SLOVENSKI INŠTITUT ZA REVIZIJO
LJUBLJANA

ZAKLJUČNO DELO

ZA PRIDOBITEV STROKOVNEGA NAZIVA

PREIZKUŠENEGA REVIZORJA INFORMACIJSKIH SISTEMOV

REVIZIJSKO POROČILO O DELOVANJU VARNOSTNO-NADZORNEGA SISTEMA MICROSOFT SENTINEL ZA ZAGOTAVLJANJE SKLADNOSTI Z ZAHTEVAMI GDPR / ZVOP-2, NIS-2 / ZINFV-1 IN DORA.

SEPTEMBER 2025

GAŠPER BERTONCELJ

IZJAVA

GAŠPER BERTONCELJ, vpisan v izobraževalni program za pridobitev strokovnega naziva preizkušeni revizor informacijskih sistemov izjavljam, da sem avtor tega zaključnega dela in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovoljujem objavo zaključnega dela na spletnih straneh Slovenskega inštituta za revizijo.

V Medvodah 23. septembra 2025

Podpis:  2025.10.24 14:18:42 +02'00'

Vsebina

Kazalo tabel

Kazalo slik

Uvod

Ozadje in kontekst

Paketek, d. o. o., v nadaljevanju revidiranec, nastopa kot bistveni subjekt po ZInfV-1[1] ter hkrati kot tretja oseba IKT[2] za zavezance po *DORA*[3]. V okviru krepitve kibernetske varnosti in regulatorne skladnosti, je v organizaciji uveden varnostno-nadzorni sistem Microsoft Sentinel (*SIEM*[4] / *SOAR*[5]) za spremljanje dogodkov, zaznavo incidentov ter podporo poročanju pristojnim organom in naročnikom. Ključna tveganja, ki jih obravnava ta naloga, vključujejo:

(i) pokritost in hrambo dnevnikov,
(ii) učinkovitost zaznave in eskalacije incidentov
(iii) priglasitev *CSIRT*[6] in poročanje po *GDPR*[7] / ZVOP-2[8], *NIS 2*[9] / ZinfV-1 in DORA,
(iv) upravljanje dostopov (*RBAC*[10] / *PIM*[11] / *JIT*[12]) ter
(v) evidence, vezane na obdelavo OP[13] in pogodbene obveznosti v razmerjih IKT.

Namen in cilji

Namen naloge je presoditi, ali delovanje Microsoft Sentinel pri revidirancu, zadostno podpira skladnost z zahtevami ZInfV-1[14], ZVOP-2[15], GDPR[16] ter DORA[17] in povezanimi *RTS*[18,19] / *ITS*[20,21].

---

[1] Zakon o informacijski varnosti (ZInfV-1) (Državni zbor Republike Slovenije, 2025).
[2] IKT – informacijsko-komunikacijska tehnologija
[3] UREDBA (EU) 2022/2554 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011. (European Parliament and Council of the European Union, 2022, str. OJ L 333, pp. 1–79)
[4] SIEM, angl. Security Information and Event Management – sistem za upravljanje varnostnih informacij in dogodkov.
[5] SOAR, angl. Security Orchestration and Response – orkestracija in varnostno odzivanje.
[6] CSIRT, angl. Computer Security Incident Response Team – skupina za odzivanje na incidente na področju računalniške varnosti.
[7] UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). (European Parliament and Council of the European Union, 2016)
[8] Zakon o varstvu osebnih podatkov (ZVOP-2). (Uradni list RS, 2022)
[9] DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2). (European Parliament & Council of the European Union, 2022)
[10] RBAC, angl. Role Based Access Control – upravljanje dostopa glede na vlogo/nalogo uporabnika.
[11] PIM, angl. Privileged Identity Management – upravljanje privilegiranih identitet. Upravljavski mehanizem za časovno omejeno (»just-in-time«) dodeljevanje in nadzor privilegiranih vlog v imeniku in oblačnih storitvah. V okolju Microsoft Entra ID (nekdanji Azure AD) PIM omogoča, da so skrbniške vloge upravičene (angl. eligible) in se aktivirajo le po potrebi, običajno z odobritvijo, MFA, utemeljitvijo ter z revizijsko sledjo in periodičnimi pregledi dostopov. S tem se odpravlja trajni (angl. standing) skrbniški dostop in uveljavlja načelo najmanjših pravic.
[12] JIT, angl. Just In Time – ravno ob pravem času.
[13] OP – osebni podatek. Vsak podatek ki lahko kaže na določenega ali določljivega posameznika.
[14] Zlasti 21., 22., 24., 30. in 36. člen.
[15] 22. člen.
[16] 33. člen.
[17] 19., 28. in 30. člen.
[18] RTS, angl. Regulatory Technical Standard - regulativni tehnični standardi. Pravno zavezujoči podrobni standardi, ki tehnično dopolnijo osnovni zakon (t. i. “raven 1”). Osnutke pripravijo evropski nadzorni organi (ESA: EBA, ESMA, EIOPA), sprejme pa jih Evropska komisija kot delegirane akte. Namen je natančno določiti merila, prage, podatkovna polja ipd., da je izvajanje enotno po EU.
[19] Delegirana uredba (EU) 2025/301 (European Commission, 2025).
[20] ITS, angl. Implementing Technical Standard - izvedbeni tehnični standardi. Pravno zavezujoči standardizirani postopki, obrazci in predloge, ki zagotavljajo enotno izvajanje zakonodaje po vsej EU. Osnutke pripravi ESA, Komisija jih sprejme kot izvedbene akte (implementing acts).
[21] Izvedbena uredba (EU) 2025/302. (European Commission, 2025)

Cilji so:

- C1: Ovrednotiti pokritost virov in hrambo / nespremenljivost dnevnikov (vsaj 6 mesecev; lokacije RS / EU).
- C2: Oceniti zadostnost detekcijskih pravil in *IR*[22], vključno s priglasitvami CSIRT in režimom visoka / kritična ogroženost.
- C3: Preveriti zahteve glede VOP[23] (dnevnik obdelave, rok hrambe 2–5 let, dostopnost nadzornemu organu).
- C4: Oceniti organizacijski in pogodbeni okvir revidiranca, glede na zahteve DORA, kadar nastopa kot tretja oseba, ki s storitvijo IKT omogoča kritično ali pomembno funkcijo stranke, ki je zavezanec za DORA (register, obvezne klavzule, pomoč ob incidentih, nadaljnje pod izvajanje, izhodna strategija).
- C5: Izvesti analizo vrzeli in pripraviti prednostno razvrščena priporočila, vezana na tveganja in skladnost.

Predmet in delovni okvir

Predmet presoje je delovanje sistema Microsoft Sentinel in spremljajočih procesov (IR, poročanje CSIRT, upravljanje dostopov, evidence obdelave OP, pogodbeni vidiki DORA). Vključeni so: povezovalniki[24] in tabele (Log Analytics / Archive), pravila analitike, scenariji odziva / SOAR, nastavitve hrambe in dostopov, evidence incidentov, dnevnik obdelave in vzorčni nabor pogodb / registra IKT. Izključeno je: vdorno testiranje, forenzika in pravno svetovanje; ocena DORA pri naročnikih je omejena na sposobnost revidiranca podpreti njihove obveznosti.

Raziskovalna vprašanja (RV)

- RV1: Ali je pokritost virov in rok hrambe[25] ter nespremenljivost[26] zapisov v Sentinelu zadostna za skladnost in dokazljivost?
- RV2: Ali detekcijska pravila in proces IR omogočajo pravočasno zaznavo, klasifikacijo in poročanje nadzornim organom (ZinfV-1 → CSIRT, GDPR / ZVOP-2 → IP[27])?
- RV3: Ali so evidence, vezane na obdelavo OP (dnevnik obdelave, sledljivost posredovanj) vzpostavljene v skladu z ZVOP-2?
- RV4: Ali PIM / JIT / MFA praktično uresničujejo načelo najmanjših pravic in revizijsko sled?
- RV5: Ali vsebujejo, register IKT in pogodbe revidiranca z zavezanci za DORA, obvezne klavzule po DORA ter podpirajo poročanje po RTS / ITS?
- RV6: Kje so ključne vrzeli in katere ukrepe je smiselno prioritetno izvesti?

[22] IR, angl. Incident Response – odziv na incident. Procesi za zaznavo, triažo, analizo, zajezitev, izkoreninjenje, obnovitev in poročanje. ZInfV-1 predpisuje načrt odzivanja na incidente s sistemom zaznave, vlogami / odgovornostmi in protokolom obveščanja pristojnega CSIRT; ureja tudi priglasitev pomembnih incidentov in vrednotenje.
[23] VOP – varstvo osebnih podatkov.
[24] Angl. connectors.
[25] Angl. retention. Čas hrambe.
[26] Angl. immutability.
[27] IP – Informacijski pooblaščenec, nacionalni nadzorni organ za zadeve VOP v RS.

Metodološki okvir

Uporabimo kombinirani pristop:

1. Dokumentarni pregled (politike SUIV[28] / SUNP[29], IR / *BCP*[30], politika hrambe, register IKT, pogodbe, izvozi konfiguracij).
2. Intervjuji (*CISO*[31], skrbniki sistemov, *DPO*[32], pravna služba).
3. Tehnični pregled Sentinela: T1–T4 (pokritost virov, čas hrambe, zagotavljanje nespremenljivosti, PIM / JIT, pravila ter fino uravnavanje[33] z vzorčenjem (uporaba KQL[34], okno 30 dni; za pregled časa hrambe pa 180 dni).
4. Simulacije (table-top): T5–T7 za IR / CSIRT / GDPR in DORA RTS / ITS poročila.
5. Preverjanje pravic posameznikov (vezano na obdelavo OP): T8 (dnevnik obdelave: polja oz. atributi, rok hrambe, dostopnost IP).
6. Režim *H/C*[35]: T9 (preverjanje beleženja, zmožnost pogostejšega poročanja, nadzorna[36] plošča).

Rezultati se sledljivo preslikajo v *RTM*[37], oblikuje se seznam vrzeli z razvrščenimi priporočili in evidenco dokazil (ID povezave RTM↔T-test↔dokazilo). Omejitve: brez vdornih testov in forenzike; ugotovitve temeljijo na vzorčenju in razpoložljivih dokazilih.

Struktura naloge

- Uvod: ozadje, namen / cilji, predmet in okvir, raziskovalna vprašanja, metodologija, struktura.
- Teoretična izhodišča in normativni okvir: ZInfV-1[14]; NIS 2, ZVOP-2[15]; GDPR[16]; DORA[17] s povezanima RTS[19] / ITS[21]; relevantni standardi (ISO/IEC 27001/27002, smernice *ENISA*[38]).
- Metodologija: raziskovalni pristop, tehnike zbiranja podatkov, vzorčenje, merila in testni program T1–T9.
- Empirični del: opis okolja revidiranca in Sentinela; rezultati pregledov / testov z artefakti; RTM in seznam vrzeli.
- Razprava: interpretacija rezultatov; posledice za skladnost in obvladovanje tveganj.
- Sklep: sinteza glavnih ugotovitev, omejitve, možnosti nadaljnjega dela.
- Priloge: revizijski načrt, program testiranja, vprašalniki, RTM, seznam ugotovljenih vrzeli, evidenca dokazil.

---

[28] SUIV – sistem upravljanja varovanja informacij. Organizacijski upravljavski okvir (politike, procesi, odgovornosti, merjenje in nenehno izboljševanje) za obvladovanje tveganj glede zaupnosti, celovitosti in razpoložljivosti informacij. V slovenski regulativi je to poimenovano kot »dokumentiran sistem upravljanja varovanja informacij« (poleg sistema upravljanja neprekinjenega poslovanja).

[29] SUNP – Sistem upravljanja neprekinjenosti poslovanja.

[30] BCP, angl. Business Continuity Plan – načrt neprekinjenega poslovanja. Politika, postopki in vloge za ohranjanje ali obnovitev ključnih dejavnosti ob motnjah; ZInfV-1 ga navaja kot obvezni del varnostne dokumentacije (skupaj z oceno vpliva na poslovanje in minimalno ravnijo poslovanja).

[31] CISO, angl. Chief Information Security Officer – vodja informacijske varnosti.

[32] DPO, angl. Data Protection Officer – pooblaščena oseba za varstvo osebnih podatkov.

[33] Angl. fine tuning.

[34] KQL, angl. Kusto Query Language – poizvedbeni jezik Kusto.

[35] H/C, angl. High/Critical - visoka/kritična ogroženost. V ZInfV-1 je ocena ogroženosti državne kibernetske varnosti razvrščena v stopnje zelo nizka, nizka, srednja, visoka, kritična. Ko pristojni organ razglasi visoko (H) ali kritično (C) ogroženost, nastopijo za zavezance dodatne obveznosti.

