# OT-järjestelmän kyberturvan tilannekuva

| Dokumentin tiedot | |
|---|---|
| Dokumentin nimi | OT-järjestelmän kyberturvan tilannekuva |
| Päivämäärä | 14.11.2026 |
| Versio | 01 |
| Muutokset | Ensimmäinen versio |



info@elpartner.fi

# SISÄLLYS


1 Palvelun tarkoitus ..... 3
2 Kohteen ja tarkastuksen rajaus ..... 4
3 Laitteiden tunnistaminen ja tietojen kerääminen ..... 5
4 Laitteiden kovennuksen tarkastus ..... 6
5 Tunnettujen haavoittuvuuksien selvittäminen ..... 7
6 Raportointi ja toimenpidesuositukset ..... 8
7 Toteutus ja asiakkaan osallistuminen ..... 9
8 Palvelun rajaukset ..... 10
9 Lisäpalvelut ..... 11





info@elpartner.fi

# 1 PALVELUN TARKOITUS

Palvelu antaa asiakkaalle dokumentoidun tilannekuvan OT-järjestelmän laitteista, niiden kyberturva-asetuksista ja tunnetuista haavoittuvuuksista. Tarkastuksessa tunnistetaan puutteet ja laaditaan priorisoidut toimenpidesuositukset niiden korjaamiseksi.

Verkon kartoitus ja skannaus toteutetaan OMICRON electronicsin StationGuard-sensorilla. Haavoittuvuuksien tunnistamisessa hyödynnetään StationGuard-järjestelmän haavoittuvuustietokantaa.

Palvelu soveltuu sähköasemien, voimalaitosten, energiavarastojen ja teollisuuden automaatiojärjestelmien tarkastamiseen. Se voidaan toteuttaa uuden järjestelmän käyttöönoton yhteydessä tai käytössä olevan järjestelmän määräaikaistarkastuksena.



info@elpartner.fi

# 2 KOHTEEN JA TARKASTUKSEN RAJAUS

Ennen toteutusta sovitaan tarkastettavat verkot, laitteet ja järjestelmät sekä käytettävät menetelmät. Samalla määritellään tarvittavat käyttöoikeudet, toteutusajankohta ja asiakkaan yhteyshenkilöt.

Lähtötietoina hyödynnetään saatavilla olevia verkkokaavioita, laiteluetteloita, konfiguraatioita sekä asiakkaan tietoturvavaatimuksia.



info@elpartner.fi

# 3 LAITTEIDEN TUNNISTAMINEN JA TIETOJEN KERÄÄMINEN

Kohteen verkon kartoitus ja skannaus tehdään StationGuard-sensorilla. Tiedonkeruussa hyödynnetään verkkoliikenteen passiivista havainnointia ja erikseen sovittuja aktiivisia kyselyjä. Tietoja täydennetään tarvittaessa laitteiden konfiguraatioista ja asiakkaan dokumentaatiosta.

Laitteista kerätään mahdollisuuksien mukaan:

- Valmistaja, malli ja laitetunnus sekä käyttötarkoitus ja sijainti järjestelmässä.
- IP- ja MAC-osoitteet sekä verkkosegmentti.
- Laiteohjelmiston, käyttöjärjestelmän ja sovellusten versiot.
- Käytössä olevat palvelut, protokollat ja hallintarajapinnat.
- Saatavilla olevat tiedot valmistajan tuesta ja elinkaaritilanteesta.

Tuloksena muodostetaan laiteluettelo. Puuttuvat tiedot ja tunnistamiseen liittyvät epävarmuudet merkitään näkyviin.



info@elpartner.fi

# 4 LAITTEIDEN KOVENNUKSEN TARKASTUS

Laitteiden asetukset tarkastetaan sovitussa laajuudessa valmistajan ohjeita, asiakkaan vaatimuksia ja kohteelle määriteltyä tarkastuslistaa vasten. Tarkastus perustuu asetusten ja konfiguraatioiden tarkasteluun sekä kartoituksessa saatuihin havaintoihin.

| Tarkastettava alue | Tarkastuksen sisältö |
|---|---|
| Käyttäjät ja käyttöoikeudet | Oletustunnusten hallinta, tarpeettomat tunnukset, henkilökohtaiset tunnukset ja roolikohtaiset oikeudet. |
| Tunnistautuminen | Salasanakäytännöt ja käytettävissä olevat vahvemman tunnistautumisen asetukset. |
| Palvelut ja protokollat | Tarpeettomien palvelujen poistaminen käytöstä ja protokollien suojausasetukset. |
| Hallinta ja etäkäyttö | Hallintayhteyksien suojaus, käyttörajaukset ja huoltoyhteyksien toteutus. |
| Portit ja rajapinnat | Käyttämättömien verkkoliitäntöjen ja muiden rajapintojen rajoitukset laitteen mahdollistamassa laajuudessa. |
| Lokitus ja aika | Tapahtumalokien, lokien siirron ja aikasynkronoinnin asetukset. |
| Ohjelmistot ja palautettavuus | Ohjelmistoversiot sekä tiedot konfiguraatioiden varmuuskopioinnista ja palautusmenettelyistä. |

