

Digiturbe seire

Digiturbe seire on kuutasu põhine teenus, mis aitab leida IT-süsteemide nõrgad kohad enne, kui seda teevad ründajad.



Mida annab digiturbe seire

- ✓ Kaitseb mainet ja tulu: Regulaarne haavatavuste skaneerimine aitab ära hoida turvarikkumisi, mis võivad kahjustada usaldust ja tuua kaasa regulatiivseid trahve (NIS2)
- ✓ Toetab strateegilist riskijuhtimist: Pidev nähtavus turvaaukude osas annab võimaluse teha teadlikke otsuseid ja suunata ressursse vastavalt
- ✓ Tugevdab äritegevuse toimepidevust: Proaktiivne skaneerimine tagab vastavuse nõuetele ja tegevuse järjepidevuse, kaitstes ettevõtet üha kasvamas ja vaenulikumas küberkeskkonnas

Mis sisaldub kuutasulises teenuses

- ✓ Vähemalt korra kuus automatiseeritud turvanõrkuste sisest ja välist skaneerimist
- ✓ Igakuist automaatset raportit
- ✓ Korra kvartalis raporti tõlgendus ja soovitusi maandustegevusteks (kuni 3h turvaspetsialisti aega)
- ✓ Ligipääsu halduskeskkonda

Mis ei sisaldu teenuses

- ✓ Leitud turvanõrkuste kõrvaldamist
- ✓ Turvanõrkuste kõrvaldamine toimub lisatasu eest või edastame leiud IT halduspartnerie



Erinevus välise ja sisemise kontrolli vahel

Sisemine haavatavuste skaneerimine - Kontrollib süsteeme, rakendusi ja seadmeid ettevõtte sisevõrgus.

- ✓ **Eesmärk:** tuvastada nõrkused, mida võivad ära kasutada sisemised ohud või ründajad, kes on juba perimeetri kaitse ületanud.
- ✓ **Äriline väärtus:** vähendab riski, et ründajad liiguvad võrgus edasi ja kompromiteerivad andmeid, tagades vastavuse nõuetele ja kaitstes kriitilisi varasid.

Väline haavatavuste skaneerimine - Kontrollib internetiga ühendatud süsteeme, nagu veebilehed, tulemüürid ja pilveteenused.

- ✓ **Eesmärk:** avastada haavatavused, mida ründajad saavad kasutada väljastpoolt organisatsiooni.
- ✓ **Äriline väärtus:** kaitseb brändi mainet ja kliendi usaldust, vältides perimeetrist algavaid turvarikkumisi.

Mõlemad on hädavajalikud kihilise kaitse strateegias

- ✓ Välised skaneeringud kaitsevad avalikku kuvandit
- ✓ Sisemised skaneeringud kaitsevad aga ettevõtte tuuma
- ✓ Koos minimeerivad need finants-, regulatiivseid ja mainekahjusid.

Hinnastamine:

Regulaarne haavatavuse kontroll

Sise- ja välisvõrgu kuupõhine haavatavuse kontroll

Seadmete arv ja kuutasu

- ✓ Kuni 50 seadet — **150 € / kuus**
- ✓ Kuni 100 seadet — **250 € / kuus**
- ✓ Kuni 200 seadet — **375 € / kuus**
- ✓ Üle 200 seadme — **küsi pakkumist**

- ✓ Ühekordne seadistustasu — **500 €**
- ✓ Konsultatsioon — **90 € / tund**

Ühekordne haavatavuse kontroll

Sise- ja välisvõrgu haavatavuse ühekordne kontroll

- ✓ Kuni 3 tundi konsultatsiooni
- ✓ Ühekordne skaneerimine
- ✓ Ühekordne raport

Kuni 500 seadet — **1000 €**

Leitud turvanõrkuste kõrvaldamine ei sisaldu hinnas

Küsi pakkumist

primend.sales@primend.com

