CRA & NIS2

(OT) saugos reikalavimai

Evaldas Valūnas
Saugumo sprendimų kompetencijos centras

CRA

(Cyber Resilience Act)

Kibernetinio atsparumo aktas

Kibernetinio atsparumo aktas

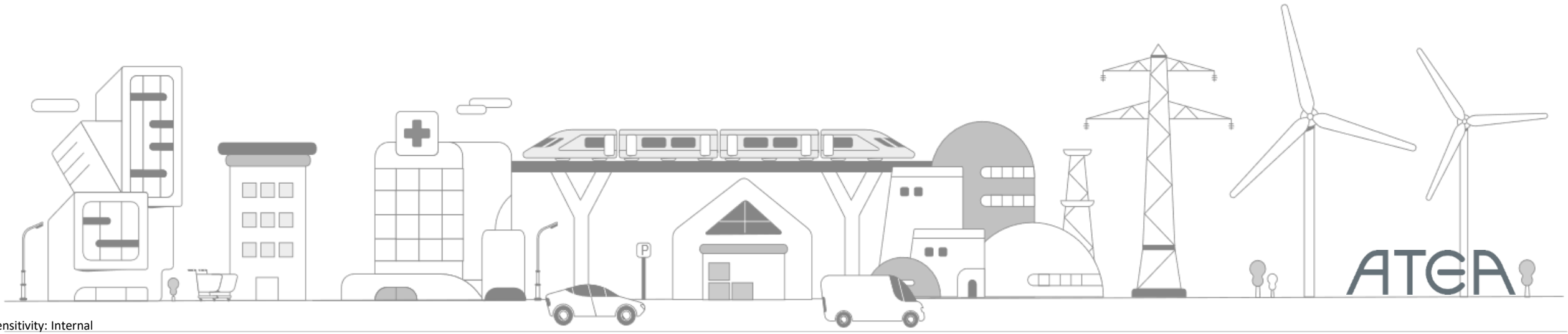
Šiuo reglamentu nustatoma:

a) produktų su skaitmeniniais elementais tiekimo rinkai taisyklės, siekiant užtikrinti tokių produktų kibernetinį saugumą;

b) produktų su skaitmeniniais elementais projektavimo, kūrimo ir gamybos esminiai kibernetinio saugumo reikalavimai ir ekonominės veiklos vykdytojų pareigos, susijusios su tų produktų kibernetiniu saugumu;

c) pažeidžiamumo valdymo procesų, kuriuos gamintojai nustatė, kad užtikrintų produktų su skaitmeniniais elementais kibernetinį saugumą per numatomą produktų naudojimo laikotarpį…