[36] Angl. log-health dashboard.

[37] RTM, angl. Request Tracibility Matrix - matrika sledljivosti zahtev.

[38] ENISA, angl. European Network and Information Security Agency.

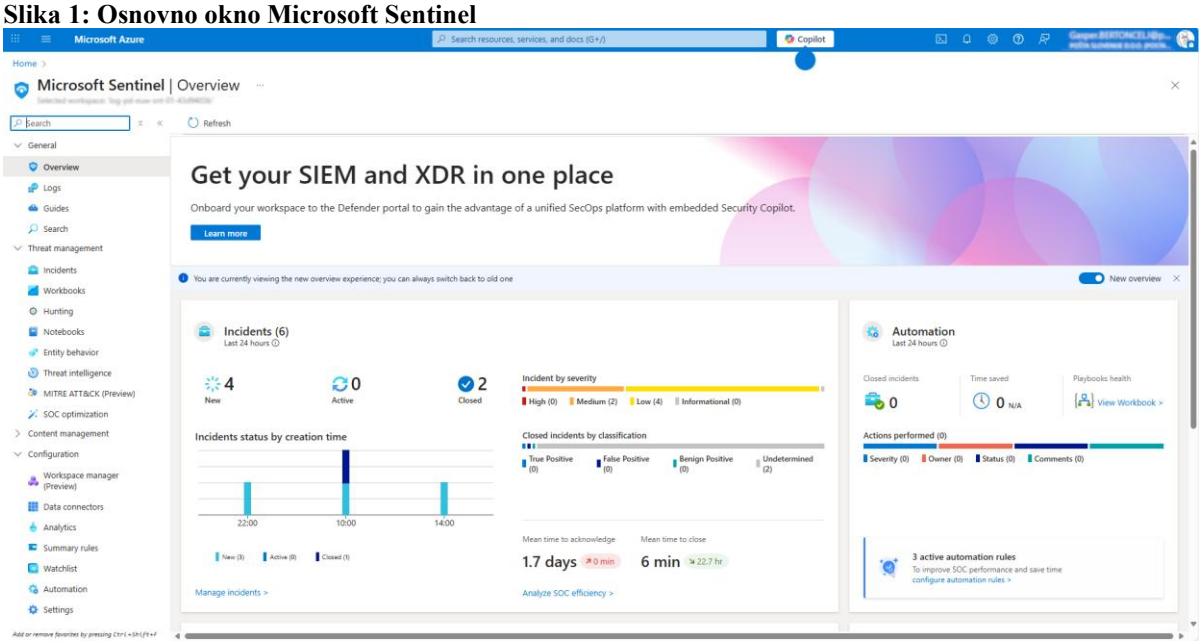
1 Teoretična izhodišča in pregled literature

1.1 Ključni pojmi in opredelitve

SIEM / SOAR (Microsoft Sentinel).

SIEM je sistem za zbiranje, korelacijo in analitiko varnostnih dogodkov, SOAR pa nudi orkestracijo in avtomatizacijo odziva. Microsoft Sentinel je oblačni SIEM / SOAR, ki podpira več-oblačna in hibridna okolja, nudi vsebine (pravila, povezovalniki) ter avtomatizacijo preko Logic Apps. V njem se podatki shranjujejo v *Azure Monitor* / *Log Analytics*, analitika poteka s KQL, odziv pa s scenariji odziva. (Microsoft, 2025) (Microsoft, brez datuma) (Microsoft, 2025) (Microsoft, 2023).

Slika 1: Osnovno okno Microsoft Sentinel



Vir: lasten

Dnevniški zapisi, rok hrambe in nespremenljivost (WORM[39]).

Dnevniški zapisi so strukturirani ali nestrukturirani zapisi dogodkov, ki omogočajo analizo in rekonstrukcijo incidentov. Rok hrambe določa čas hrambe v analitični / arhivski ravni; nespremenljivost (WORM) zagotavlja, da zapisov ni mogoče spreminjati ali brisati znotraj določenega obdobja. V Azure so na voljo politike nespremenljivosti za Blob Storage. (Državni zbor Republike Slovenije, 2025) (Microsoft, 2025) (Microsoft, 2024)

Incident in odzivanje na incidente (IR).

Incident razumemo kot kršitev ali neposredno grožnjo kršitvi varnostnih politik ali običajnega delovanja informacijskih virov oz. sistemov IKT. Učinkovit odziv na incidente zahteva pripravo, zaznavo / analizo, zajezitev, odpravo, obnovo in učenje na podlagi incidenta. Posodobljena usmeritev

[39] WORM, angl. Write Once, Read Many – zapiši enkrat, beri večkrat / nespremenljiva hramba. Način hrambe, pri katerem se podatek ne more več spremeniti ali izbrisati v času veljavnosti politike hrambe.

NIST (SP 800-61) IR umešča v širši okvir upravljanja kibernetskega tveganja in CSF 2.0. (Nelson, Rekhi, Souppaya, & Scarfone, 2025)

CSIRT in poročanje. CSIRT je skupina za odzivanje na incidente, ki sprejema prijave, svetuje in koordinira ukrepe; okvire poročanja predpisujeta NIS 2 in nacionalna zakonodaja (ZInfV-1), za finančni sektor pa DORA z RTS / ITS. (European Parliament & Council of the European Union, 2022, str. L 333, 80–152), (Državni zbor Republike Slovenije, 2025) (European Commission, 2024)

Upravljanje identitet in pravic (RBAC, PIM / JIT) in MFA. Načelo najmanjših pravic se uresničuje z modelom osnovanem na vlogi, funkciji oz. zadolžitvah, ki jih oseba opravlja , časovno omejenimi povišanji (Privileged Identity Management, Just-In-Time) in večfaktorsko overjenje, kar pomembno zmanjšuje površino orodij, kot je Sentinel za vdor oz. napad. (Podprto tudi v Microsoft Entra in Sentinelu.) (Microsoft, 2025)

KPI[40] / *KRI*[41]. Kazalniki uspešnosti in tveganj (npr. *MTTD*[42] / *MTTR*[43], delež avtomatiziranih odzivov, delež onemogočenih pravil) omogočajo merjenje zrelosti zaznavanja/odzivanja; smernice o metrikah in upravljanju dnevnikov izhajajo iz NIST SP 800-92 (v prenovi r1) in dobre prakse ISO. (Scarfone & Souppaya, 2023) (International Organization for Standardization; International Electrotechnical Commission, 2022)

RTM in analiza vrzeli . RTM vzpostavi sledljivost: zahteva → kontrola/proces → test → dokazilo → rezultat, kar omogoča sistematično analizo vrzeli (zahtevano–ugotovljeno–odstopanje–priporočilo) ter s tem skladnost z revizijskimi merili. Način je skladen z ITAF (ISACA) o merilih, dokazilih in poročanju. (ISACA, 2014)

1.2 Regulativni okvir in standardi

NIS 2 in ZInfV-1 (nacionalna implementacija)

Direktiva NIS 2 (2022/2555) določa izhodiščne zahteve upravljanja kibernetskih tveganj ter obveznosti poročanja za bistvene in pomembne subjekte po sektorjih, z mehanizmi zgodnjega opozarjanja in nadaljnjih poročil. (European Parliament & Council of the European Union, 2022, str. L 333, pp. 80–152)

ZInfV-1 (Uradni list RS, št. 40/2025) prenaša NIS 2 in natančneje ureja obveznosti v Sloveniji. Ključne točke za to nalogo: (i) vzpostavitev in vzdrževanje sistemov upravljanja (SUIV/SUNP) ter dokumentacije, (ii) dnevniški zapisi – obseg, integriteta in obvezen rok hrambe najmanj 6 mesecev ter zahteve glede lokacije hrambe RS/EU, (iii) priglasitev incidentov pristojni skupini CSIRT ter (iv)

[40] KPI, angl. Key Performance Indicators – ključni kazalnik učinkovitosti. Količinski kazalniki, s katerimi se meri učinkovitost varnostnih ukrepov/procesov (npr. MTTD, MTTR, pokritost virov dnevnikov, delež pravočasnih priglasitev). ZInfV-1 zahteva, da dokumentacija vključuje postopke za oceno učinkovitosti in določitev kazalnikov učinkovitosti ter analizo zbranih podatkov.

[41] KRI, anlg. Key Risk Indicators – ključni kazalnik tveganja. Metrika, ki zgodaj signalizira povečano izpostavljenost tveganju ali preseganje toleranc/apetita (npr. rast nerazrešenih incidentov visoke resnosti, stopnja neuspešnega krpanja kritičnih ranljivosti, delež neuspešnih privilegiranih prijav).

[42] MTTD, angl. Mean Time to Detect - the average time a problem or incident exists before it is detected. Povprečni čas, ko težava ali varnostni incident obstaja, preden ga organizacija zazna (tj. od začetka nezaželenega dogodka do trenutka odkritja).

[43] MTTR, angl. Mean Time to Recovery - the average time it takes to recover from a failure and return to normal service. Povprečni čas, potreben za obnovitev delovanja po okvari ali incidentu.

režim visoka/kritična ogroženost z dodatnimi preveritvami beleženja in pogostejšim poročanjem. (Državni zbor Republike Slovenije, 2025)

ZInfV-1 tudi opredeli dnevnike ("dnevniški zapisi") in zahteva sinhronizacijo časovnih virov, kar je neposredno relevantno za korelacijo znotraj SIEM. Za subjekte v dometu DORA, določa ZInfV-1 posebna razmerja in delne izključitve, da se prepreči prekrivanje obveznosti. (Državni zbor Republike Slovenije, 2025)

(Sklic in preslikava členov na merila in teste sta povzeta v revizijskem načrtu – RTM-01 do RTM-04, T1–T7/T9.)

GDPR in ZVOP-2

GDPR (EU 2016/679) predstavlja splošni okvir varstva osebnih podatkov v EU. Za to nalogo je najpomembnejši 33. člen (obveščanje nadzornega organa o kršitvi osebnih podatkov v 72 urah, če je verjetno tveganje za pravice in svoboščine posameznikov) ter usmeritve *EDPB*[44] o štetju rokov in vsebini poročil. (European Parliament and Council of the European Union, 2016)

ZVOP-2 (UL RS, št. 163/22) dopolnjuje GDPR na nacionalni ravni. Za ta projekt je ključen 22. člen – dnevnik obdelave, ki ob določenih pogojih zahteva vodenje revizijske sledi dejanj obdelave ter določa rok hrambe praviloma 2 leti (možno podaljšanje na podlagi ocene tveganj). Nadzornemu organu (IP) se na zahtevo omogoči dostop do dnevnika. (Uradni list RS, 2022) (Inštitut za lokalno samoupravo Maribor, 2023)

(Ti zahtevi sta preslikani v RTM-05/RTM-06 in test T8; v Sentinelu to vpliva na zasnovo tabel / časov hrambe in sledljivost dostopov.)

DORA (Digital Operational Resilience Act) in podzakonski akti

DORA (EU 2022/2554) velja od 17. januarja 2025 za finančne subjekte neposredno in ureja upravljanje tveganj IKT, klasifikacijo in poročanje o večjih incidentih ter razmerja s ponudniki storitev IKT (tretje osebe). Posebej relevantna sta člena 28 (register razmerij s tretjimi osebami, ki izvajajo storitve IKT) in 30 (pogodbene zahteve: lokacije, *SLA*[45], vračilo podatkov, pomoč ob incidentih, pod izvajanje). (European Parliament and Council of the European Union, 2022, str. OJ L 333, pp. 1–79)

Komisija je sprejela RTS za klasifikacijo incidentov in pragove (Delegirana uredba (EU) 2024/1772) ter ITS s standardnimi obrazci/šablonami za poročanje (Izvedbena uredba (EU) 2025/302). To omogoča enotno poročanje (začetno/vmesno/končno) in natančno preslikavo polj iz SIEM / SOAR v regulatorne obrazce. (European Commission, 2024) (European Commission, 2025)

ZInfV-1 v 3. členu ureja razmerje do DORA (izključitve / posebni režim), da se preprečijo dvojno poročanje in neskladja. To je pomembno za revidiranca kot tretjo osebo IKT nasproti zavezancem za DORA. (Državni zbor Republike Slovenije, 2025)

[44] EDPB, angl. European Data Protection Board
[45] SLA, angl. Service Level Agreement – dogovor o ravni storitev.

