SecMeter Audit

TIETOLIIKENNETURVALLISUUDEN KÄSITTEISTÖ

Arviointikriteerien käyttäjille

Käsitteistö selittää tietoliikenneturvallisuuden arviointikysymyksissä käytetyt lyhenteet, vieraskieliset ilmaisut ja tekniset ammattikäsitteet selkokielellä. Käsitteistö on laadittu SecMeter Audit - tietoliikenneturvallisuuden arviointikysymysten käyttöä varten. Termit on kuvattu yleisellä, teknologianeutraalilla tasolla

Versio 1.0

Käsitteistön käyttö

Määritelmä ei korvaa yrityksen omaa ohjeistusta

Yritys voi käyttää eri nimityksiä tai toteutustapoja. Arvioinnissa ratkaisevaa on, täyttääkö käytäntö hyväksymiskriteerin ja voidaanko se todentaa luotettavalla näytöllä.

Tekninen ratkaisu ei yksin riitä

Arvioijan tulee tarkastaa myös omistajuus, vastuut, hyväksynnät, muutostenhallinta, valvonta, poikkeamien käsittely ja jatkuva kehittäminen.

Näyttö arvioidaan kokonaisuutena

Todentavana näyttönä voidaan käyttää asiakirjoja, asetuksia, lokeja, järjestelmäraportteja, havaintoja, haastatteluja ja teknisiä testejä. Pelkkä myönteinen haastatteluvastaus ei yleensä ole riittävä.

Lyhenteet avataan ensimmäisellä käyttökerralla

Dokumentoinnissa on suositeltavaa käyttää ensin suomenkielistä käsitettä ja sen jälkeen vakiintunutta lyhennettä sulkeissa, esimerkiksi ”verkkopääsyn hallinta (NAC)”.

Arviointi on riskiperusteista

Saman käsitteen edellyttämä suojaustaso voi vaihdella ympäristön kriittisyyden, tietojen luokituksen, uhkien ja liiketoimintavaikutusten perusteella.

Huomautus: Käsitteistön ”Arvioinnissa huomioitavaa” -kohdat ovat käytännön tarkistusohjeita. Ne eivät korvaa varsinaisten arviointikysymysten hyväksymiskriteerejä.

