Kibernetinis saugumas – ar suprantame, kas yra mūsų priešas?

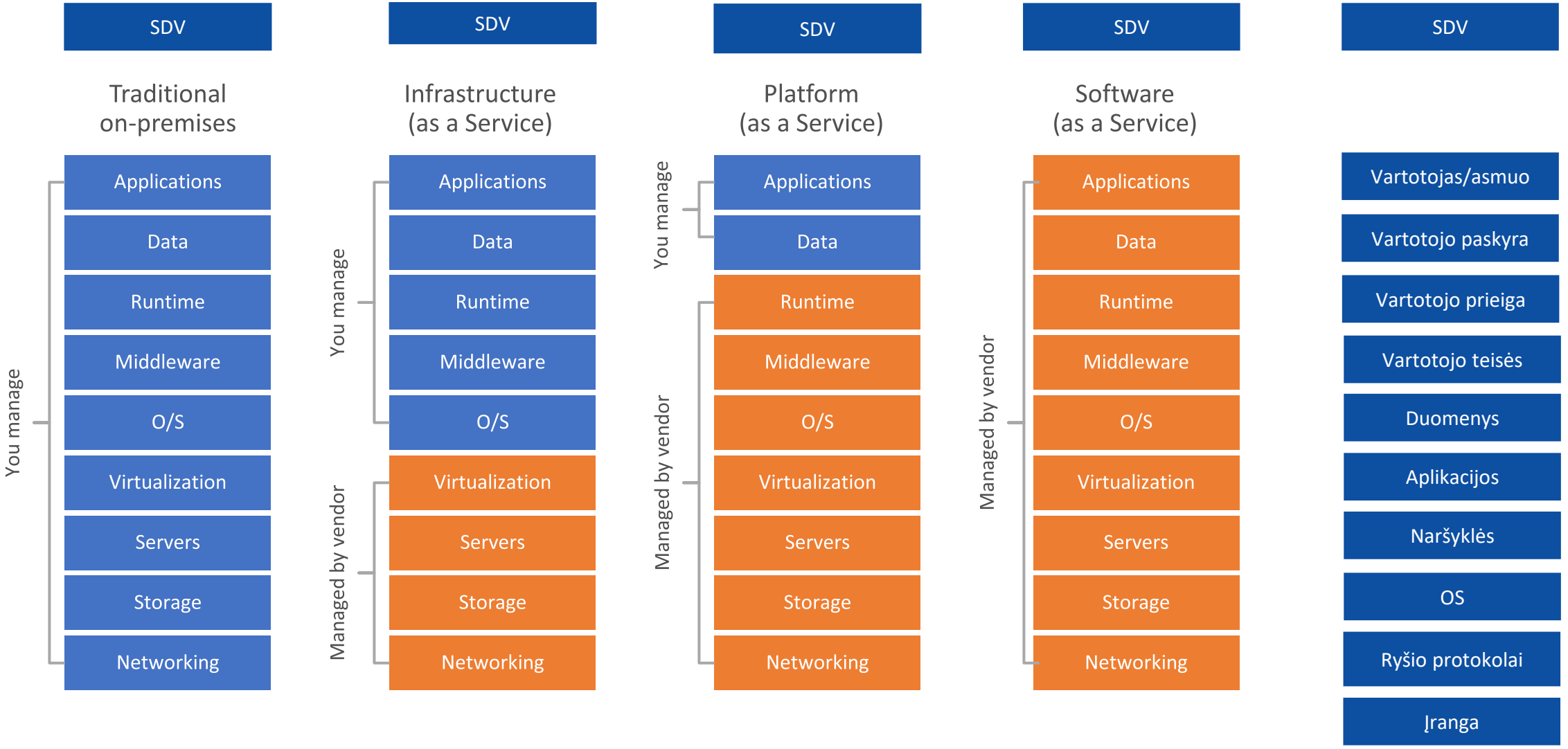
Rimas Kareiva
Skaitmeninių darbo vietų kompetencijų centras
Grupės vadovas