Mednarodni standardi in strokovne smernice

ISO/IEC 27001:2022 (z amandmajem 2024) in ISO/IEC 27002:2022 predstavljata referenčni okvir za SUIV in kontrole (ukrepe); sta izhodišče za politike, procese IR/BCP in pregled privilegiranih dostopov. (International Organization for Standardization; International Electrotechnical Commission, 2022) (International Organization for Standardization, 2024)

NIST SP 800-61r3 (2025) in SP 800-92 (log management; v prenovi r1) podajata praktične smernice za IR, upravljanje dnevnikov, metrike in integriteto revizijskih sledi. (Nelson A. , Rekhi, Souppaya, & Scarfone, 2025)

ITAF (ISACA) določa merila, dokazila, načrtovanje in poročanje za IT revizije; to je neposredna metodološka podlaga za RTM, program testiranja in poročanje v tej nalogi. (ISACA, 2014)

Povzetek posledic za predmet naloge

NIS 2 / ZInfV-1 zahtevata celovit nabor dnevnikov, čas hrambe vsaj 6 mesecev, integriteto (npr. WORM), sinhronizacijo časa in poročanje CSIRT, vključno z režimom visoka / kritična ogroženost (dodatne preverbe, pogostejša poročila). (Državni zbor Republike Slovenije, 2025)

GDPR / ZVOP-2 zahtevata 72-urni rok za obveščanje IP ob kršitvah osebnih podatkov in – kjer je to predpisano – dnevnik obdelave z ustrezno vsebino / rokom hrambe. (European Parliament and Council of the European Union, 2016)

DORA uvaja standardizirano klasifikacijo in obrazce za večje IKT-incidente ter obvezne pogodbene klavzule za IKT tretje osebe; ZInfV-1 priznava posebni režim DORA, da se izogne prekrivanju. (European Parliament and Council of the European Union, 2022, str. OJ L 333, pp. 1–79) (European Commission, 2025)

Standardi in smernice (ISO / NIST / ITAF) dajejo izvedbeni okvir za merila (RTM), testne postopke in dokazila ter za metrike (KPI / KRI). (International Organization for Standardization; International Electrotechnical Commission, 2022) (Nelson A. , Rekhi, Souppaya, & Scarfone, 2025) (ISACA, 2014)

(Zgoraj povzete pravne in standardne reference so v revizijskem načrtu preslikane v konkretna merila in teste – T1–T9, RTM-01…-09 – na katere se bo naslonil empirični del naloge.)

2 Metodologija

2.1 Raziskovalni pristop, tehnike in viri podatkov

Metodološka zasnova naloge temelji na okviru ITAF™ (3. izdaja), ki strukturira poklicno prakso revizije informacijskih sistemov na tri ravni: (1) standarde (obče, izvedbene in poročevalske), (2) smernice (generalne, izvedbene in poročevalske) ter (3) orodja in tehnike. Ta hierarhija zagotavlja, da je načrtovanje, izvedba, dokazovanje in poročanje revizije skladno z mednarodno priznanimi zahtevami stroke. V ITAF 3. izdaji so poročevalski standardi (1401–1402) jasno ločeni od spremljajočih smernic (2401–2402), medtem ko izvedbeni del podrobno naslavlja načrtovanje (1201), oceno tveganj (1202), pomembnost (1204), dokazila (1205), uporabo dela drugih strokovnjakov (1206) ter obravnavo nepravilnosti in protipravnih dejanj (1207). Smernice za izvedbo dodatno vključujejo 2201–2208, med drugim tudi vzorčenje (2208); presek orodij in tehnik je zbran v posebnem delu okvira. (ISACA, 2014)

Načelni temelji in etika.

Obči standardi ITAF (serija 1000) izhajajo iz etike, neodvisnosti, strokovne skrbnosti in usposobljenosti revizorja, ter izpostavljajo določitev revizijske listine, razumne potrebe deležnikov, strokovno presojo in opredelitev meril za presojo. Ti elementi so v 3. izdaji dodatno podprti z ustreznimi generalnimi smernicami (2001–2008), ki operacionalizirajo npr. strokovno skrbnost (Due Professional Care) in usposobljenost skozi življenjski cikel naloge. Vzporedno Kodeks poklicne etike ISACA zavezuje nosilce nazivov in člane k integriteti, objektivnosti, zaupnosti in strokovni usposobljenosti. Skupaj tvorijo normativno podstat za neodvisno presojo in kakovost dokazil. (ISACA, 2014) (ISACA, brez datuma)

Načrtovanje in ocena tveganj.

V fazi načrtovanja se pripravi projektni načrt z jasno opredeljenimi cilji in obsegom (Standard 1201), pri čemer se uporablja ustrezna metodologija ocene tveganj za določitev prioritet in obsega postopkov (Standard 1202). ITAF zahteva dokumentiranje ključnih predpostavk in predstavitev revidiranca v delovnih dokumentih ter sprotno upravljanje sprememb obsega. (ISACA, 2014)

Pomembnost (materialnost) in dokazila.

ITAF razlikuje med zadostnostjo (količina) in ustreznostjo (kakovost) dokazil, na katerih temeljijo zaključki (Standard 1205). Smernice za vzorčenje (Guideline 2208) podpirajo presojo zadostnosti in statistično/naključnostno izbiro vzorcev, skladno z zastavljenimi cilji in tveganji. (ISACA, 2014)

Uporaba dela drugih strokovnjakov.

Kadar je primerno, se lahko uporabi delo drugih strokovnjakov (Standard 1206), ob obvezni presoji njihove ustreznosti, načrtu pregleda njihovega dela in oceni, ali njihovi izsledki zadostujejo za cilje naloge; v nasprotnem primeru je treba razširiti postopke ali odraziti omejitve v poročilu. (ISACA, 2014)

Poročanje in spremljanje izvedbe priporočil.

Po zaključenih postopkih je treba izdati poročilo, v katerem so ugotovitve podprte z zadostnimi in ustreznimi dokazili (Standard 1401), ter izvesti nadaljnje spremljanje za preveritev odziva vodstva na priporočila (Standard 1402). Smernice (2401–2402) podajajo tipologijo poročil, dodatne komunikacije in obravnavo naknadnih dogodkov. (ISACA, 2014)

Povezava ITAF in revizijskega načrta.

V praktični izvedbi naloge je okvir ITAF preslikan v naš Revizijski načrt PRIS-PAKETEK-RN-2025-01, ki opredeljuje cilje in merila, obseg in meje, metodologijo ter program testiranja kontrol (T1–T9), vključno z viri dokazil in merili sprejemljivosti. Načrt določa tudi vzorčenje (opazovalno okno in velikosti vzorcev), upravljanje dokazil in kakovosti ter poročanje, kar ustreza izvedbenim in poročevalskim standardom po ITAF.

Raziskovalni pristop.

Naloga uporablja študijo primera z elementi mešane metodologije (kvalitativni in kvantitativni prijemi), saj se revizijski dokazi pridobivajo tako iz dokumentacije in intervjujev kot iz tehničnih pregledov konfiguracij, dnevniških zapisov in simulacij postopkov odziva na incidente. Namen pristopa je triangulacija dokazov (uskladitev treh perspektiv: dokumenti ↔ tehnična opazovanja ↔ pričevanja), s čimer se krepi veljavnost sklepov skladno z zahtevami ITAF glede zadostnih in ustreznih dokazov.

Tehnike zbiranja in analiziranja podatkov.

a) Pregled dokumentacije: politike varovanja informacij (SUIV / SUNP), postopki IR / BCP, register pogodb IKT, konfiguracije Microsoft Sentinel, evidence CSIRT priglasitev in dnevnik obdelave. Cilj je preverjanje skladnosti, celovitosti in ažurnosti, ter sledenje različicam dokumentov.
b) Intervjuji in usmerjeni razgovori: pol-strukturirani razgovori s CISO, skrbniki sistemov, DPO in pravno službo, osredotočeni na razumevanje vlog (RACI), operativnih praks in odločitev o eskalacijah.
c) Tehnični pregledi in opazovanja (observacija): pregled nastavitev časa hrambe, lokacije podatkov, RBAC / PIM / JIT, analitičnih pravil, scenarijev odziva; poizvedbe KQL za preverjanje integritete, časovnih žigov in neprekinjenosti beleženja.
d) Program testiranja kontrol (T1–T9): preverjanja (npr. pokritost dnevnikov, rok hrambe / WORM, RBAC / PIM, analitika & nastavitve, IR od začetka do konca, priglasitev CSIRT, poročanje po DORA, dnevnik obdelave po ZVOP-2, režim visoke/kritične ogroženosti) z opredeljenimi postopki, vzorčenjem, dokazili in kriteriji sprejema.

Vzorčenje in opazovalna okna.

Načrt določa opazovalno okno zadnjih 30 dni za aktivne dnevnike in 180 dni za preverjanje časa hrambe; predvideno je najmanj 10 ključnih virov dnevnikov, 5 vzorčnih incidentov/opozoril ter 5 ključnih pogodb IKT (DORA). Sprejemljivost je vezana na dokazno sled in ponovljivost poizvedb/testov, kar je v skladu z načeli zadostnosti/ustreznosti dokazil in vzorčenja po ITAF.

Upravljanje dokazil, kakovost in sledljivost.

Dokazila se vodijo v registru z referencami na RTM in posamezne teste, izvajata se notranji pregled in sledljivost, hrambo pa se omeji skladno z GDPR/ZVOP-2 in akademskimi zahtevami PRIS. To odraža, po ITAF, zahteve po dokumentiranju delovnih papirjev in sistematičnem shranjevanju predstavitev revidiranca.

Viri podatkov.

- Sistemski viri: Microsoft Sentinel (povezovalnik, tabele SecurityEvent / SigninLogs, pravila, scenariji, rok hrambe / arhiv), Entra ID / PIM, *CMDB*[46], *EDR*[47], požarni zidovi, ključne aplikacije.
- Organizacijski viri: varnostne politike, načrti *BIA*[48] / BCP / IR, register IKT-pogodb (DORA), evidence priglasitev CSIRT, dnevnik obdelave (kjer je zahtevan).
- Osebni viri: intervjuji (CISO, skrbniki, DPO, pravna služba).

Analitične metode.

- Identifikacija in preslikava tveganj: primerjava registra tveganj (če obstaja) s konfiguracijami SIEM in aktivnimi detekcijskimi pravili; kjer register ni vzpostavljen, se ugotovitev evidentira in oceni vpliv na vključevanje virov dnevnikov, glede na primere uporabe. (To je skladno s programom testa T4 Analitika & nastavitve.)
- Primerjalna analiza: presoja skladnosti[49] nastavitev časa hrambe / nespremenljivost z zakonskimi merili (ZInfV-1, ZVOP-2) in z zahtevami poročanja po DORA (RTS / ITS).
- Sledenje procesom[50]: sledljivost incidentov od začetka do konca (zaznava → triaža → klasifikacija → eskalacija → zaključek) nasproti internim SLA in normativnim rokom (npr. 72h do nadzornega organa).
- Triangulacija in validacija: primerjava izpiskov KQL, administrativnih dnevnikov (npr. PIM) in izjav iz intervjujev; dopolnilna uporaba dela drugih strokovnjakov, kjer je smiselno (npr. pravna interpretacija DORA / RTS), skladno z ITAF 1206.

Omejitve obsega.

Načrt izrecno izključuje tehnični vdorni test / forenziko in pravno svetovanje ter omejuje presojo DORA na zmožnost revidiranca kot tretje osebe (ponudnika storitev IKT) – vpliv na interpretacijo rezultatov je zato obravnavan v diskusiji.

Povezava na ITAF – poročanje in nadaljnje spremljanje.

Končna dostava vključuje analizo vrzeli in priporočila, razvrščena po tveganju / skladnosti, z izvlečkom za upravo in tehnično prilogo (KQL / testi). Po izdaji poročila je predvideno nadaljnje spremljanje v skladu z ITAF 1402, tj. spremljanje, ali je vodstvo načrtovalo / izvedlo pravočasen odziv na ugotovitve.

---

[46] CMDB, angl. Configuration Management Database – konfiguracijska baza podatkov. Osrednji repozitorij konfiguracijskih elementov (CI) in njihovih odnosov (strojna oprema, programska oprema, storitve, odvisnosti). CMDB poda logični model IT-okolja in je temelj za upravljanje sprememb, incidentov in skladnosti.

[47] EDR, angl. Endpoint Detection and Response - zaznavanje in odzivanje na končnih točkah. Varnostna tehnologija in nabor orodij, ki z agenti na končnih točkah (npr. delovne postaje, prenosniki, strežniki, mobilne naprave) neprekinjeno zbirajo telemetrijo, jo analizirajo na osrednjem strežniku in omogočajo hitro zaznavanje, preiskovanje in odzivanje na sumljive ali nepooblaščene dejavnosti. EDR praviloma omogoča tudi proaktivni lov na grožnje (angl. threat hunting) in izvedbo odzivnih ukrepov (npr. izolacija naprave, ubijanje procesov, karantena datotek).