Lyhenteet ja vieraskieliset termit

Vieraskielinen nimi on esitetty vain lyhenteen avaamiseksi. Arviointitekstissä kannattaa käyttää ensisijaisesti suomenkielistä vastinetta.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
802.1X	Porttikohtainen verkkoon pääsyn valvontamenetelmä. Käyttäjä tai laite tunnistetaan ennen kuin verkkoyhteys avataan.	Tarkasta, että menetelmä on käytössä soveltuvissa langallisissa ja langattomissa verkoissa, tunnistuspalvelu on suojattu ja poikkeustilanteet on määritelty.
ACL (Access Control List)	Pääsynhallintalista, joka sallii tai estää verkkoliikennettä esimerkiksi lähde- ja kohdeosoitteen, protokollan tai portin perusteella.	Varmista, että säännöillä on perusteltu tarve, omistaja, hyväksyntä ja säännöllinen katselmointi.
CMDB (Configuration Management Database)	Konfiguraationhallintatietokanta, johon kuvataan laitteet, palvelut, omistajat, sijainnit, versiot ja riippuvuudet.	Arvioi tietojen kattavuus ja ajantasaisuus vertaamalla rekisteriä todelliseen verkkoympäristöön.
DDoS (Distributed Denial of Service)	Hajautettu palvelunestohyökkäys, jossa suuri määrä lähteitä kuormittaa yhteyttä tai palvelua niin, ettei normaali käyttö onnistu.	Tarkasta suojauspalvelut, hälytys- ja eskalointimenettelyt, kapasiteettivaraukset sekä harjoitusten tulokset.
DHCP (Dynamic Host Configuration Protocol)	Palvelu, joka jakaa laitteille automaattisesti IP-osoitteen ja muita verkkoasetuksia.	Tarkasta palvelinten hallinta, osoitealueet, lokitus, varajärjestelyt ja luvattomien DHCP-palvelinten havaitseminen.
DLP-hälytykset	Hälytykset tilanteista, joissa luottamuksellista tietoa saatetaan lähettää, kopioida tai tallentaa väärään paikkaan.	Tutkitaanko hälytykset, kirjataanko päätökset ja erotetaanko todelliset tietovuodot virhehälytyksistä? Tarkastetaan myös poikkeuslupien hyväksyntä ja sääntöjen kattavuus.
DMZ (Demilitarized Zone)	Sisäverkosta erotettu verkkovyöhyke, johon sijoitetaan yleensä internetiin näkyviä palveluja.	Varmista, ettei DMZ:stä ole tarpeettomia yhteyksiä sisäverkkoon ja että kaikki liikenne on rajattu, valvottu ja dokumentoitu.
DNS (Domain Name System)	Nimipalvelu, joka muuntaa verkkotunnuksia IP-osoitteiksi ja välittää muita nimialueen tietoja.	Arvioi DNS-palvelujen suojaus, muutosten hyväksyntä, lokitus, varmistukset ja häiriönsieto.
DNSSEC (Domain Name System Security Extensions)	DNS-tietojen alkuperän ja eheyden varmistava digitaalinen allekirjoitusmenetelmä. Se ei salaa DNS-kyselyjä.	Tarkasta allekirjoituksen kattavuus, avainten hallinta, voimassaolo ja virhetilanteiden valvonta.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
EDR- tai virustorjuntaraportit	Raportit työasemien ja palvelimien haittaohjelmasuojauksesta ja havaituista epäilyttävistä tapahtumista.	Ovatko kaikki laitteet suojauksen piirissä, ovatko ohjelmistot ja tunnisteet ajan tasalla ja käsitelläänkö hälytykset? Tarkastetaan myös suojaamattomat tai pitkään yhteydettömänä olleet laitteet.
Failover	Automaattinen tai hallittu siirtyminen ensisijaisesta yhteydestä, laitteesta tai palvelusta vararatkaisuun.	Pyydä näyttöä säännöllisistä siirtymistesteistä, palautumisajoista ja siitä, ettei vararatkaisu käytä samaa vikaantumispistettä.
Firmware	Laitteen sisäinen laiteohjelmisto, joka ohjaa esimerkiksi reitittimen, kytkimen tai palomuurin toimintaa.	Tarkasta tuetut versiot, päivitysmenettely, haavoittuvuuksien seuranta ja palautusmahdollisuus.
HSM- tai avainholvin lokit	Tapahtumatiedot järjestelmästä, jossa säilytetään salausavaimia, varmenteita, salasanoja tai muita salaisuuksia.	Voidaanko todentaa, kuka käytti, loi, muutti tai poisti avaimen? Ovatko lokit suojattuja muuttamiselta, säilytetäänkö niitä riittävän pitkään ja tutkitaanko poikkeava käyttö?
IDS (Intrusion Detection System)	Tunkeutumisen havaitsemisjärjestelmä, joka tunnistaa epäilyttävää liikennettä tai toimintaa ja muodostaa hälytyksiä.	Arvioi kattavuus, havaintosäännöt, hälytysten käsittely ja väärien positiivisten hallinta.
IP (Internet Protocol) / IP-osoite	Verkkolaitteen looginen osoite, jonka avulla liikenne ohjataan oikeaan lähteeseen ja kohteeseen.	Tarkasta osoitteiden hallinta, omistajuus, päällekkäisyydet, julkisten osoitteiden suojaus ja tarpeettomien osoitteiden poistaminen.
IPAM (IP Address Management)	IP-osoitteiden, aliverkkojen ja osoitevarausten keskitetty hallinta.	Varmista, että IPAM-tiedot vastaavat DHCP-, DNS- ja verkkolaitteiden todellisia asetuksia.
IPS (Intrusion Prevention System)	Tunkeutumisen estojärjestelmä, joka havaitsemisen lisäksi voi automaattisesti estää haitallista liikennettä.	Tarkasta estoprofiilit, muutosten testaus, vaikutus tuotantoliikenteeseen ja ohitusmenettelyt.
MDM-raportit	Raportit organisaation puhelimien, tablettien ja tietokoneiden keskitetystä hallinnasta.	Ovatko kaikki työssä käytettävät laitteet hallinnassa? Tarkastetaan salaus, näytön lukitus, päivitykset, haitallisten laitteiden estäminen sekä kadonneiden laitteiden etälukitus ja tyhjennys.
MFA (Multi-Factor Authentication)	Monivaiheinen tunnistaminen, jossa henkilöllisyys varmistetaan vähintään kahdella eri tekijällä, kuten salasanalla ja kertakäyttökoodilla.	Varmista MFA:n käyttö etäyhteyksissä ja hallintakäytössä sekä hätä- ja palautusmenettelyjen turvallisuus.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
NAC (Network Access Control)	Verkkopääsyn hallinta, joka tarkastaa käyttäjän tai laitteen ennen verkkoon päästämistä ja voi rajata käyttöoikeuksia.	Arvioi tunnistus, laitevaatimukset, roolit, karanteeni, lokitus ja toiminta tunnistuspalvelun häiriössä.
NMS (Network Management System)	Verkonhallinta- ja valvontajärjestelmä, jolla seurataan laitteiden tilaa, kapasiteettia, virheitä ja muutoksia.	Tarkasta valvonnan kattavuus, hälytysrajat, käyttöoikeudet, lokitus ja järjestelmän oma suojaus.
NTP-asetukset	Asetukset, joilla tietokoneiden, palvelimien ja verkkolaitteiden kellot pidetään samassa ajassa.	Käytetäänkö hyväksyttyjä aikapalvelimia, synkronoituvatko kaikki kriittiset järjestelmät ja havaitaanko liian suuret aikaerot? Oikea aika on tärkeä lokien ja tapahtumien jäljittämisessä.
RACI	Vastuumalli: Responsible = toteuttaja, Accountable = lopullisesti vastuullinen, Consulted = kuultava ja Informed = tiedotettava.	Varmista, että kriittisille tehtäville on nimetty selkeät roolit eikä hyväksyntä ja toteutus ole perusteettomasti samalla henkilöllä.
RADIUS (Remote Authentication Dial-In User Service)	Keskitetty tunnistus-, valtuutus- ja tapahtumakirjauspalvelu, jota käytetään usein 802.1X- ja VPN-yhteyksissä.	Tarkasta palvelun saatavuus, salatut yhteydet, lokit, käyttöoikeudet ja varajärjestelyt.
RPO (Recovery Point Objective)	Suurin hyväksyttävä tietojen menetys ajassa ilmaistuna. Esimerkiksi RPO 15 minuuttia tarkoittaa, että enintään 15 minuutin tiedot saavat hävitä.	Arvioi, onko tavoite määritelty kriittisille tiedoille ja vastaavatko varmistukset sekä replikointi tavoitetta.
RTO (Recovery Time Objective)	Tavoiteaika, jonka kuluessa palvelu tai yhteys on palautettava häiriön jälkeen.	Vertaile tavoitetta mitattuihin palautumisaikoihin ja harjoitusten tuloksiin.
SIEM (Security Information and Event Management)	Järjestelmä, joka kerää ja yhdistää turvallisuuslokeja, tunnistaa poikkeamia ja tuottaa hälytyksiä.	Tarkasta lokilähteiden kattavuus, havaintosäännöt, aikaleimojen luotettavuus, hälytysten käsittely ja lokien säilytys.
SLA (Service Level Agreement)	Palvelutasosopimus tai -sitoumus, jossa määritellään esimerkiksi saatavuus, vasteajat ja korjausajat.	Varmista, että tietoliikenteen kriittiset palvelutasot ovat mitattavia, seurattuja ja sopimuksissa yhdenmukaisia.
SoD-matriisi	Taulukko, joka osoittaa, mitkä tehtävät ja käyttöoikeudet pitää erottaa eri henkilöille väärinkäytösten estämiseksi.	Voiko sama henkilö esimerkiksi tehdä ja hyväksyä saman maksun tai myöntää itselleen oikeuksia? Tarkastetaan ristiriitaiset roolit, poikkeusten hyväksyntä ja korvaavat valvontatoimet.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
SSID (Service Set Identifier)	Langattoman verkon nimi, jonka käyttäjä tai laite näkee verkkoa valitessaan.	Tarkasta SSID:iden omistajat, käyttötarkoitukset, suojausasetukset ja tarpeettomien verkkojen poistaminen.
TLS (Transport Layer Security)	Tiedonsiirtoa salaava protokolla, jota käytetään esimerkiksi verkkopalveluissa ja järjestelmien välisissä yhteyksissä.	Arvioi sallitut versiot, salausasetukset, varmenteet ja heikkojen protokollien estäminen.
VLAN (Virtual Local Area Network)	Looginen lähiverkko, jolla saman fyysisen verkkoinfrastruktuurin liikennettä erotetaan eri ryhmiin.	Varmista, että VLAN-jako perustuu riskiin ja käyttötarkoitukseen eikä pelkkä VLAN korvaa palomuurivalvontaa.
VPN (Virtual Private Network)	Salattu yhteystunneli, jolla käyttäjä, toimipiste tai kumppani yhdistetään verkkoon epäluotettavan verkon yli.	Tarkasta vahva tunnistaminen, salaus, käyttöoikeuksien rajaus, päätelaitteiden vaatimukset, lokitus ja oikeuksien poistaminen.
WAF (Web Application Firewall)	Verkkosovelluspalomuuri, joka suodattaa verkkosovellukseen kohdistuvaa HTTP- ja HTTPS-liikennettä.	Arvioi suojattujen palvelujen kattavuus, sääntöjen viritys, lokitus, poikkeukset ja reagointi havaintoihin.
WIDS (Wireless Intrusion Detection System)	Langattoman verkon tunkeutumisen havaitsemisjärjestelmä, joka etsii esimerkiksi luvattomia tukiasemia ja poikkeavaa radioliikennettä.	Tarkasta peittoalue, hälytysten käsittely, laiteluettelon ajantasaisuus ja säännölliset tarkastukset.
WIPS (Wireless Intrusion Prevention System)	Langattoman verkon tunkeutumisen estojärjestelmä, joka voi havaitsemisen lisäksi torjua luvattomia yhteyksiä.	Varmista, että automaattiset estotoimet on hyväksytty, testattu ja rajattu niin, etteivät ne häiritse luvallisia verkkoja.
WLAN (Wireless Local Area Network)	Langaton lähiverkko eli Wi-Fi-verkko.	Arvioi salaus, käyttäjien ja laitteiden tunnistaminen, vierailijaverkon erottelu, tukiasemien hallinta ja radiokattavuus.
WORM (Write Once, Read Many)	Tallennustapa, jossa tietoa voidaan kirjoittaa kerran mutta sitä ei voi muuttaa tai poistaa määritellyn säilytysajan aikana.	Tarkasta, että muuttumattomuutta käytetään tarvittaessa lokien ja muun todistusaineiston suojaamiseen ja että säilytysajat on määritelty.

