANOJEN YHDISTÄMINEN

1 G – PALOMUURI	2 F – TARKASTUS	3 D – KÄYTTÖOIKEUS	4 B – SEGMENTOINTI
5 H – REITITIN	6 E – LAITEKUNTO	7 C – IAMJÄRJESTELMÄ	8 A – TODENNUS

KESKUSTELUMUISTIINPANOT OPETTAJILLE

Avaintermit:
Tarkista, osaavatko oppilaat selittää termit TARKISTUS, SEGMENTOINTI ja IAM omin sanoin ja antaa jokaisesta esimerkin.

Tapaustutkimukset:
Pyydä oppilaita perustelemaan suosituksensa monisteen tosiasioilla eikä oletuksilla.

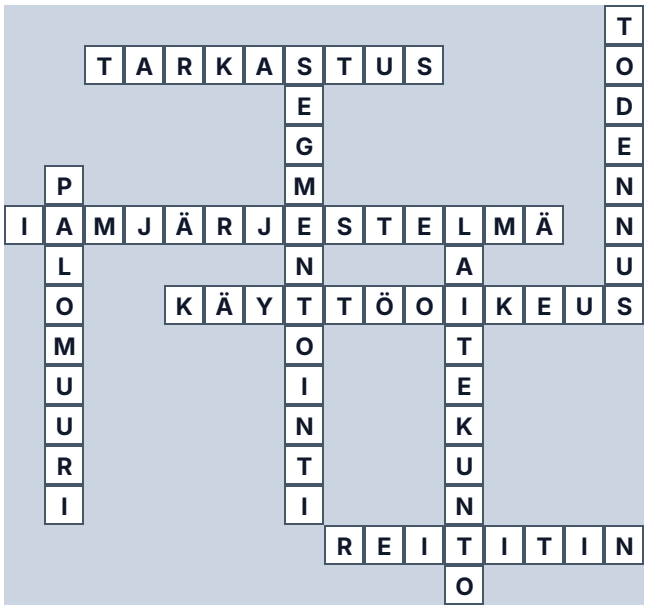
Lähteiden arviointi:
Pyydä oppilaita tarkistamaan vähintään yksi väite monisteen lähteistä ja keskustelkaa siitä, miksi luvut, hinnat ja säännöt voivat muuttua ajan myötä.

Tehtäväavaimet ja opettajan muistiinpanot

SANAHAUN RATKAISU

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

RISTIKON RATKAISU



OPETTAJAN OPAS RISTIKON RATKAISUIHIN

VAAKASUORAAN

2 vaakasuoraan: TARKASTUS Kirjattujen pääsyistuntojen läpikäynti. (9 kirjainta)

5 vaakasuoraan: IAMJÄRJESTELMÄ Käyttäjien tunnistetietojen ja käyttöoikeuksien hallinta. (14 kirjainta)

7 vaakasuoraan: KÄYTTÖOIKEUS Vähimpien käyttöoikeuksien periaate. (12 kirjainta)

8 vaakasuoraan: REITITIN Verkkopakettiliikenteen reititys. (8 kirjainta)

PYSTYSUORAAN

1 pystysuoraan: TODENNUS Käyttäjien tunnistetietojen jatkuva tarkistaminen. (8 kirjainta)

3 pystysuoraan: SEGMENTOINTI Sisäisten verkkovyöhykkeiden jakaminen. (12 kirjainta)

4 pystysuoraan: PALOMUURI Ulkoisen verkon rajasuojaus. (9 kirjainta)

6 pystysuoraan: LAITEKUNTO Laitteen terveydentilan arviointi. (10 kirjainta)

Sekoitettujen sanojen ja salakirjoituksen ratkaisuavain

Arviointiavain sanaston kirjainsekoitustehtävälle ja Salakirjoitushaasteelle.

SANOJEN JÄRJESTELYN VASTAUSAVAIN

1. UENTNOSD	TODENNUS	5. ENOTIGEINSTM	SEGMENTOINTI
2. ÄARMJMILEÄTESJ	IAMJÄRJESTELMÄ	6. STKEÖUIKÄOYT	KÄYTTÖOIKEUS
3. LKTUAEOTNI	LAITEKUNTO	7. STUSTKAAR	TARKASTUS
4. MIROUUPAL	PALOMUURI	8. TEINRITI	REITITIN

SALAKIRJOITUSHAASTEEN AVAIN

"VARMISTA AINA NOLLALUOTTAMUKSEN ARKKITEHTUURILLA"

Tapaustutkimusten vastausavain

A Tapaustutkimus 1: Siirtyminen Zero Trust -verkkoarkkitehtuuriin

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Suuri yritys käyttää tällä hetkellä tasaista sisäverkkoa, jossa mikä tahansa paikallisen verkon laite pääsee kaikkiin yrityksen palvelimiin ja tietokantoihin.
- Suositeltu strategia ja ratkaisu: Jaa tasainen verkko eristettyihin osastokohtaisiin vyöhykkeisiin. Asenna sisäiset palomuurit hallitsemaan vyöhykkeiden välistä liikennettä ja edellytä yhteystunnisteen validointia kaikessa pääsyssä.

B Tapaustutkimus 2: Vähimmäisoikeuksien periaatteen mukaisten pääsynhallintojen käyttöönotto

Opettajan ratkaisu

ARVIOINTIOHJE

Opiskelijoiden vastausten tulisi kattaa seuraavat kohdat:

- Tilanneanalyysi: Tarkastuslokit paljastavat, että tilapäisillä tietokantakäyttäjillä ja alemman tason työntekijöillä on yleiset luku- ja kirjoitusoikeudet kriittisiin kirjanpitotietokantoihin.
- Suositeltu strategia ja ratkaisu: Peruuta kaikki yleiset hallinnolliset oikeudet. Ota käyttöön roolipohjainen käyttöoikeuksien hallinta (RBAC), joka vastaa tarkkoja työtehtäviä, ja perusta viikoittaiset automaattiset käyttöoikeustarkastukset.