…



Kibernetinio atsparumo aktas

10.12.2024
Priimta

11.09.2026
Įsigalioja
14 straipsnis

Gamintojų pareiga pranešti

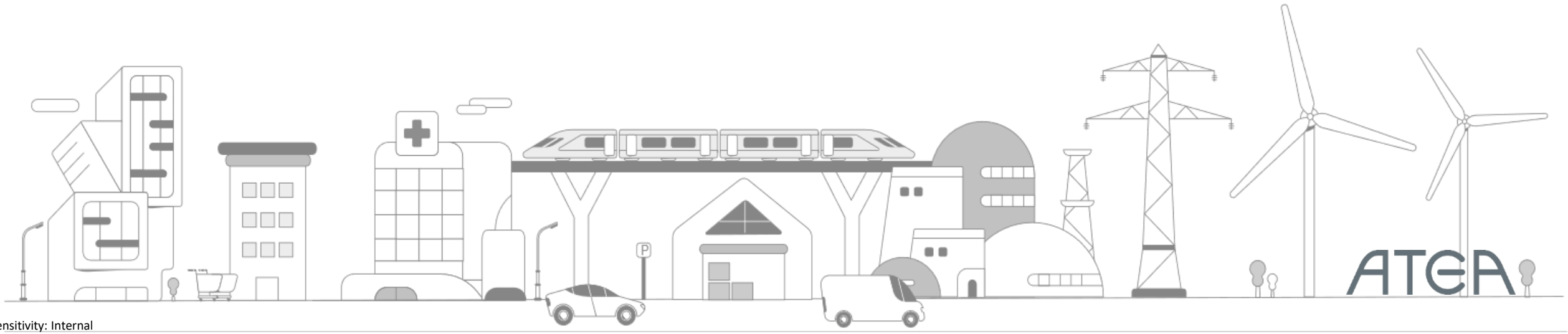
11.12.2027
Pilnai įsigalioja

Kibernetinio atsparumo aktas

14 straipsnis
Gamintojų pareiga pranešti

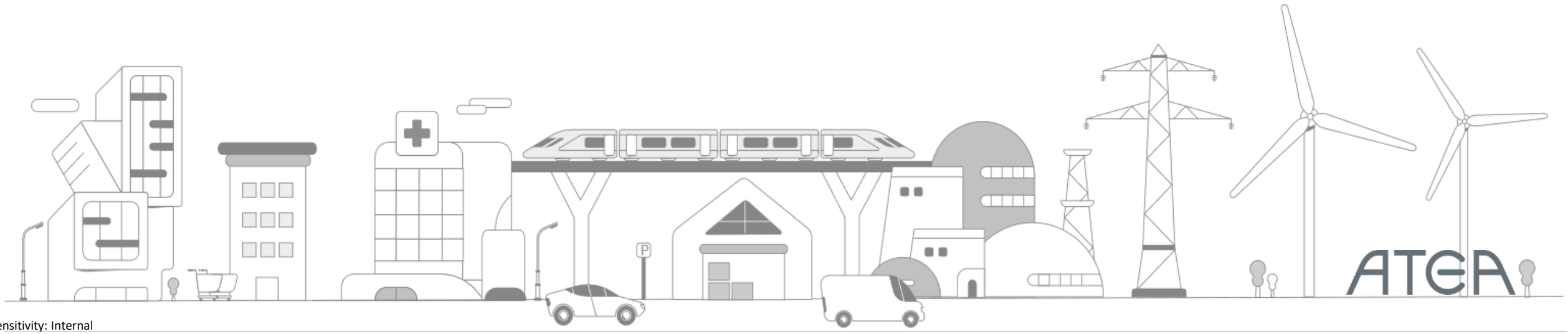
1. Gamintojas praneša apie visus aktyviai išnaudojamus produkto su skaitmeniniais elementais pažeidžiamumus, apie kuriuos sužino,

…



Kibernetinio atsparumo aktas

13 straipsnis
Gamintojų pareigos
…
6. **Nustatę pažeidžiamumą komponente**, įskaitant atvirojo kodo komponentą, integruotą į produktą su skaitmeniniais elementais, **gamintojai praneša** apie pažeidžiamumą tą komponentą gaminančiam ar techniškai prižiūrinčiam asmeniui arba subjektui ir sprendžia bei **pašalina pažeidžiamumo problemą** laikantis I priedo II dalyje nustatytų pažeidžiamumo valdymo reikalavimų. Jei gamintojai yra sukūrę programinės ar aparatinės įrangos pakeitimą to komponento pažeidžiamumo problemai spręsti, jie, kai tinkama, kompiuterio skaitomu formatu dalijasi atitinkamu kodu arba dokumentais su tą komponentą gaminančiu ar techniškai prižiūrinčiu asmeniu arba subjektu.



NIS2/TIS2

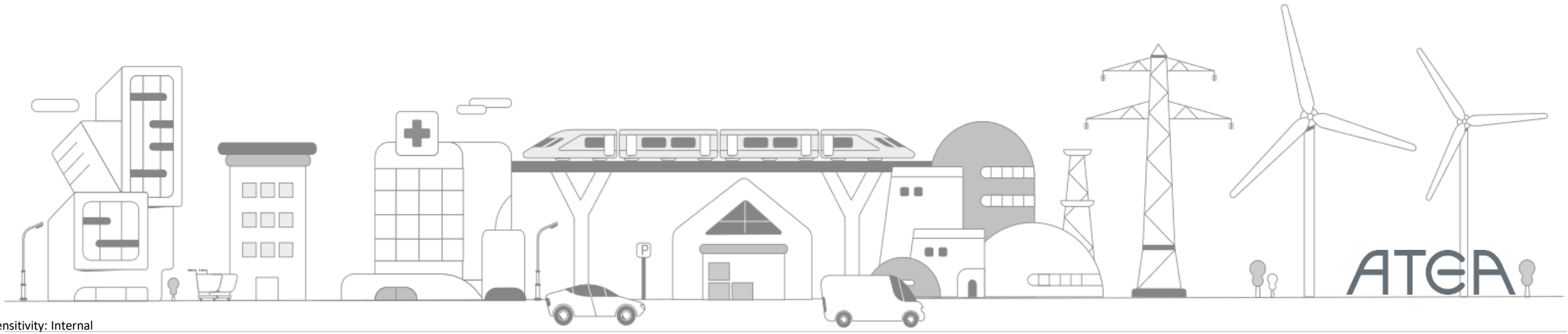
Tinklų ir Informacinių Sistemų direktyva

