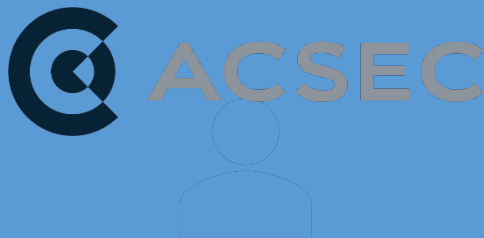




Monitoring cyberbezpieczeństwa

Nowa UoKSC i praktyki CISO

Artur Cieślik



Artur Cieřlik
politykabezpieczenstwa.com.pl



- **Założyciel i główny ekspert ACSEC Sp. z o.o.:**
- Audytor wiodący normy ISO/IEC 27001.
- Audytor wiodący normy ISO/IEC 22301.
- Certified Information Systems Auditor (CISA).
- Audytor wiodący normy ISO/IEC 42001.
- Członek SABI – Stowarzyszenia Inspektorów Ochrony Danych.
- Członek IIA – Instytutu Audytorów Wewnętrznych IIA Polska
- Redaktor naczelny miesięcznika „IT Professional”.
- Członek rady programowej „ABI Expert”.
- Szkolenia i wykłady: Akademia Leona Koźmińskiego, Politechnika Wrocławska, Uniwersytet Ekonomiczny we Wrocławiu, Uniwersytet im. Kardynała Wyszyńskiego „IT Professional Academy” „Informacja Publiczna”, „Forbes Academy”, „IT w Administracji”.

UoKSC po zmianach z 2026 r.

Data	Znaczenie dla planu monitorowania
3 kwietnia 2026	Wejście w życie nowelizacji
3 października 2026	Wpis do wykazu KSC*
3 kwietnia 2027	Wdrożenie nowych obowiązków i podłączenie do S46*
3 kwietnia 2028	Pierwszy audyt nowych podmiotów kluczowych*

Wymagania dla organizacji

Podstawa	Co trzeba wykazać	Przykład realizacji
Art. 8 ust. 1 pkt 2 lit. g	Monitoring w trybie ciągłym	Telemetria, detekcja, dyżur i eskalacja
Art. 8 ust. 1 pkt 2 lit. h	Ocena skuteczności zabezpieczeń	Wskaźniki, testy, działania korygujące
Art. 10	Dokumentacja i nadzór nad nią	Polityki, zapisy operacyjne, retencja
Art. 11–12b	Obsługa i zgłaszanie incydentów	Triage, rejestr, terminy, CSIRT

2024/2690 to obowiązek dla wskazanych dostawców. Dla innych podmiotów może stanowić wzorzec praktyk.

Powiązania z ISO/IEC 27001

Obszar	Odniesienie ISO/IEC 27001:2022
Pomiar, audyt, przegląd kierownictwa	9.1, 9.2, 9.3
Informacja udokumentowana	7.5
Logowanie, monitoring, czas	A.8.15, A.8.16, A.8.17
Podatności, malware, konfiguracja	A.8.8, A.8.7, A.8.9
Incydenty i dowody	A.5.24–A.5.28
Dostawcy i nadzór nad usługami	A.5.19–A.5.22, dla chmury A.5.23
Informacje o zagrożeniach	A.5.7

Retencja zapisów/logów według art. 10

Ust. 4: dokumentacja operacyjna obejmuje zapisy wykonania czynności, w tym automatyczne zapisy w dziennikach systemów.

Ust. 7: co najmniej 2 lata od wycofania dokumentacji z użytkowania lub zakończenia usługi, z ustawową regułą liczenia okresu.

Ust. 8: zniszczenie dokumentacji wymaga protokołu brakowania, a protokoły przechowuje się trwale.

IR (UE) 2024/2690 – kogo dotyczy i co dokładnie wymaga

Dyrektywa **NIS2** stawia szereg szczegółowych wymogów, które z założenia mają zbudować zunifikowany system cyberbezpieczeństwa, zapewniający właściwy poziom zabezpieczenia podmiotów, jak również wymiany informacji.

