



**SECURITY
DAYS**

ATSPARUMAS EKSTREMALIOMIS SĄLYGOMIS: KURIOS KONTROLĖS IŠ TIKRŲJŲ VEIKIA UKRAINOJE



GEDIMINAS ČERNIAUSKAS

„PwC“ kibernetinio saugumo
paslaugų vadovas Lietuvoje



Kai elektros tiekimas, infrastruktūra, ryšys su darbuotojais, partneriais ir tiekėjais yra sutrikdyti...

Ar jūsų kontrolės vis dar veikia?



Kai elektros tiekimas, infrastruktūra, ryšys su darbuotojais, partneriais ir tiekėjais yra sutrikdyti...

Ar jūsų kontrolės vis dar veikia?



Taikos metu jaučiamės pasiruošę

Turime tvarkas ir politikas, atsarginės kopijos padarytos, incidentų valdymo planas atnaujintas, MFA įjungta



Kai elektros tiekimas, infrastruktūra, ryšys su darbuotojais, partneriais ir tiekėjais yra sutrikdyti...

Ar jūsų kontrolės vis dar veikia?



Taikos metu jaučiamės pasiruošę

Turime tvarkas ir politikas, atsarginės kopijos padarytos, incidentų valdymo planas atnaujintas, MFA įjungta



Kas veikia, kai neveikia niekas?

...

Trys atvejai, trys įprastos kibernetinio saugumo prielaidos



HermeticWiper

„Mūsų administravimo įrankiai yra saugūs.“



Viasat – AcidRain

„Ryšys bus prieinamas krizės metu.“



Kyivstar

„Ataką pastebėtume prieš pagrindinių paslaugų pažeidimus.“

HermeticWiper

Nestebima centralizuoto valdymo infrastruktūra gali tapti užpuoliko masinio diegimo priemone

HermeticWiper

Nestebima centralizuoto valdymo infrastruktūra gali tapti užpuoliko masinio diegimo priemone

01

**AD domenas
kompromituotas**

Prieiga prie privilegijuotų paskyrų

HermeticWiper

Nestebima centralizuoto valdymo infrastruktūra gali tapti užpuoliko masinio diegimo priemone

01

**AD domenas
kompromituotas**

Prieiga prie privilegijuotų paskyrų

02

**Perprastas administravimo /
SYSTEM kontekstas**

Privilegija + kontekstas įgalina
maksimalią žalą

HermeticWiper

Nestebima centralizuoto valdymo infrastruktūra gali tapti užpuoliko masinio diegimo priemone

01

**AD domenas
kompromituotas**

Prieiga prie privilegijuotų paskyrų

02

**Perprastas administravimo /
SYSTEM kontekstas**

Privilegija + kontekstas įgalina
maksimalią žalą

03

**Centralizuoto diegimo
išnaudojimas**

AD / GPO / WMI / automatiniai
atnaujinimai

HermeticWiper

Nestebima centralizuoto valdymo infrastruktūra gali tapti užpuoliko masinio diegimo priemone

01

**AD domenas
kompromituotas**

Prieiga prie privilegijuotų paskyrų

02

**Perprastas administravimo /
SYSTEM kontekstas**

Privilegija + kontekstas įgalina
maksimalią žalą

03

**Centralizuoto diegimo
išnaudojimas**

AD / GPO / WMI / automatiniai
atnaujinimai

04

**Masiškas duomenų
naikinimas**

Gynybai galėjo atrodyti kaip
teisėtas administravimo procesas

HermeticWiper

Nestebima centralizuoto valdymo infrastruktūra gali tapti užpuoliko masinio diegimo priemone

01

**AD domenas
kompromituotas**

Prieiga prie privilegijuotų paskyrų

02

**Perprastas administravimo /
SYSTEM kontekstas**

Privilegija + kontekstas įgalina
maksimalią žalą

03

**Centralizuoto diegimo
išnaudojimas**

AD / GPO / WMI / automatiniai
atnaujinimai

04

**Masiškas duomenų
naikinimas**

Gynybai galėjo atrodyti kaip
teisėtas administravimo procesas

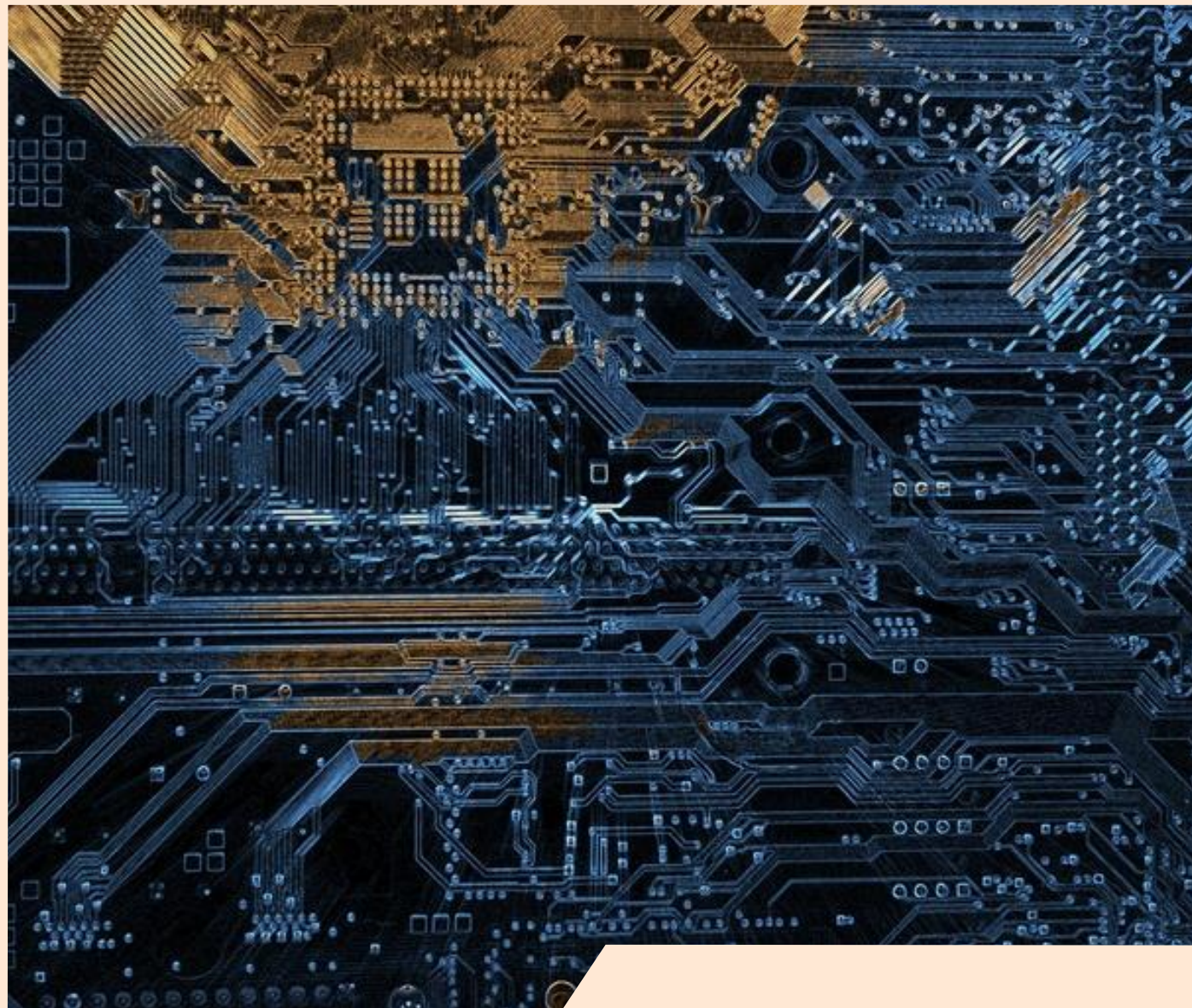
TAIKOS METU ATRODO GERAI

- „EDR įdiegtas“
- „Atsarginės kopijos saugomos“
- „Pakeitimų valdymas yra dokumentuotas“
- „Domeno administratorių skaičius ribotas“

