SECURITY DAYS

PRIVILEGIJUOTŲ PASKYRŲ VALDYMAS IR SAUGUMO RIZIKŲ MAŽINIMAS SU PAM ĮRANKIU

Gediminas Mikelionis - Baltimax kibernetinio saugumo inžinierius, ESET ekspertas

Rugsėjo 5 d. 2024

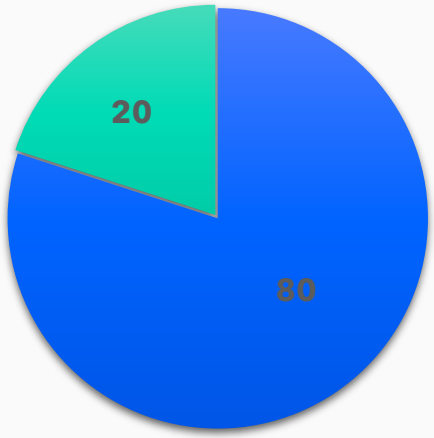
KIBERNETINIO SAUGUMO KONFERENCIJA

esd.eset.lt

13

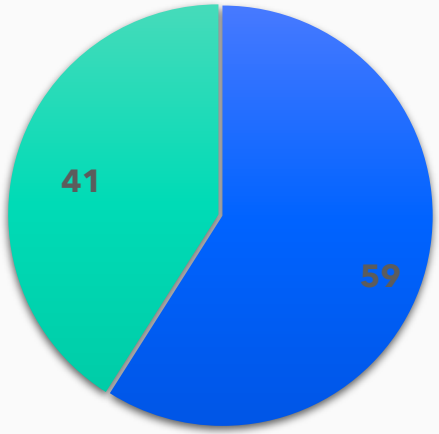
Panaudoti slaptažodžiai

Vartotojai tą patį slaptažodį naudoja vidutiniškai 13 kartų



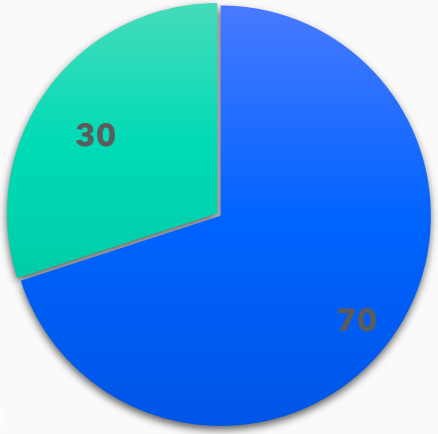
Įsilaužimai

Sėkmingi įsilaužimai fiksuojami dėl slaptažodžių pažeidimų



Slaptažodžių kūrimas

Vartotojų slaptažodžiai yra glaudžiai susiję su jų aplinka



Saugumo pažeidimai