Muut tietoliikenneturvallisuuden ammattikäsitteet

Käsitteet on järjestetty aakkosittain. Selitys kuvaa termin merkityksen juuri tietoliikenneturvallisuuden arvioinnin yhteydessä.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Aliverkko	IP-verkon rajattu osa, jolla on oma osoitealue. Aliverkkoja käytetään liikenteen, laitteiden ja palvelujen erotteluun.	Tarkasta, että aliverkot on dokumentoitu, nimetty käyttötarkoituksen mukaan ja suojattu asianmukaisilla liikennesäännöillä.
Allekirjoitus (IDS/IPS)	Havaintomalli tai tunniste, jonka avulla suojausjärjestelmä tunnistaa tunnetun hyökkäyksen tai haitallisen liikenteen. Ei tarkoita tässä sähköistä allekirjoitusta.	Varmista allekirjoitusten päivitys, testaus ja vanhentuneiden sääntöjen hallinta.
Arkkitehtuuri	Kuvaus siitä, miten verkot, laitteet, palvelut, yhteydet, suojausratkaisut ja riippuvuudet muodostavat kokonaisuuden.	Arvioi, vastaavatko kaaviot todellista ympäristöä ja onko turvallisuus huomioitu jo suunnittelussa.
Arkkitehtuurikatselmus	Ennalta määritelty tarkastus, jossa suunniteltu ratkaisu arvioidaan ennen toteutusta tai merkittävää muutosta.	Pyydä katselmuspöytäkirjat, riskihavainnot, hyväksynnät ja ehdollisten hyväksyntöjen seurantatiedot.
Auditointi	Riippumaton ja järjestelmällinen arviointi, jossa vaatimusten toteutuminen varmistetaan näytön perusteella.	Pelkkä haastatteluvastaus ei riitä, vaan johtopäätösten tulee perustua asiakirjoihin, järjestelmätietoihin, havaintoihin ja otantaan.
Auditointijälki	Tiedot, joiden avulla tapahtuma, muutos, hyväksyntä tai päätös voidaan jäljittää tekijään, aikaan ja kohteeseen.	Tarkasta, että jälki on riittävä, suojattu muuttamiselta ja säilytetty vaaditun ajan.
Autentikointi	Henkilön, laitteen tai palvelun ilmoittaman identiteetin todentaminen eli tunnistaminen.	Arvioi tunnistusmenetelmän vahvuus suhteessa riskiin sekä epäonnistuneiden tunnistusten seuranta.
Avaimenhallinta	Salausavainten luominen, jakaminen, säilyttäminen, käyttö, vaihtaminen, varmistaminen ja turvallinen poistaminen.	Varmista vastuut, käyttöoikeudet, avainten voimassaolo, vaihto, varakopiot ja toiminta avainvuodossa.
Eheys	Ominaisuus, jonka mukaan tieto, loki tai asetustieto ei ole muuttunut luvattomasti tai huomaamatta.	Tarkasta eheystarkastukset, allekirjoitukset, muuttumaton säilytys ja muutoslokit.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Elinkaari	Kohteen vaiheet hankinnasta ja käyttöönotosta ylläpitoon, muutoksiin ja käytöstä poistoon.	Arvioi, hallitaanko turvallisuusvaatimukset kaikissa vaiheissa ja poistetaanko vanhat laitteet, tunnukset ja säännöt hallitusti.
Eskalointi	Asian siirtäminen sovitulle ylemmälle päätös- tai asiantuntijatasolle vakavuuden, vaikutuksen tai viiveen vuoksi.	Varmista selkeät kriteerit, yhteystiedot, aikarajat ja näyttö toteutuneista eskaloinneista.
Estoprofiili	Suojausjärjestelmän asetuskokonaisuus, joka määrittää, millainen liikenne estetään, sallitaan tai ainoastaan kirjataan.	Tarkasta profiilien omistajat, hyväksynnät, testaus ja vaikutus luvalliseen liikenteeseen.
Haavoittuvuus	Heikkous laitteessa, ohjelmistossa, asetuksessa tai toimintatavassa, jota voidaan käyttää väärin.	Arvioi tunnistaminen, riskiluokitus, korjausajat, poikkeusten hyväksyntä ja toteutuneiden korjausten varmistus.
Haavoittuvuusskannaus	Automaattinen tekninen tarkastus, jolla etsitään tunnettuja haavoittuvuuksia ja virheellisiä asetuksia.	Tarkasta skannauksen kattavuus, ajantasaiset tunnisteet, tulosten käsittely ja väärien havaintojen varmistaminen.
Hallintayhteys	Yhteys, jota käytetään verkkolaitteen tai palvelun ylläpitoon ja asetusten muuttamiseen.	Varmista erillinen hallintaverkko, vahva tunnistaminen, salaus, rajatut lähteet ja kattava lokitus.
HR-ilmoitukset	Henkilöstöhallinnon ilmoitukset työntekijän aloittamisesta, tehtävämuutoksesta, poissaolosta tai työsuhteen päättymisestä.	Saapuvatko ilmoitukset oikeille tahoille ajoissa? Poistetaanko tai muutetaanko käyttöoikeudet viivytyksettä, palautetaanko laitteet ja kulkutunnisteet sekä dokumentoidaanko tehdyt toimet?
Hyväksymiskriteeri	Ehto, jonka täyttyessä arviointikohde voidaan todeta vaatimusten mukaiseksi.	Varmista, että kriteeri on yksiselitteinen ja että kaikki sen olennaiset osat voidaan todentaa näytöllä.
Häiriönsieto	Kyky jatkaa toimintaa yksittäisestä viasta, yhteyskatkosta tai laitteen menetyksestä huolimatta.	Pyydä näyttöä redundanssista, varayhteyksistä, testauksista ja yhteisten vikaantumispisteiden tunnistamisesta.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Hälytysraja	Ennalta määritelty arvo tai ehto, jonka ylittyminen tai täyttyminen muodostaa hälytyksen.	Arvioi rajojen perustelut, omistajat, säännöllinen tarkistus ja hälytysten käsittelyajat.
