VILNIAUS UNIVERSITETAS
ŠIAULIŲ AKADEMIJA

INFORMACINIŲ TECHNOLOGIJŲ VALDYMO MAGISTRO STUDIJŲ PROGRAMA

KĘSTUTIS VENSKŪNAS

Magistro studijų baigiamasis darbas

KIBERNETINĖS SAUGOS PRIEMONIŲ TAIKYMAS TINKLO LYGMENYJE MVĮ NIS2 ATITIKČIAI, NAUDOJANT ATVIRO KODO SPRENDIMUS

Darbo vadovas (-ė) Asist. dr. Giedrimas Vaidas

Šiauliai, 2025

Studijuojančiojo, teikiančio baigiamąjį darbą, GARANTIJA

WARRANTY of Final Thesis

Vardas, pavardė *Name, Surname*	**Kęstutis Venskūnas**
Padalinys *Faculty*	**Šiaulių akademija** ***Šiauliai Academy***
Studijų programa *Study Programme*	**Informacinių technologijų valdymas** ***Information technology management***
Darbo pavadinimas *Thesis topic*	**Kibernetinės saugos priemonių taikymas tinklo lygmenyje MVĮ NIS2 atitikčiai, naudojant atviro kodo sprendimus** ***Application of Cybersecurity Measures at the Network Level for NIS2 Compliance in Small and Medium-Sized Enterprises Using Open-Source Solutions***
Darbo tipas *Thesis type*	**Baigiamasis darbas** ***Final Thesis***

Garantuoju, kad mano baigiamasis darbas yra parengtas sąžiningai ir savarankiškai, kitų asmenų indėlio į parengtą darbą nėra. Jokių neteisėtų mokėjimų už šį darbą niekam nesu mokėjęs. Šiame darbe tiesiogiai ar netiesiogiai panaudotos kitų šaltinių citatos yra pažymėtos literatūros nuorodose.

I guarantee that my thesis is prepared in good faith and independently, there is no contribution to this work from other individuals. I have not made any illegal payments related to this work. Quotes from other sources directly or indirectly used in this thesis, are indicated in literature references.

Aš, Kęstutis Venskūnas, pateikdamas (-a) šį darbą, patvirtinu (*pažymėti*) ☒

Embargo laikotarpis
Embargo Period

Prašau nustatyti šiam baigiamajam darbui toliau nurodytos trukmės embargo laikotarpį:
I am requesting an embargo of this thesis for the period indicated below:

☐ _____ mėnesių / *months*
(embargo laikotarpis negali viršyti 60 mėn. / *an embargo period shall not exceed 60 months*).

☒ Embargo laikotarpis nereikalingas / *no embargo requested.*

Embargo laikotarpio nustatymo priežastis / *Reason for embargo period*:

VILNIAUS UNIVERSITETO ŠIAULIŲ AKADEMIJOS DIRBTINIO INTELEKTO ĮRANKIŲ NAUDOJIMO RAŠTO DARBUOSE DEKLARACIJA

Vardas, pavardė:___Kęstutis_Venskūnas_____
Studijų programa, kursas:_ Informacinių technologijų valdymas [6211BX001],_____
Rašto darbo pavadinimas:_ Kibernetinės saugos priemonių taikymas tinklo lygmenyje MVĮ NIS2 atitikčiai, naudojant atviro kodo sprendimus_____
Rašto darbo tipas *(pvz., referatas, kursinis darbas, baigiamasis darbas):* _baigiamasis darbas_____
Modulio / dalyko pavadinimas *(išskyrus baigiamojo darbo atveju):*

_____
Deklaracijos pateikimo data___2025_12_16_____

Patvirtinu, kad vertinimui pateiktas savarankiškai atliktas rašto darbas yra parengtas laikantis Vilniaus universiteto Akademinės etikos kodekso[1], Vilniaus universiteto studijuojančiųjų rašto darbų rengimo, gynimo ir kaupimo nuostatai[2], Vilniaus universiteto Šiaulių akademijos rašto darbų rengimo ir gynimo tvarkos[3] ir Dirbtinio intelekto naudojimo Vilniaus universitete gairių[4].
Pažymiu, kad rašto darbo rengimui *buvo naudojami / nebuvo naudojami (pabraukti tinkamą variantą)* generatyvinio dirbtinio intelekto (toliau - DI) įrankiai.
Tuo atveju, jei darbo rengimui buvo pasitelkti DI įrankiai, pateikiu tikslią ir išsamią informaciją apie jų naudojimo tikslus ir apimtį:

1. DI įrankiai:

   - Naudoti įrankiai (pvz.: Connected Papers, Midjourney, GitHub Copilot ar kiti, *įrašyti*): _____Copilot_____
   - Naudojimo tikslas (duomenų rinkimas, redagavimas, vertimas, priedų generavimas ar kitas, *įrašyti*):_____Naudotas kaip papildomas paieškos varikliukas akademinės literatūros bazės, tiek Google paieškos rezultatų tikrinimui. _____

2. Esminiai DI panaudojimo atvejai:

Darbo dalis/vieta (puslapis, pastraipa)	Naudojimo tikslas	Užklausų pavyzdžiai

[1] Vilniaus universiteto akademinės etikos kodeksas, https://www.vu.lt/site_files/Akademines_etikos_kodeksas_suvestine_redakcija.pdf

[2] Vilniaus universiteto studijuojančiųjų rašto darbų rengimo, gynimo ir kaupimo nuostatai, 2024-05-21_Studijuojanciuju_RD_rengimo_gynimo_ir_kaupimo_nuostatai.pdf

[3] Vilniaus universiteto Vilniaus universiteto Šiaulių akademijos rašto darbų rengimo ir gynimo tvarka, https://www.sa.vu.lt/external/sa/files/Studiju_skyrius/VUSA_Rasto_darb%C5%B3_rengimo_ir_gynimo_tvarka_2024.pdf

[4] Dirbtinio intelekto naudojimo Vilniaus universitete gairės, https://www.vu.lt/site_files/SPN-54_2024_priedas.pdf

3. Savarankiškumas ir autorystė:

   - Patvirtinu, kad esu atsakingas(-a) už rašto darbo savarankiškumą ir autorystę: visos DI sugeneruotos rašto darbo dalys mano atidžiai patikrintos, patikslintos, pataisytos ir pažymėtos literatūros nuorodose. Darbas parengtas užtikrinant jame pateikiamų DI įrankiais sugeneruotų teksto dalių ir (ar) priedų tikslumą, patikimumą ir korektiškumą;

   - Patvirtinu, kad DI įrankiai nenaudoti darbe pateikiamų duomenų, informacijos, autorių minčių klastojimui, iškraipymui ar kitokio pobūdžio klaidinančiam pateikimui.

4. Akademinė etika:

   - Patvirtinu, kad pateikta informacija apie DI įrankių naudojimą yra tiksli ir išsami;

   - Patvirtinu, kad DI įrankiai naudoti savarankiško duomenų rinkimo, tyrimo, analizės, teksto ar priedų (*pabraukti tinkamą; jei reikia, įrašyti papildomą informaciją*_____) (pa)pildymui, o ne kaip savarankiško darbo pakaitalas;

   - Suprantu, kad nenurodytas DI įrankių naudojimas gali būti laikomas draudimo plagijuoti pažeidimu, kuris numatytas Vilniaus universiteto Akademinės etikos kodekse.

TURINYS

SANTRAUKA

NIS2/TIS2 direktyvos įsigaliojimas didina reikalavimus MVĮ kibernetinio saugumo valdymui, tačiau praktinių, finansiškai pagrįstų atviro kodo sprendinių diegimo ir vertinimo pavyzdžių tinklo lygmenyje trūksta.

Šio darbo tikslas – ištirti atviro kodo sprendimus, skirtus tinklo pažeidžiamumų, atakos vektorių ir kibernetinių incidentų identifikavimui bei užkardymui, ir sukurti MVĮ pritaikomą prototipą NIS2 21 straipsnio reikalavimų kontekste.

Darbas apima NIS2, ENISA gairių ir susijusių standartų literatūros analizę, laboratorinį eksperimentą, lyginamąją analizę bei indukcinį vertinimą.

Praktinėje dalyje sukonstruota izoliuota aplinka, kurioje integruota ugniasienė pfSense (filtravimas ir srauto veidrodinimas), NDR sensorius Zeek (protokolinė telemetrija ir anomalijų aptikimas), SIEM ELK (logų agregavimas, archyvavimas ir vizualizacijos), Nmap (pažeidžiamumų ir SSH bruteforce scenarijai) ir iperf3 (apkrovos metrikos).

Prototipas buvo vertintas simuliuojant DoS ir bruteforce atakas prieš SSH paslaugą: abi atakos aptiktos, FAR sudarė 0 %, o MTTD siekė ~45 min (DoS) ir ~23 min (bruteforce), tačiau aptikimo laiką iškreipė ELK ingestavimo vėlavimai (30–60 min) ir foninis interneto triukšmas.

Centralizuoti Zeek ir tinklo įrenginių įvykiai ELK aplinkoje leido atkurti incidento laiko juostą ir suformuoti techninių įrodymų bazę, reikalingą incidentų analizės ir pranešimo procesams.

Vertinimas išryškino sprendinio privalumus: maži kaštai, lankstumas ir audituojami įvykių žurnalo detalumas, bei ribotumus: būtinybė nuolat derinti taisykles, riboti administracinių paslaugų prieigą (pvz.: per VPN / IP ribojimą) ir optimizuoti logų apdorojimo grandinę, kad sprendinys būtų efektyvus realiose eksploatacinėse sąlygose.

SUMMARY

The NIS2/TIS2 directive increases cybersecurity governance requirements for small and medium-sized organisations, yet practical, cost-effective implementation and evaluation cases of open-source network-level security solutions remain limited.

The aim of this thesis is to examine open-source solutions for identifying and mitigating network-level vulnerabilities, attack vectors, and cybersecurity incidents, and to develop an SME-applicable prototype in the context of NIS2 Article 21 requirements.

The study combines a literature review of NIS2, ENISA guidance and related standards with a laboratory experiment, comparative analysis and inductive evaluation.

In the practical part, an isolated test environment was implemented integrating a pfSense firewall (traffic filtering and mirroring), a Zeek NDR sensor (protocol-level telemetry and anomaly detection), an ELK SIEM stack (log aggregation, storage and visualisation), Nmap (vulnerability scanning and SSH bruteforce scenarios) and iperf3 (load and performance metrics).

The prototype was evaluated by simulating DoS and SSH bruteforce attacks against an SSH service: both attack scenarios were detected, the false alarm rate (FAR) was 0%, and the mean time to detect (MTTD) was approximately ~45 minutes for DoS and ~23 minutes for bruteforce; however, detection time was affected by ELK ingestion delays (30–60 minutes) and background Internet noise.

Centralised Zeek and network device events in ELK enabled incident timeline reconstruction and the formation of an evidence base required for incident analysis and reporting processes.

The evaluation highlighted key advantages—low cost, flexibility and auditable artefacts—as well as limitations, including the need for continuous tuning, restricting administrative service exposure (e.g., via VPN or IP allow-listing), and optimising the log processing pipeline to ensure operational effectiveness in real-world environments.

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

1. ACL (Access Control List) – prieigos kontrolės sąrašas, apibrėžiantis leidžiamus ir draudžiamus ryšius tinkle.
2. Anomalijų aptikimas – procesas, kurio metu nustatomi nukrypimai nuo įprasto tinklo ar sistemų elgesio.
3. Bruteforce ataka – automatizuoti, pasikartojantys autentifikacijos bandymai, siekiant atspėti naudotojo prisijungimo duomenis.
4. CPU (Central Processing Unit) – pagrindinis kompiuterio procesorius, atliekantis skaičiavimo operacijas.
5. CSIRT (Computer Security Incident Response Team) – komanda, atsakinga už kibernetinių saugumo incidentų valdymą ir reagavimą.
6. CSIRTs Network – Europos Sąjungos CSIRT komandų bendradarbiavimo tinklas.
7. DoS (Denial of Service) – paslaugos trikdymo ataka, kurios tikslas – padaryti paslaugą nepasiekiamą teisėtiems naudotojams.
8. EDR (Endpoint Detection and Response) – galinių įrenginių saugumo sprendimas, skirtas incidentų aptikimui ir reagavimui.
9. ELK (Elasticsearch, Logstash, Kibana) – atviro kodo platforma, skirta logų rinkimui, indeksavimui ir vizualizavimui.
10. ENISA (European Union Agency for Cybersecurity) – Europos Sąjungos kibernetinio saugumo agentūra.
11. EU-CyCLONe (European Cyber Crisis Liaison Organisation Network) – ES kibernetinių krizių koordinavimo ryšių tinklas.
12. FAR (False Alarm Rate) – klaidingų aliarmų rodiklis, parodantis klaidingai sugeneruotų perspėjimų dalį.
13. IDS (Intrusion Detection System) – įsibrovimų aptikimo sistema, skirta identifikuoti galimus saugumo incidentus.
14. IDPS (Intrusion Detection and Prevention System) – įsibrovimų aptikimo ir prevencijos sistema.
15. Incidento laiko juosta – nuoseklus incidento įvykių atkūrimas pagal laiko žymas loguose.
16. ISMS (Information Security Management System) – informacijos saugumo valdymo sistema.
17. ISO/IEC 27001 – tarptautinis informacijos saugumo valdymo sistemos standartas.

18. Logų koreliacija – skirtingų sistemų įvykių susiejimas į vieną loginį incidento vaizdą.
19. MTTD (Mean Time to Detect) – vidutinis laikas nuo incidento pradžios iki jo aptikimo.
20. MVĮ – mažos ir vidutinės įmonės.
21. NDR (Network Detection and Response) – tinklo srauto analizės sprendimas, skirtas incidentų aptikimui ir reagavimui.
22. NIS2 – Europos Sąjungos direktyva (ES) 2022/2555 dėl tinklo ir informacinių sistemų saugumo.
23. NKSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos.
24. Nmap – atviro kodo tinklo skenavimo įrankis, naudojamas prievadų, paslaugų ir pažeidžiamumų analizei.
25. NSE (Nmap Scripting Engine) – Nmap scenarijų variklis, leidžiantis automatizuoti saugumo testus.
26. NTP (Network Time Protocol) – laiko sinchronizavimo protokolas.
27. Pasyvi tinklo stebėsena – tinklo srauto analizė, nedarant tiesioginės įtakos perduodamiems duomenims.
28. pfSense – atviro kodo ugniasienė ir maršrutizatorius, naudojamas tinklo filtravimui ir srauto veidrodinimui.
29. Port mirroring (SPAN) – tinklo srauto kopijavimo funkcija, leidžianti perduoti srautą stebėsenos sistemoms.
30. SIEM (Security Information and Event Management) – saugumo įvykių ir informacijos valdymo sistema.
31. SSH (Secure Shell) – saugus nuotolinio prisijungimo protokolas.
32. Techniniai įrodymai – audituojami artefaktai (logai, konfigūracijos, testų rezultatai), pagrindžiantys saugumo priemonių veikimą.
33. Zeek – atviro kodo NDR sprendimas (anksčiau „Bro“), skirtas protokolų lygmens tinklo srauto analizei.
34. Zero Trust – saugumo architektūros principas, grindžiamas nuolatiniu prieigos tikrinimu ir minimaliu pasitikėjimu.

ĮVADAS

NIS2 direktyva (ES 2022/2555), skirta apsaugoti ES piliečius, tiek kitus paveiktus asmenis nuo galimų kibernetinių incidentų ir grėsmių, bei sukuria vieningą teisinę struktūrą, skirtą sustiprinti kibernetinį saugumą Europos Sąjungoje [1]. Ji pakeičia ankstesnę NIS1 direktyvą ir išplečia taikymo sritį, apimdama 18 strategiškai svarbių sektorių.

Direktyva įpareigoja valstybes nares:

1. Kurti nacionalines kibernetinio saugumo strategijas, įskaitant tiekimo grandinių apsaugą, pažeidžiamumų valdymą ir švietimą.
2. Bendradarbiauti su ES institucijomis tarpvalstybiniam reagavimui ir priežiūrai.
3. Reguliariai atnaujinti esminių paslaugų teikėjų sąrašą.
4. Užtikrinti, kad įmonės taikytų rizikos valdymo priemones ir praneštų apie incidentus.

NIS2 stiprina priežiūros ir įgyvendinimo mechanizmus, siekiant aukštesnio bendro kibernetinio saugumo lygio visoje ES. Tam įkurtas tarpvalstybinis „CSIRTs“ - ES kompiuterinio saugumo incidentų reagavimo komandų tinklas, kuriam priskirtos informacijos apsikeitimo, kibernetinių incidentų valdymo funkcijos [2]. Ypač didelio masto kibernetinėms atakoms įkurtas „EU-CyCLONe“ – Europos kibernetinių krizių ryšių organizacijų tinklas. Jo tikslas, koordinuoti veiksmus tarp ES valstybių narių, įtraukiant ir „CSIRTs“ narius, vykstant ypatingo dydžio kibernetinėms atakoms [3].

„CSIRTs“ vaidmenį Lietuvoje atlieka „NKSC“ - Nacionalinis kibernetinio saugumo centras, kuriam priskirtas NIS2 direktyvos įgyvendinimas, bei priežiūra.

Šiame darbe koncentruosimės į direktyvos 21 straipsnį, kuriame nurodyti techniniai reikalavimai jos atitikčiai.

Darbo problema: Nėra aiškaus, efektyvaus ir finansiškai pagrįsto mechanizmo tinklo pažeidžiamumų, atakos vektorių aptikimui ir jų užkardymui mažo, bei vidutinio dydžio įmonių IT infrastruktūrose.

Darbo objektas: Praktinis atviro kodo sprendimų panaudojimas tinklo dalies pažeidžiamumų identifikavimui, bei jų užkardymui.

Magistrinio darbo tikslas yra ištirti atviro kodo sprendimus, skirtus tinklo dalies kibernetinių incidentų identifikavimui, bei užkardymui. Įgyvendinti sprendinį, pritaikyti smulkaus ir vidutinio dydžio organizacijų infrastruktūrai.

Darbo uždaviniai:

1. Atlikti atviro kodo NIS2 atitikties sprendinių literatūros analizę.

2. Nustatyti iššūkius, su kuriais susiduriama įgyvendinant atviro kodo technologijos sprendimus reglamento atitikčiai.
3. Panaudojant atviro kodo technologijas, sukurti sprendinį tinklo pažeidžiamumų skanavimui, incidentų identifikavimui ir užkardymui.
4. Atlikti prototipo privalumų ir trūkumų vertinimą.

Tyrimo metodai. Darbo tikslui pasiekti taikomi literatūros analizės, eksperimento, lyginamosios analizės bei indukcijos metodai.

1. NIS2/TIS2 TECHNOLOGINIŲ REIKALAVIMŲ SANTRAUKA MVĮ KONTEKSTE

1.1. NIS2 taikymo sritis MVĮ sektoriuje

Subjektų, kuriems taikomas reglamentas, klasifikacija priklauso ne tik nuo sektoriaus, bet ir nuo organizacijos dydžio (taikoma jei įmonėje yra > 50 darbuotojų arba > 10 mln. EUR apyvarta), išskyrus kai kuriuos kritinius subjektus (pvz.: sveikatos sektorių) [4][5]. Remiantis statistikos departamento duomenimis apie 3000 smulkaus ir vidutinio dydžio įmonių Lietuvoje atitinka darbuotojų kriterijų, o apie 4400 įmonių juos atitinka pagal pajamas [6].