Pagrindinės žinutės

Jūsų skaitmeninės darbo vietos nėra saugios

Šiandien puiki diena imtis naujų priemonių

Skaitmeninė darbo vieta



Naujos priemonės

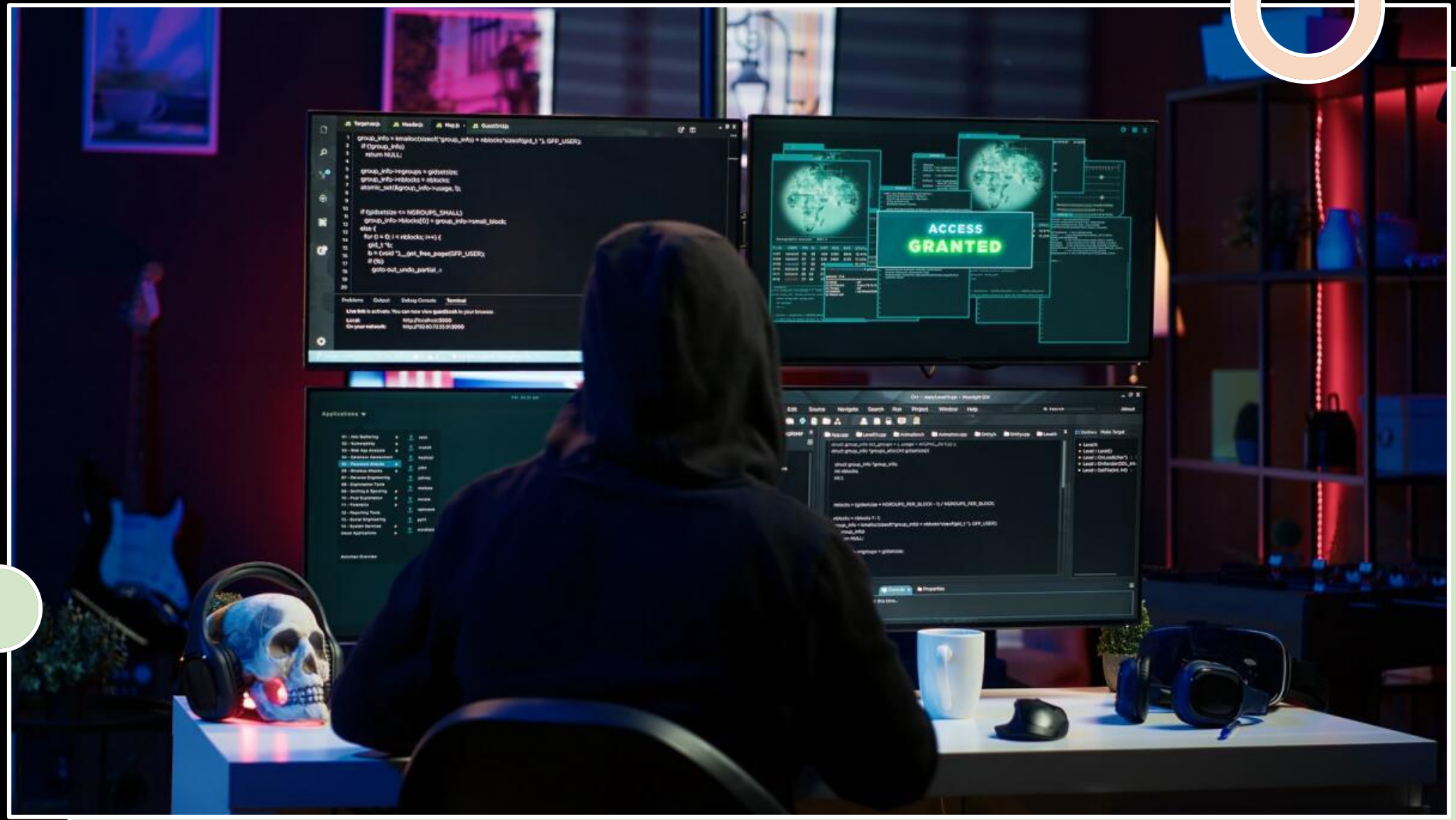
- Darbo vietų saugumo prioriteto kėlimas
- Bazinės darbo vietų higienos nuolatinė kontrolė:
  - kelių lygių autentifikacija (angl. *MFA*)
  - atnaujinta aparatinė ir programinė įranga
  - standartizavimas visais įmanomais lygiais
  - prieigos teisių periodinė patikra
  - vartotojų edukacija
- UEM (angl. *unified endpoint management*) naudojimas
- Saugumo reikalavimų darbo vietų įrangos tiekėjams didinimas