IT specialistų patyrė duomenų saugumo pažeidimus dėl silpnų slaptažodžių

BALTIMAX

Tinklo skenavimas

Automatinis parinkimas

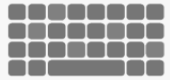
Slaptažodžių el. bylos

Slaptažodžių knygutė

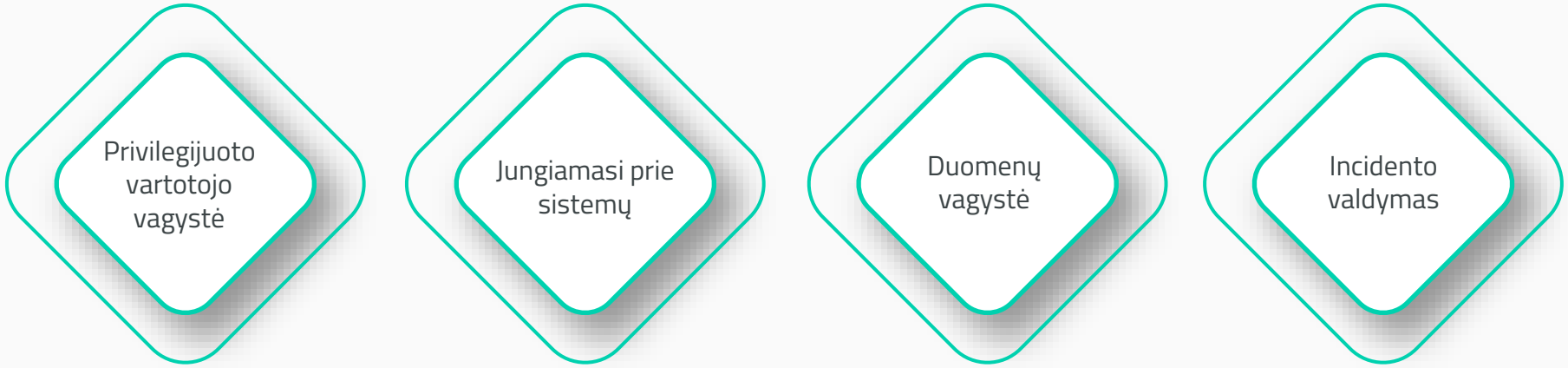
Artimas stebėjimas

Socialinė inžinerija

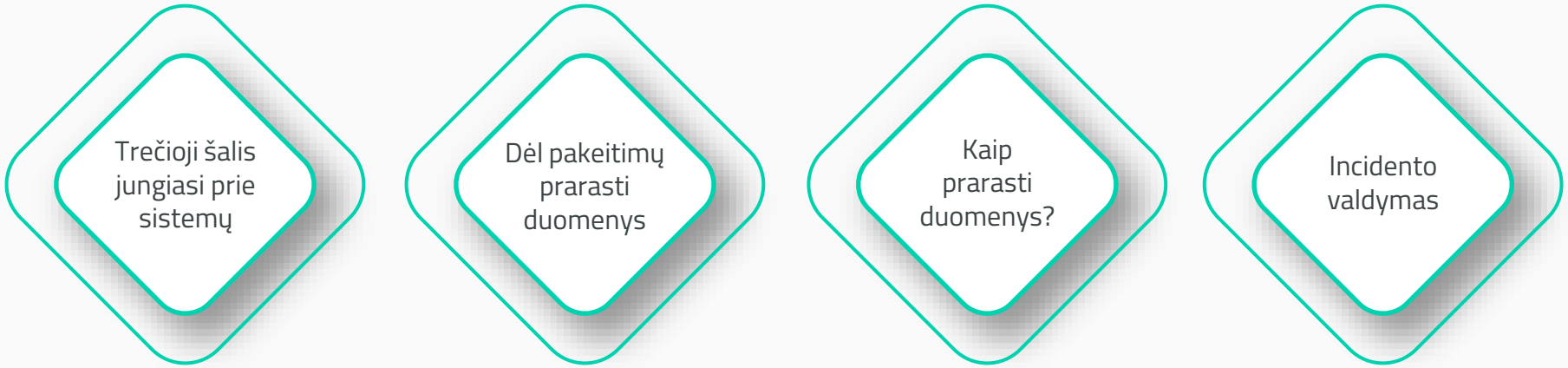
Atspėti slaptažodžiai



Paspaudimų fiksavimas


Privilegijuoto vartotojo vagystė
Jungiamasi prie sistemų
Duomenų vagystė
Incidento valdymas

BALTIMAX


Trečioji šalis jungiasi prie sistemų
Dėl pakeitimų prarasti duomenys
Kaip prarasti duomenys?
Incidento valdymas

BALTIMAX

Privilegijuotų vartotojų administravimas (PAM)