[48] BIA, angl. Business Impact Analysis – analiza vpliva na poslovanje. Sistematična analiza učinkov motenj na procese/storitve; rezultat se uporabi za določitev obsega SUIV/SUNP, prioritet obnovitve (RTO / RPO) in zahtev za neprekinjeno poslovanje. ZInfV-1 izrecno zahteva, da subjekti obseg upravljanja določijo na podlagi rezultatov BIA.

[49] Angl. conformance checking.

[50] Angl. process tracing.

Sklici na normative in interne akte, uporabljene v metodologiji

- ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition – standardi 1201 (načrtovanje), 1202 (ocena tveganj), 1204 (pomembnost), 1205 (dokazila), 1206 (uporaba dela drugih strokovnjakov), 1401 (poročanje), 1402 (follow-up); smernice 2001–2008, 2201–2208 (vključno z vzorčenjem), 2401–2402; orodja in tehnike.
- Revizijski načrt PRIS-PAKETEK-RN-2025-01 – obseg, metodologija (dokumenti, intervjuji, tehnični pregledi, simulacije), program testiranja kontrol T1–T9, vzorčenje in okna opazovanja, upravljanje dokazil in kakovost, poročanje.
- ISACA Code of Professional Ethics – obveznosti glede integritete, objektivnosti, zaupnosti in strokovne usposobljenosti.

3 Empirični del / študija primera

3.1 Opis organizacije in okolja

Osnovni podatki in regulativni položaj

Revidiranec nastopa kot bistveni subjekt po ZInfV-1 ter hkrati kot IKT tretja oseba v razmerju do zavezancev po DORA (nudi storitve IKT, ki podpirajo kritične ali pomembne funkcije finančnih institucij). Organizacija zato hkrati izpolnjuje obveznosti po NIS 2 / ZInfV-1, DORA ter zahteve glede VOP (GDPR / ZVOP-2). Revizijska obravnava se osredotoča na delovanje Microsoft Sentinel (SIEM / SOAR) kot ključnega sistema za nadzor skladnosti in kibernetske varnosti.

Ureditev upravljanja varovanja informacij

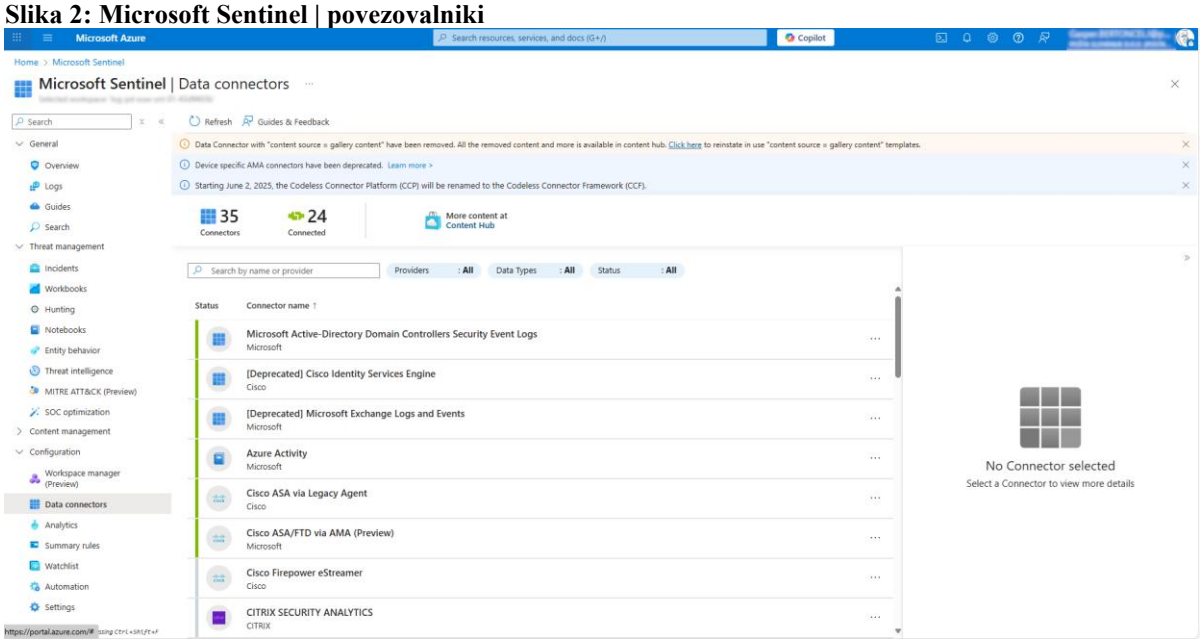
Upravljanje varovanja informacij je pri revidirancu organizirano prek vlog CISO, skrbnikov posameznih sistemov, DPO in pravne službe. Na ravni dokumentacije so predmet presoje politike in načrti SUIV / SUNP (vključno z BIA / BCP / IR), postopki priglasitve incidentov CSIRT ter politika hrambe dnevnikov z opredeljenimi kazalniki KPI / KRI. Ureditve se presojajo z vidika skladnosti z ZInfV-1 (20., 21., 25. in 33. člen) ter ZVOP-2 (22. člen).

Tehnološko okolje in platforma SIEM / SOAR

Revidiranec uporablja Microsoft Sentinel kot osrednji varnostno-nadzorni sistem. Sentinel temelji na Azure Monitor / Log Analytics in omogoča:

- povezovanje dnevniških virov prek povezovalnikov (npr. M365 / Entra ID / Defender, on-prem AD, požarne pregrade, aplikacije),
- analitična pravila (odkrivanje) in proaktivno iskanje groženj s poizvedbami KQL,
- SOAR z avtomatiziranimi scenariji odziva (Logic Apps),
- upravljanje dostopov preko RBAC in PIM / JIT.
- Posebna presoja je namenjena nastavitvam hrambe (rok hrambe / arhiv), integriteti (npr. WORM) in lokaciji hrambe (RS / EU), saj te točke neposredno pogojujejo zahtevano raven skladnosti in dokazljivosti.

Slika 2: Microsoft Sentinel | povezovalniki

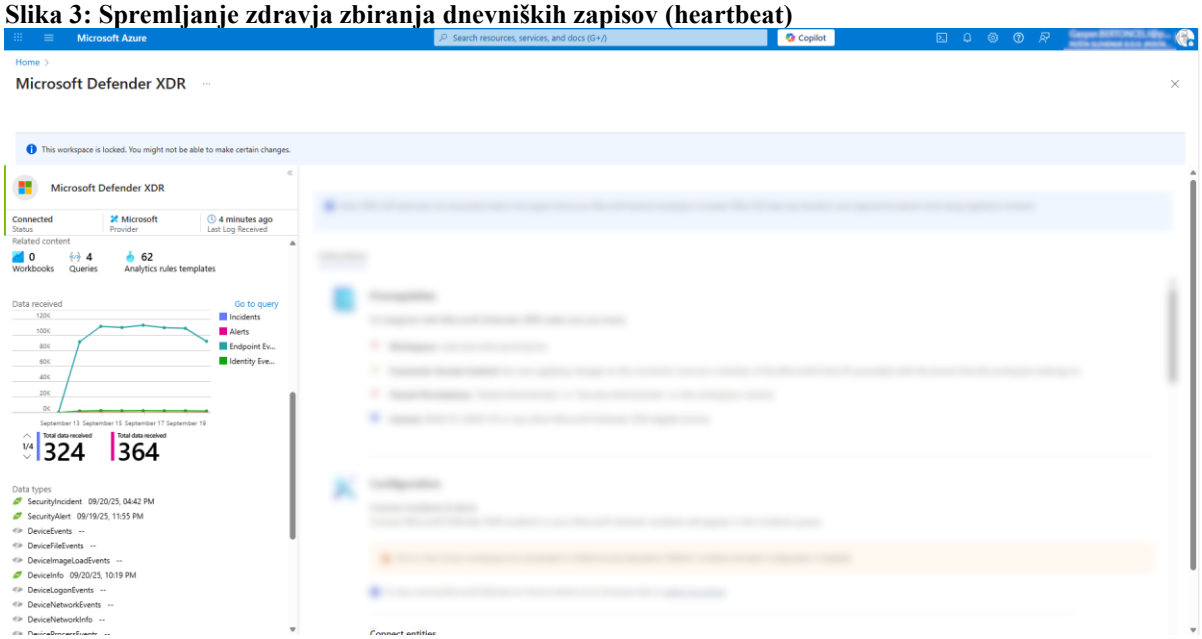


Vir: lasten

Dnevniški viri in tok podatkov

Za zagotavljanje celovitosti nadzora načrtuje revidiranec preslikavo CMDB ↔ Sentinel (kritična sredstva / vplivni procesi ↔ aktivni povezovalniki in tabele) ter spremljanje zdravja zbiranja (npr. heartbeat). Vključeni viri pokrivajo zapise (prijave, aktivacije privilegiranih dostopov), končne točke in strežniško okolje, omrežje (FW / WAF) ter aplikativne dnevnike za poslovne funkcije. Tokovi podatkov se parametrično nastavljajo glede na primer uporabe (tveganje→pravilo→vir), rok hrambe pa je predmet preverjanja s KQL po obdobjih.

Slika 3: Spremljanje zdravja zbiranja dnevniških zapisov (heartbeat)



Vir: lasten

Procesi IR in poročanje (CSIRT, GDPR, DORA)

Operativni okvir obsega celoten cikel IR: zaznava → triaža → klasifikacija → eskalacija → zaključek, s sledljivimi časovnicami in SLA. V kontekstu ZInfV-1 je ključna priglasitev pomembnih incidentov

pristojni skupini CSIRT (zgodnje opozorilo, priglasitev, vmesno / končno poročilo), v kontekstu GDPR pa 72-urni rok obvestila nadzornemu organu ob kršitvi osebnih podatkov. Kot tretja oseba IKT mora revidiranec podpreti zavezance po DORA pri klasifikaciji incidentov po RTS in pripravi poročil po ITS (začetno / vmesno / končno), zato so taksonomija resnosti, podatkovna polja in predloge poročil sestavni del okolja.

Meje presoje, odvisnosti in predpostavke

Presoja ne vključuje vdornih testov in forenzike, prav tako ne podaja pravnega mnenja; obseg DORA se omejuje na presojo sposobnosti revidiranca kot IKT ponudnika, da naročnikom omogoča izpolnitev njihovih obveznosti (register razmerij IKT, pogodbene klavzule, poročanje o večjih incidentih). Presoja temelji na dokumentarnem pregledu, intervjujih, tehničnih pregledih in simulacijah po programu testiranja T1–T9; dokazila se vodijo v registru s sledljivostjo RTM.

Povzetek

Revidiranec deluje v regulativno zahtevnem okolju, kjer se križajo obveznosti NIS 2 / ZInfV-1, GDPR / ZVOP-2 in DORA. Tehnološko jedro (Microsoft Sentinel) je zato obravnavano z vidika pokritosti virov, hrambe in integritete dnevnikov, učinkovitosti odkrivanj in IR, ter poročanja (CSIRT / GDPR / DORA) – vse s sledljivostjo do opredeljenih meril in testov iz revizijskega načrta.