1.1.1. Esminiai subjektai pagal NIS2 direktyvos I priedą. Šiems subjektams taikomi griežčiausi saugumo ir priežiūros reikalavimai, nes jų veikla yra laikoma kritiškai svarbia visuomenei, ekonomikai ir valstybės saugumui:

1.1.1.1. Energetika

1.1.1.1.1. Elektros energijos gamyba, tiekimas, perdavimas.

1.1.1.1.2. Gamtinių dujų importas, paskirstymas.

1.1.1.1.3. Naftos gavyba, perdirbimas, tiekimas.

1.1.1.1.4. Šilumos energijos tiekimas.

1.1.1.2. Transportas

1.1.1.2.1. Oro uostų operatoriai ir oro navigacijos paslaugos.

1.1.1.2.2. Geležinkelių infrastruktūros ir vežimo paslaugų tiekėjai.

1.1.1.2.3. Vidaus vandenų ir jūrų transporto paslaugų teikėjai.

1.1.1.2.4. Kelių transporto tinklų valdytojai.

1.1.1.3. Bankininkystė

1.1.1.3.1. Kredito įstaigos.

1.1.1.4. Finansų rinkų infrastruktūra

1.1.1.4.1. Prekybos vietos.

1.1.1.4.2. Centriniai kliringo partneriai

1.1.1.4.3. Atsiskaitymo sistemos.

1.1.1.5. Sveikatos sektorius

1.1.1.5.1. Ligoninės, klinikos.

1.1.1.5.2. Privatūs sveikatos paslaugų teikėjai.

1.1.1.5.3. Laboratorijos.

1.1.1.5.4. Biotechnologijų įmonės.

1.1.1.5.5. Vakcinų ir vaistų gamintojai.

1.1.1.6. Geriamojo vandens tiekimas.

1.1.1.7. Nuotekų valymas.

1.1.1.8. Skaitmeninė infrastruktūra:

1.1.1.8.1. Interneto mainų taškai (IXP).

1.1.1.8.2. DNS paslaugų teikėjai.

1.1.1.8.3. Duomenų centrų ir debesijos infrastruktūros paslaugų teikėjai.

1.1.1.9. Viešojo administravimo institucijos:

1.1.1.9.1. Centrinės, regioninės ir savivaldybių valdžios institucijos.

1.1.1.10. Kosmoso paslaugos:

1.1.1.10.1. Kritinės palydovinės paslaugos, kurių sutrikdymas gali turėti poveikį saugumui.

1.1.2. Svarbūs subjektai pagal NIS2 direktyvos II priedą, tai svarbios, bet ne kritinės paslaugas teikiančios organizacijos. Jiems taikomi tokie pat saugumo reikalavimai, bet priežiūra vykdoma tik kilus pagrįstam įtarimui:

1.1.2.1. Pašto ir siuntų paslaugos.

1.1.2.2. Pašto siuntų surinkimas, rūšiavimas, pristatymas.

1.1.2.3. Atliekų tvarkymas.

1.1.2.4. Atliekų surinkimas, perdirbimas, šalinimas.

1.1.2.5. Cheminių medžiagų gamyba ir platinimas.

1.1.2.6. Maisto tiekimo grandinė.

1.1.2.7. Maisto produktų gamyba, perdirbimas, didmeninė prekyba.

1.1.2.8. Gamybos sektorius.

1.1.2.9. Vaistų gamyba.

1.1.2.10. Medicinos prietaisų gamyba.

1.1.2.11. Kompiuterių, elektronikos gamyba.

1.1.2.12. Transporto priemonių gamyba.

1.1.2.13. Skaitmeninės paslaugos.

1.1.2.14. Internetinės paieškos sistemos.

1.1.2.15. Internetinės prekyvietės (marketplaces).

1.1.2.16. Socialinės platformos.

1.1.2.17. Mokslinių tyrimų veikla.

1.1.2.18. Institucijos, vykdančios strateginius ar su kritine infrastruktūra susijusius tyrimus.

1.1.2.19. Telekomunikacijų paslaugos.

1.1.2.20. Viešieji elektroninių ryšių tinklai ir paslaugų tiekėjai.

1.2. Būtinosios organizacijų pareigos pagal LR įstatymus

Remiantis „LR kibernetinės saugos įstatymu“ visoms organizacijoms, kurios patenka į nacionalinį esminių ar svarbių subjektų sąrašą, tvirtinamą Nacionalinio kibernetinio saugumo centro (NKSC) taikomos šios prievolės [7]:

1.2.1.1. Rizikų valdymo pareigos. Organizacijos privalo atlikti informacinių ir ryšių technologijų (IRT) saugumo rizikos vertinimą. Įgyvendinti tinkamas technines ir organizacines saugumo priemones, atitinkančias:

1.2.1.1.1. NIS2 direktyvos 21 straipsnį.

1.2.1.1.2. ENISA rekomendacijas.

1.2.1.1.3. Vertinimą atnaujinti bent kartą per metus po reikšmingų pokyčių (pvz., naujų sistemų diegimo).

1.2.1.1.4. Papildomai reikalaujama dokumentuoti priemones (politikas, planus) ir saugoti jų versijas.

1.2.1.2. Incidentų valdymo pareigos. Organizacija įpareigojama turėti incidentų valdymo procedūras, kurios apimtų:

1.2.1.2.1. Aptikimą.

1.2.1.2.2. Vertinimą.

1.2.1.2.3. Pranešimą.

1.2.1.2.4. Atsaką.

1.2.1.2.5. Atsigavimą.

1.2.1.3. Įpareigojimas laikytis incidentų pranešimo terminų:

1.2.1.3.1. Per 24 val. nuo žinojimo apie incidentą – preliminarus pranešimas NKSC.

1.2.1.3.2. Per 72 val. – išsamus pranešimas.

1.2.1.3.3. Per 1 mėnesį – baigiamoji ataskaita su įgyvendintomis priemonėmis.

1.2.1.4. Užtikrinti komunikaciją ir grįžtamąjį ryšį su prižiūrinčiomis institucijomis:

1.2.1.4.1. CSIRT-LT (NKSC).

1.2.1.4.2. EU-CyCLONe ar kitomis ES institucijomis, jei incidentas turi tarpvalstybinį poveikį.

1.2.1.5. Taip pat įvedama CISO rolė (už kibernetinę saugą atsakingo asmens vaidmuo pagal Lietuvos teisės aktus ir ENISA rekomendacijas):

1.2.1.5.1. Subjektai (organizacijos) privalo paskirti atsakingą asmenį už kibernetinį saugumą. Dažniausiai tai CISO (angl. Chief Information Security Officer) arba kibernetinio saugumo vadovas. Pareigybės gali turėti panašų

pavadinimą (pvz.: informacinės saugos pareigūnas, ar kibernetinės saugos pareigūnas), tačiau apibrėžtos atsakomybės identiškos CISO rolei.

1.2.1.5.2. CISO atsako už:

1.2.1.5.2.1. Rizikų vertinimo vykdymą ir priežiūrą.

1.2.1.5.2.2. Incidentų valdymo plano parengimą.

1.2.1.5.2.3. Informacijos teikimą valstybinėms institucijoms.

1.2.1.5.2.4. Ataskaitų rengimą pagal NKSC reikalavimus.

1.2.1.5.2.5. Saugumo švietimo organizavimą įmonės viduje.

1.2.1.5.3. Jeigu organizacijoje nėra galimybių turėti pilno etato CISO, leidžiama:

1.2.1.5.3.1. Sudaryti sutartį su išoriniu ekspertu.

1.2.1.5.3.2. Naudoti bendrą CISO funkciją kelioms įmonėms (grupės lygiu).

1.2.2. Atsakomybė ir sankcijos. Remiantis „LR kibernetinės saugos įstatymu“ (po NIS2 įgyvendinimo) už NIS2 reikalavimų nesilaikymą gali būti taikomos:

1.2.2.1.1. Administracinės baudos.

1.2.2.1.2. Veiklos ribojimai.

1.2.2.1.3. Viešas įspėjimas.

1.2.2.2. Nesilaikant reikalvimų, taikoma maksimali bauda esminiams subjektams:

1.2.2.2.1. Iki 10 mln. EUR arba 2 % metinės apyvartos (atsižvelgiant į tai, kuri suma didesnė).

1.2.2.3. Svarbiems subjektams:

1.2.2.3.1. iki 7 mln. EUR arba 1,4 % apyvartos.

1.2.2.3.2. Už pakartotinį ar sąmoningą pažeidimą gali būti taikomas didesnio griežtumo vertinimas bei valstybinis auditas.

1.3. Techninės kontrolės pagal NIS2 21 straipsnį

Šiame poskyryje aprašomos techninės kontrolės priemonės, kurios praktiniu lygmeniu padeda įgyvendinti NIS2 21 straipsnyje nustatytus kibernetinio saugumo rizikų valdymo reikalavimus. Dėmesys sutelkiamas į mažųjų ir vidutinių įmonių (MVĮ) kontekstą, kuriame dažnai būtina rinktis priemones, užtikrinančias adekvatų saugumo lygį ribotų išteklių sąlygomis.

1.3.1. Tinklo stebėjimas.

Tinklo stebėsenos tikslas – rinkti, analizuoti ir koreliuoti su tinklo srautu susijusius duomenis, leidžiančius identifikuoti įtartinus veiklos modelius tiek perimetro sraute (angl. *north–south*), tiek vidinio tinklo komunikacijoje (angl. *east–west*).

1.3.1.1. Reikalavimai pagal NIS2. Tinklo stebėsenos priemonėmis rekomenduotina užtikrinti:

1.3.1.1.1. Įeinančio ir išeinančio srauto stebėseną, prioritetą teikiant kritinių sistemų segmentams;

1.3.1.1.2. Saugumo įvykių fiksavimą, analizę ir tarpusavio koreliaciją;

1.3.1.1.3. Automatizuotų įspėjimų generavimą bei žurnalų analizę.

1.3.1.2. MVĮ atviro kodo tinklo saugos sprendimų pavyzdžiai:

1.3.1.2.1. Zeek (anksčiau – Bro) – išplėstinė tinklo telemetrija ir protokolų (pvz., HTTP, DNS, TLS/SSL, SMB) analizė [28].

1.3.1.2.2. Suricata – IDS/IPS sprendimas, paremtas taisyklėmis (pvz., *ET Pro* / *ET Open*).

1.3.1.2.3. Wazuh + ELK – centralizuotas įvykių rinkimas ir analizė (SIEM), įskaitant tinklo žurnalų indeksavimą [29].

1.3.1.2.4. Arkime – paketų fiksavimas ir paieška, orientuota į PCAP analizės scenarijus.

1.3.1.2.5. ntopng – realaus laiko srautų analizė ir statistinis profiliavimas.

1.3.2. Tinklo sauga.

MVĮ aplinkoje tinklo stebėsena gali veikti kaip kompensacinė priemonė tais atvejais, kai nėra galimybių pilnai diegti galutinių įrenginių aptikimo ir reagavimo (EDR) sprendimų; tokiu būdu tinklo telemetrija ir įvykių koreliacija prisideda prie aptikimo bei incidentų valdymo gebėjimų stiprinimo, siejamų su NIS2 21 straipsnio nuostatomis.

1.3.2.1. Pagrindinis tikslas. Pažeidžiamumų identifikavimo tikslas – sistemingai aptikti nevaldytus ar netinkamai sukonfigūruotus įrenginius, atviras paslaugas, operacinių sistemų ir taikomųjų komponentų pažeidžiamumus bei konfigūracijų spragas.

1.3.2.2. Reikalavimai pagal NIS2.

1.3.2.2.1. Reglamento praktiniam įgyvendinimui tinklo dalyje aktualu:

1.3.2.2.1.1. Periodiškai vykdyti pažeidžiamumų skenavimą.

1.3.2.2.1.2. Dokumentuoti identifikuotus pažeidžiamumus, nurodant CVE identifikatorius, CVSS vertinimus ir taikomas valdymo, užkardymo priemones (pvz., pataisas, konfigūracinius pakeitimus).

1.3.2.2.1.3. Vertinti pažeidžiamumus tiek operacinių sistemų, tiek tinklo paslaugų lygmeniu.

1.3.2.3. MVĮ sprendimų pavyzdžiai:

1.3.2.3.1. OpenVAS / Greenbone – tinklo pažeidžiamumų skenavimas, taikant NVT (angl. *Network Vulnerability Tests*).

1.3.2.3.2. Trivy / Grype – konteinerių ir atvirojo kodo komponentų (OSS) pažeidžiamumų tikrinimas pagal CVE.

1.3.2.3.3. Nmap + NSE – prievadų, paslaugų ir OS identifikavimas, taikant NSE scenarijus.

1.3.2.3.4. Wazuh pažeidžiamumų detektoriai – integracija su CVE duomenų šaltiniais ir automatizuotas pažeidžiamumų inventorizavimas.

1.3.3. Tinklo skanavimas ir žurnalų rinkimas.

MVĮ infrastruktūrose neapsaugoti įrenginiai ir viešai pasiekiamos paslaugos dažnai sudaro pirminį atakos vektorių. Reguliarus tinklo skenavimas leidžia identifikuoti ne tik įrenginių pažeidžiamumus, bet ir infrastruktūros anomalijas (pvz., netikėtai atsiradusias paslaugas, nepagrįstai atvertus prievadus), kurios gali sudaryti prielaidas incidento eskalacijai, įskaitant šoninį judėjimą ar brutalaus prisijungimo bandymus (angl. Bruteforce attack).

1.3.3.1. Tikslas. Žurnalų rinkimo ir koreliacijos tikslas – centralizuoti iš tinklo saugumo priemonių gaunamus įvykius, vykdyti jų analizę bei koreliaciją ir, remiantis nustatytais kriterijais, formuoti incidentų įrašus ir įspėjimus.

1.3.3.2. MVĮ sprendimų pavyzdžiai.

1.3.3.2.1. Elasticsearch – žurnalų surinkimas ir indeksavimas iš Zeek, ugniasienių ir kitų šaltinių.

1.3.3.2.2. Logstash – žurnalų apdorojimas ir įvedimas (angl. *ingestion*), įskaitant tinklinius *syslog* įėjimus.

1.3.3.2.3. Kibana – vizualizavimas ir analitinė peržiūra grafinėje sąsajoje.

2. TEORINIS PAGRINDAS IR PRAKTINIO TINKLO SAUGUMO TAIKYMO GAIRĖS

2.1. ISVS/ISMS vaidmuo įgyvendinant tinklo saugumo kontrolės priemones MVĮ

Informacijos saugumo valdymo sistema (ISVS/ISMS) apibrėžia struktūrinį pagrindą, pagal kurį organizacijoje planuojamos, diegiamos, prižiūrimos ir tobulinamos tinklo saugumo kontrolės priemonės. ISMS kontekste tinklo saugumas vertinamas ne kaip atskirų techninių sprendimų rinkinys, bet kaip valdomas procesas, susietas su rizikos vertinimu, atsakomybėmis ir nuolatine priežiūra.

2.1.1. ISMS vaidmuo įgyvendinant tinklo saugumo kontrolės priemones pasireiškia per šiuos aspektus:

2.1.1.1. Rizikos pagrįstumas. ISMS nustato, kokios tinklo saugumo priemonės turi būti taikomos, remiantis rizikos vertinimo rezultatais, o ne technologiniu pasirinkimu savaime.

2.1.1.2. Valdymo struktūra. ISMS apibrėžia atsakomybes už tinklo saugumo kontrolės priemonių planavimą, konfigūravimą, peržiūrą ir keitimą.

2.1.1.3. Kontrolės gyvavimo ciklas. ISMS užtikrina, kad tinklo kontrolės priemonės būtų periodiškai peržiūrimos, atnaujinamos ir koreguojamos.

2.1.1.4. Dokumentavimas ir atsekamumas. ISMS reikalauja dokumentuoti tinklo architektūrą, taisykles ir jų keitimus, sudarant pagrindą techninių įrodymų rinkimui.

2.1.1.5. Incidentų valdymo sąsaja. ISMS susieja tinklo saugumo įvykių aptikimą su incidentų registravimo ir reagavimo procesais.

Mažo ir vidutinio dydžio organizacijų kontekste ISMS dažnai įgyvendinama supaprastinta forma, tačiau jos vaidmuo išlieka esminis. Be ISMS, tinklo saugumo kontrolės dažnai tampa fragmentiškos, sunkiai prižiūrimos ir nepakankamai pagrįstos rizikos požiūriu. ISMS leidžia MVĮ užtikrinti, kad net ribotų resursų sąlygomis tinklo saugumo priemonės būtų diegiamos nuosekliai ir tikslingai.

ISMS taip pat sudaro formalų pagrindą NIS2 reikalavimų įgyvendinimui, nes leidžia susieti technines tinklo saugumo kontrolės priemones su organizaciniais sprendimais ir pateikti jų veikimą pagrindžiančius techninius įrodymus. Tokiu būdu ISMS veikia kaip jungiamoji grandis tarp norminių NIS2 reikalavimų ir praktinio tinklo saugumo priemonių taikymo MVĮ aplinkoje.

2.2. Procesinis požiūris į tinklo saugumą

Procesinis požiūris į tinklo saugumą grindžiamas prielaida, kad tinklo saugumo užtikrinimas nėra vienkartinis techninių priemonių diegimo veiksmas, bet nuolatinis, valdomas ir cikliškai vykdomas procesas. Toks požiūris atitinka šiuolaikinių informacijos saugumo valdymo sistemų logiką ir leidžia integruoti tinklo saugumo kontrolės priemones į bendrą organizacijos rizikos valdymo sistemą.

Procesinis požiūris apima tarpusavyje susijusių veiklų visumą, kuri apibrėžia tinklo saugumo kontrolės priemonių planavimą, įgyvendinimą, eksploatavimą, stebėseną ir tobulinimą. Šios veiklos formuoja nuoseklų valdymo ciklą, užtikrinantį, kad tinklo saugumo priemonės išliktų veiksmingos kintančių grėsmių ir organizacijos aplinkos sąlygomis.

2.2.1. Pirmasis procesinio požiūrio etapas yra planavimas, kurio metu identifikuojamos tinklo lygmens rizikos, apibrėžiami saugomi informaciniai ištekliai ir nustatomos tinklo saugumo kontrolės priemonės. Planavimo etape formuojamas tinklo architektūros modelis, nustatomi tinklo segmentai, apibrėžiami leidžiami ryšiai ir pasirenkami incidentų aptikimo mechanizmai. Šiame etape priimti sprendimai turi būti pagrįsti rizikos vertinimu ir organizacijos veiklos poreikiais.

2.2.2. Antrasis etapas yra įgyvendinimas, kurio metu planuotos tinklo saugumo kontrolės priemonės realizuojamos techniniu lygmeniu. Tai apima tinklo segmentavimo konfigūravimą, prieigos kontrolės taisyklių diegimą, incidentų aptikimo sistemų įjungimą ir tinklo stebėsenos mechanizmų sukonfigūravimą. Įgyvendinimo etapas turi užtikrinti, kad techninės konfigūracijos atitiktų planavimo etape nustatytus reikalavimus.