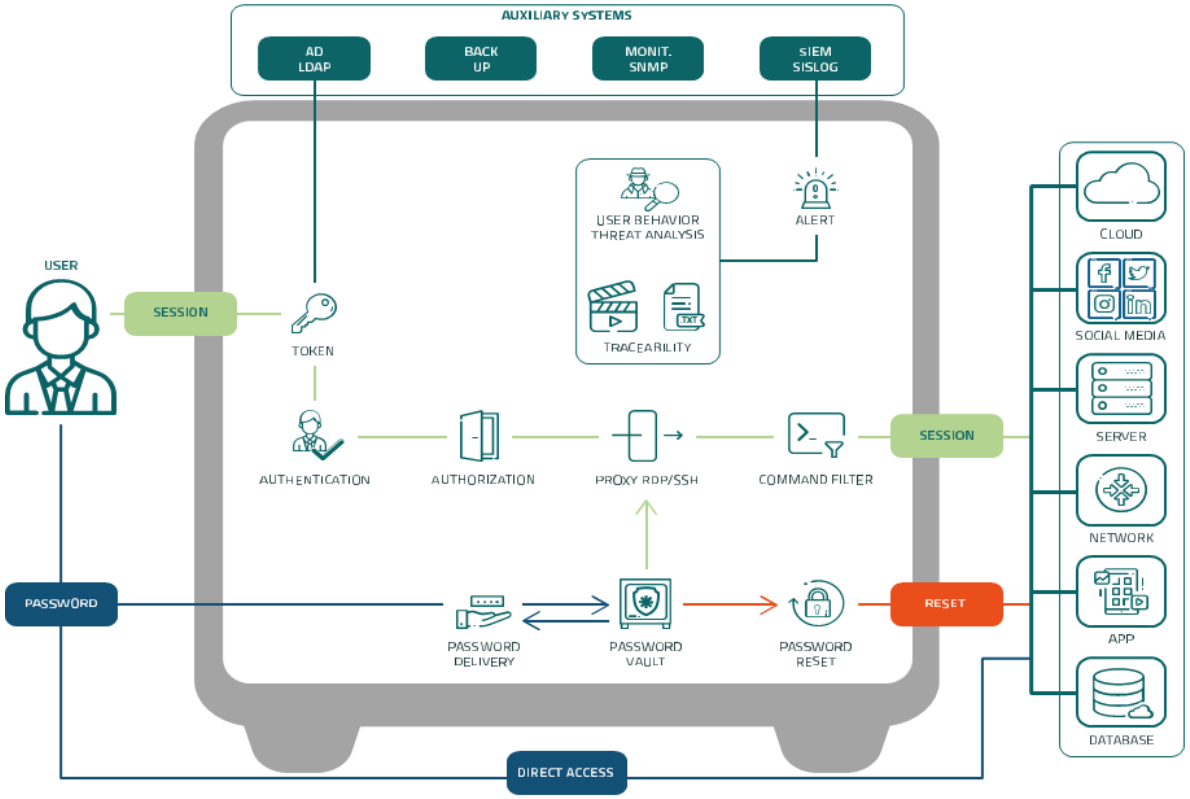
Prieigos valdymas:
- Įmonės tinklo administratoriai,
- Trečiųjų šalių specialistai,
- Kiti vartotojai.

Teisių valdymas:
- resursų priskyrimas (vidinių ir išorinių resursų, aplikacijų ar interneto svetainių, Windows, Linux sistemų, tinklo įrenginių),
- Veiksmų plano valdymas,
- Laiko tinklelio valdymas.

Sesijų valdymas:
- Sesijų loginimas,
- Sesijų įrašymas,
- Paieška sesijų įrašų archyvuose pagal kriterijus.

Slaptažodžių valdymas:
- Kūrimas (generavimas),
- Saugojimas,
- Administravimas.

Kaip tai veikia?



Problema

Kas kontroliuoja administratoriaus veiksmus? Tarkim, jei administratorius netikėtai išėjo iš darbo, ar įmonėje dar kažkas be jo turi prisijungimus prie sistemų?

Sprendimas

Atraskite ir centralizuokite visus privilegijuotus kredencialus, vartotojus ir sukurkite tvirtą autentifikavimą, įgaliojimą ir atskaitomybę už jo naudojimą.

