primend

“Primend Shield”

Kibernetinių incidentų stebėjimo ir valdymo paslauga

- **Saugokite savo duomenis!**
- **Priverskite kibernetinius nusikaltėlius ir pakenkti norinčius darbuotojus atsakyti už savo veiksmus!**
- **Užsitikrinkite atitiktį kibernetinio saugumo teisės aktams!**

„Primend Shield“ tai valdoma kibernetinio saugumo paslauga, kuri apima centralizuotą saugumo registrą, reagavimą į kibernetines grėsmes ir kibernetinio saugumo konsultacijas.

Vidutinis pažeidimo gyvavimo ciklas – 287 dienos („Blumira“ ir IBM, 2021 m.). Pažeidimo priežastys gali būti nulinės dienos klaida, apie kurią jūs dar nieko nežinote (angl. zero-day bug) arba nepataisyta sistema, tačiau dažnai pažeidimą sukelia neinformuotas vartotojas arba piktybiški įgalioto vartotojo veiksmai. Su klaidomis susijusius pažeidimus arba tiesiogines atakas galima greitai aptikti ir suvaldyti taikant automatines atsakomąsias priemones. Sunku aptikti piktybinius pažeidimus, todėl reikia įrodymų, kad būtų galima imtis teisinių veiksmų.

Kas yra „Primend Shield“ paslauga?

Centralizuota „Primend Shield“ saugumo informacijos ir įvykių valdymo sistema (angl. Security Information and Event Management, SIEM) renka saugumo įvykių įrodymus iš serverių, kompiuterių, ugniasienių ir kitų tinklo įrenginių. Surinkti įrašai saugomi bent vienerius metus, kad būtų galima atpažinti modelius, mokytis ir naudoti kaip teisinius įrodymus.

Automatizuota reagavimo sistema, apmokyta pagal atpažintus modelius, iš karto reaguoja į aptiktą kenkėjišką veiklą ir inicijuoja iš anksto nustatytus poveikio mažinimo scenarijus. SIEM sistemą galima integruoti su bet kuria tinklo sistema.

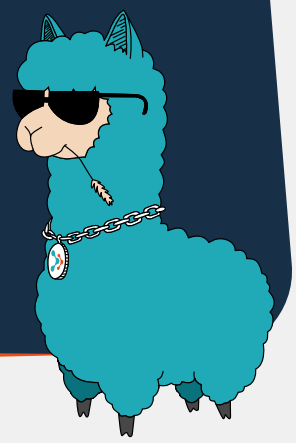
„Primend Shield Team“ kasdien tikrina saugos įvykių ir techninės priežiūros žurnalus, kad nustatytų naujus atakų modelius, galimus sistemų pažeidimus, kurių neaptiko modelio atpažinimo sistema, ir sistemas, kurioms nutrūko ryšys su SIEM. Kai aptinkami, apibrėžiami nauji modeliai ir atsakymai, patvirtinami jų grėsmės mažinimo scenarijai.

Bendrovės „Microsoft Sentinel SIEM“, kurią „Primend Shield“ paslauga naudoja saugumo įvykiams rinkti ir analizuoti, yra pripažinta geriausia rinkoje. Tyrimų ir konsultacijų bendrovė „Forrester“ pripažino, kad tai saugumo analizės platforma, kurios inovacijų planas, produkto saugumas, atvejų valdymas ir architektūra yra geriausi rinkoje.

Remiantis 2021 m. „Blumira“ ir IBM ataskaita, vidutinis pažeidimo gyvavimo ciklas trunka 287 dienas, iš kurių 212 dienų organizacijoms užtrunka aptikti pažeidimą, o 75 dienas – jį suvaldyti.

Įvykių, kuriuos „Primend Shield SIEM“ sistema išmokyta aptikti, pavyzdžiai:

- vartotojas kopijuoja neįprastai daug failų iš serverio (piktybinis darbuotojas);
- sukurta nauja privilegijuota paskyra;
- užkarda tikrinama, ar nėra pažeidžiamų vietų;
- keliuose kompiuteriuose aptiktas virusas;
- organizacija tapo sukčiavimo atakos taikiniu;
- prieiga prie konfidencialių įmonės dokumentų neįprastu metu;
- vartotojo autentifikavimas ir prieiga prie duomenų iš neįprastų vietų.



Sistema ir paslaugos

- Serveriai
- Duomenų bazė
- Microsoft 365
- Ugniasienės ir jungikliai
- Kompiuteriai ir telefonai

Debesų platforma

- Įvykių stebėjimas
- Žurnalo saugykla
- Šablonų atpažinimas
- Automatizuoti veiksmai

Sertifikuoti specialistai

- Įvykių stebėjimas
- Greitas reagavimas
- Auditas ir analizė
- Ataskaitų teikimas ir konsultacijos

Susisiekite su mumis

Tadas Jankauskas | Pardavimo vadovas

tadas.jankauskas@primend.com

primend

bm certification

ISO 9001
ISO 27001
System certification