2.2.3. Trečiasis etapas yra eksploatavimas, kurio metu tinklo saugumo kontrolės priemonės veikia kasdienėje aplinkoje. Šiame etape vykdoma tinklo stebėsena, analizuojami saugumo įvykiai, vertinami incidentų aptikimo signalai ir atliekami būtini operaciniai veiksmai. Eksploatavimo metu taip pat išryškėja praktiniai kontrolės priemonių trūkumai, pavyzdžiui, klaidingi pavojaus signalai ar per griežtos prieigos kontrolės taisyklės.

2.2.4. Ketvirtasis etapas yra stebėsena ir vertinimas, kurio metu vertinamas tinklo saugumo kontrolės priemonių efektyvumas. Šiame etape analizuojami techniniai rodikliai, tokie kaip incidentų aptikimo laikas, įvykių skaičius, žurnalų pilnumas ir tinklo srautų matomumas. Vertinimo rezultatai naudojami sprendžiant, ar esamos kontrolės priemonės atitinka nustatytus saugumo tikslus.

2.2.5. Paskutinis procesinio požiūrio etapas yra tobulinimas, kurio metu, remiantis vertinimo rezultatais ir įvykusiais incidentais, koreguojamos tinklo saugumo kontrolės priemonės. Tobulinimas apima prieigos kontrolės taisyklių peržiūrą, incidentų aptikimo

mechanizmų optimizavimą ir stebėsenos procesų pritaikymą prie naujų grėsmių. Šis etapas užtikrina nuolatinį tinklo saugumo brandos didinimą.

Mažo ir vidutinio dydžio organizacijų kontekste procesinis požiūris leidžia taikyti tinklo saugumo priemones proporcingai turimiems resursams. Vietoje plataus techninių sprendimų diegimo akcentuojamas aiškus procesų apibrėžimas, periodinės peržiūros ir įrodymais pagrįstas sprendimų priėmimas. Tokiu būdu procesinis požiūris sudaro praktinį pagrindą NIS2 direktyvos reikalavimų įgyvendinimui tinklo saugumo srityje [5].

2.3. Literatūros analizė tinklo saugumo valdymo srityje

Mokslinėje literatūroje tinklo saugumas vis dažniau analizuojamas ne kaip atskirų techninių sprendimų visuma, bet kaip valdomas procesas, integruotas į bendrą informacijos saugumo valdymo sistemą.

Tyrėjai pabrėžia, kad techninių tinklo kontrolės priemonių efektyvumas tiesiogiai priklauso nuo to, kaip jos parenkamos, eksploatuojamos ir prižiūrimos organizaciniame kontekste (Behl & Behl, 2017; Siponen & Willison, 2009) [9].

Didelė dalis tinklo saugumo valdymo tyrimų skirta įsibrovimų aptikimo sistemoms (IDS) ir tinklo srauto stebėsenai. Ankstyvieji Paxson (1999) darbai, kuriais buvo sukurti „Bro“ sistemos (dabartinio Zeek) pagrindai, pabrėžė pasyvios tinklo stebėsenos svarbą ir atskyrė techninį mechanizmą nuo saugumo politikos [12]. Šis požiūris vėliau tapo pagrindu tinklo saugumo valdyme, nes leido organizacijoms taikyti aptikimo mechanizmus nepriklausomai nuo galinių įrenginių saugumo būklės.

Vėlesnėje literatūroje didelis dėmesys skiriamas anomalijų aptikimui ir elgseninei analizei. Tačiau Sommer ir Paxson (2010) kritiškai vertina akademiniuose tyrimuose demonstruojamus rezultatus, pažymėdami, kad laboratorinėmis sąlygomis pasiektas aptikimo tikslumas dažnai nėra perkeliamas į realias organizacines aplinkas [15]. Autoriai teigia, kad realiuose tinkluose „normalus“ elgesys yra dinamiškas, o tai apsunkina patikimų anomalijų modelių kūrimą ir palaikymą. Ši kritika ypač aktuali MVĮ kontekste, kur trūksta resursų sudėtingų modelių priežiūrai.

IDS efektyvumo valdymo problematika taip pat nagrinėjama per klaidingų aliarmų prizmę. Axelsson (2000) suformuluota bazės dažnio problema parodo, kad net ir aukšto tikslumo aptikimo sistemos, esant retoms atakoms, generuoja didelį klaidingų perspėjimų (angl. false positives) skaičių [8]. Šis reiškinys literatūroje įvardijamas kaip vienas pagrindinių operacinių iššūkių, nes reikalauja nuolatinio triažo, taisyklių derinimo ir prioritetų nustatymo. Todėl tinklo saugumo valdymas apima ne tik aptikimo technologijas, bet ir procesus, skirtus perspėjimų kokybei palaikyti.

Segmentavimo ir prieigos kontrolės tematika literatūroje siejama su atakų plitimo ribojimu ir lateral movement mažinimu. NIST Zero Trust Architecture koncepcija pabrėžia, kad implicitinis

pasitikėjimas pagal tinklo vietą turi būti pakeistas aiškiai apibrėžtomis politikomis ir srautų ribojimu [13]. Nors mikrosegmentavimo sprendimai literatūroje vertinami kaip veiksmingi, tyrimai taip pat nurodo jų diegimo ir palaikymo sudėtingumą bei poveikio verslo procesams riziką [11]. Tai leidžia daryti išvadą, kad MVĮ aplinkoje segmentavimas turi būti taikomas proporcingai, pasirenkant ribotą, bet valdomą saugumo zonų skaičių.

Tinklo saugumo valdymo literatūroje reikšmingą vietą užima žurnalų (log) valdymas ir atsekamumas. NIST SP 800-92 gairėse pabrėžiama, kad žurnalai yra būtini ne tik incidentų tyrimui, bet ir atitikties įrodymų formavimui (Kent & Souppaya, 2006). Tyrimai rodo, kad be centralizuoto logų rinkimo ir koreliacijos tinklo saugumo kontrolės tampa sunkiai patikrinamos ir neauditуojamos. Šis aspektas ypač aktualus NIS2 kontekste, kuriame reikalaujama ne tik taikyti saugumo priemones, bet ir gebėti pagrįsti jų veikimą techniniais įrodymais.

Apibendrinant literatūros analizę, galima teigti, kad tinklo saugumo valdymas grindžiamas trimis tarpusavyje susijusiais principais: matomumu, kontrole ir įrodymų atsekamumu. Literatūra pagrindžia, kad efektyvus tinklo saugumas MVĮ priklauso ne nuo maksimalios technologinės aprėpties, bet nuo gebėjimo valdyti pasirinktų kontrolės priemonių veikimą, sumažinti operacinį triukšmą ir užtikrinti objektyvius techninius įrodymus. Šios išvados sudaro teorinį pagrindą tolimesnei atviro kodo tinklo saugumo sprendimų analizei ir empiriniam jų vertinimui pagal NIS2 reikalavimus.

2.4. ENISA rekomenduojamos tinklo saugumo priemonės

ENISA 2025 m. birželio 26 d. paskelbtoje „NIS2 Technical Implementation Guidance“ (versija 1.0) tinklo saugumo priemonės pateikiamos kaip praktinės, neįpareigojančios rekomendacijos, skirtos padėti įgyvendinti Komisijos įgyvendinimo reglamente (ES) 2024/2690 detalizuotus NIS2 21 straipsnio (2) dalies kibernetinių rizikų valdymo reikalavimus. Šiame kontekste ENISA tinklo saugumo priemones interpretuoja kaip techninių ir metodologinių parametrų rinkinį, kuris turi būti diegiamas rizikos vertinimu grįstu būdu ir palaikomas periodiškomis peržiūromis bei įrodymais pagrįsta kontrole.

Pirma, ENISA tinklo saugumą sieja su bendra pareiga taikyti priemones, apsaugančias tinklo ir informacines sistemas nuo kibernetinių grėsmių, bei rekomenduoja remtis pripažintais tinklo saugumo standartais kaip atskaitos tašku (pvz., ISO/IEC 27033 serija) [18], [19], [20]. Praktiniu lygmeniu akcentuojama būtinybė turėti suprantamai ir aktualiai dokumentuotą tinklo architektūrą (topologiją), nes ji laikoma prielaida tiek rizikos vertinimui, tiek segmentavimo ir srautų kontrolės sprendinių audituojamumui.

Greta dokumentavimo ENISA tinklo saugumą sieja su administruojamomis taisyklėmis ir jų gyvavimo ciklu: rekomenduojama planuoti peržiūras, kurios apimtų nuolatinę tinklų stebėseną

realaus laiko grėsmėms, periodinius pažeidžiamumų skenavimus, ugniasienių ir kitų tinklo kontrolės priemonių taisyklių peržiūrą (pvz., kas mėnesį) ir periodinį viso tinklo vertinimą (pvz., kasmet). Šis peržiūrų principas atitinka valdomos kontrolės sampratą: tinklo saugumas laikomas ne statine konfigūracija, o palaikomu režimu, kuriame keitimai, patvirtinimai ir įgyvendinimo datos turi būti atsekami per įrašus ir audito žurnalus.

Antra, ENISA tinklo saugumo priemonių branduolį sudaro segmentavimas. Gairėse nurodoma, kad sistemos turi būti segmentuojamos į tinklus ar zonas pagal rizikos vertinimo rezultatus ir turi būti atskirtos nuo trečiųjų šalių sistemų bei tinklų.

Segmentavimo logika apibrėžiama ne vien kaip techninis VLAN ar potinklių sukūrimas, bet kaip rizikos pagrindu apibrėžtas prieigos suteikimas tinklo zonai, kritinių sistemų laikymas „saugiose zonose“ ir segmentavimo integravimas į tinklo diagramą kaip valdomą artefaktą.

ENISA taip pat akcentuoja segmentavimo peržiūrų būtinybę: segmentavimas turi būti peržiūrimas planuotais intervalais (gairėse pateikiama indikacija bent kartą per metus) ir po reikšmingų incidentų arba reikšmingų veiklos / rizikos pokyčių, o peržiūras siūloma pagrįsti testavimo įrodymais, tokiais kaip penetraciniai testai ar pažeidžiamumų vertinimai.

Trečia, ENISA tinklo saugumo priemones tiesiogiai susieja su aptikimu ir anomalijų identifikavimu tinklo lygmenyje. Gairėse, aptariant tinklo saugumo priemonių spektrą, kaip praktiniai pavyzdžiai minima IDS/IPS egzistencija ir (kur tinkama) sprendiniai, galintys rinkti bei analizuoti duomenis, siekiant aptikti anomalijas, įsilaužimus, eksfiltraciją ir pažangias grėsmes. Ši nuostata svarbi tuo, kad tinklo saugumo valdymas ENISA požiūriu apima ne tik prevenciją (filtravimą, segmentavimą), bet ir aptikimo funkciją bei jos išlaikymą per nuolatinį stebėsenos režimą ir taisyklių valdymą.

Ketvirta, ENISA tinklo saugumo priemonių įgyvendinimą sieja su stebėsena ir žurnalų (log) valdymu. Gairėse aiškiai nurodoma pareiga nustatyti procedūras ir naudoti įrankius veiklų stebėsenai ir registravimui, kad būtų aptinkami įvykiai, galintys būti laikomi incidentais, ir būtų galima laiku reaguoti mažinant poveikį.

ENISA rekomenduoja monitoringą ir loggingą pradėti nuo tikslų apibrėžimo (pavyzdžiui, grėsmių aptikimas, atitikties užtikrinimas, incidentų valdymo palaikymas, anomalijų aptikimas), o įrankių pasirinkimą grįsti praktiniais kriterijais, tokiais kaip naudojimo paprastumas, integracija su esama infrastruktūra, rankinio darbo minimizavimas ir gebėjimas rinkti duomenis iš įvairių šaltinių, įskaitant tinklus, sistemas ir aplikacijas.

Taip pat pabrėžiami techniniai patikimumo reikalavimai: laiko sinchronizacija (pvz., NTP/PTP protokolų pagalba), logų saugojimo ciklišKumas ir monitoringo/registravimo sistemų prieinamumo stebėjimas nepriklausomai nuo sistemų, kurias jos stebi. Galiausiai, procedūrų ir „kas registruojama“ (aparatinės/programinės įrangos sąrašo) peržiūra turi būti atliekama reguliariai (bent

kasmet) ir po reikšmingų incidentų, kas įvykių žurnalų (logų) valdymą paverčia audituojamu procesu, o ne vien techninių įrašų kaupimu.

Apibendrinant, ENISA rekomenduojamos tinklo saugumo priemonės iš esmės formuoja valdomą kontrolės modelį, kuriame tinklo architektūra dokumentuojama, segmentavimas ir srautų kontrolė grindžiami rizika, aptikimo priemonės integruojamos į nuolatinę stebėseną, o visas priemonių rinkinys palaikomas per planuotas peržiūras, pakeitimų apskaitą ir techninius įrodymus.

2.5. Gairių atitikimas NIS2 21 straipsniui

NIS2 direktyvos 21 straipsnis nustato pareigą esminėms ir svarbioms organizacijoms taikyti tinkamas ir proporcingas technines bei organizacines kibernetinių rizikų valdymo priemones.

Šiame straipsnyje sąmoningai neapibrėžiami konkretūs technologiniai sprendimai, bet įvardijamos funkcinės saugumo sritys ir pasiektini rezultatai, paliekant organizacijoms ir valstybėms narėms lankstumą pasirenkant įgyvendinimo būdus. ENISA parengtos techninio įgyvendinimo gairės veikia kaip tarpinis interpretacinis sluoksnis, kuris šiuos abstrakčius teisės akto reikalavimus perkelia į praktiškai taikytinus techninius ir metodologinius kriterijus.

Analizuojant ENISA gairių ir NIS2 21 straipsnio santykį, matyti, kad ENISA rekomendacijos struktūriškai atitinka straipsnyje įvardytas kibernetinių rizikų valdymo priemonių kategorijas. NIS2 21 straipsnio 2 dalyje numatytos priemonės, tokios kaip rizikos analizė, incidentų prevencija ir aptikimas, veiklos tęstinumo užtikrinimas, tiekimo grandinės saugumas, stebėsena ir incidentų valdymas, gairėse yra detalizuojamos per konkrečius techninius scenarijus, konfigūracijų principus ir tikėtinus įrodymų tipus. Tokiu būdu ENISA gairės nekuria naujų reikalavimų, bet išplečia ir operacionalizuoja jau egzistuojančius teisės akto reikalavimus.

Tinklo saugumo kontekste gairių atitikimas NIS2 21 straipsniui pasireiškia per aiškų ryšį tarp reikalaujamo saugumo tikslo ir rekomenduojamos techninės kontrolės. Pavyzdžiui, NIS2 reikalavimas užkirsti kelią incidentams ir sumažinti jų poveikį gairėse siejamas su tinklo segmentavimo, srautų filtravimo ir prieigos kontrolės priemonėmis. Incidentų aptikimo ir reagavimo reikalavimai gairėse detalizuojami per nuolatinės stebėsenos, IDS/IPS ar kitų aptikimo mechanizmų taikymą, taip pat per aiškiai apibrėžtus įvykių registravimo ir analizės procesus.

Stebėsenos ir atsekamumo reikalavimai atitinka NIS2 nuostatą dėl savalaikio incidentų nustatymo ir pranešimo, nes gairėse nurodoma, kokie žurnalai ir kokio detalumo duomenys turi būti renkami siekiant užtikrinti laiko, apimties ir poveikio įvertinimą.

Svarbus gairių ir NIS2 21 straipsnio atitikimo aspektas yra proporcingumo principas. NIS2 aiškiai įtvirtina, kad priemonės turi būti proporcingos organizacijos dydžiui, veiklos pobūdžiui ir rizikos lygiui. ENISA gairėse šis principas atsispindi per rekomendacijų pateikimą kaip „gerosios praktikos“ ir per galimybę taikyti skirtingo detalumo bei sudėtingumo kontrolės priemones. Tai

leidžia MVĮ taikyti bazines, tačiau valdomas tinklo saugumo priemones, neperžengiant jų operacinių ir finansinių galimybių, kartu išlaikant atitiktį teisės akto reikalavimams.

ENISA gairės (Priedas Nr.3) taip pat atitinka NIS2 21 straipsnio nuostatą dėl atskaitomybės ir patikrinamumo. NIS2 reikalauja, kad organizacijos galėtų pagrįsti taikomų priemonių veiksmingumą priežiūros institucijoms. Gairėse šis reikalavimas realizuojamas per techninių įrodymų koncepciją: kiekvienai rekomenduojamai priemonei pateikiami galimi artefaktai, tokie kaip konfigūracijų išrašai, tinklo architektūros schemos, stebėsenos ataskaitos ir įvykių žurnalai. Tokie artefaktai leidžia susieti abstraktų teisės normos reikalavimą su konkrečiu, patikrinamu techniniu rezultatu.

Apibendrinant galima teigti, kad ENISA techninės gairės veikia kaip praktinis NIS2 21 straipsnio įgyvendinimo instrumentas, kuris padeda užtikrinti nuoseklų ir vienodą teisės akto interpretavimą techniniame lygmenyje. Gairių atitikimas NIS2 21 straipsniui pasireiškia per struktūrinį reikalavimų atkartojimą, proporcingumo principo išlaikymą ir aiškų ryšį tarp saugumo tikslų, techninių kontrolės priemonių ir įrodymų. Dėl šių savybių ENISA gairės sudaro tinkamą teorinį ir metodologinį pagrindą tinklo saugumo kontrolės priemonių analizei ir empiriniam vertinimui MVĮ kontekste.

2.6. Reikalaujami techniniai įrodymai tinklo lygmenyje

NIS2 direktyvos taikymo kontekste techniniai įrodymai yra esminė priemonė, leidžianti organizacijoms pagrįsti ne tik formalią saugumo priemonių egzistenciją, bet ir jų faktinį veikimą. Skirtingai nuo deklaratyvių politikų ar procedūrų, techniniai įrodymai tinklo lygmenyje yra objektyvūs, patikrinami ir pakartojami duomenys, kuriuos galima naudoti tiek vidiniam vertinimui, tiek išoriniam auditui ar priežiūros institucijų patikrinimams. NIS2 21 straipsnis implikuoja pareigą organizacijoms gebėti parodyti, kad taikomos techninės priemonės realiai prisideda prie rizikos mažinimo ir incidentų valdymo, o ENISA techninio įgyvendinimo gairės šią pareigą operacionalizuoja per aiškiai apibrėžtus įrodymų tipus.

Tinklo saugumo srityje techniniai įrodymai pirmiausia siejami su tinklo architektūros ir segmentavimo dokumentacija. Tinklo topologijos schemos, saugumo zonų aprašymai, VLAN ar potinklių struktūros ir jų tarpusavio ryšiai sudaro bazinį įrodymų sluoksnį, leidžiantį patikrinti, ar segmentavimas iš tiesų įgyvendintas ir ar jis atitinka rizikos vertinimo rezultatus. Šie dokumentai turi būti aktualūs, t. y. atspindėti realią eksploatuojamą infrastruktūrą, ir susieti su konfigūracijomis, kurios faktiškai riboja tinklo srautus tarp segmentų.