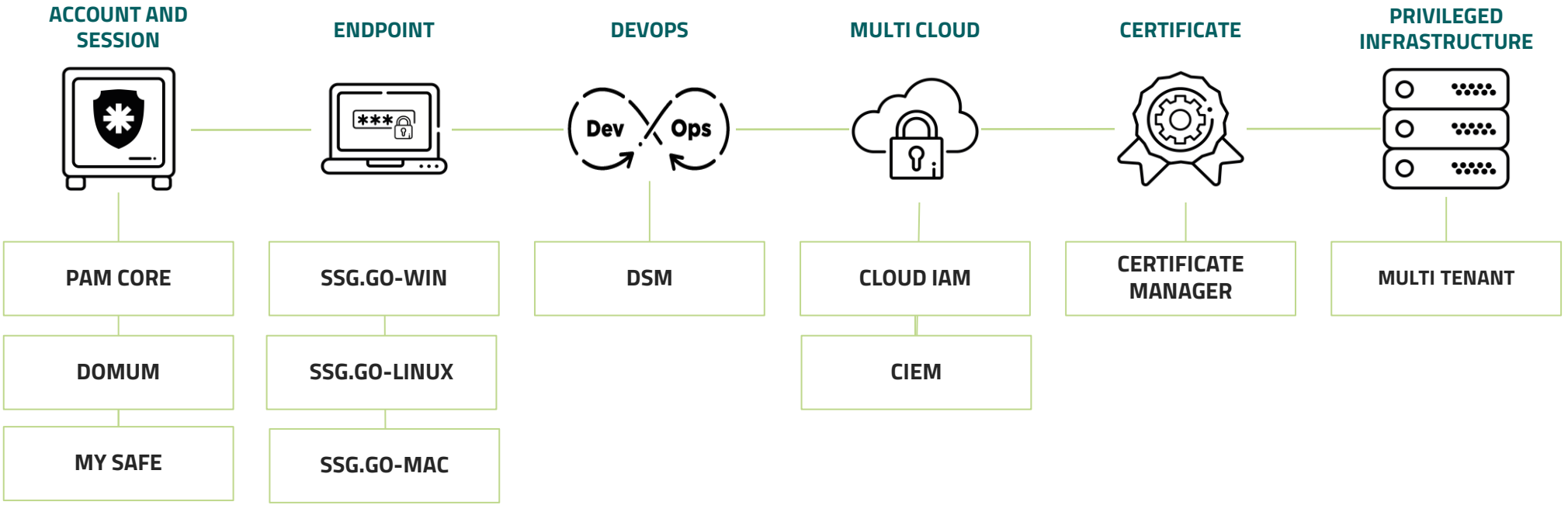
PAM leidžia saugoti slaptažodžius ir perduoti kitiems administratoriams.

Poveikis

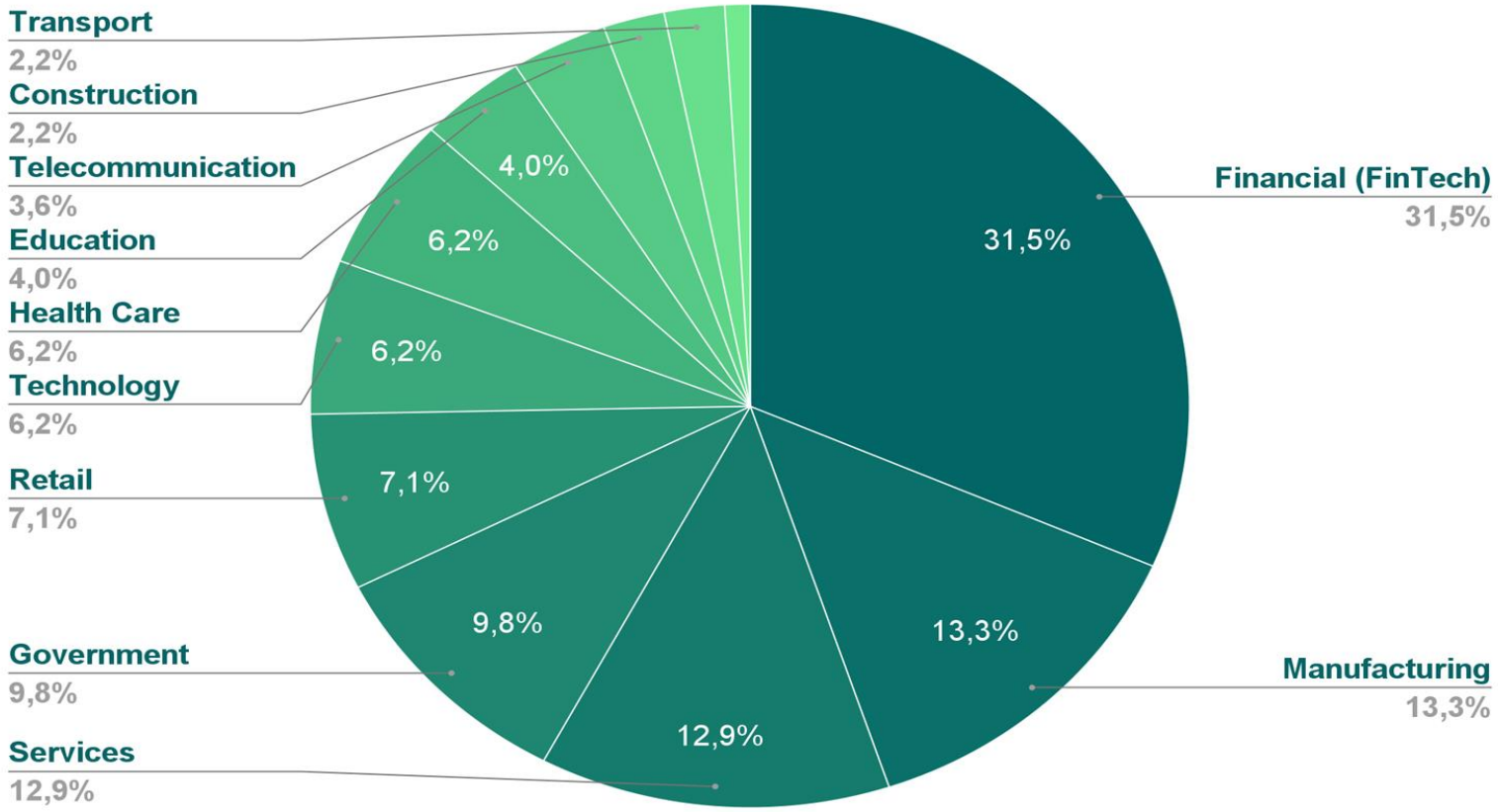
Sumažinkite atakos riziką pašalindami nereikalingus kredencialus.