➡ LR Kibernetinio saugumo įstatymas

Kibernetinio saugumo įstatymas

7 skirsnis

45. … spragų valdymo ir atskleidimo nuostatos...
45.4. ...spragų nustatymo programinės įrangos naudojimas...
45.8. ...spragų skenavimą atlikti ne rečiau kaip kas 6 mėnesius;



Kibernetinio saugumo įstatymas

1 lentelė

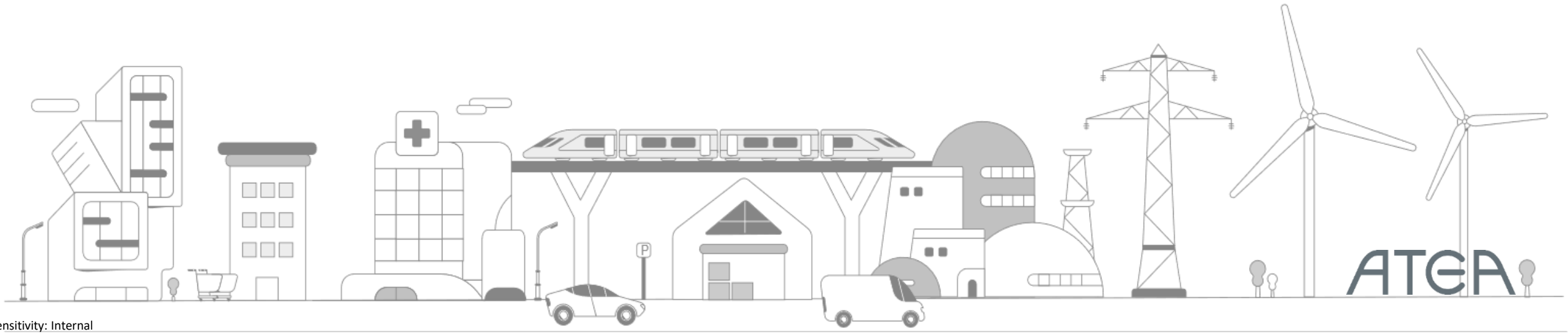
1. Turi būti fiksuojami bent jau šie žurnaliniai įrašai:

...

1.4 administratorių atliekami veiksmai;

...

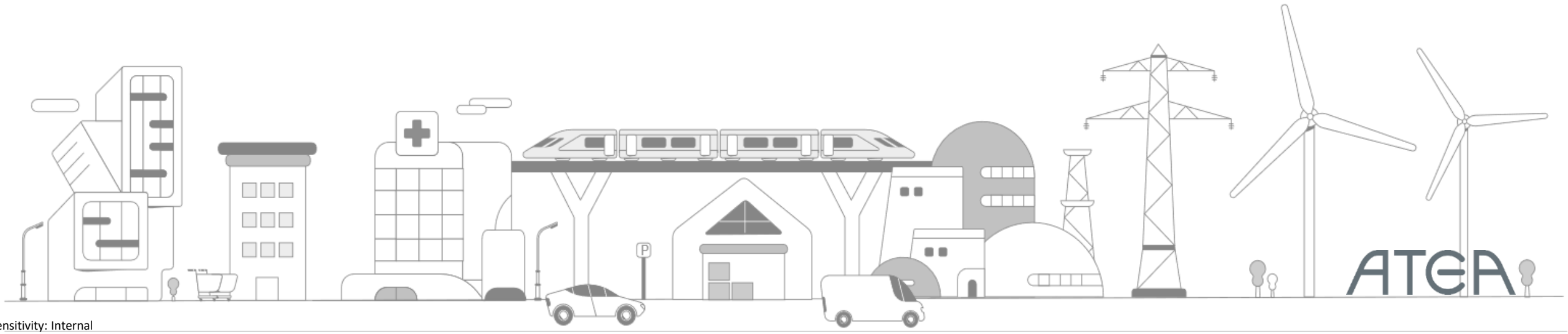
12. Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų į tinklų ir informacinę sistemą įeinantį ir iš jos išeinantį duomenų srautą.