Antras svarbus techninių įrodymų lygmuo apima tinklo srauto filtravimo ir prieigos kontrolės konfigūracijas. Ugniasienių taisyklių rinkiniai, prieigos kontrolės sąrašai ir tarpsegmentinių ryšių leidimų aprašymai leidžia patikrinti, ar tinklo prieigos kontrolė taikoma pagal „mažiausių privilegijų“

principą. Šios konfigūracijos taip pat sudaro pagrindą vertinti, ar leidžiami ryšiai yra pagrįsti verslo poreikiais ir ar jie periodiškai peržiūrimi. Techninių įrodymų kokybė šiuo atveju priklauso ne tik nuo taisyklių egzistavimo, bet ir nuo jų struktūros, nuoseklumo bei pakeitimų atsekamumo.

Trečiasis techninių įrodymų tipas susijęs su incidentų aptikimu tinklo lygmenyje. IDS, IPS ar NDR sprendimų generuojami įvykių žurnalai, perspėjimai ir metaduomenys leidžia patikrinti, ar organizacija turi realius gebėjimus aptikti kenkėjišką ar anomalų tinklo srautą. Šie įrodymai turi apimti ne tik aptikimo faktą, bet ir laiko žymas, leidžiančias įvertinti incidentų aptikimo savalaikiškumą. Tinklo aptikimo įrodymai ypač svarbūs NIS2 kontekste, nes jie sudaro pagrindą vėlesniam incidentų klasifikavimui ir pranešimo terminų laikymuisi.

Ketvirtasis techninių įrodymų sluoksnis apima stebėsenos ir žurnalų valdymo artefaktus. Centralizuoto logų rinkimo architektūra, logų šaltinių sąrašai, laiko sinchronizacijos sprendimai ir saugojimo politikos leidžia įvertinti, ar tinklo saugumo įvykiai yra renkami sistemingai ir ar jie gali būti koreliuojami. Tokie įrodymai yra būtini norint rekonstruoti incidentų eigą, įvertinti jų poveikį ir pagrįsti atliktus reagavimo veiksmus.

Akademinėje literatūroje pabrėžiama, kad be centralizuotos stebėsenos tinklo saugumo kontrolės tampa fragmentiškos ir sunkiai audituojamos, todėl logų valdymas laikomas viena iš kertinių techninių kontrolės sričių.

Papildomą techninių įrodymų kategoriją sudaro testavimo ir vertinimo rezultatai. Kontroliuojamų incidentų simuliacijų, penetracinių testų ar pažeidžiamumų vertinimų ataskaitos leidžia įvertinti, ar tinklo saugumo kontrolės priemonės veikia numatytais scenarijais. Šie įrodymai svarbūs tuo, kad jie parodo ne tik konfigūracijų egzistavimą, bet ir jų veiksmingumą realiomis arba imituotomis grėsmės sąlygomis.

Apibendrinant galima teigti, kad techniniai įrodymai tinklo lygmenyje sudaro daugiapakopį atitikties pagrindą, apimantį architektūrą, konfigūracijas, stebėsenos duomenis ir vertinimo rezultatus. Šių įrodymų visuma leidžia organizacijai ne tik deklaruoti, bet ir empiriškai pagrįsti NIS2 21 straipsnyje numatytų tinklo saugumo priemonių įgyvendinimą. MVĮ kontekste techninių įrodymų reikšmė yra ypač didelė, nes jie leidžia kompensuoti ribotus organizacinius resursus ir užtikrinti atitiktį per objektyvius, patikrinamus ir audituojamus duomenis.

2.7. ENISA gairių taikymo ribotumai MVĮ aplinkoje

ENISA parengtos NIS2 techninio įgyvendinimo gairės (Priedas Nr.3) pateikia išsamų kibernetinių rizikų valdymo priemonių modelį, tačiau jų praktinis taikymas mažų ir vidutinių įmonių aplinkoje susiduria su struktūriniais ribotumais. Gairėse numatomas saugumo brandos lygis dažnai grindžiamas prielaida apie pakankamus organizacinius ir žmogiškuosius resursus, kurių MVĮ paprastai neturi. Dėl to tokios veiklos kaip nuolatinė tinklo stebėsena, reguliarios konfigūracijų

peržiūros ir sistemingas dokumentavimas MVĮ dažnai vykdomos fragmentiškai arba reaguojant į incidentus, o ne kaip nuoseklaus valdymo dalis.

Technologiniu požiūriu ENISA gairės suponuoja pakankamai centralizuotą ir homogenišką infrastruktūrą, leidžiančią efektyviai taikyti segmentavimą, stebėseną ir centralizuotą žurnalų rinkimą. MVĮ aplinkoje dažnai vyrauja mišrios infrastruktūros, apimančios vietines sistemas, debesijos paslaugas ir trečiųjų šalių sprendimus, kurių integracija į vieningą saugumo valdymo modelį reikalauja papildomų techninių ir organizacinių pastangų. Be to, gairėse rekomenduojama tinklo telemetrijos ir žurnalų apimtis MVĮ gali sukelti neproporcingas saugojimo ir administravimo sąnaudas, todėl praktikoje dažnai taikomas selektyvus duomenų rinkimas, mažinantis bendrą tinklo matomumą.

Operaciniu lygmeniu reikšmingą ribotumą sudaro tinklo saugumo priemonių eksploatavimo sudėtingumas. Aptikimo sprendimai, tokie kaip IDS ar NDR, reikalauja nuolatinio taisyklių derinimo ir perspėjimų analizės, o riboti triage pajėgumai MVĮ didina riziką, kad saugumo perspėjimai taps neefektyvūs dėl perteklinio triukšmo. Papildomą neapibrėžtumą sukuria ir gairių teisinis statusas, nes jos nėra privalomos ir gali būti skirtingai interpretuojamos nacionalinių priežiūros institucijų, o tai apsunkina atitikties lygio planavimą.

Apibendrinant galima teigti, kad ENISA gairės sudaro vertingą techninį ir metodologinį pagrindą NIS2 reikalavimų įgyvendinimui, tačiau jų taikymas MVĮ aplinkoje reikalauja proporcingumo principu grindžiamos adaptacijos. Riboto, bet valdomo tinklo saugumo kontrolės priemonių rinkinio pasirinkimas ir aiškiai apibrėžti techniniai įrodymai tampa pagrindinėmis prielaidomis siekiant suderinti gairių rekomendacijas su MVĮ praktinėmis galimybėmis.

3. ATVIRO KODO TINKLO SAUGUMO ARCHITEKTŪRA MVĮ NIS2 ATITIKČIAI

3.1. Tinklo architektūros modelis NIS2 reikalavimams

NIS2 direktyvos kontekste tinklo architektūra laikytina esmine organizacinės ir techninės kibernetinio saugumo sistemos dedamąja, tiesiogiai lemiančia kritinių paslaugų tęstinumą, incidentų lokalizavimo galimybes ir bendrą informacinių sistemų atsparumą.

Tinklo architektūros modelio formavimas turi būti grindžiamas sisteminiu, rizika paremtu požiūriu, integruojančiu saugumo pagal projektą ir numatytąjį saugumą (security by design ir security by default), taip užtikrinant atitiktį tiek direktyvos techniniams, tiek organizaciniams reikalavimams. Vienas fundamentalių tokio modelio principų yra loginė ir fizinė tinklo segmentacija, leidžianti diferencijuoti prieigos lygius pagal informacinių išteklių funkcijas, jautrumą ir kritiškumą.

Loginė segmentacija, įgyvendinama pasitelkiant potinklius, VLAN ir programiškai apibrėžtus tinklus, sudaro sąlygas taikyti granuliuotą prieigos kontrolę ir sumažinti neautorizuoto šoninio

judėjimo galimybes, tuo tarpu fizinė segmentacija užtikrina aukštesnio lygmens izoliaciją toms sistemoms, kurių kompromitavimas galėtų sukelti disproporcingai didelį poveikį organizacijos veiklai.

Papildomai, architektūroje privalo būti aiškiai atskiriami „North–South“ ir „East–West“ duomenų srautai, nes šių srautų pobūdis ir rizikos profilis iš esmės skiriasi. „North–South“ srautų valdymas orientuojamas į perimetro apsaugą ir sąveiką su išorinėmis sistemomis, o „East–West“ srautų kontrolė reikalauja vidinių ryšių mikrosegmentacijos, nuolatinės stebėsenos ir detalaus srautų filtravimo, siekiant riboti grėsmių plitimą tinklo viduje net ir kompromitavus atskirus komponentus.

Šių architektūrinių sprendimų sinergija sudaro pagrindą sistemingam atakos paviršiaus mažinimui tinklo lygmenyje, kuris realizuojamas eliminuojant nereikalingus ryšius, paslaugas ir prieigos taškus, diegiant griežtas, politikomis pagrįstas prieigos kontrolės taisykles bei taikant nuolatinę tinklo srautų analizę. Tokiu būdu tinklo architektūra tampa ne pasyvia infrastruktūros dalimi, bet aktyvia rizikos valdymo priemone, leidžiančia organizacijoms ne tik formaliai atitikti NIS2 direktyvos nuostatas, bet ir sukurti adaptyvią, atsparią ir ilgalaikę kibernetinio saugumo ekosistemą.

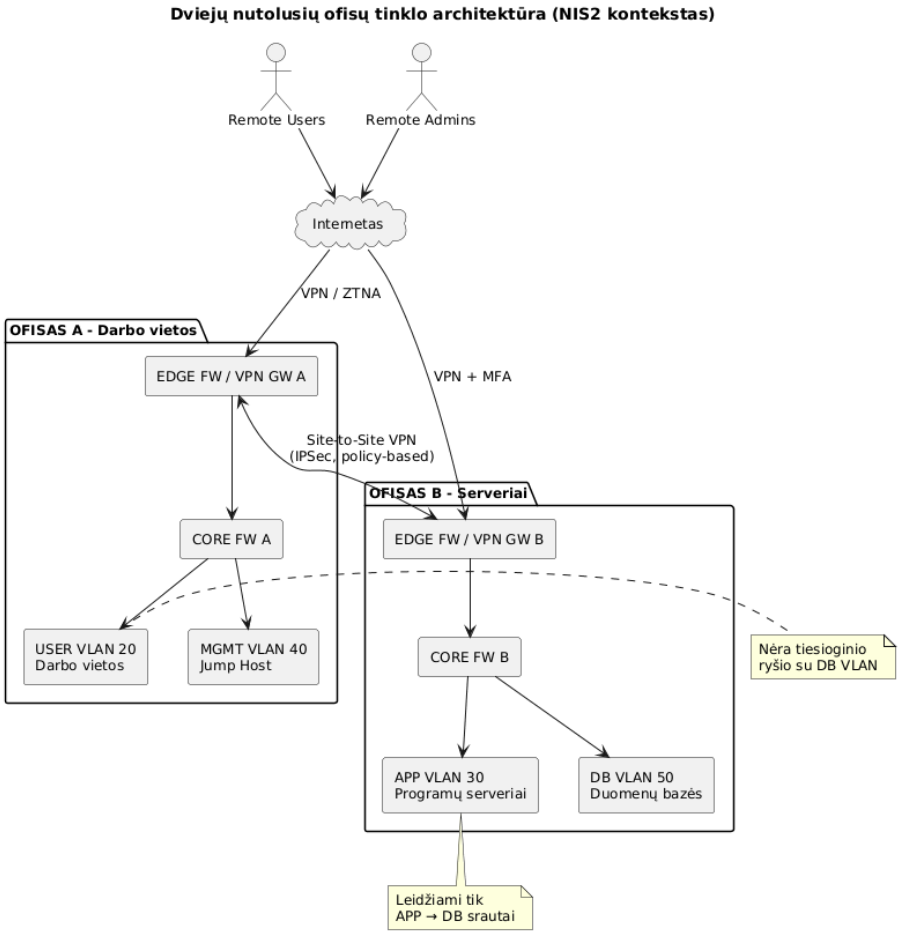
3.1.1. Galimos tinklo architektūros pavyzdys pasirinktam schenarijui (kontekstui):

3.1.1.1. Ofisas A – naudotojų ofisas (kelios darbo vietos).

3.1.1.2. Ofisas B – serverių ofisas (programos, DB, paslaugos).

3.1.1.3. Prisijungimai vyksta iš išorės per saugius prieigos taškus (VPN / ZTNA).

3.1.1.4. Tarp ofisų – šifruotas, politikomis ribojamas ryšys.



pav. 1 Dviejų nutolusių ofisų architektūros pavyzdys (PlantUML).

3.2. Tinklo srauto filtravimas ir incidentų prevencija

Tinklo srauto filtravimas ir prevencinės kontrolės priemonės sudaro fundamentalią kibernetinio saugumo architektūros dalį, užtikrinančią informacinių sistemų atsparumą ir atitiktį NIS2 direktyvos reikalavimams, kadangi jos leidžia sistemiškai valdyti įeinančius, išeinančius ir vidinius duomenų srautus, taikant rizikos valdymu pagrįstas ir politikomis apibrėžtas metodikas.

Daugiasluoksnis filtravimo modelis realizuojamas pasitelkiant būseninį paketų filtravimą (angl. stateful packet inspection), prieigos kontrolės sąrašus (ACL), taikomųjų protokolų lygmens inspekciją (angl. Deep Packet Inspection) bei mikrosegmentaciją, apimančią perimetro, vidinių tinklo segmentų ir paslaugų tarpusavio sąveikos lygmenis, taip sudarant prielaidas nuosekliai taikyti „deny-by-default“ principą ir reikšmingai sumažinti atakos paviršių.

Prevencinis aspektas įgyvendinamas integruojant statines filtravimo taisykles su dinaminėmis metodikomis, tokiomis kaip įsibrovimų aptikimo ir prevencijos sistemos (IDS/IPS), tinklo srauto elgsenos analizė (Network Detection and Response) bei srautų koreliacija centralizuotose stebėsenos platformose, leidžiančiose realiuoju laiku identifikuoti anomalijas, aptikti galimus šoninio judėjimo scenarijus ir inicijuoti automatizuotas reagavimo priemones.

Papildomai, išeinančio srauto (egress) kontrolė, domenų vardų filtravimas, šifruoto ryšio politikomis pagrįsta inspekcija ir komandų bei valdymo kanalų (C2) blokavimo metodikos prisideda prie duomenų nutekėjimo prevencijos, todėl tinklo srauto filtravimas tampa ne pasyvia apsaugos funkcija, o aktyvia, nuolat adaptuojama rizikos valdymo priemone, integruota į bendrą organizacijos kibernetinio saugumo ekosistemą.

3.3. Atviro kodo ugniasienės sprendimai

Atviro kodo ugniasienės sprendimai yra plačiai taikomi tinklo srauto filtravimo ir prevencijos architektūrose, nes jie suderina funkcionalumą, skaidrumą ir galimybę lanksčiai pritaikyti saugumo kontrolės mechanizmus pagal organizacijos rizikos profilį ir NIS2 direktyvos reikalavimus.

Praktikoje vieni dažniausiai naudojamų sprendimų yra „pfSense“ ir „OPNsense“, kurios veikia „FreeBSD“ pagrindu ir palaiko būseninį paketų filtravimą, taikomųjų protokolų inspekciją, VPN technologijas (IPSec, OpenVPN, WireGuard) bei integraciją su įsibrovimų aptikimo ir prevencijos sistemomis, tokiomis kaip „Suricata“ [30].

Kitas reikšmingas pavyzdys yra „iptables“ ir „nftables“ mechanizmai „Linux“ operacinėse sistemose, leidžiantys realizuoti žemo lygmens, itin granuliuotą srauto filtravimą tiek perimetro, tiek vidinių segmentų lygmenyje, ypač serverių ir debesijos aplinkose. Taip pat plačiai taikomas „VyOS“ sprendimas, orientuotas į maršrutizavimą ir ugniasienės funkcijas, kuris leidžia kurti politikomis pagrįstas tinklo architektūras ir yra dažnai naudojamas nutolusių ofisų ar hibridinių infrastruktūrų apsaugai.

Šie konkretūs pavyzdžiai rodo, kad atviro kodo ugniasienės sprendimai ne tik technologiškai atitinka modernius tinklo saugumo reikalavimus, bet ir sudaro sąlygas organizacijoms įgyvendinti skaidrias, audituojamas ir adaptyvias srauto filtravimo strategijas, kurios yra būtinos siekiant ilgalaikio kibernetinio atsparumo.

3.4. Tinklo srautų analizė ir anomalijų aptikimas

Tinklo srautų analizė ir anomalijų aptikimas yra viena pažangiausių šiuolaikinių kibernetinio saugumo praktikų, leidžianti organizacijoms pereiti nuo reaktyvaus incidentų valdymo prie proaktyvios grėsmių identifikacijos, kaip to reikalauja NIS2 direktyvos nuostatos dėl nuolatinio saugumo užtikrinimo.

Ši veikla grindžiama sistemingu tinklo srautų stebėjimu, statistinių ir elgsenos modelių taikymu bei įvykių koreliacija, siekiant identifikuoti nukrypimus nuo įprasto veikimo profilio. Praktikoje tinklo srautų analizė dažnai realizuojama renkant srauto metaduomenis naudojant „NetFlow“, „sFlow“ ar „IPFIX“ protokolus, kurie leidžia įvertinti ryšių kryptį, trukmę, intensyvumą ir dažnį be būtinybės analizuoti visą paketų turinį. Tokia analizė ypač naudinga didelio masto infrastruktūrose, kuriose pilna paketų inspekcija būtų techniškai ar ekonomiškai neefektyvi.

Anomalijų aptikimas tinklo srautų analizės kontekste remiasi tiek taisyklėmis pagrįstais, tiek statistiniais ir mašininio mokymosi metodais. Taisyklių pagrindu veikiančios sistemos leidžia nustatyti iš anksto apibrėžtus pažeidimus, pavyzdžiui, netikėtą ryšių inicijavimą tarp vidinių segmentų, neleistinus prisijungimus prie administracinių prievadų ar staigų srauto padidėjimą, būdingą paslaugų trikdymo (DoS) atakoms.

Tuo tarpu elgsenos analizė leidžia identifikuoti sudėtingesnius, iš anksto neaprašytus scenarijus, pavyzdžiui, lėtą ir laipsnišką duomenų nutekinimą ar paslėptą ryšį su komandų ir valdymo (C2) serveriais, kurie dažnai maskuojami kaip teisėtas šifruotas srautas. Praktiniai pavyzdžiai apima „Network Detection and Response“ (NDR) sprendimų taikymą, kai, remiantis istorinių duomenų analize, aptinkami anomalūs ryšiai tarp darbo stočių ir serverių, nesuderinami su įprastais organizacijos veiklos modeliais.

Svarbus tinklo srautų analizės aspektas yra jos integracija su kitomis saugumo priemonėmis, ypač su įsibrovimų aptikimo sistemomis (IDS), galinių taškų stebėsena ir centralizuotomis saugumo informacijos ir įvykių valdymo (SIEM) platformomis. Tokia integracija leidžia koreliuoti tinklo lygmens anomalijas su sistemų žurnalais ir naudotojų veikla, taip didinant aptikimo tikslumą ir mažinant klaidingų teigiamų rezultatų skaičių.