BALTIMAX

Papildomi PAM moduliai



Sektoriai


Transport
2,2%
Construction
2,2%
Telecommunication
3,6%
Education
4,0%
Health Care
6,2%
Technology
6,2%
Retail
7,1%
Government
9,8%
Services
12,9%
Financial (FinTech)
31,5%
Manufacturing
13,3%
31,5%
13,3%
12,9%
9,8%
7,1%
6,2%
6,2%
4,0%

TIS2 ir PAM

BALTIMAX

(49) Kibernetinės higienos politikos

Sukurti ir įgyvendinti tvirtą kibernetinės higienos politiką, kuri apimtų kruopštų slaptažodžių valdymą, administravimo paskyrų priežiūrą ir griežtą prieigos apribojimus.

Senhasegura yra specialiai sukurta siekiant apsaugoti ir valdyti administravimo paskyras ir įgaliojimus, apima patikimą slaptažodžių valdymą ir griežtą prieigos teisių kontrolę.

(53) Skaitmenizuotos komunalinės paslaugos

Sustiprinti kibernetinio saugumo apsaugą vis labiau tarpusavyje susijusius ir skaitmenizuotos komunalinės paslaugos, pvz . transporto, vandens tiekimo ir energetikos paslaugos, taip pat išmaniosios miestų sistemos, siekiant apsisaugoti nuo kibernetinių grėsmių.

Senhasegura apsaugo skaitmenines komunalines paslaugas ir išmaniųjų miestų infrastruktūrą izoliuojant sesijas, saugiai saugant įgaliojimus ir naudojant ‚just-in-time' prieigą, kad būtų sumažinta neautorizuota prieiga. „Senhasegura GO" padidina saugumą panaikindama nuolatines administratoriaus privilegijas ir stebėdama programų elgesį, kad būtų užtikrinta atitiktis saugumo politikai.

(54) Apsauga nuo Ransomware

Apsaugoti pagrindinę infrastruktūrą nuo išpirkos reikalaujančios programinės įrangos atakų, diegdami proaktyvias saugumo priemones ir patikimas gynybos mechanizmus.

Senhasegura sumažina kibernetinio saugumo riziką, nes izoliuoja, stebi, įrašinėja ir audituoja privilegijuotas sesijas, užkirsdama kelią privilegijų padidėjimui. Senhasegura GO kovoja su ransomware panaikindama administratoriaus privilegijas ir reguliuodama programų elgseną. Senhasegura PAM dar labiau sustiprina apsaugą tokiomis funkcijomis kaip prieigos kontrolė, stebėjimas realiuoju laiku, saugus slaptažodžių valdymas, 2FA ir sesijų įrašymas. Šios galimybės padeda organizacijoms sumažinti išpirkos reikalaujančių programų riziką ir apsaugoti svarbią infrastruktūrą bei duomenis.

(85) Rizika, kylanti iš ūkio subjekto tiekimo grandinės

Šalinti saugumo spragas tiekimo grandinėje atliekant rizikos vertinimą ir stiprinti saugumo protokolus visuose tiekimo tinklo lygmenyse.