REALYBĖS PATIKRINIMAS KRIZĖS METU

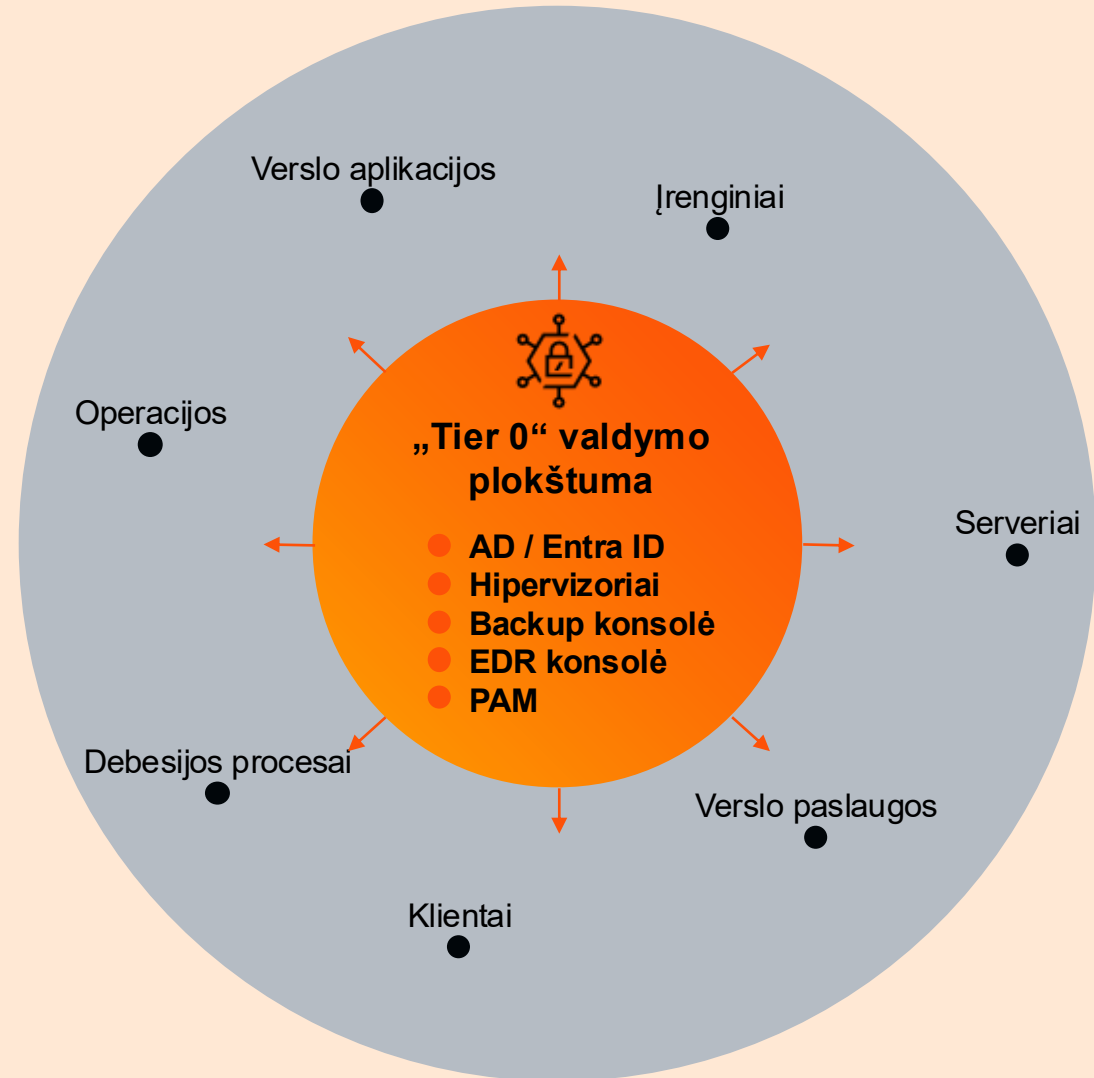
Jei šiandien viena administratoriaus paskyra bus kompromituota, kas rytoj bus išplatinta visur?

Jei užpuolikai valdo jūsų
administravimo
konsoles, jūsų įrankiai
tampa jų įrankiais.



Išvada: stebėkime valdymo aplinką

„HermeticWiper“ atvejis rodo, kodėl būtina saugoti ne tik galinius įrenginius, bet ir centralizuoto diegimo bei administravimo kelius.



Išvada: stebėkime valdymo aplinką

„HermeticWiper“ atvejis rodo, kodėl būtina saugoti ne tik galinius įrenginius, bet ir centralizuoto diegimo bei administravimo kelius.

GYNYBOS PRINCIPAI

1

„Tier 0“ atskyrimas

AD, hipervizoriai, atsarginės kopijos, EDR, PAM atskiroje administravimo zonoje

2

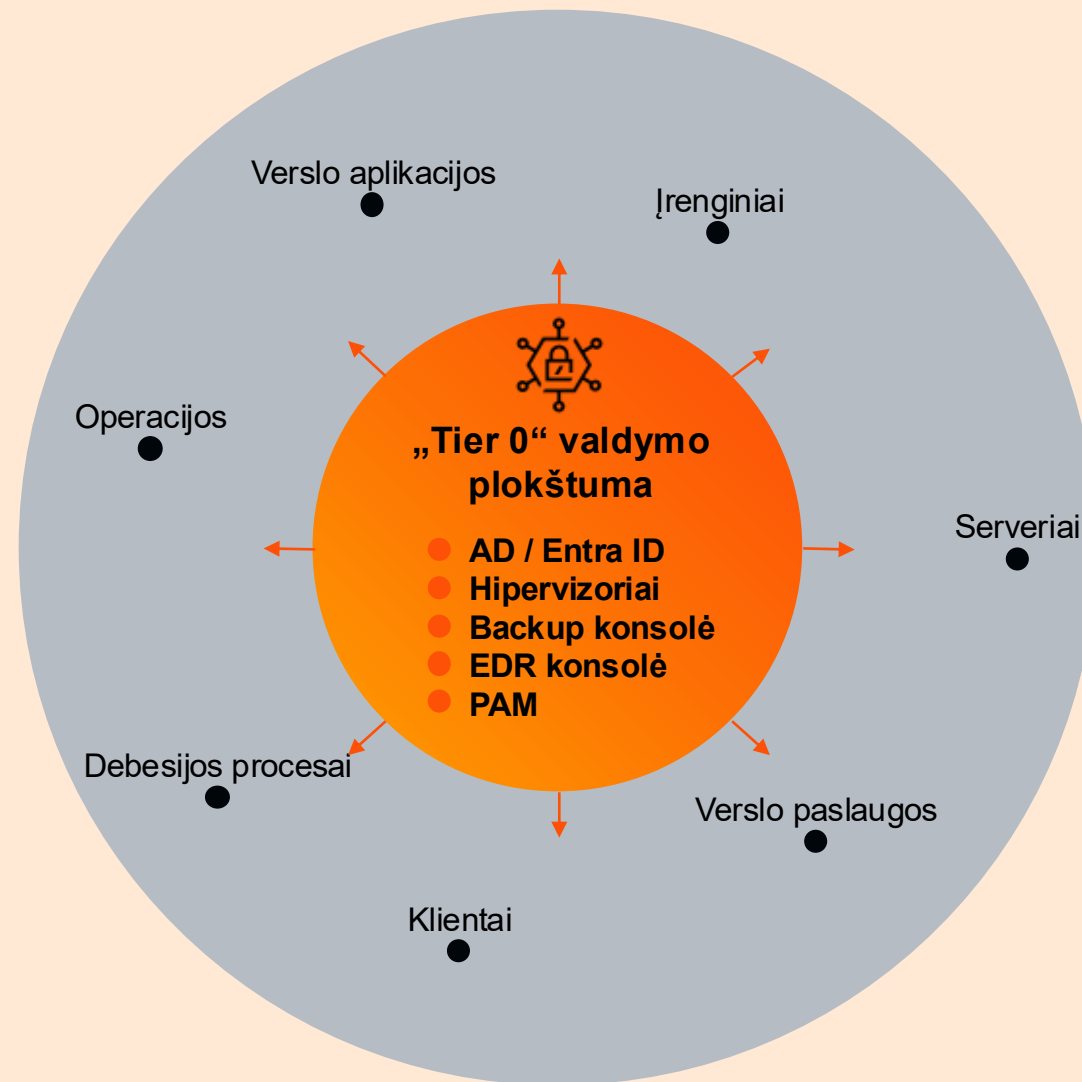
Privilegiuotos tapatybės saugumas

Fišingui atsparus MFA, "just-in-time" administravimas

3

Diegimo kelio stebėsena

Įspėjimai dėl masinių GPO / suplanuotų užduočių pakeitimų



AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

Incidentų valdymas
Žmonės, koordinuojantys
atsaką

AcidRain

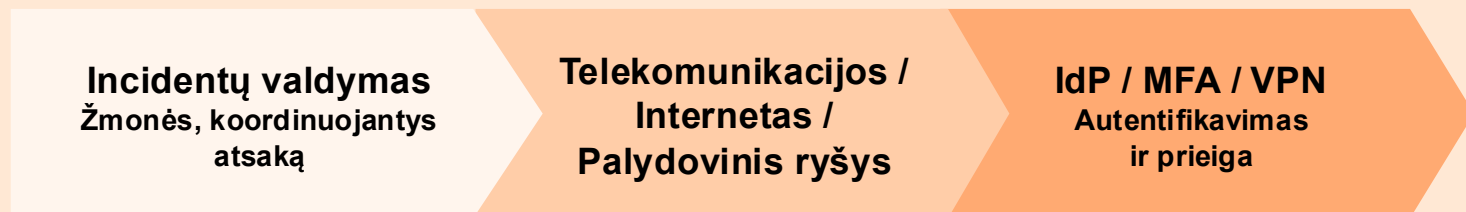
Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