Immutability-asetukset	Tarkoittaa asetuksia, joilla tieto määritetään määräajaksi muuttamattomaksi.	Arvioinnissa kannattaa tarkastaa mille tiedoille muuttamattomuus on asetettu, kuinka pitkä muuttamattomuusaika on, vastaako säilytysaika yrityksen palautumis- ja lakisääteisiä tarpeita, voiko pääkäyttäjä poistaa tai kiertää asetuksen, ovatko asetusten muutokset hyväksyttyjä ja lokitettuja, testataanko muuttamattomien varmuuskopioiden palauttamista, onko asetuksen päättymisen jälkeinen poistaminen hallittua.
Internetrajapinta	Palvelu, osoite tai yhteyspiste, joka on suoraan tai välillisesti saavutettavissa internetistä.	Tarkasta omistajuus, tarpeellisuus, suojaus, päivitykset, testaukset ja jatkuva valvonta.
IP-konflikti eli osoiteristiriita	Tilanne, jossa sama IP-osoite on käytössä usealla laitteella tai osoitevaraukset ovat ristiriidassa.	Arvioi IPAM-, DHCP- ja valvontatietojen yhdenmukaisuus sekä ristiriitojen käsittely.
Istunto	Yksittäinen kirjautumis- tai yhteysjakso käyttäjän tai järjestelmien välillä.	Tarkasta istuntojen aikakatkaisu, katkaiseminen, tallennus tarvittaessa ja poikkeavien istuntojen seuranta.
Jatkuvuus	Kyky ylläpitää tai palauttaa kriittinen toiminta hyväksyttävälle tasolle häiriössä.	Arvioi kriittiset riippuvuudet, vararatkaisut, vastuut, viestintä ja harjoitusten tulokset.
Juurisyyanalyysi	Menetelmä, jolla selvitetään poikkeaman perimmäiset syyt eikä vain korjata näkyviä oireita.	Tarkasta, että syyt johtavat konkreettisiin korjaaviin toimenpiteisiin ja niiden vaikuttavuus varmistetaan.
Jäljitettävyys	Mahdollisuus selvittää jälkikäteen, mitä tapahtui, kuka toimi, milloin, missä kohteessa ja millä hyväksynnällä.	Arvioi lokit, muutoshistoria, päätökset, aikaleimat ja tietojen suojaus muuttamiselta.
Jäännösriski	Riski, joka jää jäljelle suojaustoimenpiteiden toteuttamisen jälkeen.	Varmista, että merkittävä jäännösriski on dokumentoitu ja hyväksytty oikealla valtuustasolla määräajaksi.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Kapasiteetti	Yhteyden, laitteen tai palvelun kyky käsitellä tietty määrä liikennettä tai kuormaa.	Arvioi käyttöaste, kasvunvara, ruuhkahuiput, varayhteydet ja suunnitellut kapasiteetin lisäykset.
Karanteeniverkko	Eristetty verkkoympäristö, johon tuntematon tai vaatimustenvastainen laite ohjataan rajoitettua tarkastusta tai korjausta varten.	Varmista, ettei karanteenista pääse kriittisiin verkkoihin ja että vapauttamiselle on hyväksytty menettely.
Katselmointi	Suunniteltu tarkastus, jossa asian ajantasaisuus, riittävyys ja soveltuvuus arvioidaan.	Pyydä näyttöä ajankohdasta, osallistujista, havainnoista, päätöksistä ja jatkotoimista.
Kattavuus	Osuus soveltuvista verkoista, laitteista, lokeista tai kontrolleista, jotka ovat arvioinnin tai valvonnan piirissä.	Älä hyväksy pelkkää järjestelmän olemassaoloa; varmista, mitä kohteita se todellisuudessa kattaa.
Konfiguraatio	Laitteen, palvelun tai järjestelmän toiminnan määrittävä asetuskokonaisuus.	Tarkasta hyväksytyt asetuspohjat, poikkeamat, versiot, varmuuskopiot ja muutosten jäljitettävyys.
Konfiguraatioauditointi	Tekninen tarkastus, jossa todellisia asetuksia verrataan hyväksyttyyn turvallisuusmalliin tai vaatimuksiin.	Varmista tarkastuksen kattavuus, käytetty vertailutaso, havainnot ja korjausten uusintatestaus.
Kontrolli	Hallinnollinen, tekninen tai fyysinen suojaustoimi, jolla riskiä ehkäistään, havaitaan tai sen vaikutusta pienennetään.	Arvioi sekä kontrollin olemassaolo että sen todellinen toimivuus, kattavuus ja jatkuva käyttö.
Korjaava toimenpide	Toimi, jolla havaitun puutteen tai poikkeaman syy poistetaan tai riski pienennetään hyväksyttävälle tasolle.	Tarkasta omistaja, määräaika, tilaseuranta ja vaikuttavuuden varmistus.
Koventaminen	Tarpeettomien palvelujen, tunnusten ja toimintojen poistaminen sekä turvallisten asetusten käyttöönotto hyökkäyspinnan pienentämiseksi.	Vertaile todellisia asetuksia hyväksyttyihin kovennusmalleihin ja käsittele poikkeukset riskiperusteisesti.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Kriittinen arviointikysymys	Kysymys, jonka puutteella voi olla merkittävä vaikutus turvallisuuteen, palvelun saatavuuteen tai tietojen suojaan.	Kriittisen kohdan hyväksyminen edellyttää vahvaa ja kattavaa näyttöä; puute on eskaloitava ja käsiteltävä kiireellisesti.
Kriittisyys	Arvio kohteen merkityksestä liiketoiminnalle, turvallisuudelle tai lakisääteisille velvoitteille.	Varmista, että kriittisyysluokitus ohjaa suojausta, valvontaa, korjausaikoja ja jatkuvuusratkaisuja.
Kuormantasaaja	Ratkaisu, joka jakaa verkkoliikennettä usealle palvelimelle tai palvelukohteelle.	Tarkasta suojausasetukset, terveystarkastukset, varajärjestelyt, hallintayhteydet ja lokit.
Kuormitustesti	Testi, jossa yhteyden tai palvelun toimintaa mitataan tavallista suuremmalla tai suunnitellulla kuormalla.	Varmista hyväksytty testisuunnitelma, tuotantoriskien hallinta, tavoitearvot ja tuloksiin perustuvat toimet.
