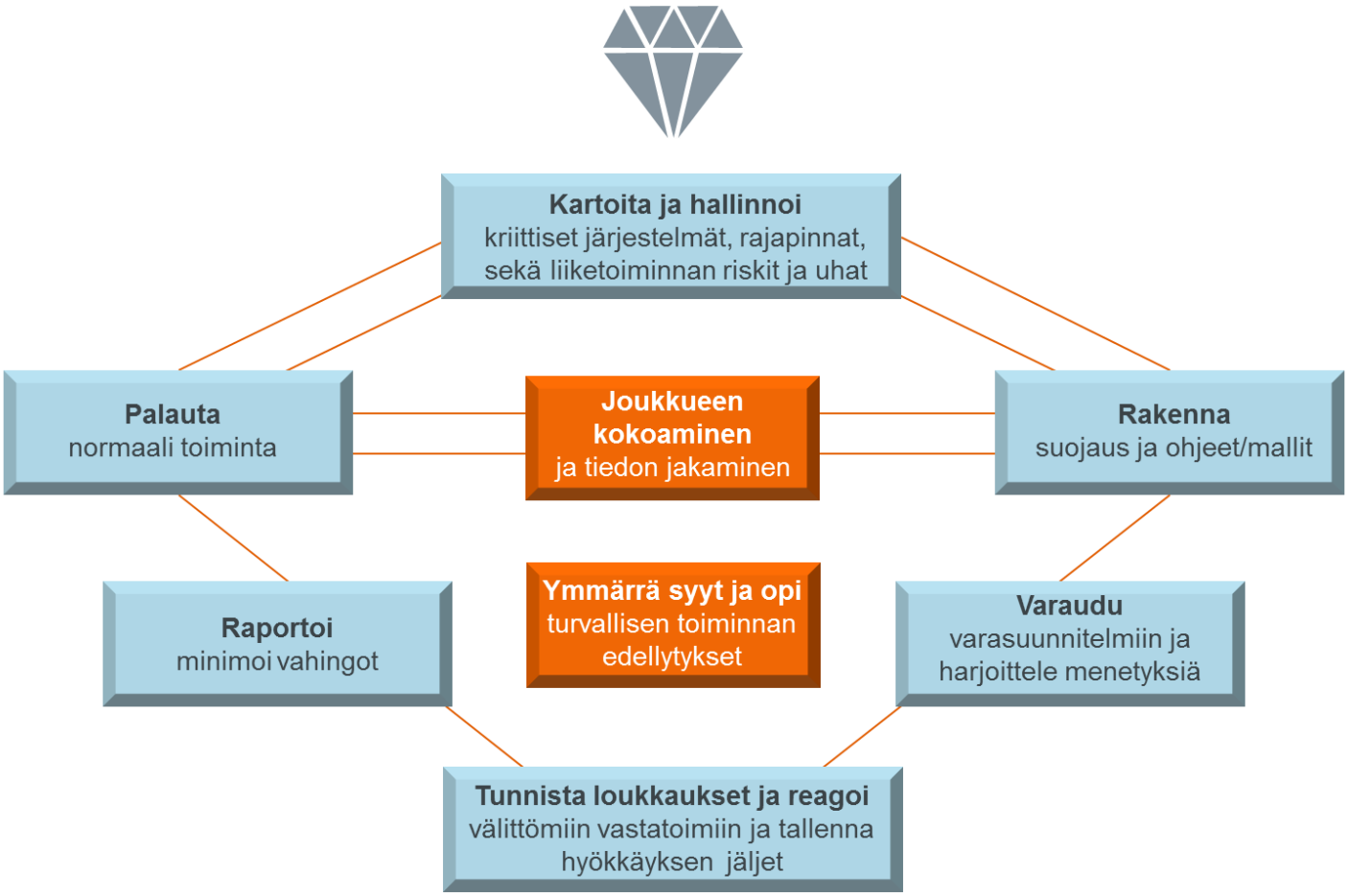
Tuotannon kyberturvan hallintamallin soveltaminen