Praktikoje tai pasireiškia automatizuotais reagavimo scenarijais, kai, aptikus neįprastą srautą, sistema inicijuoja papildomą autentifikavimo patikrą, laikinai apriboja ryšius arba izoliuoja atskirą tinklo segmentą. Apibendrinant galima teigti, kad tinklo srautų analizė ir anomalijų aptikimas yra neatsiejama adaptyvios kibernetinio saugumo architektūros dalis, leidžianti organizacijoms ne tik atitikti NIS2 direktyvos reikalavimus, bet ir reikšmingai sustiprinti gebėjimą laiku identifikuoti bei valdyti sudėtingas, ilgalaikes ir tikslines kibernetines grėsmes.

3.4.1. NDR sprendimas Zeek

„Zeek“ yra atviro kodo tinklo srautų analizės ir anomalijų aptikimo sprendimas, plačiai taikomas kaip „Network Detection and Response“ (NDR) klasės įrankis akademinėse, valstybinėse ir pramoninėse aplinkose, kuriose reikalinga išsami tinklo elgsenos stebėsena ir pažangus incidentų aptikimas.

Skirtingai nuo tradicinių įsibrovimų aptikimo sistemų, kurios dažniausiai remiasi iš anksto apibrėžtomis parašais pagrįstomis taisyklėmis, „Zeek“ orientuojasi į protokolų semantikos analizę ir įvykių pagrindu veikiančią architektūrą, leidžiančią detaliai aprašyti ir stebėti tinklo komunikacijos logiką.

Toks požiūris suteikia galimybę identifikuoti ne tik žinomus atakų modelius, bet ir sudėtingus, žemo intensyvumo ar ilgalaikius grėsmių scenarijus, kurie dažnai lieka nepastebėti naudojant tradicines saugumo priemones.

Techniniu požiūriu „Zeek“ analizuoja tinklo srautą pasyviai, rekonstruodamas aukštesnio OSI lygmens protokolų sesijas ir generuodamas struktūrizuotus įvykių žurnalus apie HTTP, DNS, TLS, SMTP ir kitų protokolų veiklą. Šie žurnalai leidžia formuoti bazinius elgsenos modelius, apibrėžiančius normalią organizacijos tinklo veiklą, ir vėliau identifikuoti nuo jų nukrypstančius reiškinius, pavyzdžiui, neįprastus DNS užklausų modelius, netikėtus šifruotus ryšius su išoriniais resursais ar neleistinus paslaugų tarpusavio ryšius vidiniuose segmentuose.

Praktikoje „Zeek“ dažnai naudojamas aptikti komandų ir valdymo kanalus, šoninį judėjimą tinkle bei galimus duomenų nutekinimo bandymus, ypač tais atvejais, kai atakos yra maskuojamos kaip teisėtas srautas.

Reikšmingas „Zeek“ privalumas NIS2 direktyvos kontekste yra jo gebėjimas integruotis su kitomis saugumo valdymo ir reagavimo sistemomis, tokiomis kaip SIEM, SOAR ir įsibrovimų prevencijos sprendimai. „Zeek“ generuojami įvykiai gali būti koreliuojami su galinių taškų duomenimis, autentifikavimo žurnalais ir tinklo filtravimo taisyklėmis, taip sudarant prielaidas automatizuotam incidentų aptikimui ir reagavimui.

Akademiniu požiūriu „Zeek“ laikytinas brandžiu NDR sprendimu, kuris ne tik išplečia tinklo matomumą ir aptikimo galimybes, bet ir prisideda prie organizacijos kibernetinio saugumo brandos didinimo, leidžiant pereiti nuo pavienių saugumo kontrolės priemonių prie integruotos, duomenimis grįstos ir adaptyvios saugumo ekosistemos.

3.4.2. Lateral movement atakų aptikimas

Šoninio judėjimo (lateral movement) aptikimas yra kritiškai svarbus pažangių kibernetinių atakų identifikavimo etapas, nes jis leidžia nustatyti situacijas, kai užpuolikas, įgijęs pradinę prieigą prie vieno tinklo elemento, siekia išplėsti savo kontrolę kitose sistemose, dažniausiai naudodamas teisėtas administravimo priemones ir protokolus.

Praktikoje šoninis judėjimas dažnai vykdomas pasitelkiant tokius protokolus kaip SMB, RDP, WinRM ar SSH, todėl jo aptikimas remiasi ne vien pačių protokolų naudojimo faktu, bet ir jų elgsenos konteksto analize. Pavyzdžiui, tinklo srautų analizės sprendimai, tokie kaip „Zeek“, leidžia identifikuoti netipinius SMB ar RDP ryšius tarp darbo stočių, kurie įprastai neturėtų inicijuoti tiesioginių tarpusavio jungčių, taip pat aptikti staigų autentifikacijos bandymų skaičiaus padidėjimą tarp skirtingų vidinių segmentų.

Kitas praktinis pavyzdys yra atvejai, kai serveris, paprastai veikiantis tik kaip paslaugų teikėjas, netikėtai pradeda inicijuoti ryšius į administravimo prievadus kitose sistemose, kas gali signalizuoti apie kompromituotą paskyrą ar pavogtus prieigos duomenis.

Tokios anomalijos, koreliuojamos su autentifikavimo žurnalais ir galinių taškų stebėsenos duomenimis, leidžia ne tik aptikti šoninį judėjimą ankstyvoje stadijoje, bet ir inicijuoti tikslines prevencines priemones, tokias kaip segmento izoliavimas ar laikinų prieigos teisių apribojimas.

3.4.3. Duomenų eksfiltracijos požymiai

Duomenų eksfiltracijos požymiai dažniausiai pasireiškia kaip subtilūs, tačiau sistemiški tinklo elgsenos nukrypimai, rodantys galimą neleistiną informacijos perdavimą iš organizacijos infrastruktūros į išorinius resursus.

Praktikoje tokie požymiai apima neįprastą išeinančio srauto (egress) padidėjimą ne darbo metu, periodinius ir mažo intensyvumo duomenų perdavimus, skirtus apeiti tradicinius srauto slenksčius, taip pat ryšius su geografiškai ar reputaciniu požiūriu netipiniais išoriniais adresais.

Tinklo srautų analizės sprendimai leidžia identifikuoti atvejus, kai vidinės sistemos inicijuoja ilgalaikius šifruotus ryšius su neįprastais domenais, dažnai pasitelkiant HTTPS ar DNS tuneliavimo metodikas, pavyzdžiui, perteklines ir struktūriškai pasikartojančias DNS užklausas.

Kitas reikšmingas požymis yra paslaugų ar darbo stočių elgsena, kai jos pradeda perduoti duomenis protokolais ar prievadais, kurie nėra būdingi jų funkcinei paskirčiai, pavyzdžiui, duomenų bazės serverio inicijuojami ryšiai į išorinius failų dalijimosi ar debesijos saugyklų servisus.

Šių požymių koreliacija su autentifikavimo įrašais, naudotojų veikla ir galinių taškų telemetrija sudaro prielaidas ankstyvam duomenų eksfiltracijos aptikimui ir leidžia inicijuoti prevencines priemones dar prieš padarant reikšmingą žalą organizacijos informaciniams ištekliams.

3.5. Tinklo stebėsena ir įrodymų bazė. Centralizuotas tinklo logų rinkimas ir ELK taikymas tinklo saugumui

Centralizuotas tinklo logų rinkimas yra kertinis elementas, leidžiantis užtikrinti nuoseklią tinklo stebėseną, efektyvų incidentų aptikimą ir patikimos įrodymų bazės formavimą, kaip to reikalauja NIS2 direktyva.

Šis procesas grindžiamas visų tinklo saugumo komponentų – ugniasienių, maršrutizatorių, perjungiklių, IDS/IPS, NDR sprendimų ir serverių – generuojamų žurnalų konsolidavimu vieningoje analizės aplinkoje, taip sudarant sąlygas visuminės tinklo veiklos analizės ir įvykių koreliacijos vykdymui.

Šiame kontekste ELK (Elasticsearch, Logstash, Kibana) platforma pasirenkama kaip pagrindinis techninis sprendimas dėl savo atviro kodo pobūdžio, mastelio keitimo galimybių ir lankstumo apdorojant heterogeninius tinklo saugumo duomenis.

Logstash leidžia centralizuotai surinkti ir normalizuoti žurnalus iš skirtingų šaltinių, Elasticsearch suteikia galimybę efektyviai indeksuoti ir ieškoti didelės apimties laiko eilučių duomenis, o Kibana sudaro sąlygas vizualizuoti tinklo saugumo įvykius, identifikuoti anomalijas ir analizuoti incidentų eigą realiuoju laiku.

Toks sprendimas ypač tinkamas tinklo saugumui, nes leidžia koreliuoti, pavyzdžiui, ugniasienių blokavimo įrašus su NDR sprendimų aptiktais anomalijų indikatoriais ar neįprastais srautų modeliais, taip padidinant aptikimo tikslumą ir sumažinant klaidingų įspėjimų skaičių.

Be operacinės vertės, ELK platforma atlieka svarbų vaidmenį formuojant įrodymų atsekamumą pagal NIS2, nes centralizuotas, laiko žymomis pagrįstas ir nuo klastojimo apsaugotas logų saugojimas leidžia atkurti įvykių seką, pagrįsti incidentų valdymo sprendimus ir pateikti audituojamus techninius įrodymus tiek vidaus, tiek išorės priežiūros institucijoms.

Dėl šių priežasčių ELK pasirenkamas ne tik kaip techninis logų analizės įrankis, bet ir kaip strateginė saugumo valdymo platforma, jungianti tinklo stebėseną, incidentų analizę ir NIS2 reikalavimų įgyvendinimą į vientisą, skaidrią ir ilgalaikę kibernetinio saugumo ekosistemą.

4. TYRIMO METODIKA

4.1. Tyrimo dizainas ir pasirinkti įrankiai

Šio tyrimo metodika grindžiama laboratorine atvejo analize MVĮ tipo tinkle, kur techninių tinklo kontrolų veikimas vertinamas per aptikimo greitį, aptikimo kokybę ir techninių įrodymų pakankamumą. Naudojama eksperimentų scenarijų lentelė su pasirinktais vertinimo kriterijais:

lentelė 1. Eksperimentų scenarijų parametrai

Scenarijus	**Tikslas**	**Komanda / įrankis**	**Trukmė**	**Srauto intensyvumas**	**Stebimi logų šaltiniai**	**Tikėtinas aptikimo signalas**
Bazinis atakos paviršiaus matavimas (port scan)	Nustatyti atvirus prievadus ir ar sensorius užfiksuoja skenavimą	Nmap (prievadų skenavimas)	Nenurodyta (pagal skenavimo trukmę)	Tipiškas nmap skenavimo srautas	Zeek sugeneruoti papildomi logai po skenavimo	Nauji/aktyvesni Zeek įrašai susiję su skenavimu (anomalus „probing“ elgesys)
Testas 1: DoS simuliacija prieš SSH	Įvertinti, ar IDS/NDR aptinka ir fiksuoja paslaugos trikdymą	Bash skriptas „ssh_bf.sh“ (DoS principų imitacija)	30 s (pirmas bandymas)	10 susijungimų/s į 22 TCP	Zeek įvykių žurnalai (fiksuojama bandymų eiga)	Pikas ryšiuose į 22/TCP + Zeek įvykių fiksavimas (incidento pradžia matoma loguose)
Testas 2: brute force prieš SSH (1 bandymas)	Įvertinti pakartotinių neteisėtų autentifikacijų aptikimą	Nmap NSE ssh-brute + user/pass sąrašas	Iki 1 min	„Daug autentifikacijos užklausų per trumpą laiką“	Zeek įvykių žurnalai; papildomai tikrinama ELK atvaizdavime	Padidėjęs nesėkmingų SSH bandymų skaičius, anomalus prisijungimų modelis (IDS/NDR perspėjimai)
Testas 2: brute force prieš SSH (2 bandymas)	Patikrinti atsparumą ilgesnės trukmės bruteforce scenarijui	Tas pats Nmap ssh-brute scenarijus	5 min	Tie patys parametrai, ilginama tik trukmė	tcpdump + Zeek įvykių žurnalai	Ilgesnis „peak“ autentifikacijų bandymuose; vėliau koreliacija/atvaizdavimas ELK (su galimu ingestavimo vėlavimu)

Zeek pasirenkamas kaip pasyvus NDR sensorius, generuojantis protokolų semantika pagrįstus įvykius (pvz., DNS, TLS, HTTP, SSH), o ELK (Elasticsearch, Logstash, Kibana) – kaip centralizuota

įrodymų bazės ir koreliacijos platforma, leidžianti normalizuoti heterogeninius logus, kurti paieškas ir atkurti incidento laiko juostą.

Nmap taikomas kaip atakos paviršiaus ir segmentacijos efektyvumo matavimo priemonė (kas iš kur pasiekiama), o iperf3 – kaip kontroliuojamo srauto generatorius (baziniam pralaidumui, foniniam triukšmui ir eksfiltracijos tipo srautams modeliuoti) [31].

4.2. Laboratorinė aplinka, diegimo logika ir techniniai įrodymai

Tiriama aplinka modeliuoja du nutolusius taškus (naudotojų biuras ir serverių biuras), kuriuose prieiga vyksta iš išorės per kontroliuojamus vartus, o vidiniai segmentai atskiriami pagal funkciją (USER, MGMT, APP, DB).

Zeek diegiamas stebėjimo taške (SPAN/TAP), o ELK konfigūruojamas taip, kad priimtų Zeek ir tinklo įrenginių logus, suvienodintų laiko laukus, užtikrintų paiešką pagal indikatorius ir palaikytų įrodymų atsekamumą (įvykių chronologiją).

Techniniai įrodymai šiame tyrime apima: Zeek žurnalus, ugniasienių/VPN įrašus, Nmap skenavimo rezultatus, testų rezultatų suvestines ir ELK užklausomis gautas koreliacijas (pvz., incidento laiko juostos išklotinę), kurios tampa pagrindimu tiek aptikimo rezultatams, tiek pranešimo turiniui.

4.3.Vertinimo kriterijai ir supaprastintos formulės

Aptikimo greičiui įvertinti taikomas vidutinis aptikimo laikas (MTTD), apibrėžiamas kaip vidutinis skirtumas tarp incidento pradžios ir pirmo patikimo aptikimo signalo ELK aplinkoje:

$$\mathrm{MTTD} = \frac{1}{\mathrm{n}}\sum_{\mathrm{i}=1}^{\mathrm{n}}\left(\mathrm{t}_{\mathrm{i}}^{\mathrm{aptikimas}} - \mathrm{t}_{\mathrm{i}}^{\mathrm{pradžia}}\right)$$

čia $t_i^{pradžia}$ – i-tojo scenarijaus pradžios laikas, $t_i^{aptikimas}$ – aptikimo laikas, n – scenarijų kartojimų skaičius. Klaidingų aliarmų rodiklis (FAR) apibūdina, kokia dalis sugeneruotų įspėjimų po patikros nepriskiriami realiam incidentui:

$$FAR = \frac{FP}{FP + TP}$$

čia FP – klaidingi teigiami, TP – tikri teigiami. Logų pilnumas (LC) naudojamas kaip įrodymų bazės pakankamumo aproksimacija, vertinant, kiek numatytų kritinių „įrodymų elementų“ realiai surenkama ir indeksuojama ELK sistemoje; formulė:

$$LC = \frac{C_{ivykdyta}}{C_{rasta}}$$

čia $C_{įvykdyta}$ – numatytų elementų skaičius, C_{rasta} – realiai surinktų elementų skaičius.

Sistemos resursų sąnaudos vertinamos kaip stebėsenos „overhead“, lyginant bazinę būseną su būsena, kai veikia „Zeek“ ir ELK ingestavimo grandinė:

$$OH_X = \frac{X_{su} - X_{be}}{X_{be}}$$

čia X – matuojamas resursas (pvz., CPU, RAM, disko I/O), X_{be} – bazinė reikšmė, X_{su} – reikšmė su įjungta stebėsena.

4.4.Incidentų simuliacijos ir laiko analizė pagal NIS2

Tyrime simuliuojami bent du incidentų tipai: (i) lateral movement, kai kompromituota darbo vieta inicijuoja netipinius „East–West“ ryšius (pvz., SMB/RDP/SSH) į kitus hostus ar segmentus, duomenų eksfiltracija, kai generuojamas neįprastas išeinantis srautas (nmap leidžia tiksliai valdyti apimtį ir trukmę), o Zeek+ELK naudojami anomalijoms ir koreliacijoms fiksuoti.

Aptikimo ir reagavimo laikas formalizuojamas per pagrindinius momentus: $t_{pradžia}, t_{aptikimas}, t_{suvaldymas}$ ir pranešimo parengties laiką $t_{raport\_parengt}$:

$$T_{aptikimas} = t_{aptikimas} - t_{pradžia}, \quad T_{suvaldymas} = t_{suvaldymas} - t_{aptikimas}$$

Pagal NIS2 incidentų pranešimo etapų logiką (ankstyvas perspėjimas per 24 val., išsamesnis pranešimas per 72 val., galutinė ataskaita per 1 mėn.) tyrime vertinama, ar suformuota ELK įrodymų bazė leidžia laiku sukurti pakankamą incidento chronologiją ir pradinį poveikio vertinimą.

5. EKSPERIMENTINĖ DALIS IR REZULTATAI

Eksperimentinei daliai sukursime dalinai izoliuotą aplinką, įmituojančią MVĮ tinklo saugos komponentus, kurioje pozicionuosime šiuos atviro kodo sprendinius:

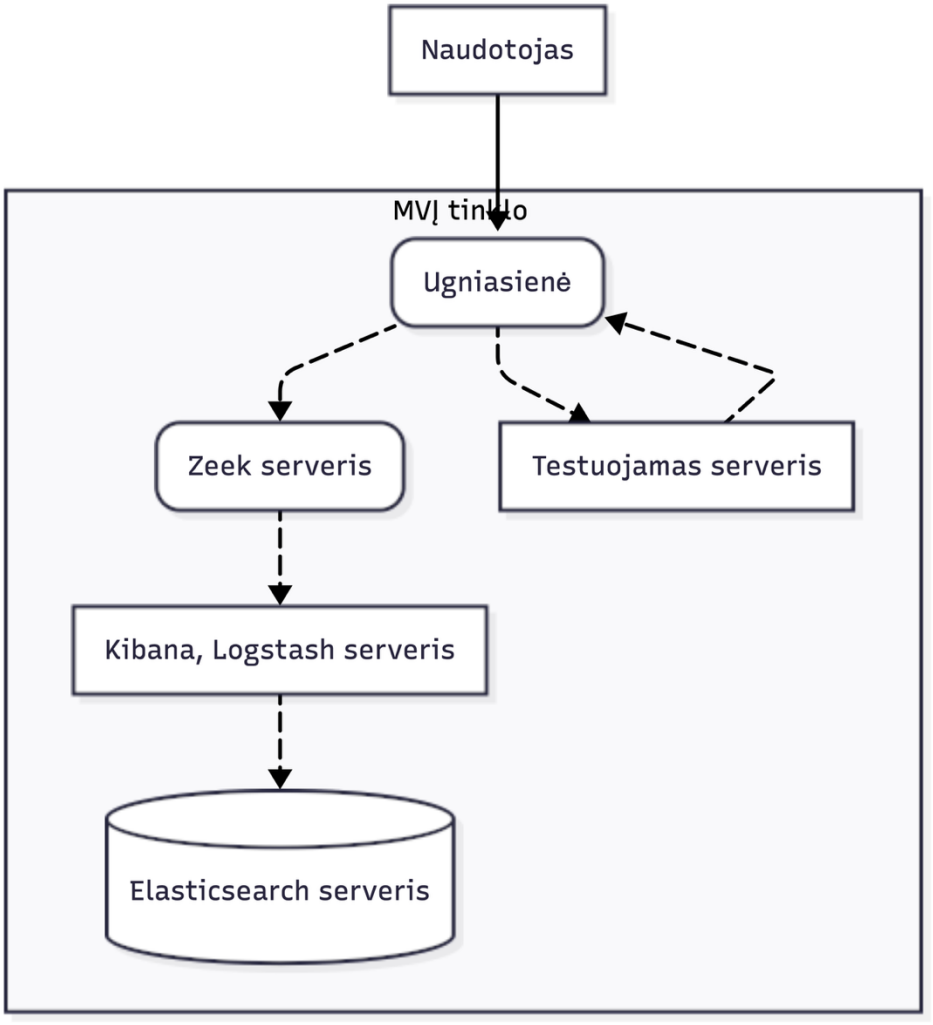
5.1. Ugniasienę (pfSense) – atlieka tiek WAF, tiek srauto veidrodinio atvaizdo siuntimo NDR moduliui funkcijas.