Šios dienos žinutės

Jūsų skaitmeninės darbo vietos vis dar nėra saugios

Žinokite kibernetinio saugumo „priešus“

Šiandien puiki diena imtis naujų priemonių


ACCESS
GRANTED

Kibernetinio saugumo „priešai“

- Veiklos tvarumo ir tęstinumo požiūriu:
  - kibernetiniai nusikaltėliai - „hacker‘iai“ - „dark web‘as“ ir pan.
  - naujų technologijų sparti plėtra
- Nacionalinio saugumo požiūriu:
  - Rusija, Kinija ir jų remiamos grupuotės
- LR Kibernetinio saugumo įstatymo požiūriu:
  - įstatymo ir TIS 2 direktyvos reikalavimų nevykdantys subjektai
- Viešojo sektoriaus paslaugų gavėjų požiūriu:
  - BDAR direktyvos nevykdantys subjektai

Kibernetinio saugumo „priešai“

- KSĮ ir saugumo direktyvų reikalavimų vykdymo požiūriu:
  - subjektų vadovybės fokuso būtinų pokyčių įgyvendinimui trūkumas / nebuvimas
  - biudžeto būtinų pokyčių įgyvendinimui stiprus trūkumas / nebuvimas
  - reikalavimų (ne)sąmoningas nežinojimas / ignoravimas
- Veiklos vykdymo principu „taip kaip dabar yra“ požiūriu:
  - vadovybės fokuso ir biudžeto kibernetinei saugai trūkumas / nebuvimas
  - pasenusi / nesaugi kompiuterinė ir/ar programinė įranga
  - prioritetas įrangos kainai vs. kokybė ir tiekėjų patikimumas
  - vartotojų edukacijos kibernetinio saugumo klausimais ignoravimas
  - vartotojų patogumo / poreikių viršenybė prieš bazinius saugumo įrankius
  - nežinojimas turimų įrankių ir jų konfigūracijos, visų galimybių neišnaudojimas

Kibernetinio saugumo „priešai“

- Vartotojų kasdienio darbo požiūriu:
  - vartotojų edukacijos kibernetinio saugumo klausimais ignoravimas
  - vartotojų patogumo / poreikių viršenybė prieš bazinius saugumo įrankius
  - vartotojų nej(si)traukimas į kibernetinio saugumo veiklas
  - vartotojų atsakomybės dėl kibernetinio saugumo nebuvimas
  - naudojamų įrankių pilnavertiško išmanymo stoka

Šios dienos žinutės

Jūsų skaitmeninės darbo vietos vis dar nėra saugios

Žinokite kibernetinio saugumo „priešus“

Šiandien puiki diena imtis naujų priemonių

Naujos priemonės

- KSĮ ir saugumo direktyvų reikalavimų vykdymo požiūriu:
  - reikalavimų sąmoningas žinojimas
  - darbas su vadovybe dėl fokuso būtinų pokyčių įgyvendinimui
- Veiklos vykdymo principu „taip kaip dabar yra“ požiūriu:
  - gilinimasis į turimus įrankius ir jų konfigūracijas, visų galimybių išnaudojimas
  - įrangos atnaujinimas
  - prioritetas įrangos kokybei ir tiekėjų patikimumui vs. įrangos kaina
  - darbas su vadovybe dėl fokuso ir biudžeto būtinų pokyčių įgyvendinimui
  - vartotojų edukacija kibernetinio saugumo klausimais
  - vartotojų patogumo / poreikių viršenybės prieš bazinius saugumo įrankius mažinimas

Naujos priemonės

- Kompiuterinė įranga su NPU procesoriais (AI based PC)
- Windows 10 --> Windows 11
- DI paremti saugumo įrankiai
- Microsoft 365 E5 Security priedas Microsoft 365 Business Premium planui