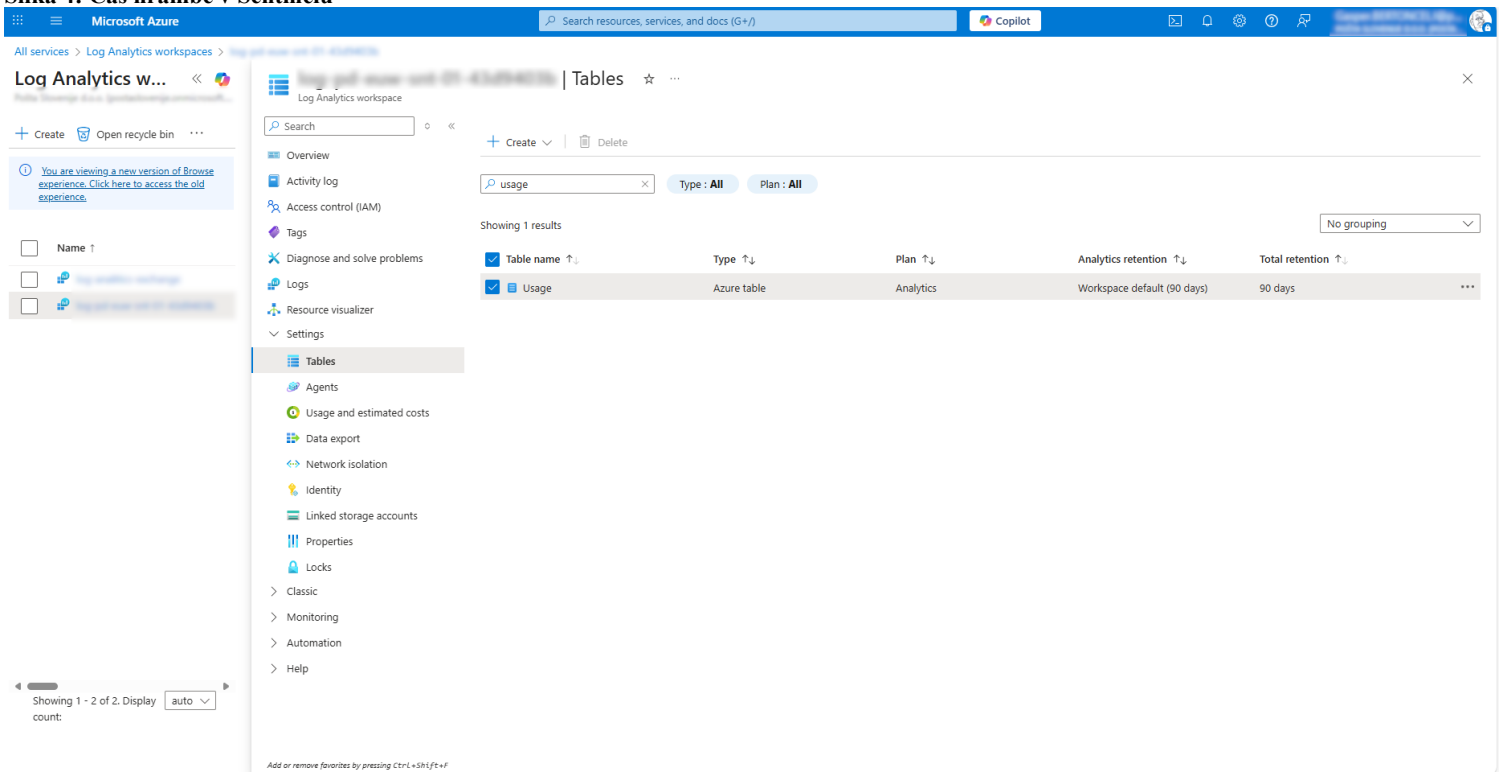
3.2 Rezultati analiz / testov

Tabela 1: T1 — Pokritost dnevnikov (RTM-02; ZInfV-1 21)

Metodološki povzetek	Primerjali smo CMDB kritičnih sredstev z aktivnimi povezovalniki / tabelami v Microsoft Sentinelu, pregledali heartbeat in izvedli vzorčenje s KQL (okno: zadnjih 30 dni). Vzorec: 12 kritičnih virov (Identiteta / M365, EDR, FW / WAF, kadrovska aplikacija, AD, strežniki).
Ugotovitve	9/12 virov je aktivnih; 3 (FW na obrobju, WAF in osrednja kadrovska aplikacija) nimajo zabeleženega spremljanja zdravja (heartbeat) oz. niso integrirani v Sentinel. Detekcijska pravila zato ne pokrivajo vseh kritičnih poti. To potrjuje U-01.
Ocena skladnosti	Delno skladno (pokrivanje ni popolno); zmerno do visoko tveganje za zaznavo in forenziko.
Ključna dokazila.	ED-T1-01 (izvleček CMDB), ED-T1-02 (seznam povezovalnikov), ED-T1-03 (izpis spremljanja zdravja KQL), ED-T1-04 (vzorci dogodkov po virih).
Normativni sklici.	ZInfV-1 – obveznost vzpostavitve ukrepov in vodenja dnevnikov ter celovite varnostne dokumentacije / ukrepov (21., 22. in 24. člen).

Vir: lasten

Tabela 2: T2 — Rok hrambe, integriteta (WORM) in lokacije (RTM-02; ZInfV-1 21)

Metodološki povzetek	Pregled nastavitev roka hrambe / arhiva v Log Analytics (produkcijsko okolje SIEM), preveritev WORM / nespremenljivost in dokumentiranih lokacij hrambe (RS / EU); KQL za časovno pokritost (6-mesečno okno).
Ugotovitve	ProdLogs ima rok hrambe 90 dni; Arhiv / WORM ni omogočen; v dveh primerih lokacije niso dokumentirane. To potrjuje U-02 in U-12. **Slika 4: Čas hrambe v Sentinelu**  Vir: lasten
Ocena skladnosti	Neskladno (rok hrambe pod 6 mesecev; nedokazana nespremenljivost in lokacije). Visoko tveganje (regulativno in forenzično).

Ključna dokazila.	ED-T2-01 (posnetki nastavitev Workspace Retention / Archive), ED-T2-02 (KQL časovna pokritost), ED-T2-03 (politika hrambe), ED-T2-04 (izjave ponudnika o lokacijah).
Normativni sklici.	ZInfV-1 – varnostni ukrepi in dnevniški zapisi (rok hrambe / integriteta, lokacije), 22. in 24. člen.

Vir: lasten

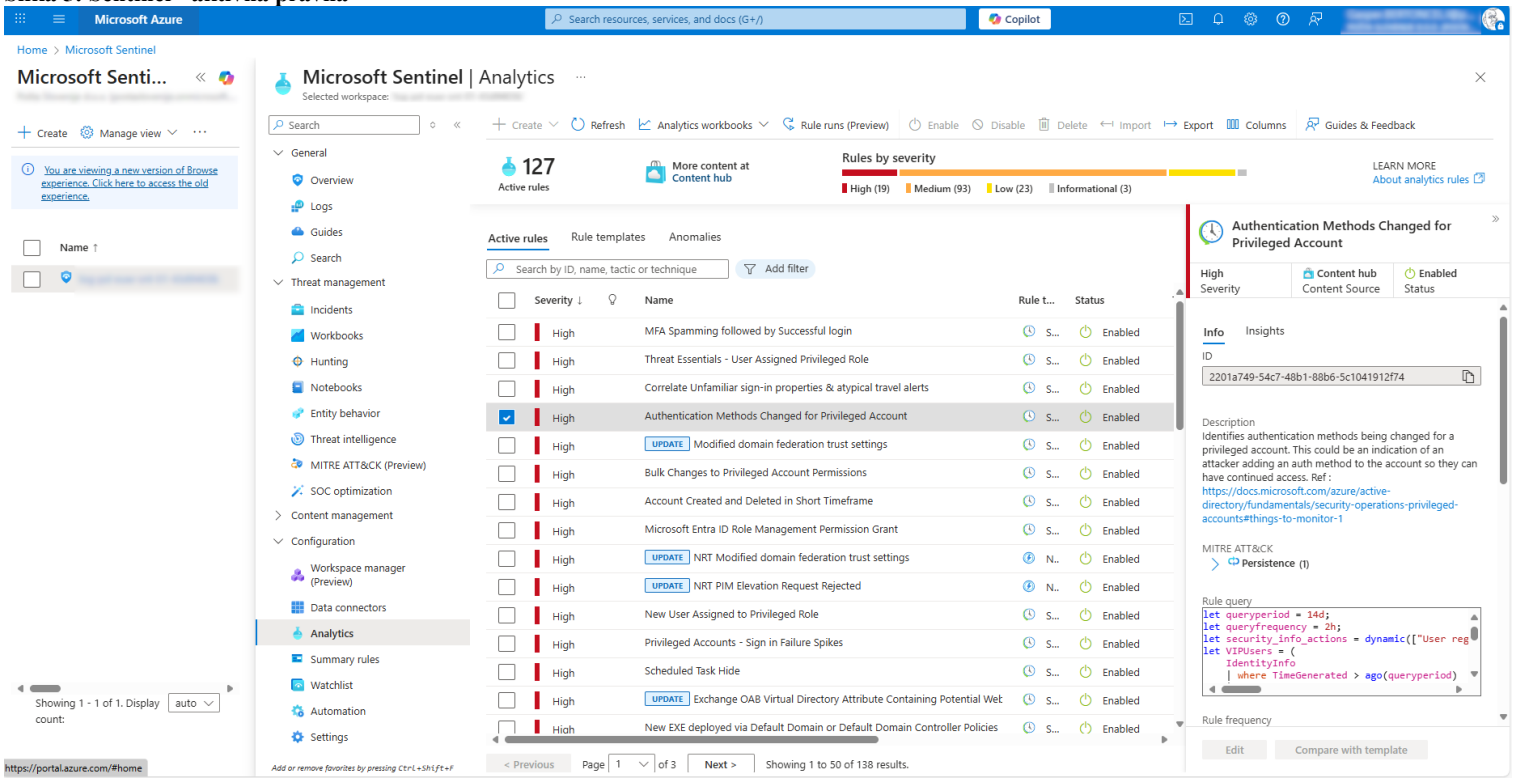
Tabela 3: T3 — RBAC / PIM / JIT / MFA (RTM-09; ISO / identitete)

Metodološki povzetek	Pregled privilegiranih vlog v Entra ID, PIM aktivacij (zahtevana MFA, odobritve, utemeljitev), izredni (break-glass) mehanizem in pregledi dostopov (četrtletno).
Ugotovitve	Dva uporabniška računa Global Administrator sta stalna; PIM za »Security Admin« ne zahteva MFA; zadnji pregled dostopov ni dokumentiran. Potrjuje U-03 in U-13.
Ocena skladnosti	Neskladno (načelo najmanjših pravic ni zagotovljeno); visoko tveganje.
Ključna dokazila.	ED-T3-01 (izvoz PIM event log), ED-T3-02 (seznam vlog), ED-T3-03 (zapisnik pregleda dostopov), ED-T3-04 (politika MFA).
Normativni sklici.	NIST SP 800-63B-4 (AAL / smernica MFA) – priporočila za dokazovanje identitete in večfaktorsko avtentikacijo; uporaba step-up MFA ob povišanju privilegijev.

Vir: lasten

(Metodološki okvir identitet dopolnjujeta ISO/IEC 27001/27002 – nadzor identitet / pravic; javno dostopne referenčne strani ISO).

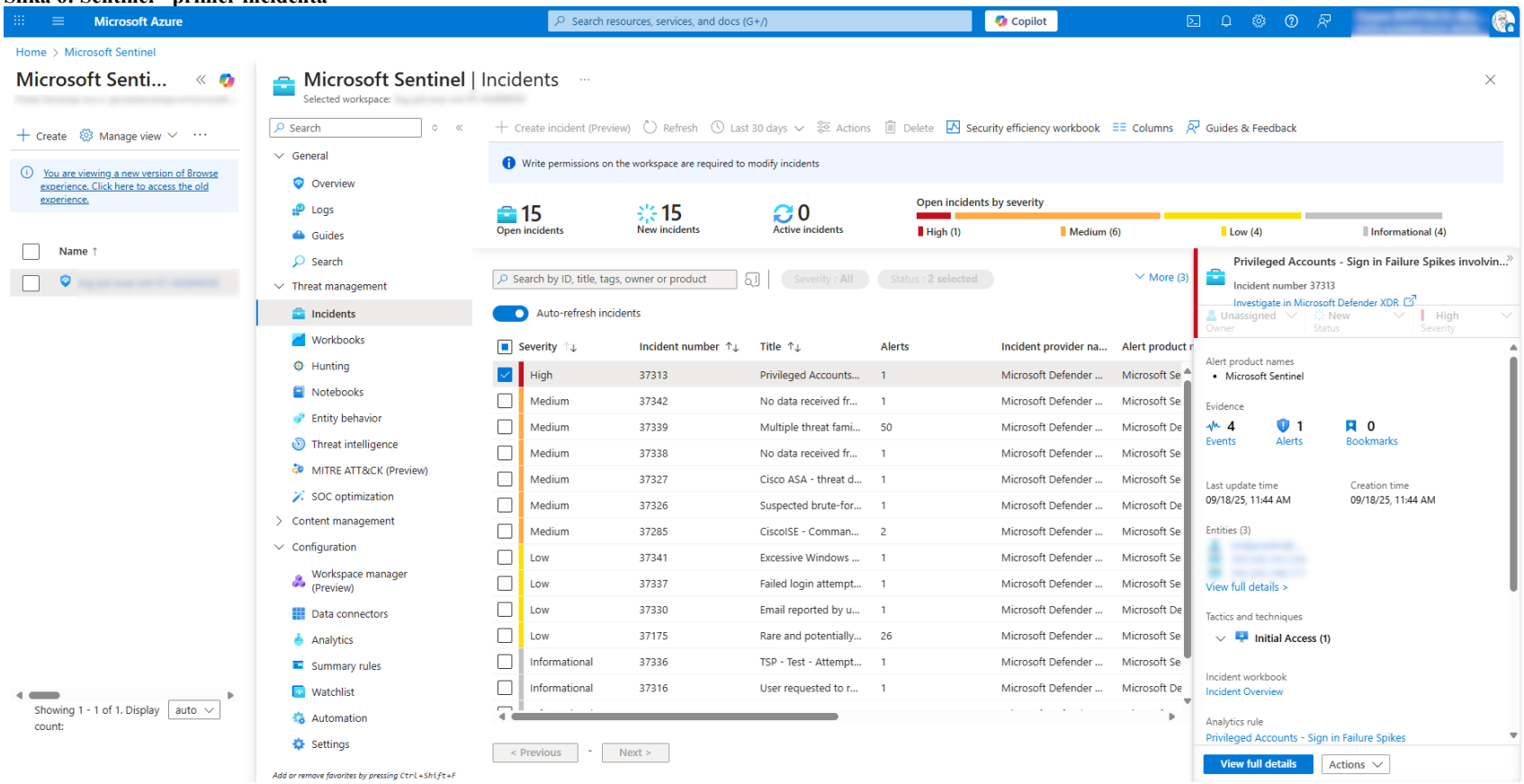
Tabela 4: T4 — Analitična pravila in nastavljanje delovanja (RTM-01/02; ZInfV-1 21)

