primend

Drošības monitoringa pārvaldība

*Managed Security Monitoring

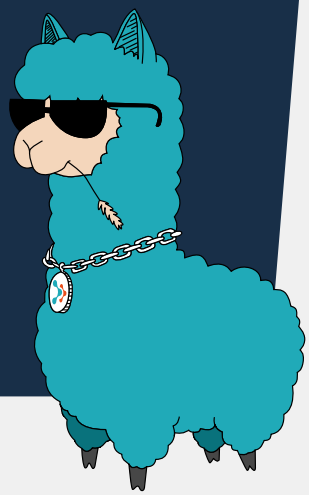
Drošības monitoringa pārvaldība ir abonēšanas pakalpojums, kas palīdz identificēt vājās vietas un riskus IT infrastruktūrā, pirms tos ļaunprātīgi izmanto kiberuzbrucēji.

Kāpēc drošības monitoringa pārvaldība ir svarīga

- **Aizsargā jūsu uzņēmuma reputāciju un finanses:** Regulāra risku pārbaude palīdz laicīgi novērst uzbrukumus. Tas ļauj saglabātu klientu uzticību un izvairīties no bargiem sodiem par drošības noteikumu (tostarp NIS2 direktīvas) neievērošanu.
- **Veic stratēģisko risku pārvaldību:** Nepārtraukta drošības nepilnību uzraudzība ļauj pieņemt datos balstītus lēmumus un precīzāk novirzīt drošībai paredzētos resursus.
- **Stiprina biznesa procesu nepārtrauktību:** Proaktīva risku noteikšana veicina atbilstību drošības standartiem un uzņēmuma darbības noturību, palīdzot aizsargāt jūsu biznesu mūsdienu sarežģītajā kibervidē.

Kas ir iekļauts ikmēneša pakalpojumā?

- Automatizēta iekšējo un ārējo risku identificēšana vismaz reizi mēnesī.
- Automatizēta ikmēneša atskaite par drošības stāvokli.
- Atskaites un rekomendācijas nepilnību novēršanai reizi (iekļauts drošības speciālista darbs līdz 3 stundām).
- Pieeja centralizētai pārvaldības un atskaišu sistēmai.



Kas nav iekļauts?

- Identificētie risku novēršana (to var iegādāties kā papildu pakalpojumu, vai arī konstatētie apdraudējumi var tikt nodoti jūsu uzņēmuma IT atbalsta sniedzējam).

Iekšējo un ārējo risku identificēšana

Iekšējo risku identificēšana - Tiek pārbaudītas sistēmas, lietotnes un ierīces uzņēmuma iekšējā tīklā.

- **Mērķis:** Identificēt vājās vietas, kuras varētu izmantot iekšējie lietotāji vai IT infrastruktūrā jau iekļuvuši kiberuzbrucēji.
- **Pievienotā vērtība biznesam:** Samazina risku, ka uzbrucējs var brīvi pārvietoties pa uzņēmuma tīklu, palīdz ievērot drošības noteikumus un pasargā svarīgākos datus un serverus.

Ārējo risku identificēšana - Tiek pārbaudītas internetam pieejamās sistēmas, piemēram, mājaslapas, ugunsmūri un mākoņpakalpojumi.

- **Mērķis:** Atklāt vājās vietas, kuras var izmantot, lai uzbruktu uzņēmumam no ārpuses.
- **Pievienotā vērtība biznesam:** Aizsargā zīmola reputāciju un klientu uzticību, novēršot ārējus uzbrukumus uzņēmuma IT sistēmām.

Kompleksā aizsardzības pieeja

Gan iekšējo, gan ārējo risku pārbaude ir kritiski svarīgi elementi kopējā drošības stratēģijā:

- Ārējās pārbaudes aizsargā uzņēmuma publiski pieejamos resursus.
- Iekšējās pārbaudes aizsargā uzņēmuma biznesa pamatus (svarīgākos datus un procesus).
- Abu līmeņu pārbaudes minimizē finansiālos, juridiskos un reputācijas riskus.

Cenas

Regulāra risku identificēšana

Ikmēneša iekšējo + ārējo risku identificēšana

Ierīču skaits un ikmēneša norēķini

- Līdz 50 ierīcēm — **150€ / mēnesī**
- Līdz 100 ierīcēm — **250€ / mēnesī**
- Līdz 200 ierīcēm — **375€ / mēnesī**
- Vairāk nekā 200 ierīces — **cena pēc vienošanās**

- Vienreizēja uzstādīšanas maksa — **500€**
- Drošības konsultācija — **90€ / stundā**

Vienreizēja risku identificēšana

Vienreizēja iekšējo + ārējo risku identificēšana

- Drošības konsultācija (ilgums 3h)
- Vienreizēja pārbaude
- Vienreizēja atskaite

Līdz **500** ierīcēm — **1000€**

Nav iekļauta identificēto risku novēršana

Pieprasīt cenu piedāvājumu

primend.sales@primend.com

primend

bm certification ISO 9001 ISO 27001 System certification