Tarkastuslista



TUOTANNON KYBERTURVAN HALLINTAMALLIN SOVELTAMINEN

Tämä kysymyslista on tarkoitettu energiayritysten käyttöön niiden soveltaessa KYBER-ENE projektissa kehitettyä hallintamallia. Tarkoituksena on auttaa konkretisoimaan hallintamallin soveltamiseen liittyviä kysymyksiä ja tehtäviä

Kannattaa huomata, että vastaukset näihin kysymyksiin ovat luottamuksellisia. Vastaukset tarjoavat hyökkääjälle tärkeää tietoa siitä, miten juuri teitä vastaan hyökättäisiin tehokkaasti.

Oletteko muodostaneet organisaatiossanne kyberturvallisuuden, tietoturvallisuuden, tai kokonaisturvallisuuden tiimin, jonka vastuulle kuuluu tietoturvan kehittäminen ja valvonta?

- Onko tiimillä organisaation johdon tuki?
- Onko kehitystiimissä mukana henkilöitä kaikilta automaation kannalta kriittisiltä osa-alueilta kuten esimerkiksi
  - tuotannon (automaation) kunnossapidosta ja kehittämisestä,
  - yritys- ja laitostason ICT-järjestelmien ylläpidosta ja kehittämisestä,
  - automaation hankinnoista,
  - tuotannon järjestelmien pääkäyttäjistä,
  - kokonaisturvallisuudesta ja sen kehittämisestä, ja
  - henkilö- ja ympäristöturvallisuuden kehittämisestä?

Oletteko järjestäneet tiedon jakamisen omassa organisaatiossanne?

- Miten ja kenelle jaatte esimerkiksi
  - kyberturvallisuuteen liittyviä kehityssuunnitelmia,
  - koulutusmateriaalia,
  - tietoturvaohjeita,
  - raportteja oman järjestelmän tietoturvatapahtumista ja heikkouksista, ja
  - tietoja ulkopuolista tietoturvatapahtumista jotka kohdistuvat samankaltaisiin järjestelmiin kuin teillä on käytössä (tai energia-alaan yleensä)?
- Miten varmistetaan automaation kannalta kriittisten toimintojen ja henkilöiden tiedonsaanti?

TUOTANNON KYBERTURVAN HALLINTAMALLIN SOVELTAMINEN

Tarkastuslista

Tunnetteko toimialanne turvallisen toiminnan edellytykset verkkoympäristössä?

Turvalliseen toimintaan kuuluvat esimerkiksi

- koko henkilöstön kyberturvallisuustietoisuuden kehittäminen,
- jatkuvuutta ja turvallisuutta tukevien toimintaohjeiden ja lupamenettelyjen käyttöönottaminen,
- tuotannon suojauskonseptien jatkuva kehittäminen ja käyttäminen,
- kyky tunnistaa teihin kohdistuvaa vakoilua ja tietomurtoja,
- jatkuva toteutuneiden häiriöiden, tehtyjen virheiden ja epäiltyjen hyökkäysten raportoinnin seuranta,
- häiriöistä palautumisen suunnittelu ja toistuva harjoitteleminen, sekä
- uusien varautumistapojen etsiminen ja käyttöönottaminen kyberuhkien muuttuessa.

Miten hallinnoitte tuotanto-omaisuutenne?

- Kuinka hyvin tunnette kaikki toimistoverkkoonne kytkeytyvät laitteet mukaan lukien niissä käytetyt ohjelmistot versioineen?
- Kuinka hyvin tunnette kaikki tuotantoverkkoonne kytkeytyvät laitteet mukaan lukien niissä käytetyt ohjelmistot versioineen?

Oletteko arvioineet kaikkien liiketoimintojenne kyberturvallisuusriskit?

Oletteko kartoittaneet mitkä ovat teidän liiketoimintanne jatkuvuuden kannalta kriittisimmät järjestelmät ja niiden rajapinnat?

- Milloin viimeisin kartoitus on tehty?

Oletteko suojanneet toimintanne ja kehittäneet tietoturvaan liittyviä ohjeita?