Metodološki povzetek	Pregledali smo 15 ključnih zaznav (M365 / privilegiji / eksfiltracija) in njihovo utemeljitev v registru tveganj; analizirali raven lažno pozitivnih rezultatov (FP rate) in dokumentacijo odločitev za fine nastavitve (tuning).
Ugotovitve	Šest visoko pomembnih pravil je onemogočenih brez dokumentirane utemeljitve; raven lažno pozitivnih rezultatov je okoli 60 % (cilj je pod 20 %); register tveganj IKT in seznam primerov uporabe (use-case library) nista vzpostavljena, zato je integracija virov privzeta in ne vodena glede na tveganja. To zajameta U-04 in U-05. **Slika 5: Sentinel - aktivna pravila**  Vir: lasten
Ocena skladnosti	Delno skladno; srednje do visoko tveganje (spregledi).

Ključna dokazila.	ED-T4-01 (seznam pravil in status), ED-T4-02 (vzorec alarmov), ED-T4-03 (tuning log), ED-T4-04 (neobstoječ register tveganj).
Normativni sklici.	ZInfV-1, 21.in 22. člen – učinkoviti varnostni ukrepi in dokumentiranost nastavitev; usklajenost detekcij z upravljanjem tveganj.

Vir: lasten

Tabela 5: T5 — Postopek odzivanja na incidente (IR od začetka do konca) (RTM-03/06; ZInfV-1 30; GDPR[16])

Metodološki povzetek	Sledili smo petim primerom / simulacijam: zaznava → triaža → klasifikacija → eskalacija → zaključek; preverili SLA in temeljni vzrok (root cause analysis).
Ugotovitve	V 2/5 primerih manjka časovni žig triaže / eskalacije; presežen je SLA; zaključni povzetki ne vsebujejo analize temeljnega vzroka. To potrjuje U-06. **Slika 6: Sentinel - primer incidenta**  Vir: lasten

Ocena skladnosti	Delno skladno; zmerno do visoko tveganje (neusklajenost s poročanjem CSIRT / GDPR).
Ključna dokazila.	ED-T5-01 (zapisniki IR), ED-T5-02 (časovnice), ED-T5-03 (metrika SLA).
Normativni sklici.	ZInfV-1, 30. člen – priglasitev pomembnih incidentov pristojni skupini CSIRT; GDPR[16] – 72-urno obvestilo nadzornemu organu ob kršitvi osebnih podatkov; smernice EDPB o obveščanju.

Vir: lasten

(Metodološka dobra praksa IR: NIST SP 800-61r3.)

Tabela 6: T6 — Priglasitev CSIRT (ZInfV-1 30)

Metodološki povzetek	Table-top simulacija: zgodnje opozorilo, priglasitev, vmesno / končno poročilo; validacija vsebinskih elementov (obseg, vpliv, čezmejnost).
Ugotovitve	Zgodnje opozorilo ni pripravljeno; kontaktni kanal do SI-CERT / CSIRT ni jasno določen; predloga poročila ne vsebuje vseh obveznih polj. Potrjuje U-07.
Ocena skladnosti	Neskladno; visoko tveganje (regulativna neizpolnitev).
Ključna dokazila.	ED-T6-01 (osnutek poročila), ED-T6-02 (komunikacijski protokol), ED-T6-03 (časovni žigi).
Normativni sklici.	ZInfV-1, 30. člen – obveznost priglasitve pomembnih incidentov in vsebinski elementi poročanja.

Vir: lasten

Tabela 7: T7 — Podpora DORA zavezancem: klasifikacija (RTS) in poročila (ITS) (RTM-07; DORA 19; RTS 2024/1772; ITS 2025/302

Metodološki povzetek	Simulacija večjega incidenta IKT (major ICT incident); preveritev pragov materialnosti in klasifikacije po RTS 2024/1772 ter generiranje začetnega / vmesnega / končnega poročila po ITS 2025/302.
Ugotovitve	Klasifikacija ni avtomatizirano preslikana na pragove RTS; obrazci ITS niso integrirani v orodje za IR; zbirnik polj nepokrit. To potrjuje U-08.
Ocena skladnosti	Neskladno; visoko tveganje za zavezance (časovnost in vsebina poročil).
Ključna dokazila.	ED-T7-01 (shema polj / pragovi), ED-T7-02 (osnutek ITS začetnega poročila), ED-T7-03 (prepis / transkript simulacije).
Normativni sklici.	DORA, čl. 19 (upravljanje incidentov, poročanje), čl. 30 (pogodbene zahteve do tretjih oseb), RTS 2024/1772 (klasifikacija in pragovi), ITS 2025/302 (standardni obrazci).

Vir: lasten

Tabela 8: T8 — ZVOP-2: dnevnik obdelave (RTM-05; ZVOP-2 22; povezava na GDPR 33)

Metodološki povzetek	Kar zadeva OP, smo pregledali dnevnik obdelave (polja, rok hrambe 2–5 let, izvoz za IP) ter sledljivost posredovanj.
Ugotovitve	Dnevnik portala za stranke ne vsebuje vseh polj (vrsta dejanja, ID uporabnika); politika določa 1-letno hrambo; izvoz za IP ni standardiziran. Potrjuje U-09
Ocena skladnosti	Neskladno; visoko tveganje (pravna sledljivost).
Ključna dokazila.	ED-T8-01 (izpis dnevnika), ED-T8-02 (politika hrambe), ED-T8-03 (postopek za IP).
Normativni sklici.	ZVOP-2, 22. člen – vsebina in rok hrambe dnevnika obdelave ter dostop IP; pojasnila IP-RS.

Vir: lasten

(Ob kršitvi OP se aktivira tudi 33. člen GDPR – 72 ur).

Tabela 9: T9 — Režim visoka / kritična ogroženost (H/C) (RTM-04; ZInfV-1 36–38)

Metodološki povzetek	Simulirali smo razglasitev visoke / kritične ogroženosti (H/C): preverjanje beleženja, pogostejša poročila, nadzorna plošča stanja dnevniških zapisov in proces priglasitev.
Ugotovitve	Protokol H/C ni dokumentiran; tedenska poročila niso predvidena; nadzorna plošča ni vzpostavljena. Potrjuje U-11.
Ocena skladnosti	Neskladno; srednje tveganje (operativna neučinkovitost v kriznem načinu).
Ključna dokazila.	ED-T9-01 (osnutek H/C), ED-T9-02 (načrt poročil), ED-T9-03 (nadzorna plošča).
Normativni sklici.	ZInfV-1, 36. – 38. člen – posebne obveznosti v režimu visoka / kritična ogroženost.

Vir: lasten

Tabela 10: DORA – Razmerja do tretjih oseb (RTM-08; čl. 28/30)

Metodološki povzetek	Vzorčni pregled 5 pogodb IKT in registra (klasifikacija kritično / pomembno, lokacije, SLA, vračilo podatkov, asistenca, pod izvajanje, izhodna strategija).
Ugotovitve	V 3/5 pogodb ni označene kritičnosti; 2/5 ne vsebujeta klavzul o lokaciji obdelave, pomoči ob incidentu, vračilu podatkov ali pod izvajanju; izhodna strategija ni preizkušena. To potrjuje U-10 in U-12.
Ocena skladnosti	Delno skladno; srednje / visoko tveganje (pogodbena / regulativna negotovost za zavezance).
Ključna dokazila.	ED-DORA-01 (register), ED-DORA-02 (vzorec 5 pogodb), ED-DORA-03 (politika upravljanje tveganj tretjih strani).
Normativni sklici.	DORA, čl. 28 (register IKT razmerij) in čl. 30 (obvezne pogodbene določbe – SLA, lokacije, pomoč, izhodna strategija, pod izvajanje).

Vir: lasten

Povzetek skladnosti in povezava na analizo vrzeli

- Kritična področja (P1): T2 (rok hrambe / nespremenljivost / lokacije), T3 (RBAC / PIM / MFA), T5–T7 (IR / CSIRT / GDPR / DORA), T8 (dnevnik po ZVOP-2).
- Pomembna področja (P2): T1 (pokrivanje virov), T4 (zaznave in fine nastavitve), pogodbe DORA, T9 (H/C).
- Organizacijska dopolnila (P3): evidenca dokazil (izvleček, rok hrambe) – glej U-14.
- Vse zgornje ugotovitve so prenesene v analizo vrzeli (ID-ji U-01 … U-14), z merili (RTM), dokazili (ED-….) in časovnicami (30–60 dni) za odpravo.

Glavni sklici na normativni okvir

- ZInfV-1 – Uradni list RS, 40/2025.
- GDPR – OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.
- Guidelines 9/2022 on personal data breach notification under GDPR (European Data Protection Board, 2023).
- ZVOP-2 – Uradni list RS, št. 163/2022.
- DORA (EU 2022/2554) – OJ L 333, 27.12.2022

- RTS / ITS (OJ L 2025/301 in 2025/302).
- NIST SP 800-61r3 (priporočila IR) in NIST SP 800-63B-4 (MFA/AAL) – metodološke smernice.
- Opomba: Presoja je izvedena skladno z revizijskim načrtom in načeli ITAF zadostnih / ustreznih dokazil; sledljivost je zagotovljena z RTM in evidenco dokazil (ED-… ID-ji).

4 Razprava

Umeščenost ugotovitev v regulativni okvir

Rezultati testov T1–T9 kažejo, da je delovanje Microsoft Sentinela pri revidirancu zrelo v smislu osnovne operativne uporabe (dostopnosti podatkov, centralizacije dnevnikov in osnovnih zaznav), vendar hkrati razkrije vrzeli, ki neposredno zadevajo zakonsko obvezne prvine iz ZInfV-1, ZVOP-2 / GDPR in DORA. V domeni NIS 2 / ZInfV-1 bi morala organizacija zagotavljati celovit nabor dnevnikov in minimalno hrambo z integriteto (najmanj šest mesecev) ter izpolnjevati obveznosti poročanja CSIRT (vključno z režimom visoka / kritična ogroženost). Identificirane vrzeli (rok hrambe manj kot 180 dni, pomanjkanje WORM, nepopolna pokritost virov, neoperativen režim H/C) pomenijo odklon od 21., 22., 24. 30., in 36.-38. člena ZInfV-1; zakon je bil objavljen v UL RS št. 40/2025 in je v veljavi od 19. 6. 2025, kar dodatno poudarja aktualnost skladnosti.

V delu varstva osebnih podatkov (ZVOP-2 in GDPR) so kritične zahteve dnevnik obdelave (22. člen ZVOP-2: obvezna polja, rok hrambe 2–5 let, dostopnost IP) ter 72-urni rok za obveščanje nadzornega organa o kršitvi osebnih podatkov (33. člen GDPR). Ugotovitve T8 (nepopolna vsebina dnevnika, prekratek rok hrambe, neobstoj standardnega izvoza) in T5/T6 (sledljivost IR, poročanje) kažejo, da je treba posodobiti evidence obdelave OP in operativno pripravo za pravočasno obveščanje.

Za DORA je ključno dvoje: (i) klasifikacija in poročanje o večjih incidentih IKT, po RTS 2024/1772 in ITS 2025/302 (polja, pragovi, obrazci) ter (ii) register razmerij s tretjimi osebami IKT in obvezne pogodbene klavzule (28. in 30. člen DORA). Simulacije T7 in pregled pogodb razkrijeta, da klasifikacija in izvoz obrazcev nista integrirana v orodje za IR, register / klavzule pa niso polno usklajene. To neposredno zadeva zmožnost revidiranca, da podpre zavezance po DORA.