Lokienhallinta	Tapahtumatietojen kerääminen, siirtäminen, suojaaminen, säilyttäminen, analysointi ja poistaminen.	Varmista lähdekattavuus, aikaleimat, eheys, käyttöoikeudet, säilytysajat ja hälytysten muodostuminen.
Luottamuksellisuus	Ominaisuus, jonka mukaan tieto on vain siihen oikeutettujen henkilöiden, laitteiden tai palvelujen käytettävissä.	Arvioi pääsynhallinta, salaus, segmentointi, lokitus ja tietovuotojen havaitseminen.
Luottamusraja	Kohta, jossa käyttäjän, laitteen, verkon tai palvelun luottamustaso muuttuu ja tarvitaan erillistä tarkastusta tai suojausta.	Tarkasta rajojen kuvaus, tunnistus, liikenteen suodatus, lokitus ja oletusarvoisesti estävä toimintamalli.
Muutoksenhallinta	Menettely, jossa muutoksen tarve, vaikutukset, riskit, hyväksyntä, testaus, toteutus ja palautus suunnitellaan ennen käyttöönottoa.	Pyydä muutospyyntö, hyväksyntä, testitulos, toteutusloki ja tarvittaessa palautuksen toteutuminen.
Nimipalvelu	Palvelu, joka yhdistää ihmisten käyttämät verkkonimet teknisiin osoitteisiin; tavallisesti DNS.	Arvioi omistajuus, muutosten valvonta, varmistukset, suojaus ja poikkeamien seuranta.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Otanta	Rajattu mutta perusteltu joukko kohteita, tapahtumia tai asiakirjoja, joiden avulla arvioidaan laajempaa kokonaisuutta.	Varmista, että otos on riittävän kattava, riskiperusteinen ja sisältää myös poikkeavia sekä kriittisiä tapauksia.
Pakettihävikki	Osuus verkkopaketeista, jotka eivät saavu määränpäähän. Hävikki voi aiheuttaa hitautta, katkoksia ja virheitä.	Tarkasta mittaustulokset, hälytysrajat, trendit ja hävikin syiden käsittely.
Palautusmenettely	Ennalta suunniteltu tapa palauttaa asetukset, yhteys tai palvelu turvalliseen aiempaan tilaan epäonnistuneen muutoksen tai häiriön jälkeen.	Tarkasta palautuspisteet, varmuuskopiot, vastuut, käynnistyskriteerit ja testitulokset.
Palomuuri	Laite tai ohjelmisto, joka valvoo ja suodattaa verkkoliikennettä määritettyjen sääntöjen perusteella.	Arvioi sääntöjen vähimmäistarve, omistajat, hyväksynnät, katselmoinnit, lokitus ja tarpeettomien sääntöjen poistaminen.
Palvelunestohyökkäys	Hyökkäys, jonka tavoitteena on estää tai heikentää palvelun normaalia käyttöä kuormittamalla resursseja tai käyttämällä teknistä heikkoutta.	Tarkasta suojaus, kapasiteetti, operaattoriyhteistyö, reagointi, viestintä ja palautuminen.
Palvelutaso	Mitattava tavoite palvelun laadulle, kuten saatavuudelle, viiveelle, vasteajalle tai korjausajalle.	Varmista, että tavoitteet on sovittu, mitataan oikeista lähteistä ja poikkeamat johtavat toimenpiteisiin.
Penetraatiotesti	Valtuutettu hyökkäyssimulaatio, jossa etsitään ja pyritään hyödyntämään haavoittuvuuksia hallitusti.	Varmista kirjallinen lupa, rajaus, pätevyys, tuotantoriskien hallinta, raportointi ja korjausten uusintatestaus.
Poikkeama	Tapahtuma tai tila, joka poikkeaa hyväksytystä vaatimuksesta, normaalista toiminnasta tai odotetusta turvallisuustasosta.	Arvioi kirjaaminen, luokittelu, rajaus, tutkinta, korjaus, eskalointi ja juurisyyanalyysi.
Poikkeuslupa	Määräaikainen, perusteltu ja hyväksytty lupa poiketa vaatimuksesta tai turvallisuusmallista.	Varmista riskinarvio, hyväksyjä, korvaavat kontrollit, voimassaoloaika ja sulkemisen seuranta.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Prosessin omistaja	Henkilö tai rooli, joka vastaa prosessin tavoitteista, toimivuudesta, resursoinnista ja kehittämisestä.	Tarkasta nimitys, valtuudet, raportointi, mittarit ja toteutuneet katselmoinnit.
Protokolla	Sääntöjoukko, jonka mukaan laitteet tai palvelut vaihtavat tietoa verkossa.	Varmista, että käytössä ovat vain tarpeelliset, hyväksytyt ja turvalliset protokollat sekä tuetut versiot.
Puhdistuspalvelu	DDoS-torjuntapalvelu, joka ohjaa liikenteen erilliseen ympäristöön, suodattaa hyökkäysliikenteen ja välittää puhtaan liikenteen palvelulle.	Tarkasta palvelun aktivointiehdot, yhteystiedot, kapasiteetti, reititysmuutokset ja harjoitukset.
Päätepiste	Yhteyden tai tietovirran lähtö- tai kohdepalvelu, laite, osoite tai rajapinta.	Arvioi omistajuus, tunnistus, suojaus, hyväksytyt yhteydet ja elinkaaren hallinta.
Rajapinta	Määritelty yhteyspiste, jonka kautta järjestelmät, palvelut tai verkot vaihtavat tietoa.	Tarkasta käyttötarkoitus, omistaja, tunnistus, salaus, syötteiden tarkastus, lokitus ja versionhallinta.
Rajaus	Poikkeaman vaikutuksen rajoittaminen esimerkiksi eristämällä laite, estämällä yhteys tai poistamalla tunnus käytöstä.	Varmista ennalta sovitut valtuudet, nopea toteutus, vaikutusten seuranta ja hallittu palautus.
Redundanssi	Kahdennus tai varajärjestely, jonka avulla toiminta jatkuu yhden osan vikaantuessa.	Tarkasta ratkaisujen riippumattomuus, kapasiteetti, automaattinen tai hallittu siirtyminen ja säännöllinen testaus.