Incidentų valdymas
Žmonės, koordinuojantys
atsaką

**Telekomunikacijos /
Internetas /
Palydovinis ryšys**

AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami



AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami



AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami



AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami



AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

TAIKOS METU ATRODO GERAI

- „Incidentų valdymas dokumentuotas“
- „Atidarysime krizės valdymo kanalą“
- „Koordinavimui naudosime VPN ir MFA“
- „Turime komunikacijos planą“

REALYBĖS PATIKRINIMAS KRIZĖS METU

Ar incidentų valdymo komanda gali koordinuoti veiksmus, jei neveikia VPN, el. paštas, „Teams“, telefonai ir interneto ryšys?

AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

01

Išnaudotas perimetro VPN įrenginys

Nepataisytas pažeidžiamumas
(CVE-2018-13379)

TAIKOS METU ATRODO GERAI

- „Incidentų valdymas dokumentuotas“
- „Atidarysime krizės valdymo kanalą“
- „Koordinavimui naudosime VPN ir MFA“
- „Turime komunikacijos planą“

REALYBĖS PATIKRINIMAS KRIZĖS METU

Ar incidentų valdymo komanda gali koordinuoti veiksmus, jei neveikia VPN, el. paštas, „Teams“, telefonai ir interneto ryšys?

AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

01

Išnaudotas perimetro VPN įrenginys

Nepataisytas pažeidžiamumas
(CVE-2018-13379)

02

Pasiektas valdymo segmentas

perėjimas prie KA-SAT valdymo konsolių

TAIKOS METU ATRODO GERAI

- „Incidentų valdymas dokumentuotas“
- „Atidarysime krizės valdymo kanalą“
- „Koordinavimui naudosime VPN ir MFA“
- „Turime komunikacijos planą“

REALYBĖS PATIKRINIMAS KRIZĖS METU

Ar incidentų valdymo komanda gali koordinuoti veiksmus, jei neveikia VPN, el. paštas, „Teams“, telefonai ir interneto ryšys?

AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

01

Išnaudotas perimetro VPN įrenginys

Nepataisytas pažeidžiamumas
(CVE-2018-13379)

02

Pasiektas valdymo segmentas

perėjimas prie KA-SAT valdymo konsolių

03

Masinis modemų ištrynimasis

Flash atmintis perrašoma vartotojų modemuose

TAIKOS METU ATRODO GERAI

- „Incidentų valdymas dokumentuotas“
- „Atidarysime krizės valdymo kanalą“
- „Koordinavimui naudosime VPN ir MFA“
- „Turime komunikacijos planą“

REALYBĖS PATIKRINIMAS KRIZĖS METU

Ar incidentų valdymo komanda gali koordinuoti veiksmus, jei neveikia VPN, el. paštas, „Teams“, telefonai ir interneto ryšys?

AcidRain

Incidentų valdymo planas dažnai remiasi prielaida, kad tinklas ir ryšio priemonės išliks prieinami

01

Išnaudotas perimetro VPN įrenginys

Nepataisytas pažeidžiamumas (CVE-2018-13379)

02

Pasiektas valdymo segmentas

perėjimas prie KA-SAT valdymo konsolių

03

Masinis modemų ištrynimasis

Flash atmintis perrašoma vartotojų modemuose

04

Ryšio sutrikdymas

Sutrikimai visoje Europoje, įskaitant 5 800 vėjo turbinų Vidurio Europoje

TAIKOS METU ATRODO GERAI

- „Incidentų valdymas dokumentuotas“
- „Atidarysime krizės valdymo kanalą“
- „Koordinavimui naudosime VPN ir MFA“
- „Turime komunikacijos planą“

REALYBĖS PATIKRINIMAS KRIZĖS METU

Ar incidentų valdymo komanda gali koordinuoti veiksmus, jei neveikia VPN, el. paštas, „Teams“, telefonai ir interneto ryšys?

Jei incidentų valdymo planas priklauso nuo sistemų, kurios pačios gali tapti atakos taikiniu, planas nėra atsparus.



Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

3

Krizinė komunikacija

Skambučių medis, „Signal“ kanalai ir susitikimo vietos:
informacija atspausdinta ir patikrinta

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

3

Krizinė komunikacija

Skambučių medis, „Signal“ kanalai ir susitikimo vietos: informacija atspausdinta ir patikrinta

4

Pratybos neveikiant tinklui

Stalo pratybos, kurių metu neveikia VPN, el. paštas, „Teams“ ir interneto ryšys

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

3

Krizinė komunikacija

Skambučių medis, „Signal“ kanalai ir susitikimo vietos: informacija atspausdinta ir patikrinta

4

Pratybos neveikiant tinklui

Stalo pratybos, kurių metu neveikia VPN, el. paštas, „Teams“ ir interneto ryšys

PRIKLAUSOMYBIŲ GRANDINĖ

Kritinės funkcijos

Krizės valdymo kanalai

El. paštas / Teams

IdP / MFA / VPN

Ryšys / internetas

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

3

Krizinė komunikacija

Skambučių medis, „Signal“ kanalai ir susitikimo vietos: informacija atspausdinta ir patikrinta

4

Pratybos neveikiant tinklui

Stalo pratybos, kurių metu neveikia VPN, el. paštas, „Teams“ ir interneto ryšys

PRIKLAUSOMYBIŲ GRANDINĖ

Kritinės funkcijos

Krizės valdymo kanalai

El. paštas / Teams

~~IdP / MFA / VPN~~

Ryšys / internetas

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

3

Krizinė komunikacija

Skambučių medis, „Signal“ kanalai ir susitikimo vietos: informacija atspausdinta ir patikrinta

4

Pratybos neveikiant tinklui

Stalo pratybos, kurių metu neveikia VPN, el. paštas, „Teams“ ir interneto ryšys

PRIKLAUSOMYBIŲ GRANDINĖ

Kritinės funkcijos

Krizės valdymo kanalai

~~El. paštas / Teams~~

~~IdP / MFA / VPN~~

Ryšys / internetas

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

3

Krizinė komunikacija

Skambučių medis, „Signal“ kanalai ir susitikimo vietos: informacija atspausdinta ir patikrinta

4

Pratybos neveikiant tinklui

Stalo pratybos, kurių metu neveikia VPN, el. paštas, „Teams“ ir interneto ryšys

PRIKLAUSOMYBIŲ GRANDINĖ

Kritinės funkcijos

~~Krizės valdymo kanalai~~

~~El. paštas / Teams~~

~~IdP / MFA / VPN~~

Ryšys / internetas

Išvada: sustiprinkime priklausomybių grandinę

Būkime pasiruošę visiškam ryšio praradimui, užuot darę prielaidą, kad ryšys visada bus prieinamas

GYNYBOS PRINCIPAI

1

Aprašyta ryšio grandinė

Ryšys – IdP – VPN – el. paštas – komunikacija – žmonės

2

Antrinis ryšio kanalas

Antrinis ryšys, alternatyvus IdP, „offline“ incidentų valdymo plano kopijos

3

Krizinė komunikacija

Skambučių medis, „Signal“ kanalai ir susitikimo vietos: informacija atspausdinta ir patikrinta