Vse navedeno je vnaprej predvideno v metodologiji in merilih revizijskega načrta PRIS-PAKETEK-RN-2025-01 (RTM in T-program), na katerega se opira presoja v empiričnem delu.

Odgovori na raziskovalna vprašanja

Tabela 11: Odgovori na raziskovalna vprašanja

ID	Ugotovitve
RV1 (pokritost / rok hrambe / nespremenljivost).	Ugotovitve T1 in T2 potrjujejo nepopolno pokritost (3/12 kritičnih virov brez preverjanja zdravja - heartbeat) ter čas hrambe, krajšo od 180 dni brez WORM. To je odklon od 24. člena ZInfV-1.
RV2 (zaznave / IR / CSIRT / GDPR).	T4–T6 pokažejo onemogočena pravila, visoka raven FP (~60 %) ter nepopolno IR sledljivost in nepripravljenost za CSIRT (manjka "zgodnje opozorilo"); 33. člen GDPR ostaja tvegan pri scenariju kršitve osebnih podatkov.
RV3 (evidenca po ZVOP-2).	T8 potrdi, da je dnevnik obdelave je nepopoln (polja) in da se hrani premalo časa; izvoz za IP ni standardiziran – odklon od 22. člena ZVOP-2.
RV4 (PIM / JIT / MFA).	T3 potrdi stalne skrbniške vloge, MFA pri PIM aktivacijah ni vsiljena.
RV5 (DORA register / poročila).	T7 in pregled pogodb potrjujeta da klasifikacija po RTS / ITS ni operativno podprta; register / klavzule so nepopolni (28., 30. člen DORA).
RV6 (ključne vrzeli / ukrepi).	Največjo regulativno izpostavljenost ustvarjajo T2, T3, T5–T8; te so v analizi vrzeli razvrščene v P1 (0–30 dni) in P2 (30–60 dni) ukrepe.

Vir: lasten

Operativne posledice in menjava paradigme

Jedro problema ni le tehnično, temveč procesno: integracija virov in nastavitev pravil se izvaja po privzetih nastavitvah namesto iz registra tveganj in primerov uporabe. To vodi do slepih peg, lažno pozitivnih alarmov in neenakomernega obvladovanja tveganj. Prehod na upravljanje temelječe na tveganjih naj zato začne s (i) procesno oceno tveganj, (ii) registrom tveganj IKT, (iii) matriko pokritosti primerov uporabe (Content Coverage Matrix): tveganje → primer uporabe → vir / pravilo → KPI / KRI → dokazilo), kar je tudi v skladu z načrtovanimi merili RTM-01/02.

Finančna realnost (strošek hrambe, strošek arhiva / WORM) zahteva stratifikacijo hrambe: glede na čas[51] prikrite prisotnosti napadalca za operativno analitiko in glede na čas hrambe za zagotavljanje skladnosti, nespremenljiv (WORM) za sporne / forenzične sklope. To neposredno naslavlja zahteve ZInfV-1 21. člen.

[51] Angl. dwell time - čas, ko je napadalec po prvem vdoru neopaženo prisoten v informacijskem okolju – najpogosteje merjen od trenutka kompromitacije do odkritja (nekateri ga merijo do zajezitve / odprave).

Kakovost dokazil in povezava z ITAF

Dokazni standardi ITAF (zadostnost / ustreznost; pomembnost; vzorčenje; uporaba dela drugih) so bili upoštevani skozi vzorčenja (30-dnevno okno, šestmesečni rok hrambe, 10–5–5 vzorcev), triangulacijo virov (dokumenti, tehnični izpisi, intervjuji) in sledljivost (RTM ↔ test ↔ dokazilo). Nadaljnje spremljanje po izdaji poročila je v skladu s Standardom 1402.

Učinek na poslovne procese in pogodbeni okvir

Za revidiranca, kot tretjo osebo IKT, so DORA 28/30 zahteve poslovno pomembne: urediti je treba register, klavzule (lokacije obdelave, SLA, vračilo / predajo podatkov, pomoč ob incidentu, pod izvajanje) in preizkus izhodne strategije. To okrepi zaupanje strank in zmanjša pogodbeno / regulativno tveganje.

Omejitve presoje in grožnje veljavnosti

Presoja je brez vdornega testa in forenzike, opira se na vzorčenje in razpoložljiva dokazila; pravna interpretacija se opira na uradne javne objave in usmeritve nadzornih organov. To je skladno z omejitvami obsega iz revizijskega načrta in metodološkim okvirom ITAF.

Sklep

Sinteza ugotovitev

Naloga je ocenila, ali delovanje Microsoft Sentinela pri zavezancu zadostno podpira skladnost z ZInfV-1, ZVOP-2 / GDPR in DORA. Odgovor je pogojno pritrdilen: osnovna funkcionalna zrelost je dosežena, vendar kritične zahteve (rok hrambe / nespremenljivost / lokacije; PIM / JIT / MFA; IR sledljivost in CSIRT; DORA RTS / ITS; ZVOP-2 dnevnik obdelave) niso v celoti izpolnjene. To tudi uokvirja P1/P2 ukrepe v analizi vrzeli.

Ključne priporočene usmeritve (ciljno stanje)

1. Upravljanje tveganj → seznam primerov uporabe. V 30–45 dneh vzpostaviti procesno oceno tveganj, register tveganj IKT in matriko preslikav - Content Coverage Matrix (preslikava tveganje → primer uporabe → vir / pravilo / KPI / KRI).
2. Rok hrambe in integriteta. Urediti čas hrambe vsaj 180 dni, aktivirati arhiv / WORM, ter dokumentirati lokacije RS / EU; prilagoditi ravni (tiering) hrambe. (ZInfV-1, 21., 22. in 24. člen.)
3. Identitete in privilegiji. Odpraviti stalne skrbniške vloge, uvesti PIM z obvezno MFA in odobritvami, ter četrtletne preglede dostopov.
4. IR / CSIRT / GDPR. Standardizirati IR postopek (odločitev glede kršitve oz. vdora da / ne), vzpostaviti časovnice / metrike SLA, pripraviti zgodnje opozarjanje in predloge poročil za CSIRT; zagotoviti operativno izpolnjevanje 72-urnega roka po 33. členu GDPR.
5. DORA. Vpeljati pragove RTS in obrazce ITS v orodje za IR; dopolniti register IKT in obvezne klavzule (28., 30. člen DORA); preizkusiti izhodno strategijo.
6. ZVOP-2 evidenca. Dopolniti dnevnik obdelave (polja), nastaviti 2–5 let hrambe in pripraviti standardni izvoz za IP. (ZVOP-2, 22. člen.)

Prispevek naloge in prenosljivost

Naloga prinaša operacionaliziran RTM, program testiranja T1–T9, analizo vrzeli in evidenco dokazil, ki sledijo načelom ITAF o merilih, zadostnih / ustreznih dokazih ter poročanju / nadaljnjemu spremljanju. Ti artefakti so prenosljivi tudi v druge ekosisteme SIEM / SOAR, ob prilagoditvi meril.

Omejitve in nadaljnje delo

Ocenjevanje je omejeno na vzorčenje in ne vključuje vdornega testiranja ali forenzike; prihodnje delo naj vključi merjenje učinka (npr. trend MTTD / MTTR, znižanje ravni FP), avtomatsko generiranje poročil ITS iz sistema SIEM / IR ter formalno preslikavo med polji DORA / RTS in shemami SIEM.

Opomba: Razprava in sklep se opirata na revizijski načrt PRIS-PAKETEK-RN-2025-01 (RTM, T1–T9) in na uradne objave / napotila NIS-2 / ZInfV-1, GDPR / ZVOP-2 in DORA. Po izpeljavi načrta odprave vrzeli (P1: 0–30 dni; P2: 30–60 dni) predlagamo nadaljnje spremljanje po ITAF 1402.

Viri

Državni zbor Republike Slovenije. (2025). *Zakon o informacijski varnosti (ZInfV-1).* Uradni list Republike Slovenije, Ljubljana. Pridobljeno 2025 iz https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2025-01-1571?utm_source=chatgpt.com

European Commission. (25. junij 2024). *Commission Delegated Regulation (EU) 2024/1772 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria for the classification of ICT-relat*. Pridobljeno iz https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=OJ:L_202401772

European Commission. (2025). *Commission Implementing Regulation (EU) 2025/302 of 23 October 2024 laying down implementing technical standards for the application of Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to the standard forms, templates, a.* Brussels: Publications Office of the European Union. Pridobljeno iz https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202500302

European Commission. (20. februar 2025). *Delegirana uredba Komisije (EU) 2025/301 z dne 23. oktobra 2024 o dopolnitvi Uredbe (EU) 2022/2554 …*. Pridobljeno iz Uradni list Evropske unije (EUR-Lex): https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=OJ:L_202500301

European Data Protection Board. (4. april 2023). *Guidelines 9/2022 on personal data breach notification under GDPR*. Pridobljeno iz European Data Protection Board: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

European Parliament & Council of the European Union. (22. december 2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).* Pridobljeno iz Official Journal of the European Union: URL: https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32022L2555

European Parliament & Council of the European Union. (27. december 2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) [OJ L 333, 27.12.2022, pp. 80–152].* Pridobljeno iz EUR-Lex (Official Journal of the European Union): https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Parliament and Council of the European Union. (4. maj 2016). *Regulation (EU) 2016/679 … (General Data Protection Regulation).* Pridobljeno iz EUR-Lex: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.* Luxembourg: Publications Office of the European Union. Pridobljeno iz https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Evropska komisija. (20. februar 2025). *Izvedbena uredba Komisije (EU) 2025/302 z dne 23. oktobra 2024 o določitvi izvedbenih tehničnih standardov … (Besedilo velja za EGP)*. Pridobljeno iz https://chatgpt.com/c/68cedeac-8f68-8327-b77e-690c310b4dc2: EUR-Lex (Uradni list Evropske unije)

Inštitut za lokalno samoupravo Maribor. (februar 2023). *Zakon o varstvu osebnih podatkov (ZVOP-2): pristojnosti in naloge občine z uvodnimi pojasnili.* Pridobljeno iz Lex localis: https://www.lex-localis.info/files/dab891d9-90c8-40a7-aa6b-d3a231fe7aa5/638132154265439378_ZVOP-2_februar%202023.pdf

International Organization for Standardization. (2024). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements — Amendment 1: Climate action changes.* Geneva, Switzerland: ISO. Pridobljeno iz https://www.iso.org/standard/88435.html

International Organization for Standardization; International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* International Organization for Standardization. Pridobljeno iz https://www.iso.org/standard/27001

ISACA. (2014). *ITAF™: A Professional Practices Framework for IS Audit/Assurance.* Rolling Meadows: ISACA. Pridobljeno iz https://cs.uns.edu.ar/~mc/ADS/downloads/Material%20Complementario/ITAF-3rd-Edition_fmk_Eng_0614.pdf

ISACA. (brez datuma). *Code of Professional Ethics*. Pridobljeno iz https://www.isaca.org/code-of-professional-ethics

Microsoft. (25. januar 2023). *Microsoft Sentinel SOAR content catalog*. Pridobljeno iz Name of Website: Microsoft Learn: URL: https://learn.microsoft.com/en-us/azure/sentinel/sentinel-soar-content

Microsoft. (1. maj 2024). *Overview of immutable storage for blob data – Azure Storage*. Pridobljeno iz Microsoft Learn: https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview

Microsoft. (22. julij 2025). *Manage data retention in a Log Analytics workspace*. Pridobljeno iz Microsoft Learn: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure?tabs=portal-3,portal-1,portal-2

Microsoft. (30. junij 2025). *Microsoft Sentinel out-of-the-box content overview*. Pridobljeno iz Microsoft Learn: https://learn.microsoft.com/en-us/azure/sentinel/sentinel-solutions

Microsoft. (22. julij 2025). *What is Microsoft Sentinel?* Pridobljeno iz What is Microsoft Sentinel?: https://learn.microsoft.com/en-us/azure/sentinel/overview

Microsoft. (brez datuma). *Microsoft Sentinel documentation*. Pridobljeno iz Microsoft Learn: https://learn.microsoft.com/en-us/azure/sentinel/

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile.* Gaithersburg, MD: National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-61r3

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile.* National Institute of Standards and Technology. Pridobljeno iz https://doi.org/10.6028/NIST.SP.800-61r3

Scarfone, K. A., & Souppaya, M. P. (2023). *Cybersecurity log management planning guide.* Gaithersburg, MD: National Institute of Standards and Technology (NIST). doi:10.6028/NIST.SP.800-92r1.ipd

Uradni list RS. (27. december 2022). *Zakon o varstvu osebnih podatkov (ZVOP-2)*. Pridobljeno iz Uradni list RS: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187/zakon-o-varstvu-osebnih-podatkov-zvop-2

Priloge

Priloga 1: Revizijski načrt

1. Kontekst in tvegana področja

Paketek, d. o. o. je bistveni subjekt po ZInfV-1 in nastopa kot tretja oseba, ki izvaja storitve IKT, ki podpirajo kritične ali pomembne funkcije zavezancev za DORA.