Kibernetinio saugumo įstatymas

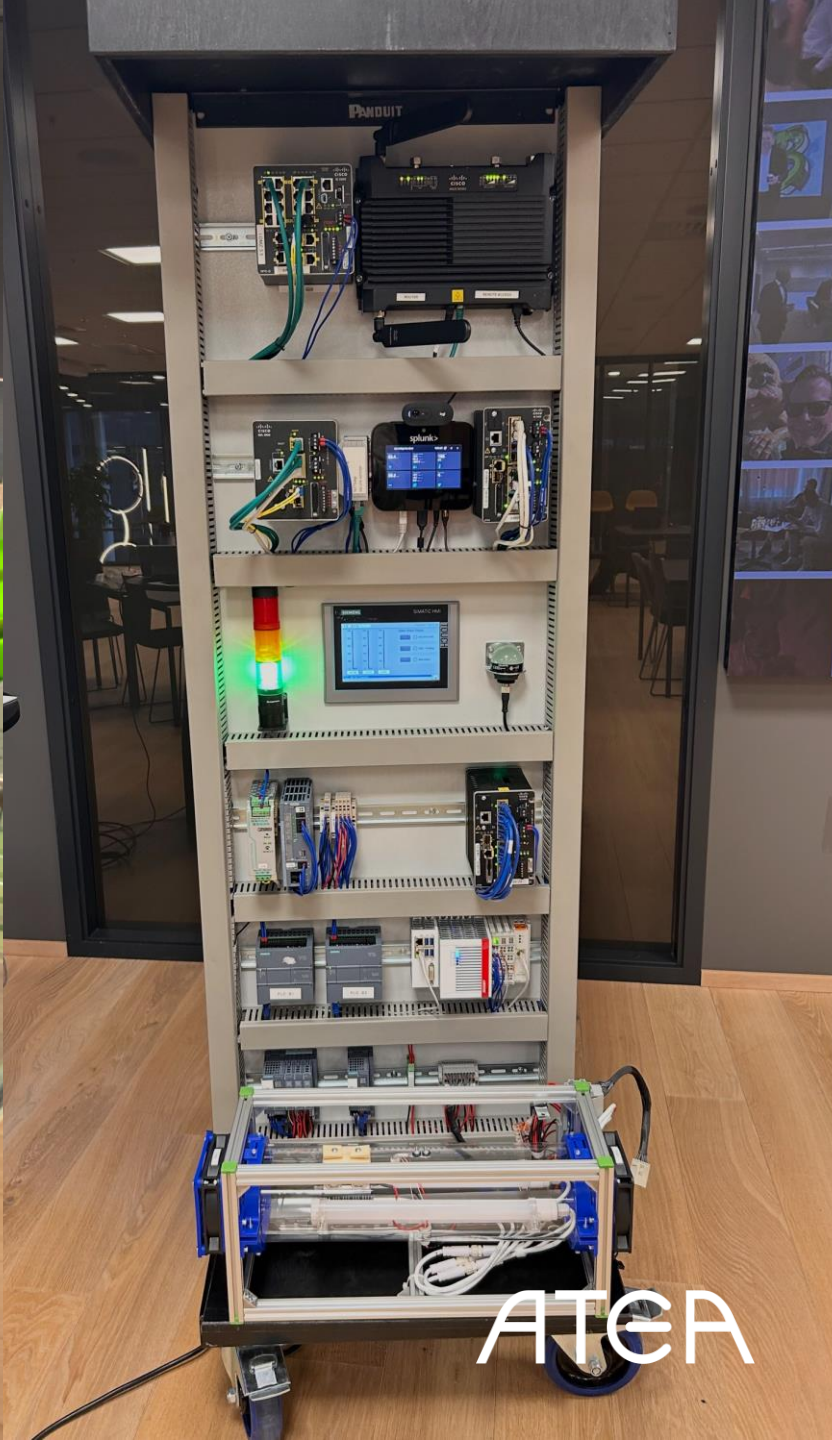
3 lentelė

21. … turi turėti aktualią ... visų tinklų ir informacinių sistemų schemas (atnaujinti joms pasikeitus)
30. Turi būti diegiami naudojamos programinės įrangos gamintojų ir operacinių sistemų rekomenduojami atnaujinimai.
31. Tinklų ir informacinės sistemos ... naudojančios nepalaikomas operacinių sistemų ir kitos programinės įrangos versijas, turi veikti atskirame tinklo segmente, atskirtame nuo pagrindinių kibernetinio saugumo subjekto veiklos funkcijų.




ATEA
CISCO


TP2B
KØBENHAVN
ATEA
BOSS


PANDUIT
splunk>
ATEA

Turite klausimų ?

Susisiekime:

evaldas.valunas@atea.lt

+370 682 55171

https://www.linkedin.com/in/evaldas-valunas/

ATEA


Kuriame Lietuvą su IT
ATEA