4

Pratybos neveikiant tinklui

Stalo pratybos, kurių metu neveikia VPN, el. paštas, „Teams“ ir interneto ryšys

PRIKLAUSOMYBIŲ GRANDINĖ

Kritinės funkcijos

~~Krizės valdymo kanalai~~

~~El. paštas / Teams~~

~~IdP / MFA / VPN~~

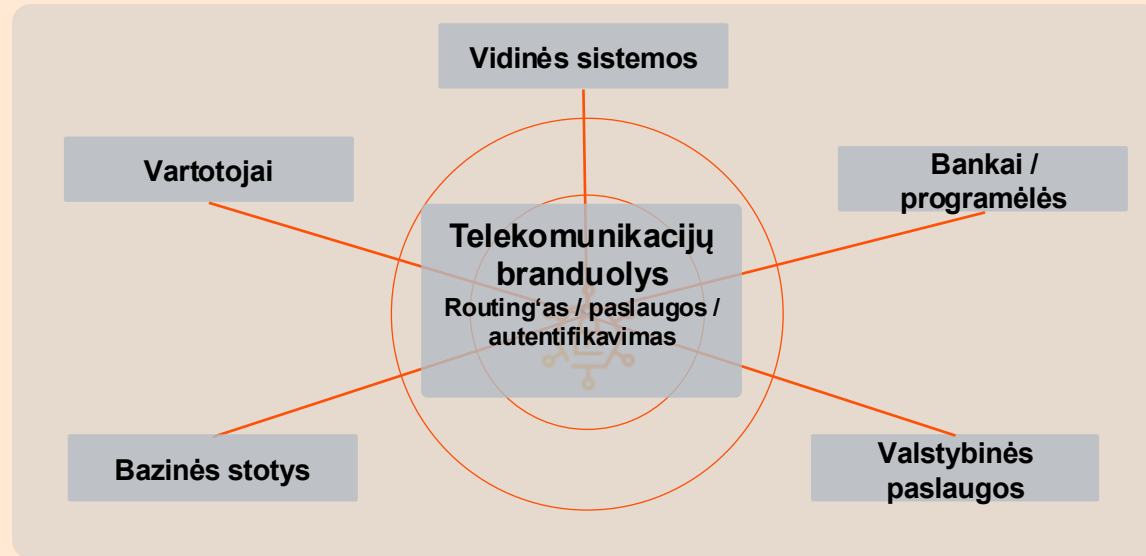
~~Ryšys / internetas~~

Kyivstar

Ilgai nepastebėti įsibrovėliai gali perprasti jūsų tinklą geriau nei jo gynėjai

Kyivstar

Ilgai nepastebėti įsibrovėliai gali perprasti jūsų tinklą geriau nei jo gynėjai

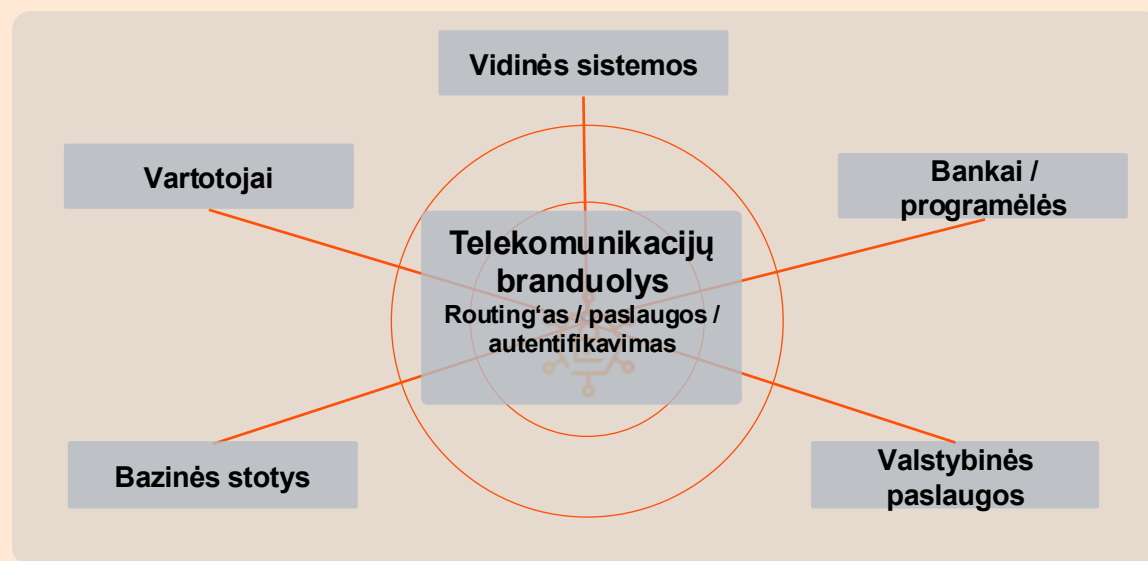


Ilgai nepastebėti įsibrovėliai gali perprasti jūsų tinklą geriau nei jo gynėjai

01

Sukompromituota partnerio paskyra

Pradinė prieiga per trečiąsias šalis



Ilgai nepastebėti įsibrovėliai gali perprasti jūsų tinklą geriau nei jo gynėjai

01

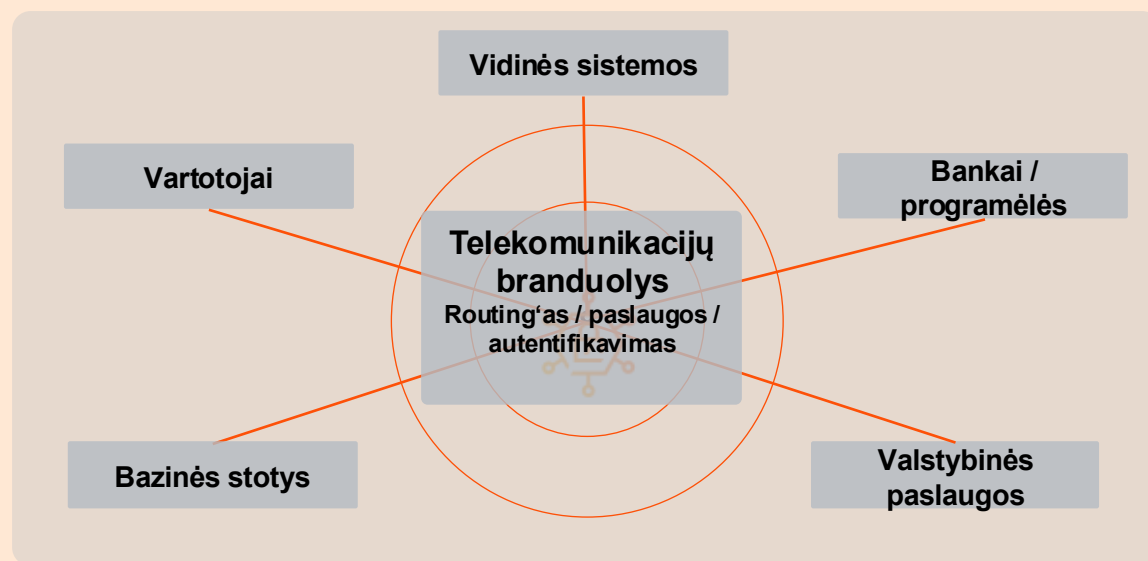
Sukompromituota partnerio paskyra

Pradinė prieiga per trečiąsias šalis

02

7 mėnesiai tinkle

Vidinė žvalgyba: tinklo struktūra, prisijungimo duomenys, atsarginių kopijų vietos



Ilgai nepastebėti įsibrovėliai gali perprasti jūsų tinklą geriau nei jo gynėjai

01

Sukompromituota partnerio paskyra

Pradinė prieiga per trečiąsias šalis

02

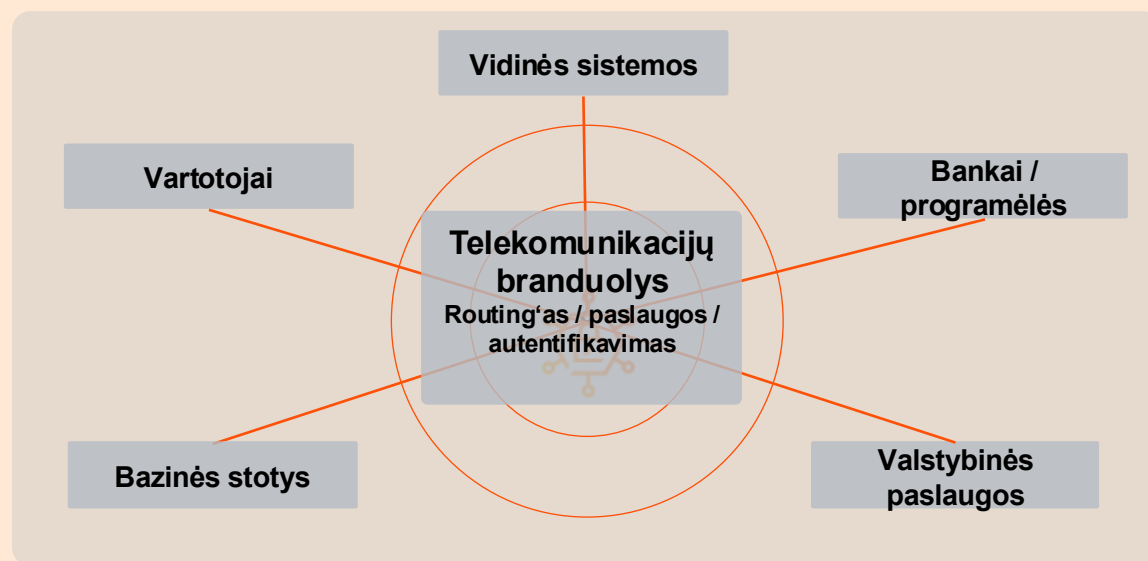
7 mėnesiai tinkle

Vidinė žvalgyba: tinklo struktūra, prisijungimo duomenys, atsarginių kopijų vietos