„Senhasegura“ teikia išsamius tiekimo grandinės saugumo sprendimus, siūlydama saugią, tik laiku atliekamą nuotolinę prieigą ir sesijų įrašymą išorės tiekėjams per ‚Senhasegura Domum‘, užtikrindama mažiausios privilegijos principą ir suteikdama galimybę atlikti išsamų auditą. „Senhasegura DevOps Secret Manager“ valdo ir kontroliuoja slaptus duomenis, tokius kaip slaptažodžiai ir raktai, DevOps aplinkoje, užtikrindama saugų programinės įrangos tiekimo grandinės valdymą

(89) Kibernetinės higienos praktika

Įdiegti kibernetinės higienos praktiką, įskaitant „nulinio pasitikėjimo“ (angl. Zero Trust) architektūrą ir veiksmingą tapatybės nustatymą.

„Senhasegura“ privilegijuotos prieigos valdymo (PAM) platforma stiprina kibernetinį saugumą, nes saugiai valdo bendruosius ir privilegijuotus įgaliojimus, užtikrina jų saugų saugojimą, atskyrimą ir atsekamumą. Ji integruota į „nulinio pasitikėjimo“ saugumo modelį, užtikrinantį griežtą prieigos kontrolę, reikalaujančią nuolatinio patikrinimo, laikantis principo „niekada nepasitikėk, visada tikrink“. Be to, ji sustiprina tapatybės patikrinimą taikant daugiafaktorinį autentiškumo patvirtinimą (MFA), dar labiau suderintą su „Zero Trust“ principais.

(98) Viešieji elektroninių ryšių tinklai ir viešai prieinamos elektroninės ryšių paslaugos

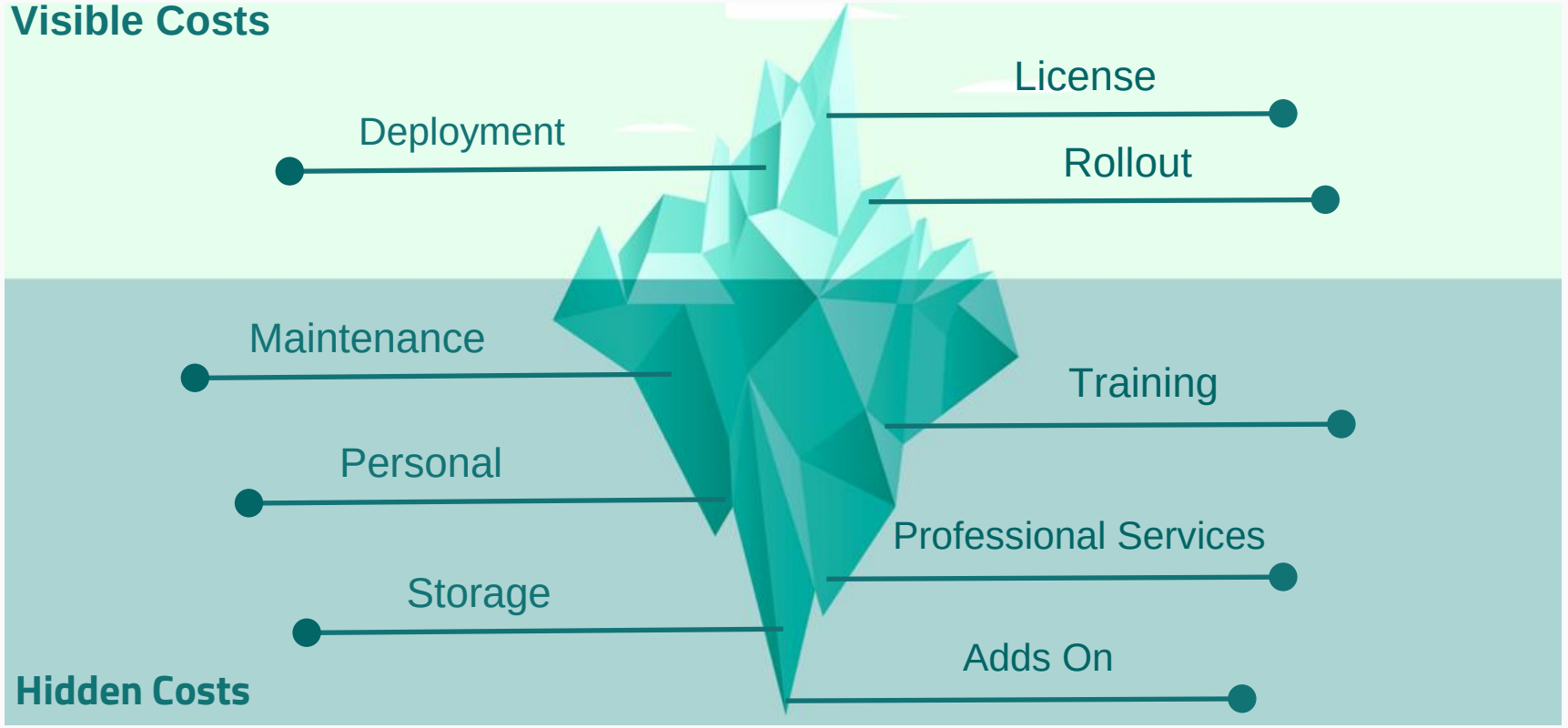
Įgyvendinti visapusišką šifravimą nuo galo iki galo ir užtikrinti į duomenis orientuotą saugumą. Kriptografijos strategijas, segmentavimą, žymėjimą ir sudėtingų priemonių kūrimą. Prieigos politiką ir valdymą. Automatinio valdymo sistemas. sprendimų dėl prieigos priėmimo.