Glavna tveganja:

- nepopolna pokritost dnevnikov,
- nezadostna hramba / nespremenljivost,
- neučinkovita korelacija / pravila in pozna eskalacija,
- neurejena priglasitev incidentov CSIRT,
- neustrezen register pogodb po DORA,
- tveganja varstva osebnih podatkov (dnevnik obdelave / sledljivost).

2. Cilji in merila

Cilji so skladni z listino o poslu.

Merila (normativni okvir):

- ZInfV-1:
  - 20. člen: Upravljanje in krovna odgovornost vodstva.
  - 21. člen: Varnostna dokumentacija (SUIV, BIA / BCP / IR, KPI / KRI)
  - 22. člen: Varnostni ukrepi.
  - 24. člen: rok hrambe in integriteta dnevnikov (vsaj 6 mesecev; lokacije RS / EU).
  - 30. člen: Priglasitev pomembnih incidentov pristojni skupini *CSIRT*.
  - 36. - 38. člen: Režim visoka / kritična ogroženost (preverbe beleženja, pogostejša poročila).
- ZVOP-2 22. člen: Dnevnik obdelave (kadar je zahtevan) in roki hrambe (2–5 let glede na tveganja).
- GDPR: 33. člen (obvestilo nadzornemu organu v 72 urah ob kršitvi osebnih podatkov).
- DORA 28. in 30. člen: Register pogodb IKT, ključne pogodbene klavzule (lokacije, SLA, vračilo podatkov), pomoč pri incidentih; oddaja storitev v nadaljnje (pod)izvajanje, upoštevani RTS/ITS, podpora klientom pri poročilih.
- Evropski in mednarodni standardi (npr. ISO/IEC 27001/27002) ter smernice ENISA.(kadar je primerno).

3. Obseg in meje

Vključeno: Microsoft Sentinel (viri dnevnikov, podatkovni vmesniki, analitična pravila, scenariji odziva na informacijske varnostne dogodke oz. incidente, nastavitve hrambe, upravljanje vlog), proces odzivanja na incidente (IR), politika hrambe dnevnikov, evidenca CSIRT obvestil in poročil, dnevnik obdelave / sledljivost posredovanj (kjer je relevantno), ter vzorčni nabor pogodb IKT s ključnimi zavezanci po DORA.

Izključeno: tehnični vdorni test ali forenzične storitve; pravno svetovanje; poglobljena presoja skladnosti DORA za stranke (obseg je omejen na presojo sposobnosti Paketka kot tretjega ponudnika / izvajalca storitev IKT, ki omogoča kritične oz. pomembne funkcije zavezancev za DORA).

4. Metodologija in tehnike

- Dokumentarni pregled (politike, IR / BCP, register IKT, pogodbe, konfiguracije Sentinela).
- Intervjuji (CISO, skrbniki, DPO, pravna služba).
- Tehnični pregledi: rok hrambe / arhiv, lokacije, RBAC / PIM, pravila / detekcije, scenariji odziva; vzorčenje KQL (integriteta, časovni žigi, anomalije).
- Table-top / simulacije: CSIRT priglasitev; GDPR 72-urni scenarij; poročanje o incidentih po DORA (RTS polja).
- Analiza vrzeli in prioritetna priporočila (tveganje / skladnost).

6. Vzorčenje in velikost vzorcev

Okno opazovanja: zadnjih 30 dni aktivnih dnevnikov in 6-mesečno obdobje za preverjanje časa hrambe. Vzorci: najmanj 10 ključnih virov dnevnikov; 5 vzorčnih incidentov / opozoril; 5 ključnih pogodb (DORA). Kriteriji za sprejemljivost: dokazna sled; ponovljivost poizvedb / testov.

7. Vloge, odgovornosti in viri

Vloge: Revizor (kandidat), mentor, CISO, skrbniki sistemov, DPO, pravna služba.
Viri: dostop do portala Sentinel (samo za branje), izvoz nastavitev, poizvedbe KQL, dokumenti, pogodbe.

8. Časovnica in mejniki

- 1. teden: zagon, potrjena listina o poslu, vprašalnik, zbiranje dokumentacije.
- 2. – 3. teden: tehnični pregledi in intervjuji; izvedba T1–T4.
- 4. teden: simulacije in testi odziva na incidente; izvedba T5–T7.
- 5. teden: ZVOP-2 in preverjanje *H/C*; izvedba T8–T9; osnutek analize vrzeli.
- 6. teden: osnutek poročila, uskladitev, končna verzija.

9. Upravljanje dokazil in kakovost

Dokazila se beležijo v registru z referencami na RTM / teste. Kakovost je zagotovljena z notranjim pregledom in sledljivostjo; po zaključku se dokazila hranijo omejeno (v skladu z ZVOP-2 / GDPR in akademskimi zahtevami PRIS).

10. Poročanje in komunikacija

Poročanje: osnutek poročila z analizo vrzeli in priporočili (razvrščeno po tveganju in skladnosti), izvleček za upravo, tehnična priloga (KQL / testi). Kritične ugotovitve se komunicirajo sproti.

Priloga 2: Program testiranja

Test (ID & naziv)	Cilj kontrole	Merilo (sklic)	Postopek (koraki)	Vzorčenje	Dokazila	Kriterij sprejema
T1 Pokritost dnevnikov	Zagotovi, da vsi kritični viri pošiljajo dnevnike.	ZInfV-1 22/24	• primerjava CMDB ↔ povezovalniki • preverjanje heartbeat; • preverjanje ključne tabele (SecurityEvent / SigninLogs).	Vsaj10 kritičnih virov	• seznam povezovalnikov • KQL izpis • izvleček CMDB	100% skladnost za kritične vire ali utemeljena izjema.
T2 Rok hrambe / nespremenljivost	• rok hrambe vsaj 6 m • celovitost / nespremenljivost • lokacije RS / EU	ZInfV-1 24	• pregled nastavitev roka hrambe / arhiva; • preverjanje WORM / nespremenljivost; • KQL za časovno pokritost.	Vse nastavitve	• posnetki nastavitev • KQL poročilo • evidence sprememb	Rok hrambe vsaj 180 dni; aktivna politika integritete.
T3 RBAC / PIM / JIT	• načelo najmanjših pravic • časovno omejena aktivacija	ISO 27001 A.5.16 / A.5.18	• identifikacija skrbniških vlog • preverjanje aktivacije PIM (MFA / odobritev / utemeljitev); • pregledi dostopov.	Vse privilegirane vloge	• PIM audit • seznam vlog • zapisniki pregledov	Brez stalnih skrbnikov; PIM / MFA ob aktivaciji; četrtletni pregledi
T4 Analitika & nastavitve	• učinkovita zaznava tveganj • dokumentirane nastavitve	ZInfV-1 22 (učinkovitost ukrepov)	• pregled prvih 15 pravil • preverjanje utemeljenosti z registrom tveganj • evidenca pravil, ki so onemogočena.	15 pravil	• seznam pravil • zapisi o nastavitvah • vzorci opozoril	Pravila preslikav na tveganja; dokumentirane nastavitve.
T5 IR end-to-end	Sledljivost od zaznave do zaključka.	ZInfV-1 22/30	Sledenje petim incidentom: zaznava→triaža→klasifikacija→eskalacija→zaključek.	5 incidentov	• zapisniki IR • časovnice	Popolna sled; skladnost s SLA.
T6 CSIRT priglasitev	Pravočasna in popolna priglasitev CSIRT.	ZInfV-1 30	• Table-top: priprava zgodnjega opozorila; priglasitev; vmesno / končno poročilo, če je zahtevano.	1 simulacija	• osnutki poročil • časovni žigi • komunikacije	Izpolnjeni roki in vsebine.
T7 DORA RTS/ITS	Podpora strankam za DORA poročila.	DORA 19 + RTS/ITS	• simulacija velikega incidenta • priprava poročila po RTS • uporaba predloge ITS	1 simulacija	• shema polj • izvoz • predloga ITS	Vse elemente RTS/ITS je možno zagotoviti v roku.
T8 ZVOP-2 dnevnik obdelave	• skladnost polj in rokov hrambe • dostop IP	ZVOP-2 22	• pregled polj • preverjanje časa hrambe 2–5 let • test izvoza za IP	10 zapisov	• izpis dnevnika • politika hrambe	Vsa polja prisotna; dokaz o dostopnosti.
T9 Režim H/C	Dodatne preverbe in poročanja v H/C.	ZInfV-1 36	• simulacija razglasitve H/C • preverjanje beleženja • tedenska poročila	1 vaja	• navodila • poročila • dashboard.	Dokaz izvedenih preveritev in poročil.

Priloga 3: Vprašalniki revidirancu

Projekt: Revizijsko poročilo o delovanju Microsoft Sentinel (GDPR / ZVOP-2, NIS 2 / ZInfV-1, DORA)

Navodilo: Vpišite odgovore in priložite dokazila.

Pri vsakem vprašanju je naveden normativni sklic (če je relevanten).

A. Upravljanje & dokumentacija (ZInfV-1 20/21)

- Ali imate vzpostavljen in vzdrževan SUIV / SUNP (politike, BIA, BCP, IR, KPI / KRI)? [ ] Da [ ] Ne Opomba / Dokazila: _____
- Kdo je odgovoren za varnost informacij in IR (RACI)? _____
- Kdaj je bila zadnja vaja IR / BCP in katere ugotovitve ste implementirali? _____

B. Dnevniki & rok hrambe (ZInfV-1 24)

- Navedite vse ključne vire dnevnikov povezane v Sentinel (AD, M365, EDR, FW, aplikacije) in njihov status (heartbeat). _____
- Kakšna je nastavljena in dejanska hramba (rok hrambe / arhiv)? Ali je vsaj 6 mesecev? _____
- Kako zagotavljate nespremenljivost (nespremenljivost / WORM) in sledljivost dejavnosti privilegiranih uporabnikov? _____
- Kje so podatki primarno / sekundarno locirani (RS / EU)? _____

C. Incidenti & CSIRT (ZInfV-1 30; GDPR 33; DORA 19/RTS)

- Opredelite klasifikacijo incidentov (ali je mapirana na RTS – pomemben incident / bistvena kibernetska grožnja?) _____
- Kakšen je protokol priglasitve CSIRT (kanali, roki, vsebina)? _____
- Kako zagotavljate 72-urni rok do IP (GDPR 33) – odločitev, evidence, odgovornost? _____
- Navedite 3 zadnje incidente / vaje s časovnicami in dokazili. _____

D. Režim visoka/kritična ogroženost (ZInfV-1 36)

- Imate dokumentiran postopek za H/C (dodatne preverbe beleženja, pogostejša poročila, takojšnja priglasitev)? _____

E. Microsoft Sentinel – konfiguracija

- Seznam ključnih analitičnih pravil in utemeljitev po tveganjih. _____
- Seznam ključnih scenarijev odziva in pogoji / sprožilci scenarijev. _____
- KPI / KRI (npr. MTTD, MTTR, % avtomatiziranih odzivov, delež lažno pozitivnih). _____

F. Dostopi (RBAC / PIM / JIT)

- Kdo ima privilegirane vloge? Ali uporabljate PIM / JIT z MFA in odobritvami? _____
- Kdaj je bil zadnji pregled dostopovnih pravic in kakšni so bili zaključki? _____

G. Zasebnost (ZVOP-2)

- Ali se vodi dnevnik obdelave (kadar je zahtevan) in evidenca posredovanj (2–5 let)? _____
- Kako zagotavljate dostopnost dnevnika nadzornemu organu? _____

H. DORA – IKT tretja oseba

- Ali vodite register IKT pogodb (kritične / pomembne) in imate odobreno TPRM strategijo? _____
- Ali pogodbe določajo lokacije, SLA, vračilo podatkov, pomoč ob incidentu in (pod)izvajanje? _____
- Ali obstaja preizkušen izhodni načrt? _____

I. Podpis odgovorne osebe

- Izjavljam, da so odgovori točni in popolni.

  Ime in priimek: _____ Datum: _____ Podpis: _____