03

Sunaikinta infrastruktūra

pažeista virtualioji infrastruktūra ir telekomunikacijų tinklo branduolio sistemos



Ilgai nepastebėti įsibrovėliai gali perprasti jūsų tinklą geriau nei jo gynėjai

01

Sukompromituota partnerio paskyra

Pradinė prieiga per trečiąsias šalis

02

7 mėnesiai tinkle

Vidinė žvalgyba: tinklo struktūra, prisijungimo duomenys, atsarginių kopijų vietos

03

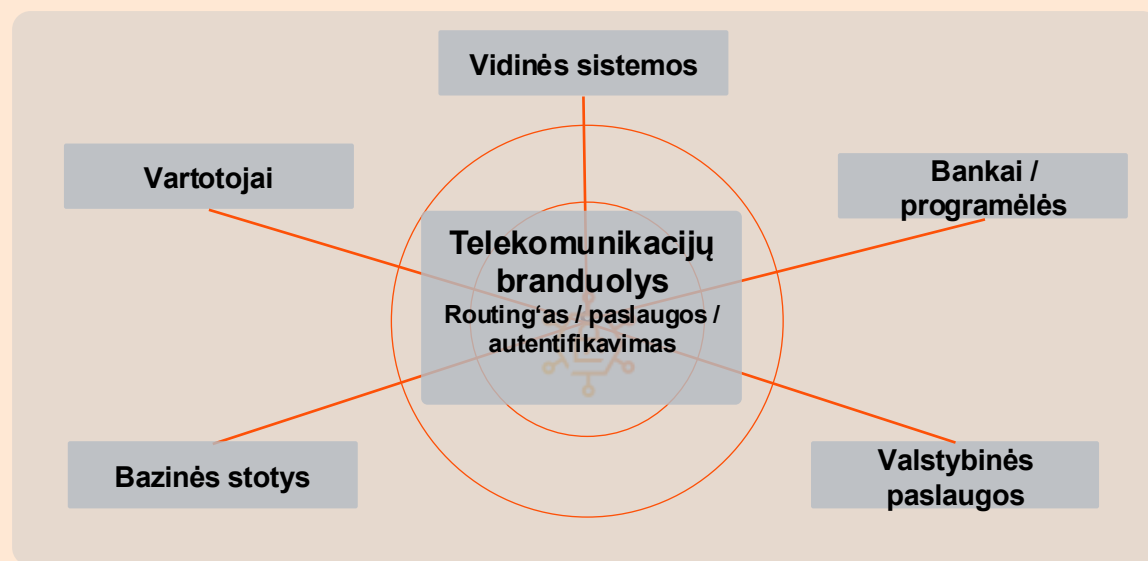
Sunaikinta infrastruktūra

pažeista virtualioji infrastruktūra ir telekomunikacijų tinklo branduolio sistemos

04

Lėtas veiklos atkūrimas

24 mln. paveiktų vartotojų, bankai ir valstybinės reikšmės paslaugos



Ilgai nepastebėti įsibrovėliai gali perprasti jūsų tinklą geriau nei jo gynėjai

01

Sukompromituota partnerio paskyra

Pradinė prieiga per trečiąsias šalis

02

7 mėnesiai tinkle

Vidinė žvalgyba: tinklo struktūra, prisijungimo duomenys, atsarginių kopijų vietos

03

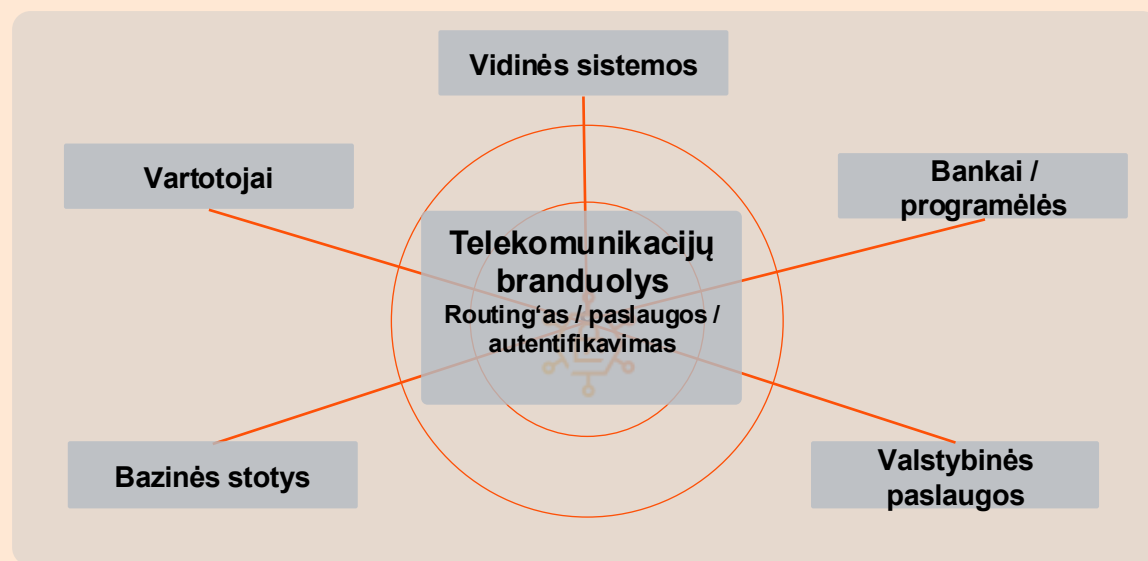
Sunaikinta infrastruktūra

pažeista virtualioji infrastruktūra ir telekomunikacijų tinklo branduolio sistemos

04

Lėtas veiklos atkūrimas

24 mln. paveiktų vartotojų, bankai ir valstybinės reikšmės paslaugos



TAIKOS METU ATRODO GERAI

- „Mes pastebėtume“
- „MFA įjungtas“
- „Trečiųjų šalių rizika įvertinta“
- „Atsarginės kopijos saugios“

REALYBĖS PATIKRINIMAS KRIZĖS METU

Kiek laiko užpuolikas galėtų būti jūsų tinkle, kol kas nors pastebėtų?