5.2. NDR (Zeek) – atlieka tinklo anomalijų aptikimo ir atsako (angl. Network detect and Response) funkcijas.

5.3. SIEM (ELK stack) – atlieka logų agregavimo, archyvavimo, bei atvaizdavimo funkcijas.

5.4. Tinklo skanavimo įrankis (nmap) – atlieka pažeidžiamumų identifikavimo, išnaudojimo funkcijas.

5.5. Tinklo, bei sisteminių metrikų monitoringas (iperf3) – atlieka tinklo, bei sistemų komponentų apkrovos metrikų fiksavimo, dokumentavimo įvykių žurnaluose funkcijas.

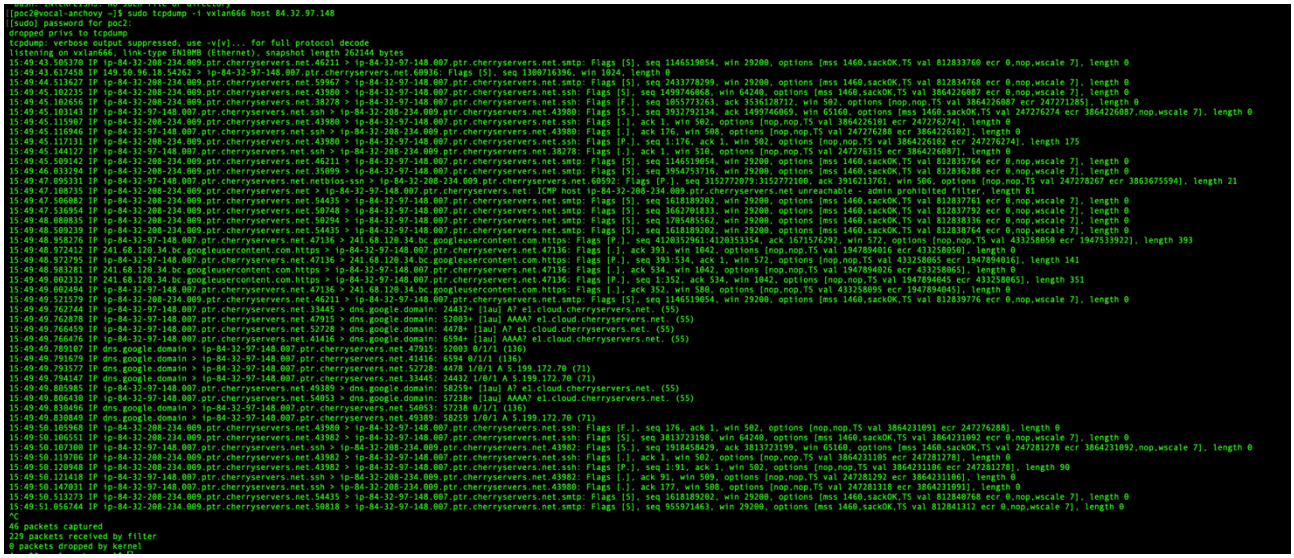


pav. 2 Principinė pasirinkto sprendinio tinklo srautų schema (Mermaid).

1.1. Tinklo saugumo būklė prieš ir po kontrolės įdiegimo

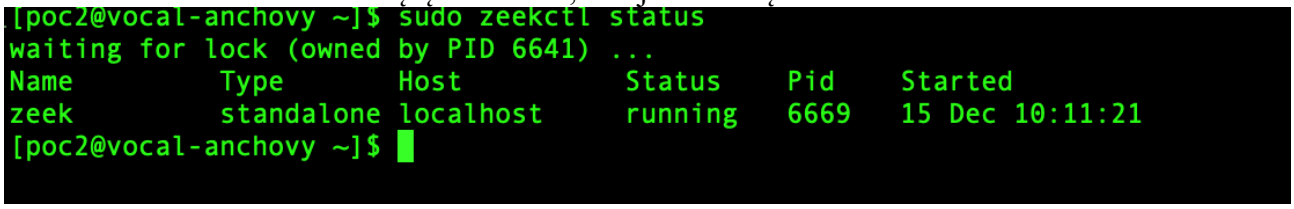
Tinklo būklės vertinimas prieš sprendinio diegimą reikalauja papildomos Zeek konfigūracijos. Zeek serveryje sukuriamas vxlan tinklo prievadas, pavadinimu „vxlan666“. Sukuriamas sąryšis tarp pagrindinio tinklo prievado eth0 ir vxlan666, naudojant 4765 UDP protokolą.

Ugniasienės pusėje atliekame port mirror konfigūraciją ir nukreipiame srautą į Zeek serverio išorinį IP adresą. Patikrinama ar matomas srautas tcpdump pagalba:



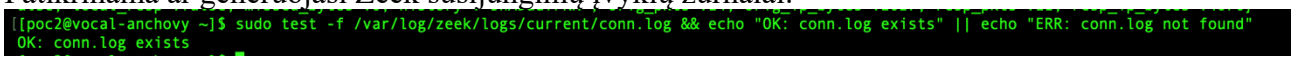
pav. 3 Tinklo paketų srautas į vxlan666 tinklo prievadą.

Patikriname Zeek serviso būklę. Įsitikiname, kad jis startavęs:



pav. 4 Zeek serviso būsena.

Patikrinama ar generuojasi Zeek susijungimų įvykių žurnalai:



pav. 5 Susijungimų žurnalo atvaizdas.

Patikrinama Zeek proceso apkrova resursams:

```
top - 15:36:13 up  5:27,  1 user,  load average: 1.34, 1.39, 2.88
Tasks:   2 total,   0 running,   2 sleeping,   0 stopped,   0 zombie
%Cpu(s):  5.2 us,  4.0 sy,  0.0 ni, 88.7 id,  0.0 wa,  0.6 hi,  1.5 si,  0.0 st
MiB Mem :  31833.8 total,  18833.6 free,   4310.0 used,   9147.5 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.  27523.7 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 164065 root      20   0 2256612 390944 152788 S  45.7   1.2   0:08.47 zeek
 164059 root      20   0    7272   3668   3340 S   0.0   0.0   0:00.00 run-zeek
```

pav. 6 Momentinė sistemos resursų apkrova. Matavimas nr. 1.

Pastebima 45.7% apkrova procesoriui 1.2% apkrova operatyvinei atminčiai.

Srautas nutraukiamas. Patikrinama apkrova sistemos resursams:

```
top - 15:36:40 up  5:28,  1 user,  load average: 1.16, 1.34, 2.82
Tasks:   2 total,   1 running,   1 sleeping,   0 stopped,   0 zombie
%Cpu(s):  3.5 us,  2.4 sy,  0.0 ni, 92.0 id,  0.0 wa,  0.5 hi,  1.7 si,  0.0 st
MiB Mem :  31833.8 total,  18764.7 free,   4363.2 used,   9163.3 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.  27470.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 164065 root      20   0 2386324 447224 152852 R  43.3   1.4   0:20.80 zeek
 164059 root      20   0    7272   3668   3340 S   0.0   0.0   0:00.00 run-zeek
```

pav. 7 Momentinė sistemos resursų apkrova. Matavimas nr. 2.

Apkrova procesoriui 43.3%, operatyvinei atminčiai 1.4%, paklaidos ribose.

Paleidžiame aukos serverio prievadų skanavimą nmap pagalba.

```
[poc2@vocal-anchovy ~]$ sudo nmap -sS -Pn --top-ports 200 -T4 84.32.97.148
Starting Nmap 7.92 ( https://nmap.org ) at 2025-12-15 15:17 EET
Nmap scan report for ip-84-32-97-148.007.ptr.cherryservers.net (84.32.97.148)
Host is up (0.0026s latency).
Not shown: 198 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
25/tcp open  smtp

Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds
[poc2@vocal-anchovy ~]$
```

pav. 8 Aukos serverio atvirų šliuzų (ports) skanavimas nmap pagalba.

Baigę skanavimą, patikriname ar susigeneravo papildomi Zeek logai:

```
[[poc2@vocal-anchovy ~]$ ls -1 /var/log/zeek/logs/current/ | head
capture_loss.log
conn.log
dns.log
dpd.log
files.log
http.log
mysql.log
notice.log
ntp.log
ocsp.log
[poc2@vocal-anchovy ~]$
```

pav. 9 Zeek žurnalų katalogas.

Sukuriame bash scriptą turinio filtravimui:

```
5  sudo awk '
4    BEGIN{FS="\t"; OFS="\t"}
3    /^#/ {print; next}                  # paliekam Zeek antraštes (#...)
2    $5=="84.32.97.148" {print}          # filtruojam tik šį IP (id.resp_h = 5 laukas)
1  ' /var/log/zeek/logs/current/conn.log |
6    sudo tee /var/log/zeek/logs/current/conn_84.32.97.148.log >/dev/null
```

pav. 10 Zeek žurnalų filtravimo scriptas.

Išsaugome scriptą *.sh formatu. Pakeičiame jo tipą į vykdomąjį „*chmod +x*" komandos pagalba ir užvardiname „zeek_logai.sh".

1.2. IDS ir NDR aptikimo rezultatų analizė

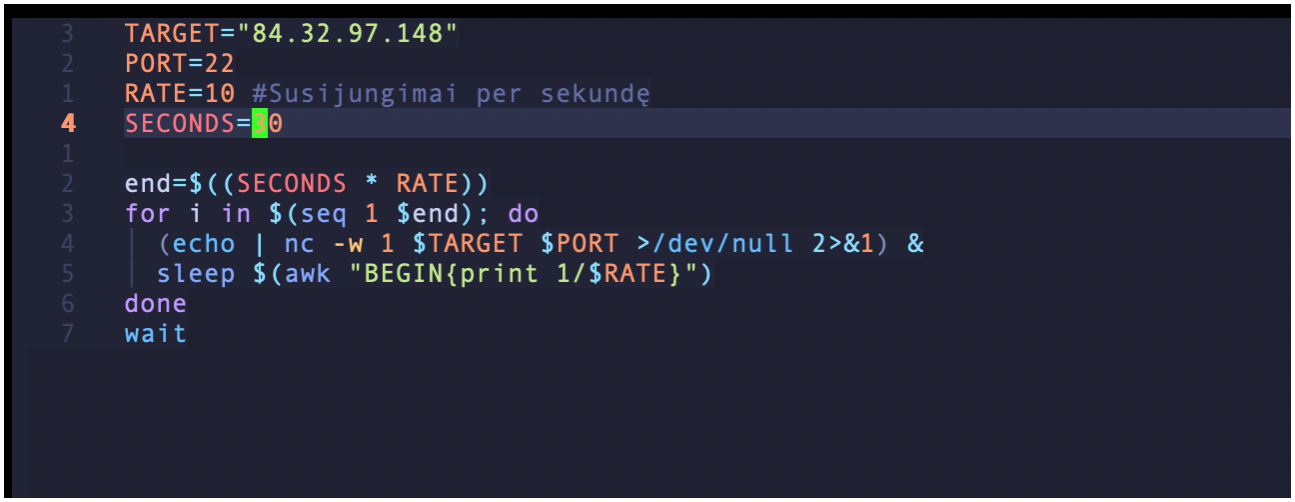
1.2.1. Testas 1. Paslaugų sutrikdymo ataka.

Testo metu bus vykdoma kontroliuojama paslaugų sutrikdymo (DoS) atakos simuliacija, siekiant įvertinti IDS ir NDR sprendimų gebėjimą aptikti ir fiksuoti tokio tipo kenkėjišką veiklą.

DoS (Denial of Service) atakos yra kibernetinio pobūdžio grėsmės, kurių tikslas – sutrikdyti informacinių sistemų, serverių ar tinklo paslaugų prieinamumą teisėtiems naudotojams.

Tokios atakos vykdomos dirbtinai generuojant didelį užklausų ar ryšių srautą, kuris išnaudoja sistemos skaičiavimo, atminties ar tinklo resursus. Dėl to paslaugos tampa nepasiekiamos arba veikia nestabiliai, pažeidžiant prieinamumo principą, kuris yra vienas iš pagrindinių informacijos saugumo ramsčių.

Pasiruošiame aukos serverio paslaugų sutrikdymo (DoS) atakos simuliacijai. Susikuriame bash scriptą, imituojantį DoS atakos principus. Padarome jį vykdomuoju, užvardiname „ssh_bf.sh" (Paveikslas 11). Scriptas generuos susijungimus į 22 TCP prievadą 10 susijungimų per sekundę dažniu. Visa ataka tęsis 30 sekundžių.

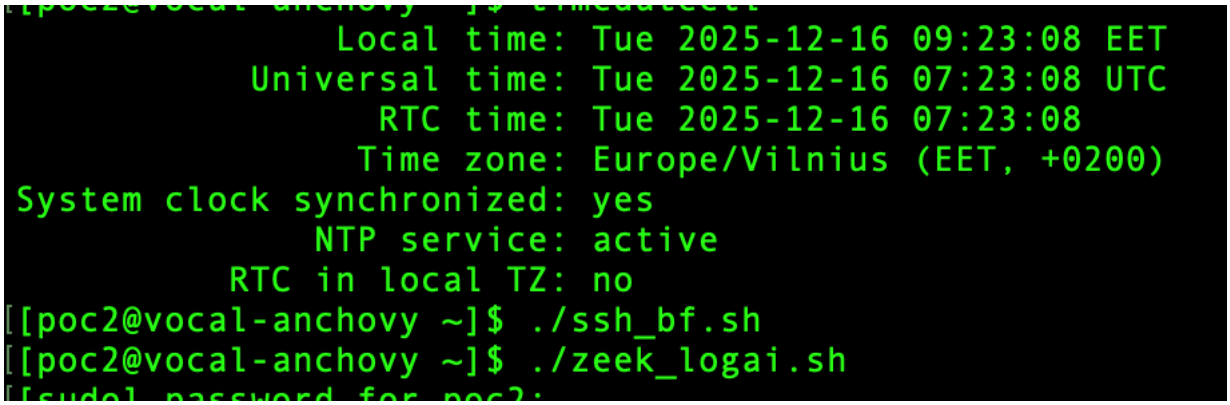


```
TARGET="84.32.97.148"
PORT=22
RATE=10 #Susijungimai per sekundę
SECONDS=30

end=$((SECONDS * RATE))
for i in $(seq 1 $end); do
  (echo | nc -w 1 $TARGET $PORT >/dev/null 2>&1) &
  sleep $(awk "BEGIN{print 1/$RATE}")
done
wait
```

pav. 11 Skriptas, skirtas kombinuotai DoS atakai imituoti.

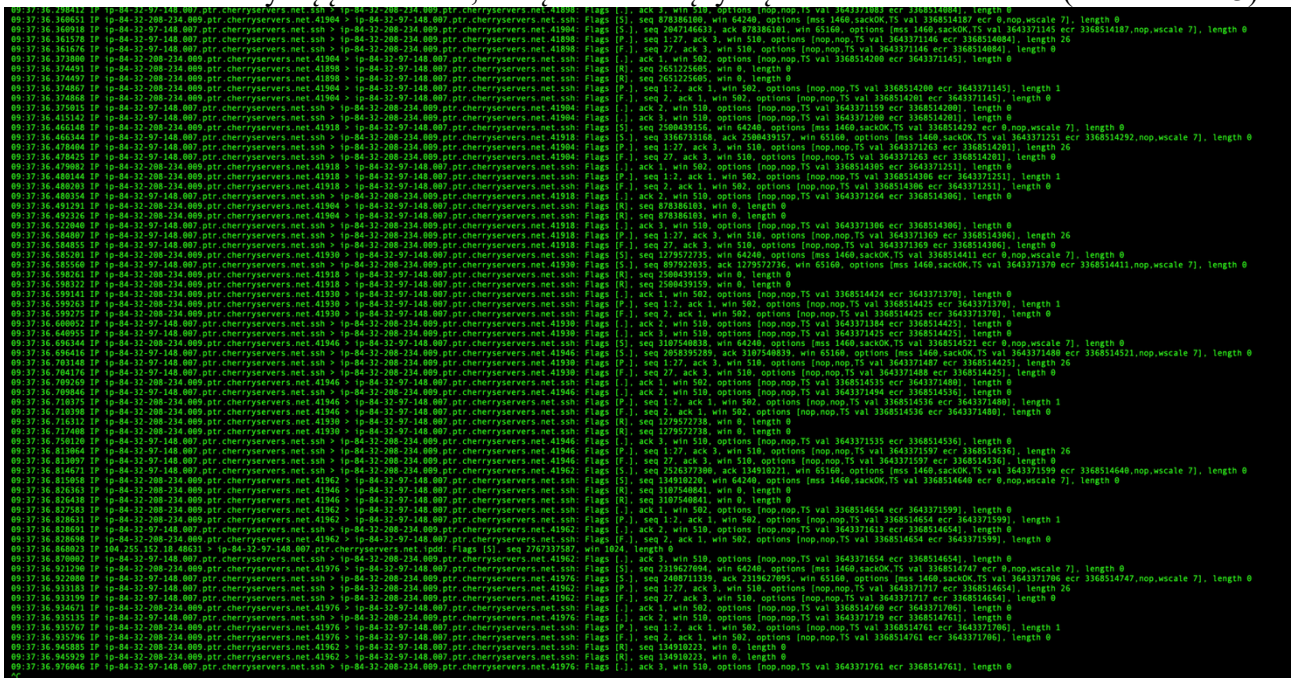
Pirmu bandymu nuimamas laikas, paleidžiamas atakos scriptas, rezultatai fiksuojami zeek įvykių žurnale (Paveikslas 12).



```
               Local time: Tue 2025-12-16 09:23:08 EET
           Universal time: Tue 2025-12-16 07:23:08 UTC
                 RTC time: Tue 2025-12-16 07:23:08
                Time zone: Europe/Vilnius (EET, +0200)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
[poc2@vocal-anchovy ~]$ ./ssh_bf.sh
[poc2@vocal-anchovy ~]$ ./zeek_logai.sh
```

pav. 12 DoS ir log filtravimo scriptų paleidimas. Pirmas bandymas.