Reititys	Menettely, jolla verkkoliikenteelle valitaan kulkureitti verkkojen välillä.	Arvioi hyväksytyt reitit, muutosten hallinta, suodatus, lokitus ja poikkeavien reittien havaitseminen.
Reititystaulu	Verkkolaitteen tieto siitä, mihin suuntaan eri kohdeverkkojen liikenne lähetetään.	Varmista taulujen muutosten jäljitettävyys, hyväksyntä ja poikkeavien reittien valvonta.
Reittikaappaus	Tilanne, jossa liikenne ohjautuu väärään tai haitalliseen reittiin virheen tai hyökkäyksen vuoksi.	Tarkasta reitityksen suodatus, valvonta, operaattoriyhteistyö ja reagointimenettely.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Riskiperusteisuus	Toimintatapa, jossa suojausten laajuus ja kiireellisyys määräytyvät uhan, haavoittuvuuden, vaikutuksen ja todennäköisyyden perusteella.	Arvioi, näkyykö riskitaso käytännössä prioriteeteissa, korjausajoissa, valvonnassa ja hyväksynnöissä.
Riskirekisteri	Ylläpidetty luettelo tunnistetuista riskeistä, niiden arvioista, omistajista, käsittelytoimista ja hyväksynnöistä.	Tarkasta ajantasaisuus, yhteys teknisiin havaintoihin, määräajat ja jäännösriskien hyväksynnät.
Saatavuus	Ominaisuus, jonka mukaan palvelu, yhteys tai tieto on käytettävissä silloin, kun sitä tarvitaan.	Arvioi palvelutasot, valvonta, redundanssi, kapasiteetti, häiriöiden käsittely ja palautumistestit.
Salaus	Tiedon muuntaminen muotoon, jota ei voi ymmärtää ilman oikeaa salausavainta.	Tarkasta salattavat tietovirrat, hyväksytyt menetelmät, avainten hallinta ja poikkeukset.
Salausalgoritmi	Matemaattinen menetelmä, jolla tieto salataan ja puretaan.	Varmista, että algoritmi ja avainpituus ovat organisaation vaatimusten mukaisia, tuettuja ja ajantasaisia.
Salausavain	Salainen tai julkinen arvo, jota käytetään tiedon salaamiseen, purkamiseen tai aitouden varmistamiseen.	Arvioi luominen, säilytys, käyttöoikeudet, vaihto, peruutus ja toiminta avaimen vaarantuessa.
Segmentointi	Verkon jakaminen erillisiin osiin, joiden välistä liikennettä rajoitetaan ja valvotaan.	Tarkasta jako riskien perusteella, sallitut tietovirrat, tekninen toteutus ja segmentoinnin testaus.
Tehtävien eriyttäminen	Periaate, jossa kriittisen toimenpiteen valmistelu, hyväksyntä ja toteutus jaetaan eri henkilöille tai rooleille.	Varmista, ettei yksi henkilö voi tehdä ja hyväksyä merkittävää muutosta ilman riippumatonta valvontaa.
Tekninen velka	Aiemmista ratkaisuista, vanhentuneista teknologioista tai lykkääntyneistä korjauksista kertynyt riski ja ylläpitotaakka.	Tarkasta rekisteri, riskiluokitus, omistajat, määräajat ja johdon hyväksyntä pitkäaikaisille poikkeamille.
Tietomurto	Luvaton pääsy tietojärjestelmään, verkkoon tai tietoihin.	Arvioi havaitseminen, rajaus, tutkinta, viranomais- ja asiakasvelvoitteet, palautuminen ja opit.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Tietovirta	Tiedon kulku määritellystä lähteestä kohteeseen verkon, palvelun tai rajapinnan kautta.	Tarkasta lähde, kohde, tiedon luokitus, protokolla, salaus, omistaja ja salliva sääntö.
Tietovuoto	Luottamuksellisen tai suojatun tiedon luvaton paljastuminen, siirtyminen tai päätyminen väärälle taholle.	Arvioi ehkäisy, havaitseminen, tiedonsiirron suojaus, rajaus, ilmoitusvelvoitteet ja tutkinta.
Todentava näyttö	Asiakirja, järjestelmätieto, loki, havainto, haastattelu tai testitulos, jolla hyväksymiskriteerin toteutuminen osoitetaan.	Näytön tulee olla ajantasainen, kattava, luotettava ja suoraan yhteydessä arvioitavaan väitteeseen.
Topologia	Kuvaus verkon rakenteesta ja siitä, miten laitteet, verkot ja yhteydet liittyvät toisiinsa.	Varmista, että topologiakuva on ajantasainen ja sisältää kriittiset yhteydet, rajat ja varareitit.
Tunkeutuminen	Luvaton tai haitallinen pääsy verkkoon, laitteeseen tai palveluun.	Tarkasta havaitsemis- ja estoratkaisut, lokitus, hälytysten käsittely ja poikkeaman rajaus.
Tunnistaminen	Yleisnimitys prosessille, jossa käyttäjän, laitteen tai palvelun identiteetti selvitetään ja todennetaan.	Erota arvioinnissa tunnistaminen valtuutuksesta: tunnistaminen kertoo kuka tai mikä, valtuutus mitä se saa tehdä.
Uusintatestaus	Korjauksen jälkeen tehtävä tarkastus, jolla varmistetaan puutteen poistuminen eikä uusia haittavaikutuksia ole syntynyt.	Pyydä alkuperäinen havainto, korjausnäyttö, uusintatestin tulos ja sulkemispäätös.
Vaikuttavuuden varmistaminen	Arvio siitä, poistiko toteutettu toimenpide puutteen syyn ja pienensikö se riskin tavoitellulle tasolle.	Varmista mittaus, uusintatestaus, toistuvuuden seuranta ja dokumentoitu sulkemispäätös.
Valtuutus	Päätös siitä, mitä tunnistettu käyttäjä, laite tai palvelu saa käyttää tai tehdä.	Tarkasta roolit, vähimmät oikeudet, hyväksyntä, määräaikaisuus ja oikeuksien säännöllinen katselmointi.
Varmenne eli sertifikaatti	Sähköinen todistus, joka yhdistää julkisen salausavaimen tunnistettuun palveluun, laitteeseen tai henkilöön.	Tarkasta myöntäjä, käyttötarkoitus, voimassaolo, uusinta, peruutus ja luottamusketju.