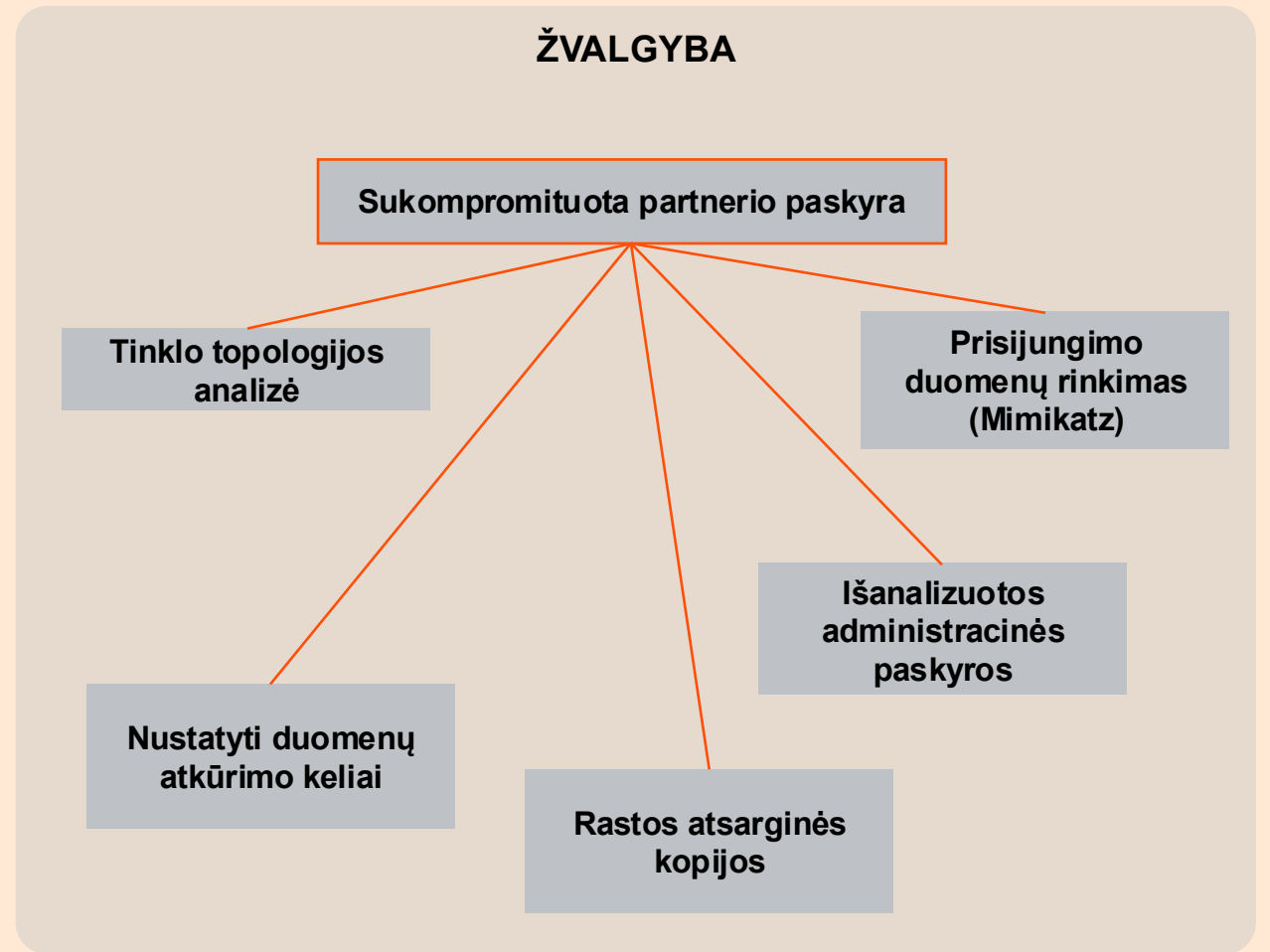
Kova vyksta ne įvykus
„sprogimui“, o tyliomis
dienomis ir savaitėmis
ieškant įsibrovėlių savo
tinkluose



Išvada: atlikime ankstyvą kenksmingos veiklos tinkle paiešką
„Kyivstar“ atvejis parodė ankstyvo aptikimo ir žalos plitimo ribojimo svarbą

Išvada: atlikime ankstyvą kenksmingos veiklos tinkle paiešką

„Kyivstar“ atvejis parodė ankstyvo aptikimo ir žalos plitimo ribojimo svarbą



Išvada: atlikime ankstyvą kenksmingos veiklos tinkle paiešką

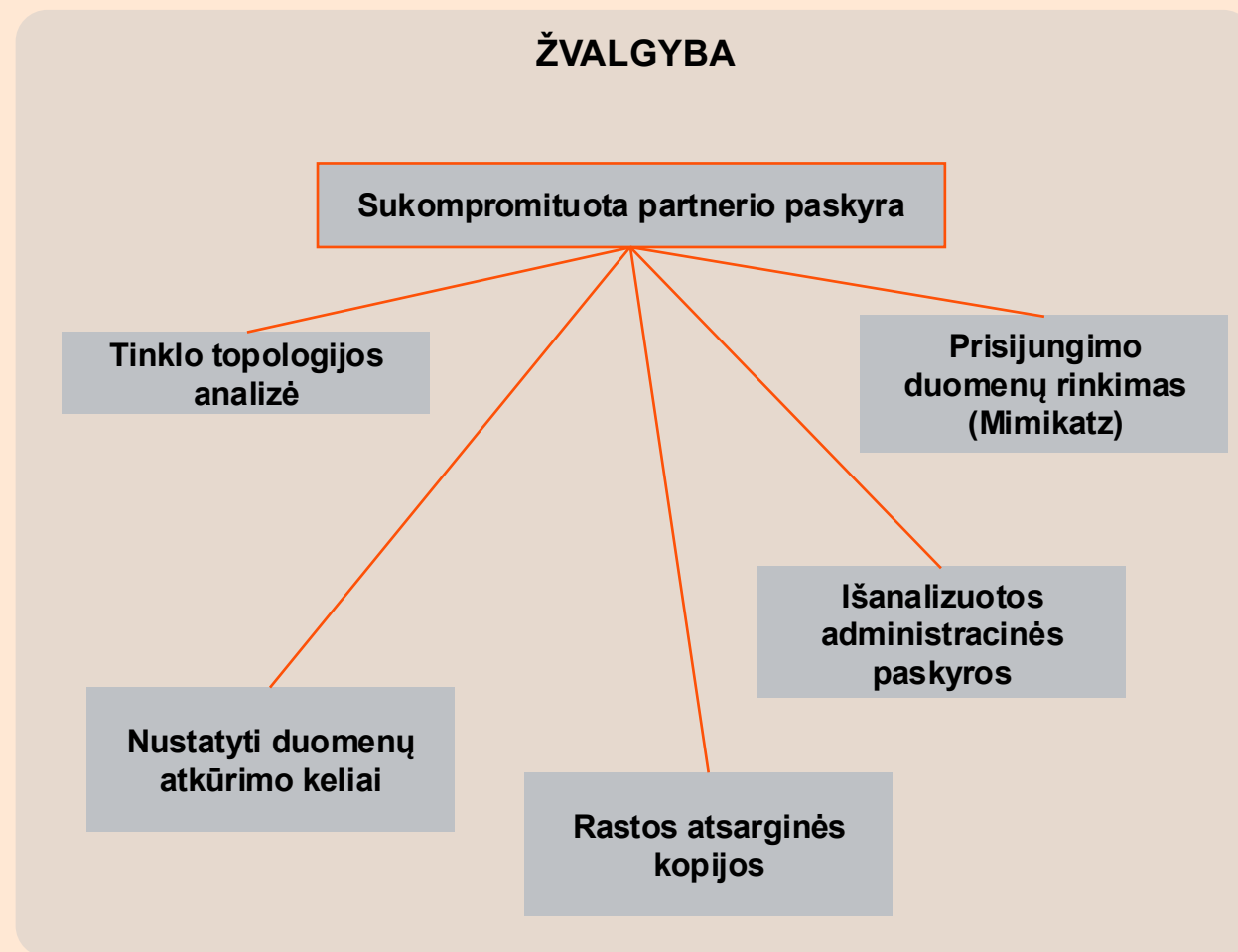
„Kyivstar“ atvejis parodė ankstyvo aptikimo ir žalos plitimo ribojimo svarbą