Atlikus bandymą įsitikinama, kad įrašai Zeek įvykių žurnaluose užfiksuoti (Paveikslas 13).



pav. 13 Paketų fiksavimas zeek loguose.

Ilginamas atakos laikas, siekiant patikrinti sprendinio atsparumą ilgesnės apkrovos laikotarpiu:

```
#!/usr/bin/env bash

TARGET="84.32.97.148"
PORT=22
RATE=10 # SSH sesijos per sekundę
SECONDS=360

end=$((SECONDS * RATE))

for i in $(seq 1 $end); do
  (
    ssh-keyscan -p $PORT -T 1 $TARGET >/dev/null 2>&1
  ) &
  sleep $(awk "BEGIN{print 1/$RATE}")
done

wait
```

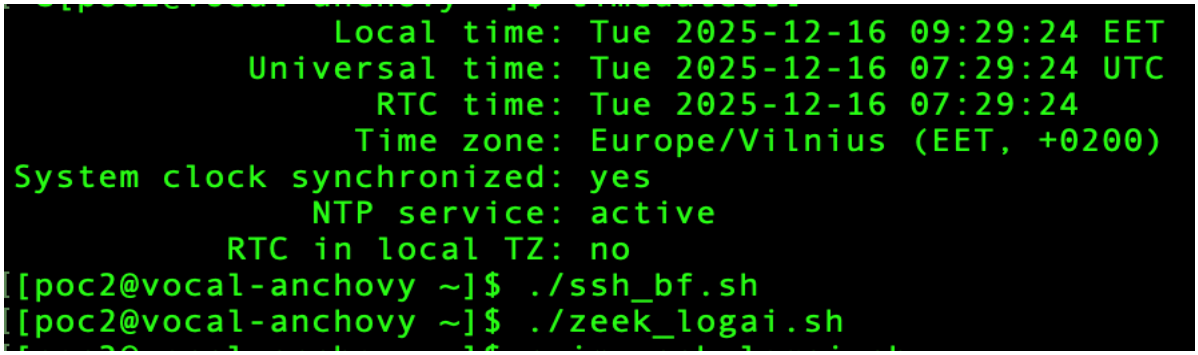
pav. 14 DoS atakos laiko koregavimas vykdomajame scripte.

Fiksuojamas laikas. Startuojamas antras bandymas (Paveikslas 15). Bandymo eigoje pastebėta, kad tinklo paketai nebepasiekia atakuojamo serverio. Bandymas nutrauktas, kartojamas po švaraus sistemos perkrovimo.

```
               Local time: Tue 2025-12-16 09:26:55 EET
           Universal time: Tue 2025-12-16 07:26:55 UTC
                 RTC time: Tue 2025-12-16 07:26:55
                Time zone: Europe/Vilnius (EET, +0200)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
[[poc2@vocal-anchovy ~]$ ./ssh_bf.sh
[[poc2@vocal-anchovy ~]$ ./zeek_logai.sh
```

pav. 15 DoS ir log filtravimo scriptų paleidimas. Antras bandymas.

Kartojant bandymą paketai sėkmingai pasiekia atakuojamą serverį. Rezultatai fiksuojami Zeek įvykių žurnale.



pav. 16 DoS ir log filtravimo scriptų paleidimas. Trečias bandymas.

1.2.2. Testas 2. Brutalios jėgos ataka.

Testo metu bus vykdoma kontroliuojama „bruteforce“ tipo atakos simuliacija, siekiant įvertinti IDS ir NDR sprendimų gebėjimą aptikti pakartotinius neteisėtus autentifikacijos bandymus.

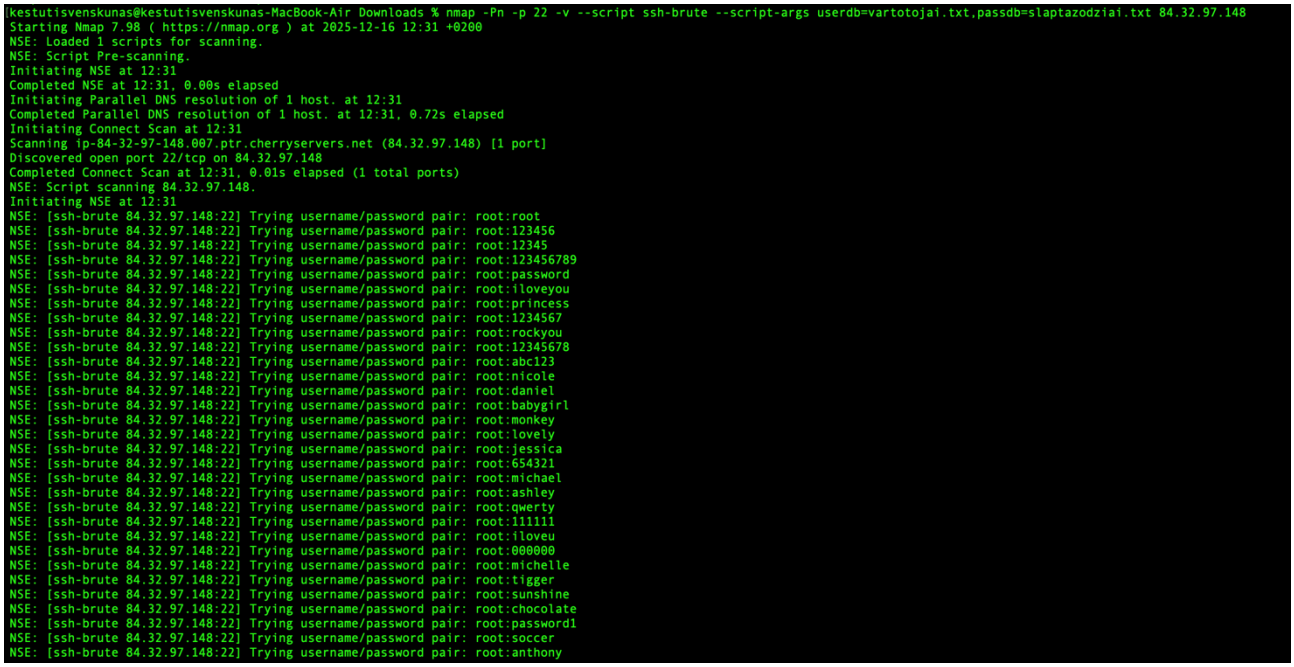
Testui paruošiamas aukos serveris su aktyvia SSH paslauga, veikiančia per 22 TCP prievadą. Bandymas atliekamas izoliuotoje laboratorinėje aplinkoje, skirtoje tik tyrimams, siekiant užtikrinti, kad nebūtų pažeistos realios sistemos ar trečiųjų šalių paslaugos.

Atakos įgyvendinimui naudojamas tinklo skenavimo įrankis „Nmap“ su NSE (Nmap Scripting Engine) scenarijumi *ssh-brute*.

Atakos metu automatizuotai vykdomi nuoseklūs prisijungimo bandymai prie SSH paslaugos, naudojant iš anksto parengtą naudotojų vardų ir slaptažodžių sąrašą. Scenarijus generuoja daug autentifikacijos užklausų per trumpą laiką, taip imituodamas bruteforce atakos elgseną ir sudarydamas sąlygas identifikuoti neįprastą prisijungimų modelį.

Testo metu stebimi IDS ir NDR sistemų registruojami įvykiai, įspėjimai ir tinklo srauto charakteristikos. Analizuojama, ar saugumo sprendimai geba aptikti didelį nesėkmingų prisijungimų skaičių, identifikuoti bruteforce atakai būdingus požymius bei laiku sugeneruoti perspėjimus. Gauti rezultatai naudojami vertinant aptikimo efektyvumą ir bruteforce atakų identifikavimo tikslumą.

Fiksuojamas laikas, paleidžiama ataka (Paveikslas 17). Atakos metu Nmap imituoja prisijungimus prie aukos serverio root vartotoju, naudojant slaptažodžius, sugeneruotus atskirame txt faile. Visa ataka trunka iki 1 min. Pirmam bandymui įvykus sėkmingai, tęsiame testavimą.



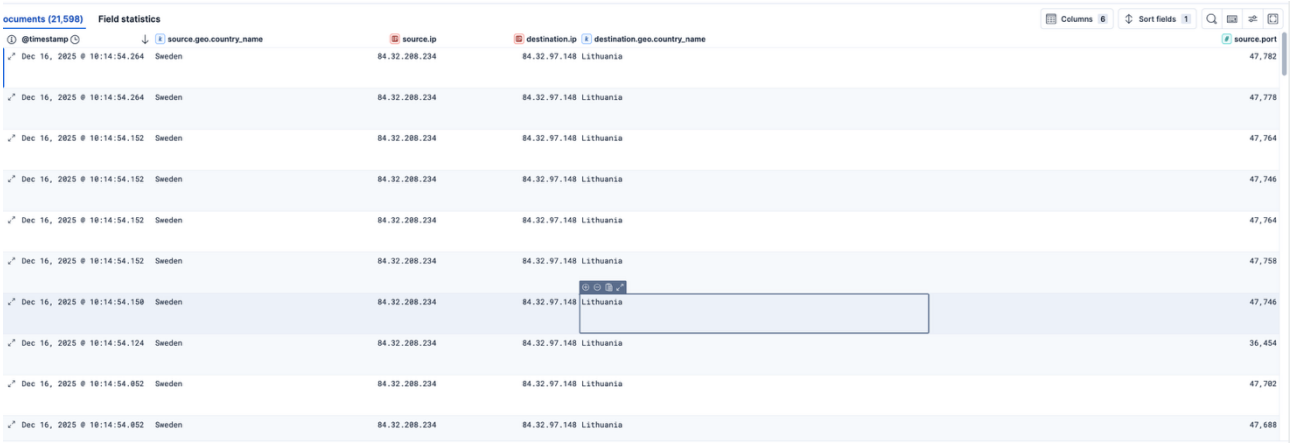
pav. 17 Brutalios jėgos atakos paleidimas. Pirmas bandymas.

Antro bandymo metu ilginame atakos laiką iki 5 minučių. Kartojame išlaikydami tuos pačius parametrus siekiant neįvesti papildomų kintamųjų (Paveikslas 18). Lygiagrečiai stebimas tinklo srautas tcpdump pagalba, bei analizuojami Zeek įvykių žurnalai.