Tarkastuksessa erotetaan asetuksilla korjattavat puutteet, laitteen tekniset rajoitteet ja erillistä järjestelmämuutosta edellyttävät havainnot.



info@elpartner.fi

# 5 TUNNETTUJEN HAAVOITTUVUUKSIEN SELVITTÄMINEN

Haavoittuvuuksien tunnistamiseen käytetään StationGuard-järjestelmän haavoittuvuustietokantaa. Tunnistettujen laitteiden ja ohjelmistoversioiden perusteella selvitetään tietokannassa tarkastushetkellä olevat, kohteeseen mahdollisesti soveltuvat tunnetut haavoittuvuudet.

Havaintojen soveltuvuus arvioidaan asiantuntijatyönä. Tarvittaessa tietoja täydennetään valmistajien tietoturvatiedotteista ja korjausohjeista. Havainnoista selvitetään mahdollisuuksien mukaan tunniste, kuvaus, tietolähde, kohteena olevat tuotteet ja versiot, hyväksikäytön edellytykset sekä saatavilla oleva korjaus tai muu riskiä pienentävä toimenpide.

Varmennetut haavoittuvuudet erotetaan mahdollisista osumista, joiden vahvistaminen edellyttää lisätietoja. Haavoittuvuuksia ei hyväksikäytetä tarkastuksen aikana.



info@elpartner.fi

# 6 RAPORTOINTI JA TOIMENPIDESUOSITUKSET

Asiakkaalle toimitetaan seuraavat tulokset:

- Johdon yhteenveto: keskeiset havainnot ja tärkeimmät kehitystarpeet.
- Laiteluettelo: tunnistetut laitteet, versiotiedot ja tiedonkeruun kattavuus.
- Kovennuksen tarkastusraportti: tarkastetut kohdat, havaitut puutteet ja tarkastamatta jääneet asiat.
- Haavoittuvuusluettelo: tunnistetut haavoittuvuudet, soveltuvuuden varmuus ja tietolähteet.
- Priorisoitu toimenpidelista: suositellut korjaukset ja ehdotettu kiireellisyys.

Priorisoinnissa huomioidaan teknisen vakavuuden lisäksi laitteen tehtävä, saavutettavuus verkosta, olemassa olevat suojaukset ja mahdollinen vaikutus prosessiin. Kiireellistä reagointia edellyttävistä havainnoista ilmoitetaan asiakkaan nimetylle yhteyshenkilölle jo tarkastuksen aikana.

Tulokset ja suositukset käydään läpi yhteisessä palautetilaisuudessa.



info@elpartner.fi

# 7 TOTEUTUS JA ASIAKKAAN OSALLISTUMINEN

Työ suunnitellaan OT-järjestelmän käytettävyyden ja prosessin toiminnan ehdoilla. Passiivista tiedonkeruuta käytetään ensisijaisesti silloin, kun sillä saadaan tarvittavat tiedot. Aktiiviset kyselyt ja skannaukset kohdistetaan vain ennalta sovittuihin laitteisiin sovituilla menetelmillä ja ajankohtina. Tarvittaessa ne toteutetaan huoltokatkon aikana.

Asiakas järjestää sovitut pääsyt ja käyttöoikeudet sekä nimeää henkilön, joka tuntee järjestelmän toiminnan. Kerättyjä tietoja käsitellään luottamuksellisesti. Tietojen toimitustavasta, säilytysajasta ja poistamisesta sovitaan ennen työn aloittamista.



info@elpartner.fi

# 8 PALVELUN RAJAUKSET

Peruspalvelu sisältää tarkastuksen, tiedonkeruun, analyysin ja raportoinnin. Asetusmuutokset, ohjelmistopäivitykset, haavoittuvuuksien korjaaminen, tunkeutumistestaus ja jatkuva valvonta sovitaan erikseen.

Tulos kuvaa sovitun tarkastuslaajuuden tilannetta tarkastusajankohtana. Haavoittuvuustarkastelun kattavuus riippuu laitteista saaduista tunnistetiedoista ja käytetyn haavoittuvuustietokannan sisällöstä. Raportissa esitetään käytetyt menetelmät ja kattavuuden rajoitukset.

Palvelu ei ole sertifiointi eikä sellaisenaan osoitus kaikkien lakisääteisten tai standardivaatimusten täyttymisestä.



info@elpartner.fi

# 9 LISÄPALVELUT

Peruspalvelun lisäksi asiakkaan kanssa voidaan sopia erikseen seuraavista lisäpalveluista:

- Havaittujen haavoittuvuuksien ja ongelmien korjaaminen
- Jatkuva haavoittuvuuksien hallinta: haavoittuvuuksien kartoitus ja raportointi neljä kertaa vuodessa.
- Jatkuva valvonta: OMICRON StationGuard -sensorin jatkuva valvonta



info@elpartner.fi