GYNYBOS PRINCIPAI

1

Partnerių prieiga yra nepatikima

fišingui atsparus MFA, „Just-in-time“ prieiga, segmentavimas



Išvada: atlikime ankstyvą kenksmingos veiklos tinkle paiešką

„Kyivstar“ atvejis parodė ankstyvo aptikimo ir žalos plitimo ribojimo svarbą

GYNYBOS PRINCIPAI

1

Partnerių prieiga yra nepatikima

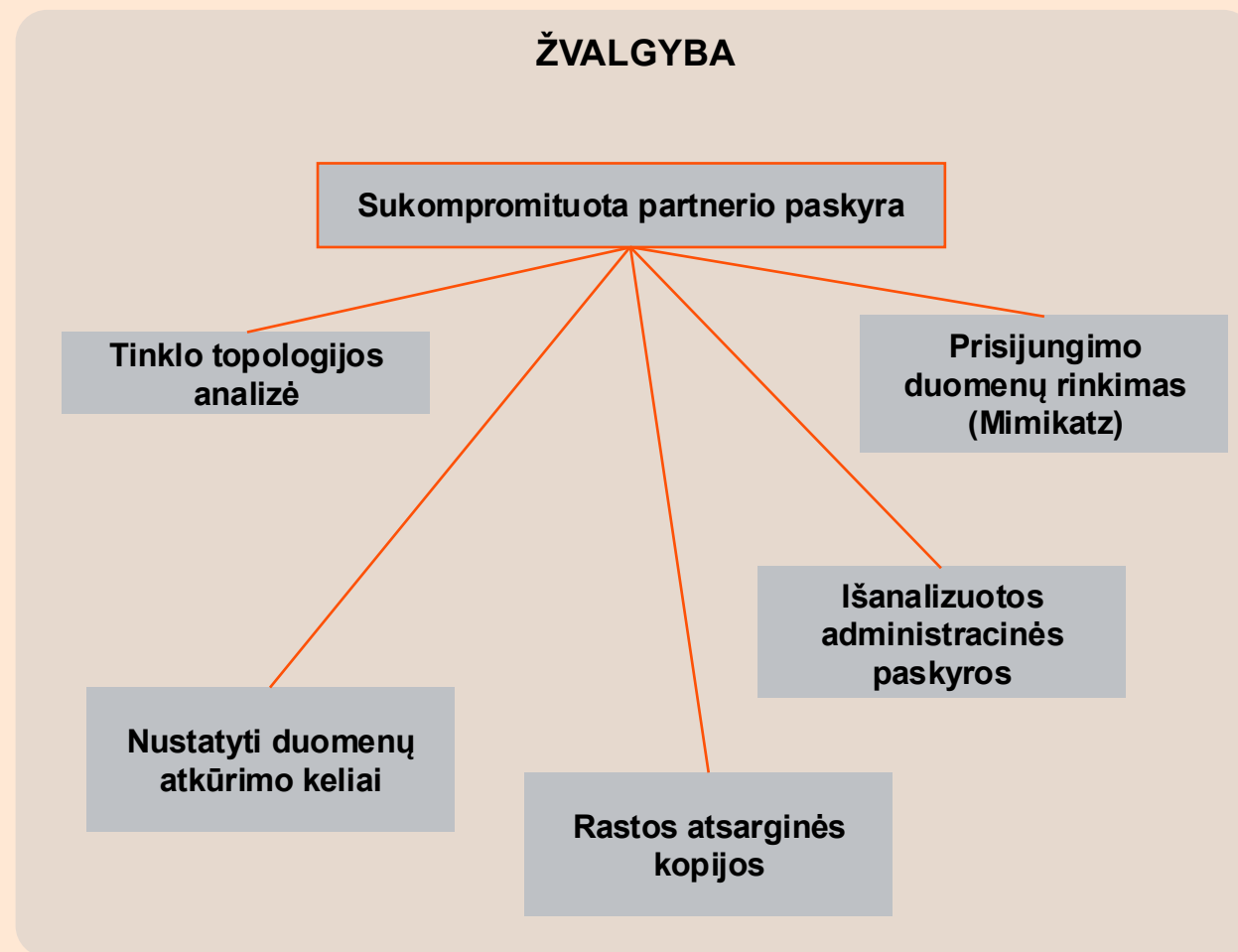
fišingui atsparus MFA, „Just-in-time“ prieiga, segmentavimas

2

Ieškokite ilgalaikio buvimo požymių

Hipotezėmis, o ne vien IOC pagrindu paremta paieška

ŽVALGYBA



Išvada: atlikime ankstyvą kenksmingos veiklos tinkle paiešką

„Kyivstar“ atvejis parodė ankstyvo aptikimo ir žalos plitimo ribojimo svarbą

GYNYBOS PRINCIPAI

1

Partnerių prieiga yra nepatikima

fišingui atsparus MFA, „Just-in-time“ prieiga, segmentavimas

2

Ieškokite ilgalaikio buvimo požymių

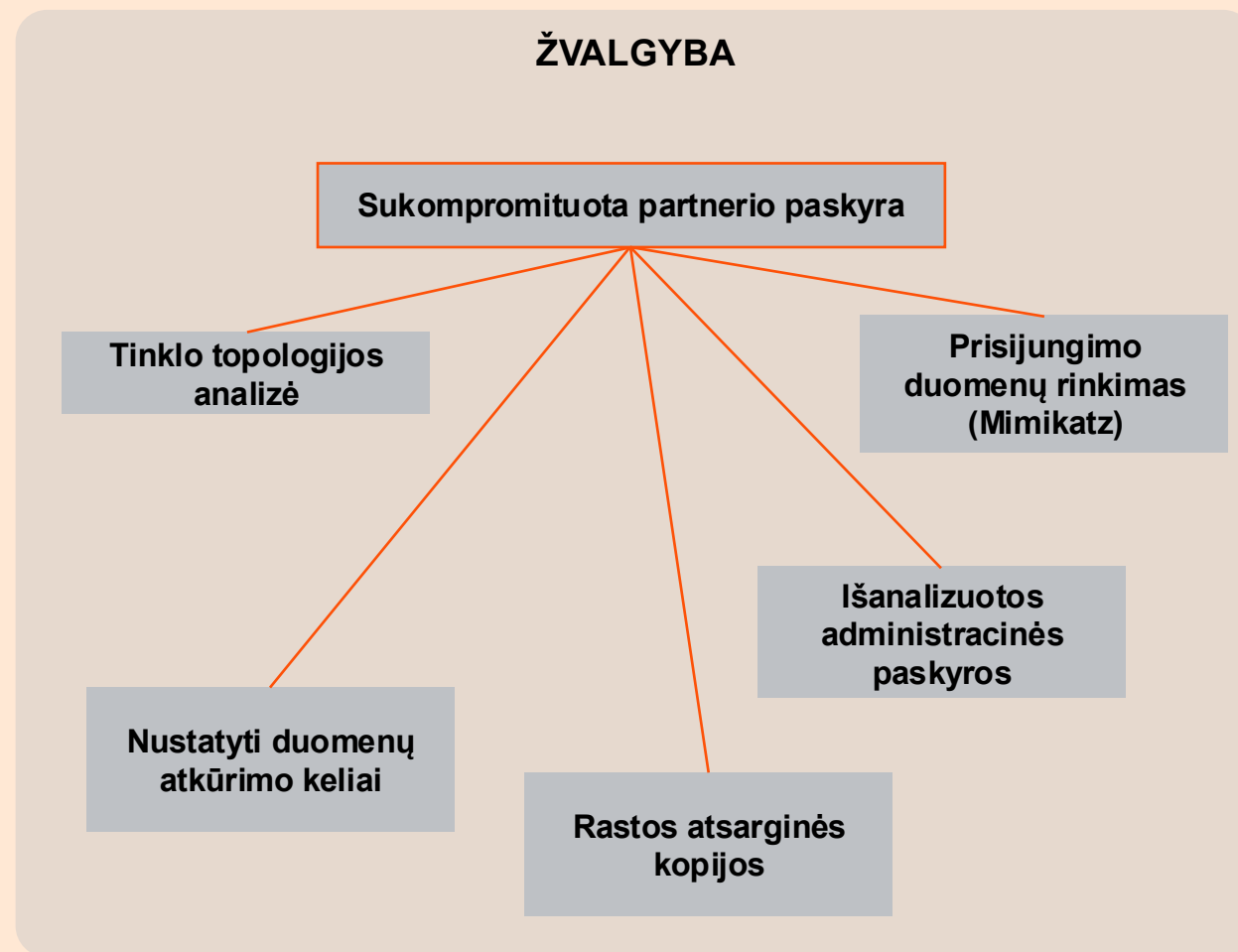
Hipotezėmis, o ne vien IOC pagrindu paremta paieška

