Tarkoitus

SecMeter SATA™ (Security Assessment and Treatment Architecture) on yrityksen turvakontrollien arviointi- ja suunnittelutyökalu. Sen avulla arvioidaan, kuinka hyvin yrityksen kontrollikokonaisuus vastaa suositeltua rakennetta ja tunnistetaan kehittämiskohteet. Työkalu jakaa kontrollit kolmeen ryhmään:

1. Ehkäisevät kontrollit (60 %)
2. Ilmaisevat kontrollit (10 %)
3. Lieventävät kontrollit (30 %)

Painotukset perustuvat hyvään tietoturvakäytäntöön, jossa ensisijaisesti pyritään estämään haitalliset tapahtumat ennen niiden toteutumista.

Käyttövaiheet

1. Täytä perustiedot

Täytä ensimmäisellä sivulla vähintään:

- Organisaatio
- Arvioitava kohde tai yksikkö
- Suunnittelija
- Päivämäärä
- Versionumero

Kirjaa lisäksi arvioinnin rajaus sekä suunnittelun lähtöoletukset.

2. Kuvaa suunnitellut kontrollit

Sivuilla 2–4 kirjoita kuhunkin taulukkoon suunnitellut tai käytössä olevat kontrollit. Yksi rivi vastaa yhtä kontrollia. Voit suunnitella kolmeen kontrollikokonaisuuteen jopa yhdeksää kontrollia. Kontrollikokonaisuudesta muodostuu kontrollikori (Kontrollikori™ Secmeter).

Esimerkkejä:

- Monivaiheinen tunnistautuminen
- Käyttöoikeuksien hallinta
- Lokien valvonta
- Varmuuskopiointi
- Harjoiteltu palautusmenettely

3. Arvioi vaikuttavuus

Jokainen arvioitava kontrolli saa vaikuttavuusarvosanan väliltä 0–5.

- Tehoton = 0
- Heikko = 1
- Välttävä = 2
- Tyydyttävä = 3
- Hyvä = 4
- Erittäin hyvä = 5

Arvioi kontrollin todellista vaikutusta, ei pelkästään sen olemassaoloa.

4. Tarkastele laskentaa

- Laskenta-sivu muodostaa automaattisesti:
- ehkäisevien kontrollien toteuman
- ilmaisevien kontrollien toteuman
- lieventävien kontrollien toteuman
- kokonaisvastaavuuden ideaalimalliin
- kokonaisarvosanan

Tarkastele raporttia

Raporttisivu kokoaa tulokset yhteen. Raporttia voidaan käyttää esimerkiksi:

- riskienhallinnassa
- tietoturvan kehittämisessä
- auditointien tukena
- johdon raportoinnissa
- kehitystoimenpiteiden priorisoinnissa

Arviointiperiaatteet

Hyvä kontrollikokonaisuus painottuu ehkäiseviin toimenpiteisiin. Tavoitetaso on:

- 60 % ehkäiseviä kontrollivaikutuksia
- 10 % ilmaisevia kontrollivaikutuksia
- 30 % lieventäviä kontrollivaikutuksia

Jos ehkäisevien kontrollien osuus jää pieneksi, turvallisuus perustuu liikaa havaitsemiseen ja vahinkojen korjaamiseen.

Arviointivinkki

Kun arvioit kontrollia, kysy aina:

- Estääkö tämä tapahtuman? → Ehkäisevä
- Havaitseeko tämä tapahtuman? → Ilmaiseva
- Pienentääkö tämä vahinkoa tai nopeuttaako palautumista? → Lieventävä

Yksi kontrolli voi vaikuttaa useampaan ryhmään, mutta arvioinnissa se kannattaa sijoittaa siihen ryhmään, jossa sen ensisijainen vaikutus on suurin.

Hyviä käytäntöjä

- Arvioi kontrollien todellinen vaikuttavuus realistisesti.
- Perustele poikkeavat arviot.
- Päivitä arvio aina merkittävien muutosten jälkeen.
- Käytä samaa arviointiasteikkoa kaikissa arvioinneissa, jotta tulokset ovat vertailukelpoisia.

Esimerkkiorganisaatio

Organisaatio: Malliyritys Oy

Kohde: Toiminnanohjausjärjestelmä

Suunnittelija: Etunimi Sukunimi

Päivämäärä: 1.1.2026

1. Ehkäisevät kontrollit (60 %)

Suunniteltu kontrolli	Vaikuttavuus
Monivaiheinen tunnistautuminen (MFA)	5
Käyttöoikeuksien roolipohjainen hallinta	5
Päätelaitteiden BitLocker-levysalaus	4
Sovellusten sallittujen ohjelmien hallinta (Application Control)	4
Palomuuri ja verkkosegmentointi	5
Tietoturvatietoisuuden koulutus	3
Vierastilien automaattinen poistaminen	4
USB-laitteiden käytön rajoittaminen	4

Toteuma: noin 85 %

2. Ilmaisevat kontrollit (10 %)

Suunniteltu kontrolli	Vaikuttavuus
Keskitetty lokien keräys (SIEM)	4
Epäonnistuneiden kirjautumisten hälytykset	4
Haavoittuvuusskannaus kuukausittain	3
Palvelinten suorituskyvyn valvonta	3
Käyttäjäpoikkeamien seuranta	3

Toteuma: noin 68 %

3. Lieventävät kontrollit (30 %)

Suunniteltu kontrolli	Vaikuttavuus
Päivittäinen varmuuskopiointi	5
Palautusten testaus kaksi kertaa vuodessa	4
Toipumissuunnitelma (DRP)	4
Poikkeamien käsittelyprosessi	4
Kyberhäiriöiden harjoitukset	3

Toteuma: noin 80 %

Esimerkkitulokset

Kontrolliryhmä	Toteuma
Ehkäisevät 85 %	60 %
Ilmaisevat 68 %	10 %
Lieventävät 80 %	30 %

Kokonaisvastaavuus

82 / 100

Arvosana

Hyvä

Tulkinta

Esimerkkiorganisaation kontrollikokonaisuus painottuu ehkäiseviin toimenpiteisiin, mikä vastaa SecMeter SATA -mallin tavoitetta. Havaitsemiskyky on riittävä, mutta sitä voidaan edelleen parantaa esimerkiksi lisäämällä automaattisia hälytyksiä ja analytiikkaa. Toipumiskyky on hyvällä tasolla varmuuskopioinnin ja palautusharjoitusten ansiosta.