Senhasegura įgyvendina pažangias saugumo priemones, naudodama aukščiausio lygio šifravimą duomenims apsaugoti, izoliuoja naudotojų sesijas, kad būtų išvengta neleistinos prieigos, ir automatizuoja prieigos valdymą, realiuoju laiku koreguodama pagal riziką. Šios funkcijos užtikrina nuoseklią duomenų apsaugą ir kontrolę visose skaitmeninėse aplinkose.

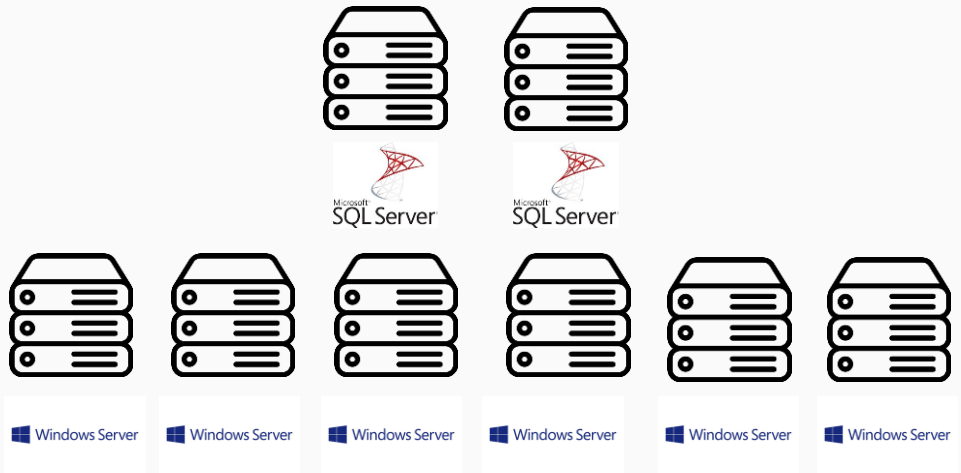
(102) Išankstinis perspėjimas ir pranešimas apie incidentus

Įpareigoti, kad ypatingos svarbos infrastruktūros subjektams nedelsiant pranešti apie bet kokius saugumo incidentus per 24 valandas, palengvinti greitą reagavimą ir sušvelninti padarinius.

Senhasegura didina saugumą automatiškai analizuodama kritinius veiksmus ir stebėdama aplinką, ar nėra įtartinų veiksmų, susijusių su privilegijuotais įgaliojimais. Ji akimirksniu įspėja saugumo komandas, todėl galima greitai reaguoti ir automatiškai blokuoti grėsmes. Pagrindinės funkcijos - išsamūs įspėjimai, sesijų analizė, komandų blokavimas ir integracija su SIEM/SYSLOG sistemomis, kuriomis siekiama veiksmingai užkirsti kelią saugumo incidentams ir juos aptikti.


Visible Costs
License
Deployment
Rollout
Maintenance
Training
Personal
Professional Services
Storage
Adds On
Hidden Costs

Kiti gamintojai (WINDOWS) vs. SENHASEGURA (LINUX) architektūros sandara



= $$$$$$$$

= $$

gediminas@baltimax.com