primend

Primend Shield

Kiberincidentu uzraudzības un pārvaldības pakalpojums

- **Rūpējies par sava uzņēmuma datu drošību!**
- **Pēdējais laiks saukt pie atbildības kibernoziedzniekus un ļaunprātīgu nodomu vadītus darbiniekus!**
- **Nodrošini atbilstību kiberdrošības standartiem!**

Primend Shield kiberdrošības pakalpojums ietver centralizētu drošības reģistru, operatīvu reaģēšanu kiberdraudu gadījumā, kā arī konsultācijas par kiberdrošību.

Vidējais kiberuzbrukumu dzīves cikls ir 287 dienas (Blumira un IBM, 2021). Incidenta iemesls var būt sistēmas kļūda, ko nav iespējams uzreiz novērst, tomēr bieži vien to izraisa nepietiekami izglītots lietotājs vai arī konkrēta lietotāja ļaunprātīga darbība. Sistēmas kļūmju izraisītas datu noplūdes vai tiešus uzbrukumus var ļoti operatīvi atklāt un neitralizēt, izmantojot automatizētus pretaizsardzības pasākumus. Ļaunprātīgi veiktus uzbrukumus atklāt ir sarežģītāk, turklāt tiem ir nepieciešami pierādījumi tiesvedības uzsākšanai.

Kas ir Primend Shield?

Primend Shield centralizētā drošības informācijas un aktivitāšu pārvaldības (SIEM) sistēma apkopo pierādījumus par aktivitātēm no serveriem, datoriem, ugunsmūriem un citām tīklā pieslēgtām ierīcēm. Apkopotie drošības datu reģistri tiek uzglabāti vismaz vienu gadu, ar mērķi vajadzības gadījumā izmantot tos atkārtotu rīcības modeļu atpazīšanai, izlūkošanas apmācībai un kā juridiskos pierādījumus.

Automātiskā reaģēšanas sistēma, kas ar MI palīdzību apmācīta pēc noteiktiem modeļiem, ir izstrādāta, lai nekavējoties reaģētu uz identificētām ļaunprātīgām darbībām un aktivizētu specifiskus seku novēršanas scenārijus. Šo sistēmu iespējams integrēt jebkurā tīkla sistēmā.

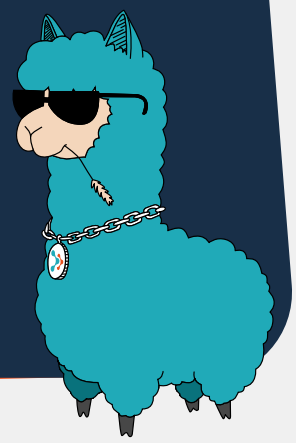
Primend Shield komandas audits katru dienu pārskata aizsardzības aktivitāšu reģistrus un apkopes reģistrus, lai identificētu jaunus uzbrukumu modeļus, atklātu potenciālus sistēmas pārkāpumus, kas ir ārpus esošo modeļu spektra, kā arī noteiktu sistēmas, kam zudis savienojums ar SIEM sistēmu. Atklājot jaunus pārkāpumu modeļus, tiek nodefinētas attiecīgas veicamās reakcijas un apstiprināti atbilstoši seku mazināšanas un novēršanas scenāriji.

Primend Shield pakalpojums izmanto Microsoft Sentinel SIEM, lai apkopotu un analizētu drošības aktivitātes. IT pētniecības uzņēmums Forrester to ir atzinis par nozares līderi drošības analītikas platformu vidū, augstu vērtējot gan ieviestās inovācijas, gan produktu drošību, gan problēmsituāciju pārvaldību, gan tās arhitektūru.

Saskaņā ar Blumira un IBM 2021. gada ziņojumu, vidējais kiberincidentu dzīves cikls uzņēmumos aizņem 287 dienas, patērējot 212 dienas problēmas identificēšanai un 75 dienas draudu ierobežošanai un novēršanai.

Primend Shield SIEM sistēma ir apmācīta automātiski identificēt šādus gadījumus:

- Lietotājs pārkopējis neierasti daudz dokumentu no servera (ļaunprātīgu nodomu vadīts darbinieks)
- Ir izveidots jauns konts ar priviliģētu pieeju
- Ticis pārbaudīts ugunsmūris, lai noteiktu ievainojamības līmeni
- Vairākos datoros ir atklāts vīruss
- Uzņēmumu skāris pikšķerēšanas uzbrukums
- Notikusi piekļuve sensitīviem uzņēmuma datiem neierastā laikā
- Veikta lietotāju autentifikācija un piekļuve datiem no aizdomīgām atrašanās vietām



Sistēma un pakalpojumi

Serveri

Datu bāze

Microsoft 365

Ugunsmūri un komutatori

Datori un tālruņi

Mākoņu platforma

Aktivitāšu uzraudzība

Reģistru krātuve

Atkārtotu darbību identificēšana

Automatizētās darbības

Sertificēti speciālisti

Aktivitāšu uzraudzība

Ātrā reaģēšana

Audits un analīze

Atskaites un konsultācijas

Sazinies ar mums
Dace Rostoka | IT biznesa konsultante
dace.rostoka@primend.com

primend

bm certification
ISO 9001
ISO 27001
System certification