primend

# Primend Shield

## Küberintsidentide jälgimise ja haldamise teenus

- **Hoia andmed turvatuna!**
- **Võta küberkurjategijad ja pahatahtlikud töötajad vastutusele!**
- **Taga vastavus küberturvalisuse nõuetega!**

Primend Shield on küberturvalisuse teenus, kus on integreeritud tsentraliseeritud turbelogimine, küberohtudele reageerimine ja küberturvalisuse konsultatsioonid.

Keskmine turvarikke avastamise tsükkel on 287 päeva (Blumira ja IBM, 2021). Rikkumise põhjused võivad olla nullpäeva turvanõrkus või paikamata süsteem, kuid sageli on rikkumine põhjustatud halvasti informeeritud kasutajast või volitatud kasutaja pahatahtlikust tegevusest. Vigadega seotud rikkumisi või otseseid rünnakuid saab kiiresti tuvastada ja tõrjuda automatiseeritud vastumeetmeega. Autoriseeritud töötaja pahatahtlikkust on keerulisem tuvastada ning on oluline, et rikkumist on võimalik faktiliselt kohtumenetlusel tõendada.

### Mis on Primend Shield?

Primend Shield teenuse tehniline lahendus sisaldab tsentraliseeritud turvateabe ja sündmuste haldamise süsteemi (SIEM). SIEM lahendus kogub turvasündmuste tõendeid serveritest, arvutitest, tulemüüridest ja muudest võrguseadmetest. Kogutud logisid säilitatakse vähemalt üks aasta mustrite tuvastamiseks, AI treenimiseks ja juriidiliseks tõendiks.

Automatiseeritud reageerimissüsteem, mis on treenitud tuvastama ründemustreid, reageerib koheselt avastatud pahatahtlikule tegevusele ja algatab eelnevalt määratletud tõrjestsenaariumid. SIEM-süsteem võimaldab integreerimist mis tahes võrgusüsteemiga.

Primend Shield meeskond analüüsib iga päev turvasündmuste logisid ja hooldusLogisid, et avastada uusi rünnakumustreid, mustrituvastusega avastamata süsteemide võimalikke rikkumisi ja süsteeme, mis on kaotanud ühenduse SIEM-süsteemiga. Kui Primendi tiim avastab uued ründemustrid, töötatakse välja tõrjestsenaarium, mis võimalusel rakendatakse automaatse toiminguna.

Microsoft Sentinel SIEM, mida Primend Shield teenus kasutab turvasündmuste kogumiseks ja analüüsimiseks, on Forresteri uuringute järgi turbeanalüüsi platvormide liider, millel on valdkonna parim innovatsiooniplaan, tooteturve, juhtumihaldus ja arhitektuur.

**Blumira ja IBMi 2021. aasta aruande kohaselt on rikkumise keskmine elutsükkel 287 päeva, organisatsioonidel kulub rikkumise esmaseks tuvastamiseks 212 päeva ja selle ohjeldamiseks 75 päeva.**

Näited sündmustest, mida Primend Shield SIEM-süsteem on treenitud tuvastama:

- Kasutaja kopeerib failiserverist ebanormaalse arvu faile (pahatahtlik töötaja)
- Loodud on uus privilegeeritud konto
- Tulemüüri skaneeritakse haavatavuste suhtes
- Viirus on tuvastatud mitmes arvutis
- Organisatsiooni on tabanud andmepüügirünnak
- Juurdepääs ettevõtte tundliku sisuga dokumentidele ebatavalisel ajal
- Kasutaja autentimine ja juurdepääs andmetele ebatavalistest asukohtadest

**Süsteemid ja teenused**

Serverid | Andmebaas | Microsoft 365 | Tulemüürid ja switchid | Arvutid ja telefonid

**Pilve-platvorm**

Sündmuste monitooring | Logide hoidla | Mustrite tuvastus | Automatiseeritud toimingud

**Sertifitseeritud spetsialistid**

Sündmuste monitooring | Kiirreageerimine | Audit ja analüüs | Aruandlus ja nõustamine


**Võta ühendust**

Joosep Truu |müügijuht

joosep.truu@primend.com


primend

bm certification ISO 9001 ISO 27001 System certification