- Kuinka usein arvioitte ohjeiden päivitystarpeen ja päivitätte niitä?
- Oletteko selvittäneet millaisia uhkia ja tietoturvaloukkauksia on esiintynyt teidän toimialallanne sekä käyttämissänne järjestelmissä?
- Oletteko arvioineet, mitkä toimenpiteet parantaisivat teidän turvallisuustilannettanne?

Kyberturvallisuutta parantaviin toimenpiteisiin voi kuulua esimerkiksi

- automaatio-omaisuuden hallinnan kehittäminen,
- hankintojen kyberturvavaatimusten määrittäminen,
- operatiivisten kumppanien & ratkaisujen arviointi ja valinta,
- tietoliikenteen salaaminen ja jakaminen alueisiin,
- turvallisten etäyhteyksien hallinta, kontrolloitu käyttö ja seuranta,
- pääsyoikeuksien hallinta automaatioympäristöissä,
- jatkuvuuden ja toiminnan palauttamisen varmistaminen, sekä
- varautuminen häiriötilanteisiin ja niiden säännöllinen harjoittelu.

TUOTANNON KYBERTURVAN HALLINTAMALLIN SOVELTAMINEN

Tarkastuslista

Oletteko kehittäneet toimintamalleja uhka- ja häiriötilanteisiin ja harjoitelleet niitä?

- Sisältyykö häiriöihin varautumiseen ja harjoitteluun myös kyberturvallisuusnäkökulmat?
- Pidättekö kyberturvallisuuteen keskittyviä harjoituksia?
    - Oletteko hyödyntäneet esimerkiksi Traficomin Kyberturvallisuuskeskusta suunnitellessanne harjoituksianne?
    - Oletteko harjoitelleet tilanteita, joissa esimerkiksi etäyhteydet järjestelmätoimittajaan on katkaistava tietoturvauhan takia tai tuotannon palvelukumppani ei ole käytettävissä?
- Oletteko osallistuneet ulkopuolisten tahojen järjestämin kyberharjoituksiin?

Onko teillä kyky tunnistaa tietoturvaloukkauksia ja reagoida itse niihin?

- Analysoitteko lokitietoa tietoturvaloukkausten varalta?
- Analysoitteko verkkoliikennettä ja päätelaitteita tietoturvaloukkausten varalta?
- Kenelle ja miten työntekijät ilmoittavat epäilyttävistä yhteydenotoista?
- Miten olette järjestäneet lokien keräämisen ja turvallisen tallentamisen?

Onko teillä vakiintunut raportointikäytäntö häiriötilanteille sisältäen tietoturvaloukkaukset?

- Mille ryhmille raportoitte organisaation sisällä ja ulkopuolella? Johto, työntekijät, kumppanit, …?
- Miten yksityiskohtaista tietoa eri ryhmille raportoidaan?
- Miten jaatte raportit organisaation sisällä ja miten säilytätte ne turvallisesti?
- Miten (kuka) seuraatte muiden organisaatioiden tekemiä raportteja tietoturvatapahtumista jotka kohdistuvat samankaltaisiin järjestelmiin kuin teillä on käytössä tai samalle toimialalle?

Millainen kyvykkyys teidän organisaatiollanne on palauttaa toiminta normaaliksi tietoturvaloukkauksen tai häiriön jälkeen?

- Miten olette tallettaneet tiedot järjestelmien puhtaasta nykytilasta, mukaan lukien
    - tiedot tuotantolaitteista ja niiden ohjelmistoista versiotietoineen,
    - asennetut vikakorjaukset (*patch*),
    - tuotannon asetusarvot ja tuotantotiedot (erityisesti ympäristö- ja viranomaisraportointijärjestelmät), sekä
    - varmuuskopiot ja palautusjärjestelmät käyttöohjeineen?
- Oletteko harjoitelleet tai testaatteko säännöllisesti järjestelmien palauttamista ja palautumista?
- Oletteko dokumentoineet oikean palauttamisjärjestyksen?