3

Ieškokite vidinės žvalgybos požymių

Prisijungimo duomenų rinkimas, tinklo skenavimas, atsarginių kopijų sekimas

ŽVALGYBA



Išvada: atlikime ankstyvą kenksmingos veiklos tinkle paiešką

„Kyivstar“ atvejis parodė ankstyvo aptikimo ir žalos plitimo ribojimo svarbą

GYNYBOS PRINCIPAI

1

Partnerių prieiga yra nepatikima

fišingui atsparus MFA, „Just-in-time“ prieiga, segmentavimas

2

Ieškokite ilgalaikio buvimo požymių

Hipotezėmis, o ne vien IOC pagrindu paremta paieška

3

Ieškokite vidinės žvalgybos požymių

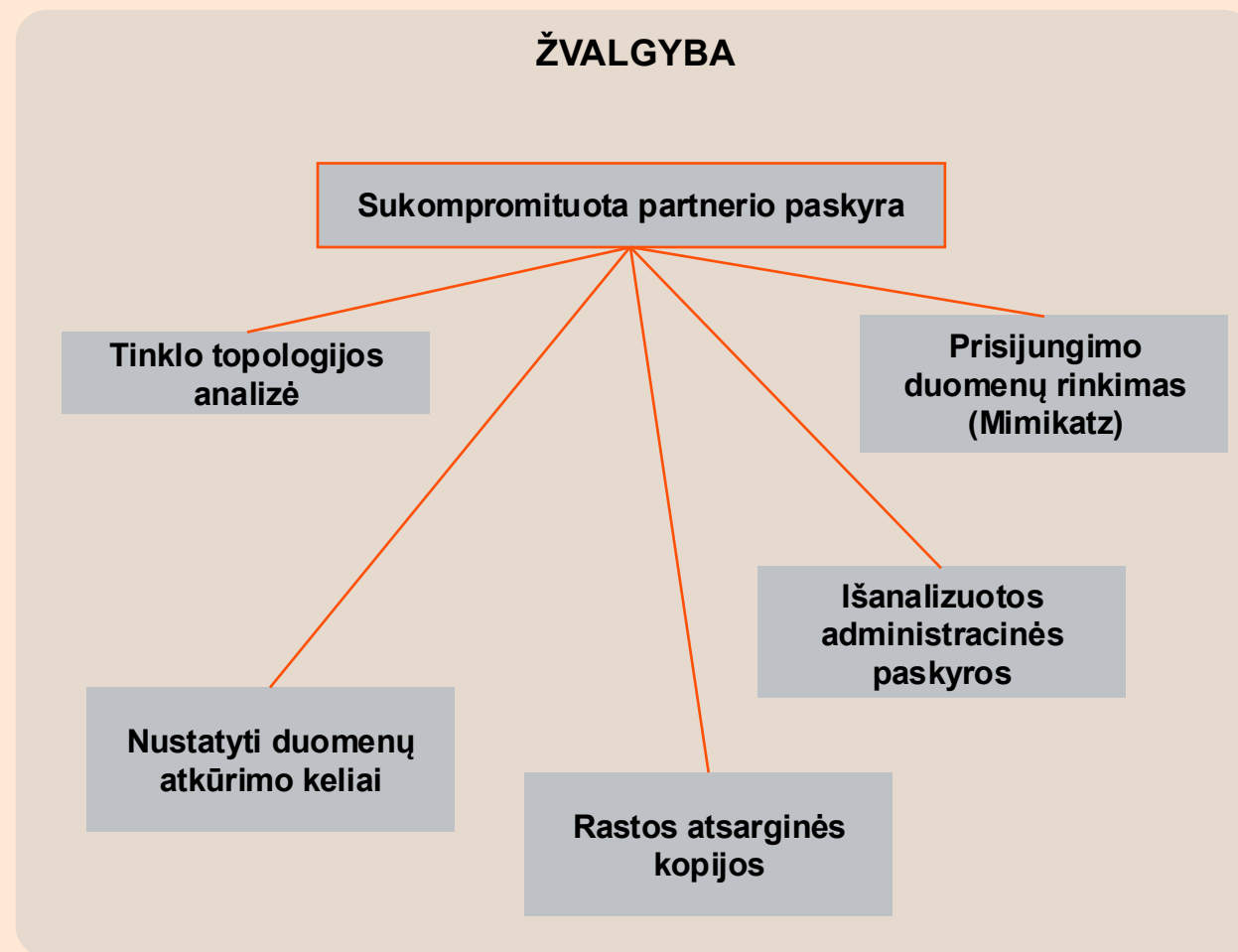
Prisijungimo duomenų rinkimas, tinklo skenavimas, atsarginių kopijų sekimas

4

Sutarkite krizės veiksmų eigą

kas gali išjungti ryšį 24 mln. vartotojų 6:30 ryto?

ŽVALGYBA



Penki klausimai rytojaus pokalbiui su kibernetinio saugumo komanda

1

Kaip valdytume incidentą likę be ryšio?

2

Kas veiktų praradus AD ar IdP?

3

Ar ieškome dar neaktyvuotų grėsmių?

4

Kaip greitai išjungtume pažeistą tiekėjo prieigą?

5

Ar esame išbandę visišką ištrynimą ir atkūrimą?



Yra dviejų tipų organizacijos: tos, kurių kontrolės buvo patikrintos krizės sąlygomis, ir tos, kurios vis dar mano, kad to nereikia.



Gediminas Černiauskas

Kibernetinio saugumo vadovas
PwC Lietuva

Nuoširdžiai dėkoju!

PwC Ukrainos kibernetinio saugumo komandai už aktualų turinį ir
įžvalgas iš pirmų lūpų.



 <https://www.linkedin.com/in/gediminascerniauskas>

Priedas: bendros įžvalgos iš kibernetinio karo Ukrainoje

- **Privatumas mirė:** plačiai paplitę duomenų nutekėjimai sunaikino asmeninį privatumą abiejose pusėse, jautri asmeninė informacija (vardai, adresai, pasų duomenys) tapo viešai prieinama informacija.
- **Anonimiškumas nyksta:** anoniminių įsilaužėlių era nyksta. Tiek konkuruojančios nusikalstamos grupės, tiek žvalgybos agentūros aktyviai viešina įsitraukusius asmenis, todėl tenka prisiimti asmeninę atsakomybę.
- **Mūšio lauko „Shadow IT“:** Milžiniškas, nevaldomas atakos paviršius, sukurtas kasdienių FPV dronų ir Starlink terminalų, nepriklausomas nuo centrinės IT ar saugumo priežiūros.
- **Viešojo ir privataus sektorių partnerystė, kuri veikia:** Pasitvirtino naujas, tikrai abipusiai naudingas modelis: kibernetinio saugumo tiekėjai nemokamai teikia Ukrainos įmonėms paslaugas mainais už neįkainojamą realių grėsmių telemetriją.
- **Tiekimo grandinė yra pagrindinis atakos kelias:** Kritinė infrastruktūra nuolat pažeidžiama per silpniausią grandį: mažiau saugius programinės įrangos tiekėjus ir IT rangovus, turinčius privilegijuotas prieigas.
- **Telegram paradoksas:** Programėlė su abejotinais savininkais ir valdymu, išlieka Ukrainos pagrindine informacijos platforma tiek oficialiems vyriausybės kanalams, tiek kasdieniams vartotojams.

Kontrolės, kurios atsilaikė

APSAUGOKITE VALDYMO APLINKĄ

- Laikykite AD, IdP, GPO, atsargines kopijas, hipervizorius ir EDR konsoles „Tier 0“ lygmeniu
- Fišingui atsparus MFA privilegijuotoms ir tiekėjų paskyroms
- Tiekėjų prieigos avariniai išjungikliai, akimirksniu atšaukiami incidento metu

SEGMENTUOKITE IR APRIBOKITE ŽALOS ZONĄ

- Naudotojų aplinkų, serverių, atsarginių kopijų zonų ir valdymo segmentų atskyrimas
- Griežta riba tarp IT ir OT su stebimais sąlyčio taškais
- Atsarginių kopijų infrastruktūra atskiroje tapatybės valdymo zonoje

GRĖSMIŲ PAIEŠKA TINKLE

- Hipotezėmis grįsta grėsmių paieška, ieškant kenkėjiškų programų ir neaktyvių paskyrų
- Vidinės žvalgybos stebėjimas: prisijungimo duomenų išgavimas, tinklo žemėlapių sudarymas, atsarginių kopijų inventorizacija
- Saugumo aptikimų derinimas pagal jūsų aplinką, o ne pagal bendrinius IOC

DARBAS SUTRIKDYTOMIS SĄLYGOMIS

- Ryšio kanalai ne pagrindiniame tinkle (out-of-band) ir neprisijungus pasiekiami (offline) reagavimo į incidentus įrankių rinkiniai
- Iš anksto patvirtinti įgaliojimai (kas turi teisę išjungti ryšį?)
- Simuliacijos, kurios prasideda nuo prielaidos, kad tinklo jau nebėra

UŽTIKRINKITE, KAD ATKŪRIMAS BŪTŲ ĮMANOMAS

- Nekeičiamos (immutable) ir neprijungtos (offline) atsarginės kopijos, izoliuotos nuo gamybinės tapatybės valdymo aplinkos
- Atkūrimo infrastruktūra atskiroje administracinėje aplinkoje
- Duomenų ištrynimo ir atkūrimo pratybos su destruktiviais atkūrimo testais