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-16 13:37 +0200
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 13:37
Completed NSE at 13:37, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 13:37
Completed Parallel DNS resolution of 1 host. at 13:37, 0.01s elapsed
Initiating Connect Scan at 13:37
Scanning ip-84-32-97-148.007.ptr.cherryservers.net (84.32.97.148) [1 port]
Discovered open port 22/tcp on 84.32.97.148
Completed Connect Scan at 13:37, 0.00s elapsed (1 total ports)
NSE: Script scanning 84.32.97.148.
Initiating NSE at 13:37
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:root
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:123456
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:12345
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:123456789
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:password
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:iloveyou
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:princess
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:1234567
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:rockyou
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:12345678
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:abc123
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:nicole
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:daniel
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:babygirl
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:monkey
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:lovely
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:jessica
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:654321
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:michael
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:ashley
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:qwerty
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:111111
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:iloveu
NSE: [ssh-brute 84.32.97.148:22] Trying username/password pair: root:000000
```

pav. 18 Brutalios jėgos atakos paleidimas. Antras bandymas.

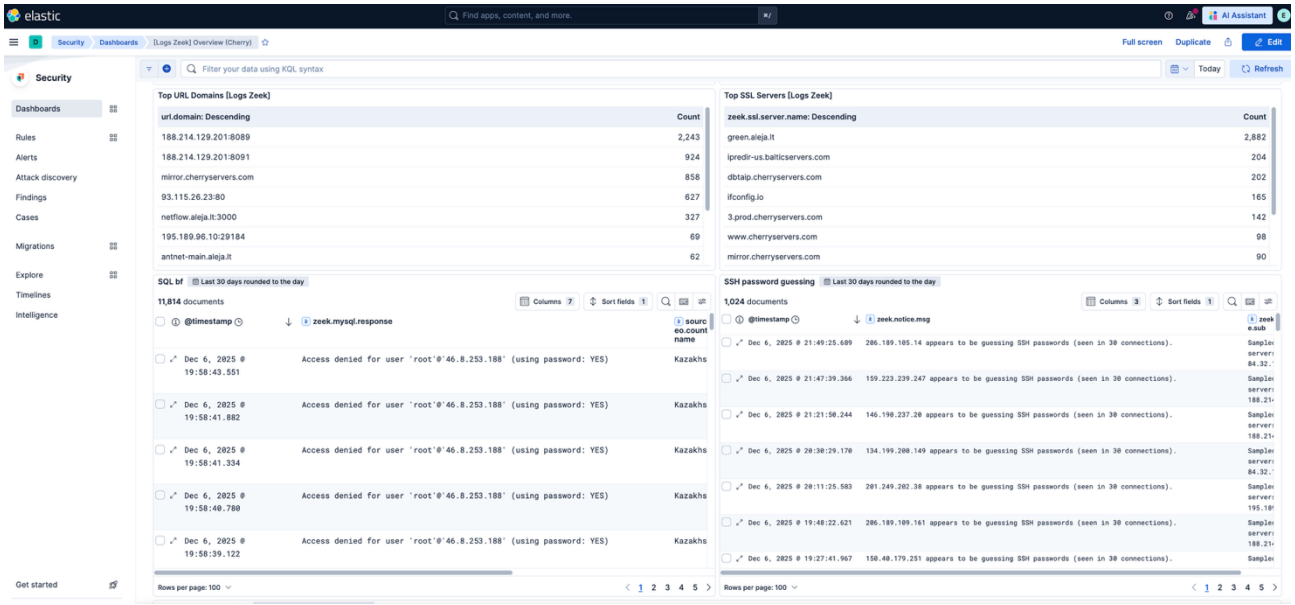
Testavimų pabaigoje patikrinama ar rezultatai atvaizduojami Elasticsearch dalyje. Matomas nuokrypis nuo atakos laiko. Akivaizdu, kad duomenys nėra momentiniai. Kai kuriais atvejais nuokrypiai svyruoja nuo 30 min. iki 1 valandos.



pav. 19 Rezultatų atvaizdavimas elasticsearch dalyje.

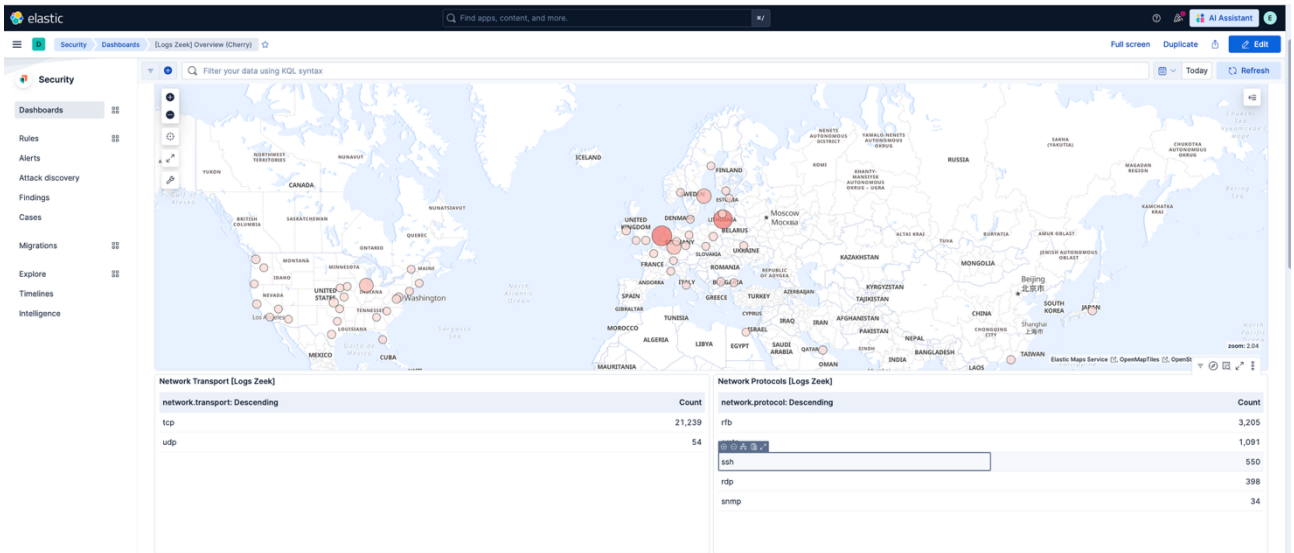
1.3. SIEM vizualizacijos ir ataskaitos

Paruoštoje SIEM dalies aplinkoje matome, jos visos atakos buvo aptiktos. Taigi, informacijos praradimų neturime. Kadangi žinome pagrindines testo eigą iš įvykių detalizacijos galime daryti išvadas apie rezultatų išsamumą ir patikimumą.



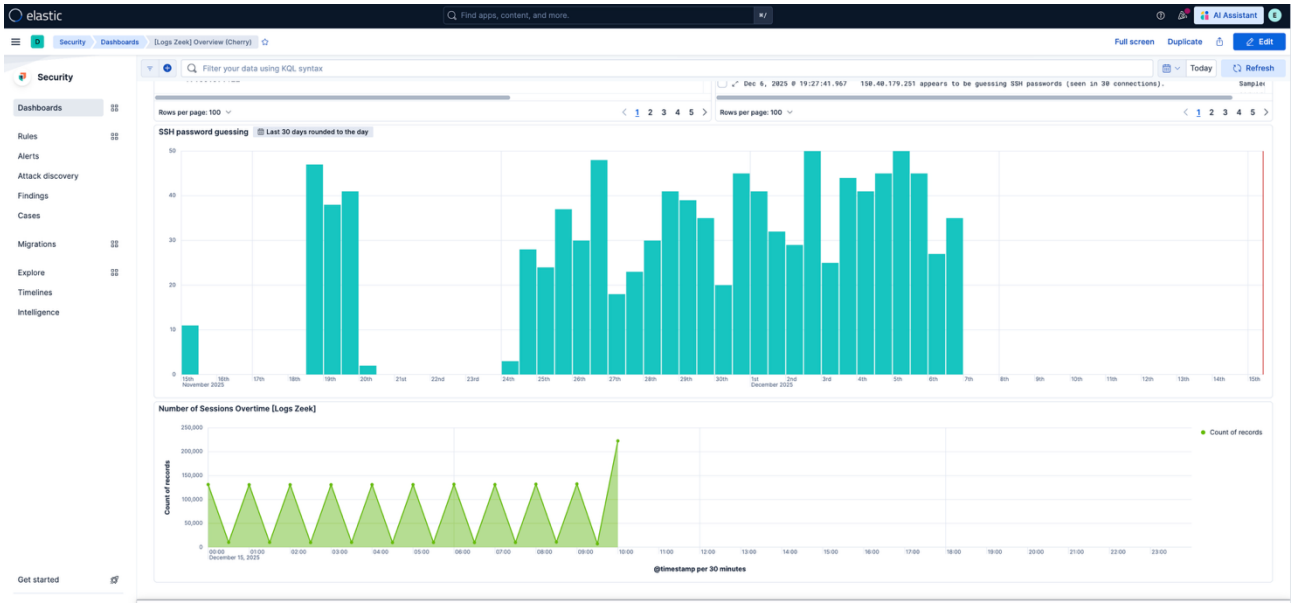
pav. 20 Ekrano infografikų pritaikymas pagal atakos pobūdį elasticsearch dalyje.

Paruoštoje geolokacijų švieslentėje galime matyti prisijungimus iš kitų lokacijų, apart mūsų testuojamų. Kadangi aukos serverio ssh prievadas nebuvo apribotas dedikuotais prisijungimais, o paliktas viešai prieinamu iš išorės, tai rodo, jog tuo pačiu metu buvo atsitiktinių bandymų jungtis prie mūsų testuojamos sistemos. Šie rezultatai taip pat fiksuoti. Matoma, kad bandyta jungtis tiek iš Pakistano, Rusijos, Bulgarijos, Indijos. Šie rezultatai buvo filtruojami, nes nesusiję su tyrimu.



pav. 21 Ekrano infografikų pritaikymas pagal geolokaciją elasticsearch dalyje.

Tinklo ir ssh sesijų apkrovos grafikuose taip pat pastebime pikus testavimo metu. Tokia galimybė leidžia vertinti duomenis istoriškai ir matyti anomalijas tinklo srauto pusėje, nenaudojant papildomų monitoringo priemonių.



pav. 22 Ekrano infografikų paruošimas tendencijų stebėjimui elasticsearch dalyje.

1.4. **Atviro kodo sprendimų ribotumai MVĮ**

Pasirinkto ir testuojamo sprendimo ribotumas pasižymi tuo, kad net turint bazinį sprendinį, jį nuolat reikia tobulinti, palaikyti ir pritaikyti pagal organizacijos poreikius. Tai reikalauja papildomų kompetencijų iš sprendimą prižiūrinčių žmonių. Kitu atveju didėja klaidos rizika, kad gali įtakoti sprendinio veikimą arba privesti prie atvirų spragų jame ir suteikti atakuotojui galimybę vykdyti eksfiltracijos ar panašaus tipo atakas.

6. DISKUSIJA

6.1.Tinklo OSS sprendimų efektyvumas MVĮ

Iš anksčiau įvardintų metrikų galime apskaičiuoti vidutinis aptikimo laikas (MTTD) ir klaidingų aliarmų rodiklis (FAR). Negalime apskaičiuoti logų pilnumo, nes neturime nustatyto etalono. Sistemos resursų apkrovimo nustatymo galimybė taip pat ribota, nes nėra pokyčio paleidus Zeek servisą be srauto nukreipimo į jo pusę, bei paleidus srauto nukreipimą. Pokytis yra kelių procentinių punktų ribose, kas gali būti traktuojama kaip paklaida. Kad realistiškai įvertinti Zeek įtaką sistemos resursams, reiktų dirbtinai generuoti tinklo užklausų srautą ir testuoti tarpinius rezultatus.

lentelė 2. MTTD ir FAR rezultatų apibendrinimas

Testo scenarijus	Incidento tipas	MTTD (vidutinis aptikimo laikas)	FAR (klaidingų aliarmų rodiklis)	Pastabos
Testas 1	DoS atakos simuliacija	~45 min	0 %	Zeek įvykiai fiksuoti realiuoju laiku, vėlavimas susijęs su ELK indeksavimu
Testas 2	Bruteforce ataka	~23 min	0 %	Aptikti visi suplanuoti bandymai, atsitiktinis interneto triukšmas neklasifikuotas kaip FP

6.2.Praktiniai diegimo iššūkiai

Praktiškai diegiant pasirinktą sprendimą susiduriame su keliomis limitacijomis. Viena iš jų – Zeek sprendimas skirtas atviro kodo platformoms Linux, Unix pagrindu. Norint pritaikyti jį Windows Server plafromai reiktų naudoti konteinerizacijos įrankius, tokius, kaip Docker, Podman ar pan. Tai gali sukelti patikimumo, bei saugumo iššūkių. Be to negarantuota, kad įrankis pilnavertiškai funkcionuos jose. Kitas iššūkis – sprendimo palaikymas ir tobulinimas. Netobulinant Zeek sprendinio, jis gali pakankamai greitai pasenti, bei neatliepti naujausių kibernetinio saugumo iššūkių. Taip pat įrankis turi būti integruojamas į kitus sprendinius, tokius kaip SIEM, IDS, IPS sprendinius, Kitu atveju jo rezultatai bus neagreguoti ir labai sunkiai skaitomi.

6.3.Atitikimo ENISA gairėms vertinimas

Atlikto tyrimo rezultatai leidžia įvertinti, kiek pasirinktas atviro kodo tinklo saugumo sprendinys atitinka ENISA pateiktas NIS2 techninio įgyvendinimo gaires, ypač tas, kurios susijusios su tinklo stebėsena, incidentų aptikimu ir techninių įrodymų formavimu. Vertinimas grindžiamas ne formaliu technologijų sąrašo atitikimu, bet funkciniu požiūriu – ar įgyvendintos priemonės realiai leidžia pasiekti ENISA apibrėžtus saugumo tikslus MVĮ kontekste.

ENISA gairėse tinklo stebėsena ir incidentų aptikimas įvardijami kaip esminės priemonės, leidžiančios laiku identifikuoti kibernetines grėsmes ir sumažinti jų poveikį. Tyrime naudotas „Zeek“ NDR sprendimas kartu su ELK platforma užtikrino nuolatinę tinklo srauto analizę, protokolų lygmens įvykių fiksavimą ir jų centralizuotą koreliaciją.

Tai atitinka ENISA rekomendaciją rinkti ir analizuoti tinklo telemetriją tiek perimetro, tiek vidinių srautų lygmenyje. Be to, eksperimentų metu buvo sėkmingai aptikti tiek paslaugų sutrikdymo, tiek bruteforce tipo incidentai, kas rodo, jog pasirinktos priemonės leidžia identifikuoti skirtingo pobūdžio grėsmes, kaip numatyta gairėse.

Svarbi ENISA gairių dalis yra techninių įrodymų ir atsekamumo užtikrinimas. Tyrime suformuota centralizuota logų rinkimo architektūra sudarė sąlygas kaupti laiko žymomis pagrįstus įvykių įrašus, rekonstruoti incidentų eigą ir pagrįsti aptikimo faktą objektyviais duomenimis. Šis aspektas tiesiogiai atitinka ENISA reikalavimą, kad organizacijos gebėtų ne tik deklaruoti saugumo priemonių taikymą, bet ir pateikti patikrinamus įrodymus priežiūros institucijoms. Nors aptikimo laikas SIEM lygmenyje nebuvo momentinis, pati įrodymų bazė buvo pakankama incidentų identifikavimui ir vėlesniam analizės procesui.

Kita vertus, tyrimas atskleidė ir tam tikrus neatitikimus ar ribotumus ENISA gairių kontekste. Gairėse akcentuojamas savalaikis aptikimas ir greitas reagavimas, tuo tarpu eksperimentuose nustatytas santykinai didelis MTTD, nulemtas duomenų ingestavimo ir indeksavimo vėlavimų.

Tai rodo, kad nors techninis aptikimas tinklo lygmenyje buvo įgyvendintas, operacinis aptikimo greitis MVĮ aplinkoje gali neatitikti realaus laiko reagavimo scenarijų be papildomų optimizacijų. Šis aspektas patvirtina ENISA gairėse įvardytą poreikį ne tik diegti priemones, bet ir nuolat vertinti jų eksploatacines savybes.

Apibendrinant galima teigti, kad pasirinktas sprendinys iš esmės atitinka ENISA technines gaires tinklo stebėsenos, incidentų aptikimo ir įrodymų formavimo srityse, ypač vertinant MVĮ proporcingumo principą. Sprendinys leidžia įgyvendinti bazinius NIS2 21 straipsnio reikalavimus ir pateikti techninius įrodymus atitikties vertinimui.

Tačiau tyrimo rezultatai taip pat rodo, kad pilnam ENISA gairių tikslų pasiekimui būtinas papildomas dėmesys operaciniam aptikimo greičiui, automatizacijai ir stebėsenos grandinės optimizavimui, ypač tais atvejais, kai siekiama ne tik atitikties, bet ir aktyvaus incidentų reagavimo realiuoju laiku.

6.4.Nepadengtos rizikos tinklo lygmenyje

Nei Zeek nei ELK neturi pažeidžiamumų skanavimo logikos, kas yra vienas iš ENISA techninių reikalavimų (Priedas Nr. 4). Tai reiškia, kad sprendinį reikia vystyti integruojant papildomai pažeidžiamumo skanavimo, kenkėjiško kodo įrankius. Nors nmap turi NSE modulius pažeidžiamumų skanavimui, pats įrankis reikalautų papildomos orkestravimo, bei rezultatų agregavimo logikos. Iš paruoštų ir pilnavertiškai galimų naudoti atviro kodo sprendinių tai galėtų būti OpenVAS (pažeidimų skanavimo mechanizmas).

7. REKOMENDACIJOS MVĮ

7.1.Minimalus NIS2 tinklo saugumo profilis

Remiantis atliktu tyrimu ir laboratorinių eksperimentų rezultatais, galima apibrėžti realų minimalų NIS2 tinklo saugumo profilį, pritaikytą mažo ir vidutinio dydžio organizacijoms.

Toks profilis grindžiamas ribotu, tačiau valdomu tinklo segmentavimu, kai infrastruktūra suskirstoma bent į naudotojų ir serverių zonas, aiškiai dokumentuojant jų tarpusavio ryšius.

Eksperimento metu taikytas centralizuotas srauto filtravimas ugniasienėje parodė, kad „deny-by-default“ politika ir kritinių paslaugų prieigos ribojimas per saugius kanalus reikšmingai sumažina atakos paviršių. Pasyvios tinklo stebėsenos sprendimas „Zeek“ užtikrino DoS ir bruteforce tipo atakų aptikimą tinklo lygmenyje, netaikant galinių taškų agentų, todėl jis laikytinas pakankamu minimaliame profilyje.

Centralizuotas logų rinkimas ELK platformoje sudarė sąlygas kaupti techninius įrodymus, atkurti incidentų laiko juostą ir pagrįsti atitiktį NIS2 21 straipsnio reikalavimams, nors operacinis aptikimo greitis buvo ribotas dėl duomenų apdorojimo vėlavimų. Papildomai nustatyta, kad periodinės incidentų simuliacijos yra būtinos minimalaus profilio dalis, nes jos leidžia patikrinti realų kontrolės priemonių veikimą ir užtikrinti audituojamą, empiriškai pagrįstą tinklo saugumo lygį.

7.2.Tipinės klaidos diegiant IDS ir NDR

Galima identifikuoti kelias tipines klaidas, kurios dažniausiai pasitaiko diegiant IDS ir NDR sprendimus mažo ir vidutinio dydžio organizacijų aplinkoje.

Viena dažniausių klaidų yra netinkamas sensorių pozicionavimas tinkle. Tyrimo metu nustatyta, kad tik tinkamai parinktas stebėjimo taškas (pvz., SPAN/TAP arba srauto veidrodinis atvaizdas iš ugniasienės) leidžia užtikrinti pakankamą tinklo matomumą. Netinkamai parinkus vietą, IDS ar NDR sprendimai fiksuoja tik dalinį srautą, o tai lemia neaptiktus incidentus ir klaidingą saugumo jausmą.

Kita reikšminga klaida – nepakankamas dėmesys logų koreliacijai ir laiko sinchronizacijai. Eksperimento metu pastebėta, kad duomenų ingestavimo ir indeksavimo vėlavimai SIEM aplinkoje tiesiogiai veikia aptikimo laiką, net jei pats sensorius įvykius fiksuoja realiuoju laiku. Laiko žymų nesuderinamumas arba neoptimizuota logų apdorojimo grandinė apsunkina incidentų laiko juostos atkūrimą ir gali trukdyti laikytis NIS2 nustatytų pranešimo terminų.

Trečioji tipinė klaida yra perteklinių arba neadaptuotų taisyklių naudojimas. IDS ir NDR sprendimai, diegiami su numatytosiomis konfigūracijomis, dažnai generuoja didelį informacinio triukšmo kiekį, kuris MVĮ aplinkoje nėra efektyviai apdorojamas. Tyrimas parodė, kad be kontekstinio filtravimo ir koreliacijos klaidingų perspėjimų rizika didėja, o analitiniai resursai eikvojami neesminiams įvykiams. Galiausiai, dažna klaida yra IDS ir NDR traktavimas kaip

vienkartinio diegimo sprendimų, neplanuojant periodinių testų ir peržiūrų. Tik reguliariai tikrinant aptikimo mechanizmus galima užtikrinti jų ilgalaikį veiksmingumą ir atitiktį NIS2 reikalavimams.

IŠVADOS

Šio darbo tikslas suformuluotas kaip atviro kodo sprendimų, skirtų tinklo dalies kibernetinių incidentų identifikavimui ir užkardymui, ištyrimas ir sprendinio pritaikymas smulkaus ir vidutinio dydžio organizacijų infrastruktūrai, o uždaviniai apima literatūros analizę, diegimo iššūkių nustatymą, prototipo sukūrimą ir jo privalumų bei trūkumų vertinimą.

Praktinėje dalyje sukonstruotas prototipas, kuriame „Zeek“ veikia kaip pasyvus NDR sensorius, o ELK – kaip centralizuota įrodymų ir koreliacijos platforma.

Papildomai taikomi Nmap ir ELK kaip matavimo ir srauto modeliavimo priemonės. Kontroliuojamų bandymų eiga parodo, kad sprendinys geba fiksuoti atakų artefaktus ir kaupti įrodymus tolesnei analizei.

Empiriškai nustatyta, jog aptikimo duomenys nėra momentiniai, todėl realus MTTD priklauso ne vien nuo sensoriaus, bet ir nuo ingestavimo/indeksavimo grandinės. Nors SIEM aplinkoje konstatuojama, kad visos atakos buvo aptiktos, foninis „interneto triukšmas“ (atsitiktiniai SSH bandymai iš įvairių šalių, kuriuos teko filtruoti) rodo klaidingų signalų riziką ir FAR jautrumą ekspozicijai. Apibendrinant, tikslai ir uždaviniai iš esmės pasiekti: atlikta analizė, suformuotas ir eksperimentiškai patikrintas MVĮ pritaikomas prototipas bei įvardyti ribotumai.

Kartu užkardymo dimensija šiame etape labiau pagrindžiama įrodymų baze ir sprendimų priėmimu (reagavimo veiksmams), nei automatizuotu blokavimu, todėl tai laikytina natūralia tolesnio darbo kryptimi.

Atviro kodo sprendimai gali būti taikomi tinklo dalies apsaugai ir atitinka NIS2 21 straipsnio gaires, ENISA techninius reikalavimus. Zeek gali pilnavertiškai atlikti NDR (angl. Network Detection and Response) tiek IDS (angl. Intrusion Detection System) funkcijas. Tačiau reikia adaptavimo specifiškai pagal organizacijos poreikius. ELK gali atlikti SIEM rolę, tačiau reikalingas švieslenčių (angl. Dashboards), užklausų paruošimas saugumo komandų poreikiams.

LITERATŪRA

1. NIS2 Directive: securing network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
2. CSIRTs Network. https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/csirts-network
3. EU CyCLONe. https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone
4. NIS2 Direktyva (ES) 2022/2555 2, 3, 21–24 straipsniai ir I–II priedai. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
5. ENISA oficiali NIS2 santrauka ir sektorių paaiškinimas. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
6. Oficialios statistikos portalas. https://osp.stat.gov.lt/statistiniu-rodikliu-analize?hash=519d17f6-2065-4653-b31b-01f6448b090a#/
7. Lietuvos Respublikos kibernetinio saugumo įstatymas. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr
8. Axelsson, S. (2000). The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security*, 3(3), 186–205. https://doi.org/10.1145/357830.357849
9. Behl, A., & Behl, K. (2017). *Cyberwar: The next threat to national security and what to do about it*. Oxford University Press.
10. Kent, K., & Souppaya, M. (2006). *Guide to computer security log management (NIST Special Publication 800-92)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92
11. Kindervag, J., Foresman, P., & Mackey, D. (2017). *Build security into your network's DNA: The zero trust network architecture*. Forrester Research.
12. Paxson, V. (1999). Bro: A system for detecting network intruders in real-time. *Computer Networks*, 31(23–24), 2435–2463. https://doi.org/10.1016/S1389-1286(99)00112-7
13. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST Special Publication 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
14. Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267–270. https://doi.org/10.1016/j.im.2009.05.002

15. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25
16. Scarfone, K., & Mell, P. (2012). *Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94
17. Stallings, W. (2018). *Network security essentials: Applications and standards* (6th ed.). Pearson.
18. International Organization for Standardization. (2018). *ISO/IEC 27033-1: Network security — Part 1: Overview and concepts*. ISO.
19. International Organization for Standardization. (2020). *ISO/IEC 27033-2: Network security — Part 2: Guidelines for the design and implementation of network security*. ISO.
20. International Organization for Standardization. (2022). *ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
21. National Institute of Standards and Technology. (2020). *Zero trust architecture (NIST Special Publication 800-207)*. https://doi.org/10.6028/NIST.SP.800-207
22. National Institute of Standards and Technology. (2012). *Guide to intrusion detection and prevention systems (IDPS) (NIST SP 800-94)*. https://doi.org/10.6028/NIST.SP.800-94
23. National Institute of Standards and Technology. (2006). *Guide to computer security log management (NIST SP 800-92)*. https://doi.org/10.6028/NIST.SP.800-92.
24. NIS2 (Direktyva (ES) 2022/2555): https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
25. CIR 2024/2690: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
26. ENISA NIS2 Technical Implementation Guidance: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
27. EK (LT) „TIS 2 direktyva“: https://digital-strategy.ec.europa.eu/lt/policies/nis2-directive
28. Zeek docs: https://docs.zeek.org/en/master/index.html
29. Elastic Zeek module: https://www.elastic.co/docs/reference/beats/filebeat/filebeat-module-zeek
30. pfSense docs: https://docs.netgate.com/pfsense/en/latest/index.html
31. Nmap manpage: https://svn.nmap.org/!svn/bc/3320/nmap/docs/nmap_manpage.html
32. NKSC (Kibernetinio saugumo įstatymas): https://www.nksc.lt/kibernetinio-saugumo-istatymas
33. MITRE ATT&CK: https://attack.mitre.org/
34. Linux kernel VXLAN docs: https://www.kernel.org/doc/html/latest/networking/vxlan.html

PRIEDAI

1. Priedas Nr. 1. PlantUML kodas.
2. Priedas Nr. 2. Mermaid kodas.
3. Priedas Nr. 3. ENISA Technical implementation guidance on cybersecurity risk management measures version 1.0.pdf
4. Priedas Nr. 4. ENISA Technical Implementation Guidance Mapping table version 1.2.xlsx