Käsite tai lyhenne	Selkokielinen merkitys	Arvioinnissa huomioitavaa
Varmenneketju	Sarja varmenteita, jonka avulla palvelun varmenne voidaan johtaa luotettuun juurivarmenteeseen.	Arvioi ketjun täydellisyys, luotetut myöntäjät, vanhentuneet varmenteet ja peruutustarkastukset.
Versionhallinta	Menettely, jolla asiakirjojen, asetusten tai ohjelmistojen versiot, muutokset ja hyväksynnät säilytetään jäljitettävinä.	Tarkasta voimassa olevan version tunnistaminen, muutoshistoria, palautettavuus ja luvattomien muutosten estäminen.
Viive	Aika, joka tiedon kulkemiseen lähteestä kohteeseen kuluu.	Arvioi tavoitearvot, mittauspisteet, hälytysrajat, ruuhkahuiput ja poikkeamien käsittely.
Vyöhykkeistäminen	Verkon ja palvelujen ryhmittely eri luottamus- tai suojaustason alueisiin, kuten käyttäjä-, palvelin-, hallinta- ja vierailijavyöhykkeisiin.	Arvioi vyöhykkeiden perusteet, rajat, sallitut tietovirrat ja niiden valvonta.
Vähimmät oikeudet	Periaate, jonka mukaan käyttäjälle, laitteelle tai palvelulle annetaan vain tehtävän edellyttämät oikeudet ja vain tarvittavaksi ajaksi.	Tarkasta roolit, määräaikaiset oikeudet, ylläpito-oikeudet, katselmoinnit ja tarpeettomien oikeuksien poistaminen.
Väärä positiivinen	Hälytys, jossa järjestelmä tulkitsee normaalin toiminnan virheellisesti haitalliseksi.	Varmista, että havainto tutkitaan, sääntöä viritetään hallitusti eikä todellisia hyökkäyksiä samalla peitetä.
Yhteinen vikaantumispiste	Yksittäinen riippuvuus, jonka vika voi samanaikaisesti estää sekä ensisijaisen että vararatkaisun toiminnan.	Tarkasta esimerkiksi yhteinen operaattori, kaapelireitti, sähkönsyöttö, tila, laite tai hallintapalvelu.
Ylikuormitus	Tilanne, jossa liikenteen tai käsittelyn määrä ylittää yhteyden, laitteen tai palvelun kapasiteetin.	Arvioi hälytysrajat, kasvunvara, kuormituksen hallinta, priorisointi ja kapasiteetin lisäyssuunnitelmat.

