SOC-PALVELUN KÄYTTÖÖNOTON TARKASTUSLISTA

SOC-PALVELUN KÄYTTÖÖNOTON TARKASTUSLISTA

Ennen hankintapäätöstä selvitettäviä kysymyksiä

Mitä SOC-palvelulta halutaan?

- Havainnointia?
- Reagointia?
- Vai molempia?

Millaisia uhkia SOC-palvelun tulisi pystyä tunnistamaan?

- Miten SOC-palvelu integroidaan oman organisaation lokitietojen keräämiseen ja käytössä oleviin monitorointijärjestelmiin?
- Miten SOC-palvelu integroidaan omaan häiriöhallintaprosessiin?

Oletteko arvioineet, kenellä SOC-toimittajalla on paras osaaminen toimialastanne (kuten energian tuotanto ja jakelu) sekä parhaat työkalut uhkien tunnistamiseksi tällä toimialalla?

- Miten hyvin SOC-palveluntarjoaja ymmärtää asiakkaan ympäristöä?
    - Palvelukoe (*Proof-of-Concept*, POC) jossa testataan tunnistaako SOC-palveluntarjoaja asiakkaan verkkoon lisättyä (haitallista) aktiviteettia.
        - Usein tarvitaan ”opetteluvaihe”, jonka kuluessa palveluntarjoaja oppii mm. tunnistamaan väärät hälytykset.
- Miten arviointi on tehty? Kenen toimesta?

Mitkä organisaation järjestelmistä ovat kriittisimpiä ihmisten ja ympäristön turvallisuuden sekä taloudellisen toiminnan jatkuvuuden kannalta?

- Mitä organisaation järjestelmiä, rajapintoja ja verkkoja tulisi monitoroida?
- Mikä on monitoroinnin ja tuen saatavuus, 24/7?
- Miten, kuinka nopeasti ja kenelle toimitetaan ilmoitus SOC-palvelun tekemistä havainnoista?
    - Onko teillä oma kyvykkyys käsitellä havaintoja ja reagoida havaintoihin 24/7?
- Miten SOC-palvelu hyödyntää historiatietoa havaitakseen pitkän aikavälin muutoksia?

Mitä informaatiota SOC-palvelulle pitää välittää, jotta keskustelu oman organisaation asiantuntijoiden kanssa on mahdollisimman sujuvaa?

Mitä informaatiota SOC-palvelulle pitää välittää, jotta uhkien tunnistaminen toimisi mahdollisimman luotettavasti ilman suurta määrää vääriä positiivisia hälytyksiä? Toimitetaanko SOC-palvelulle tietoja esimerkiksi

- tuotanto-omaisuudesta ja niissä olevista haavoittuvuuksista,
- kulunvalvonnan keräämistä tiedoista,
- sallituista etäyhteyksistä, ja
- voimassa olevista muutostyöluvista järjestelmiin?

Miten hyvin viestintä SOC-palvelun kanssa toimii käytännössä?

- Kenen kanssa SOC-palvelu viestii?
- Onko SOC-palvelun asiantuntijoilla suora yhteys automaatio-organisaation asiantuntijoihin?

Miten hyvin SOC-palvelun tarjoama tuki sopii energiayrityksen tarpeisiin käytännössä?

- Mikä on SOC-palvelun tuottama lisäarvo suhteessa omaan monitorointiin ja häiriöhallintaan?