Verkkoanalyysi - darkSOC®

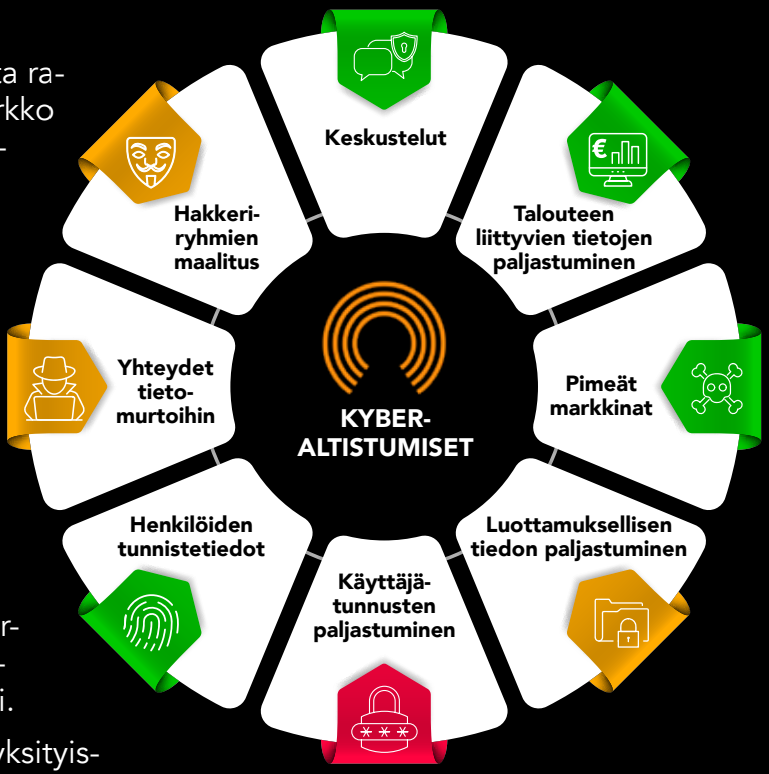
LÄHTÖTILANNEKARTOITUS

DarkSOC® pimeän ja syvän verkon analyysi

- DarkSOC® -analyysi selvittää organisaation profiilin ja altistumisen tason pimeässä ja syvässä verkossa.
- Dataa kerätään ympäri maailmaa sijaitsevilla palvelimilla taukoamatta 9 Gb sekunnissa.
- Analyysi voi paljastaa muun muassa organisaation kyberturvallisuuden puutteita, vuotaneita tietoja ja muita mahdollisia ongelmakohtia.
- Analyysin avulla tuotetaan näkemys siitä, miltä organisaatio näyttää kyberrikollisen ja vihamielisten toimijoiden silmin katsottuna.

Haavoittuvuuspinta-alan kartoitus

- Haavoittuvuuspinta-alan kartoituksessa analysoidaan kohteen verkkoinfrastruktuurin rakennetta ja sen verkon kyberturvallisuuden tilaa kuudessa eri riskitekijäryhmässä.
- Haavoittuvuuspinta-alan osalta raportoidaan, miltä kohteen verkko näyttää ulkopuolisen tarkastelijan silmissä ja se kokoaa yhteen organisaatioon liittyvät verkko-omaisuuden osat kuten palvelimet, avoimet portit, sovellukset ja verkkosivut.
- Luokittelemme kyberaltistumiset kahdeksaan havaintokategoriaan ja jaamme havainnot vakavuuden perusteella kolmeen tasoon.
- Keskeisimmät havainnot raportoidaan johdon yhteenvetoraportissa päätöksenteon tueksi.
- Raportti sisältää havaintojen yksityiskohtaisemman esittelyn sekä suositukset korjaavista toimista ja strategisen tason kehityskohteista.



MONITOROINTI

Lähtötilannekartoituksen pohjalta voidaan sopia syvän ja pimeän verkon monitoroinnista toimenpiteiden vaikuttavuuden selvittämiseksi ja uusien uhkien havaitsemiseksi. Monitoroinnissa havaittuja uusia löydöksiä tarkastellaan suhteessa aiempiin havaintoihin ja analysoidaan syitä havaintomäärien muutoksiin. Monitoroinnin tulokset raportoidaan sovituin väliajoin.

- Säännöllinen monitorointi: sovituin aikavälein toimitettava raportti, esimerkiksi kuukausittain, kvartaaleittain, puolivuosittain tai vuosittain.
- Jatkuva monitorointi: 24/7 seuranta uusista havainnoista, joista tieto suoraan asiakkaalle sekä kuukausittainen raportointi.

Toimitusketjujen turvallisuus

NIS2 HALLINTATOIMENPIDE

Toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt.

Analyysi voidaan tehdä valituille toimitusketjun organisaatioille (edellyttäen sopimusta). Havainnot jalkautetaan toimitusketjun organisaatioille, jotka vastaavat korjaavien toimenpiteiden suorittamisesta sekä raportoi tilaajalle, kun korjaavat toimenpiteet on tehty.

Palvelun sisältö esimerkiksi:

- Verkkoanalyysin esikartoitus toimitusketjun osille
- Verkkoanalyysi valituille toimitusketjun osille
- NIS2 käyttöönottokoulutus

Toimitusketjun kyberturvallisuuskäytäntöjen tarkastaminen lisää asiakasorganisaation omaa kyberkypsyyttä ja auttaa yritystä vastaamaan paremmin kyberturvallisuuslain vähimmäisvaatimuksiin. Mahdollistaa asiakkaalle esimerkiksi yritysostotilanteessa potentiaalisten yhteistyötahojen kybermaturiteettien selvittämisen ja riskiarvion tekemisen.

Cyberwatch Finland

Cyberwatch Oy | +358 40 500 8177
info@cyberwatchfinland.fi