Arvioijan muistilista käsitteiden soveltamiseen

Pyydä organisaatiota näyttämään, miten käsite toteutuu sen omassa ympäristössä. Esimerkiksi ”segmentointi” voidaan toteuttaa eri tekniikoilla, mutta sallitut tietovirrat, rajat ja valvonta on aina pystyttävä osoittamaan.

Varmista kattavuus. Yhden laitteen tai palvelun onnistunut esimerkki ei osoita, että vaatimus toteutuu koko soveltamisalalla.

Vertaa dokumentaatiota todellisiin asetuksiin. Verkkokaavio, laiteluettelo tai politiikka voi olla vanhentunut. Käytä otantaa ja teknistä näyttöä ristiriitojen tunnistamiseen.

Arvioi poikkeukset erikseen. Poikkeuksella tulee olla riskinarvio, hyväksyntä, korvaavat kontrollit, omistaja ja määräaika.

Tarkasta jatkuva toiminta, ei vain kertaluonteinen toteutus. Lokien, mittareiden, katselmusten, päivitysten ja harjoitusten tulee osoittaa, että prosessi toimii myös arviointihetken ulkopuolella.

Erota olemassaolo ja vaikuttavuus. Kontrolli voi olla asennettu mutta väärin määritetty, puutteellisesti kattava tai ilman toimivaa reagointia.