1

Adresaci

- m.in. dostawcy DNS, rejestry TLD, chmura, centra danych, CDN, **MSP/MSSP**, platformy handlowe, wyszukiwarki, serwisy społecznościowe, dostawcy usług zaufania..

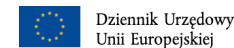
2

Zakres

- uszczegółowienie wymagań z art. 21 NIS2 m.in. zarządzanie ryzykiem, ciągłość i odtwarzanie, bezpieczeństwo łańcucha dostaw, detekcja/reakcja, logging, kryptografia, IAM/MFA, hardening konfiguracji, podatności i łatki, segmentacja, testy.

3

Zasada proporcjonalności i wymagalność dowodowa



Dziennik Urzędowy
Unii Europejskiej

2024/2690

PL
Seria L

18.10.2024

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/2690

z dnia 17 października 2024 r.

ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania

(Tekst mający znaczenie dla EOG)

Zalecenia vs. ISO/IEC 27001 (przykłady)

Propozycje uzupełnień w oparciu o wytyczne ENISA (vs. ISO/IEC 27001:2022 Zał. A)	Uzasadnienie
Kryteria incydentu istotnego i regulacyjne terminy raportowania	Zał. A nie definiuje progów prawnych ani terminów raportowania do organów/CSIRT.
Uzasadnienie proporcjonalności zgodnie z IR 2690.	27001 przewiduje podejście oparte na ryzyku, lecz nie wymaga jawnego uzasadnienia odstępstw wobec IR 2690.
Szczegółowe progi i czasy detekcji (np. MTTD krytyczne ≤ 15 min)	Zał. A wymaga monitorowania, ale nie określa progów czasowych.
SBOM dla systemów krytycznych i zarządzanie komponentami	27001 nie wymaga wprost SBOM.
SLA/OLA z MSSP/MSP (24/7, L1/L2/L3) i podział odpowiedzialności	Zał. A adresuje relacje z dostawcami ogólnie, bez precyzyjnych SLA/OLA SOC/EDR/SIEM.
Obowiązkowe testy odtworzeniowe i docelowe RTO/RPO dla usług krytycznych	27001 wymaga mechanizmów BC/ICT readiness, ale nie narzuca częstotliwości i progów.
Specyficzne wymagania dla DNS/TLD/Cloud/CDN/MSSP zgodnie z IR 2690	Zał. A nie pokrywa specyficznych wymogów sektorowych IR (np. DNS resiliency).
Integracja Threat Intelligence z detekcją (czas publikacji i adaptacji)	Zał. A nie określa tempa adaptacji TI do use-case'ów.
Repozytorium dowodów	Zał. A nie narzuca centralnego repozytorium dowodów.
Mierzalne progi patchowania oparte na ryzyku (np. MTTP ≤ 7 dni)	Zał. A nie definiuje progów czasowych dla łatek.
Wymogi komunikacji kryzysowej do regulatorów/klientów	27001 nie narzuca treści i sposoby komunikacji z regulatorem oraz klientem.
IAM/MFA/PAM na systemach krytycznych	Zał. A wskazuje kontrolę dostępu, lecz bez aż tak konkretnych wymagań.
Formalny RACI z CSP/MSSP	Zał. A nie wymaga matrycy RACI dla chmury/MSSP.

Częste braki (ENISA/IR 2024/2690 vs. ISO/IEC 27001)

Obszar IR 2024/2690	Referencja IR / NIS2	Luka (opis skrócony)	Działania wymagane	Priorytet (Niski/Średni/Wysoki)
Zarządzanie ryzykiem	IR 2024/2690 – risk management; NIS2 art.21(2)(a–j)	Brak formalnego procesu zarządzania ryzykiem BI	Zdefiniować kryteria dla ryzyka, uaktualnić metodykę, powiązać ryzyka z SoA i KPI	Wysoki
Inwentaryzacja i klasyfikacja	IR – zarządzanie aktywami i krytyczność	Niespójna klasyfikacja krytyczności	Ujednolicić klasyfikację i przypisać właścicieli	Średni
Zmiany i konfiguracja	IR – hardening, konfiguracje, change management	Brak baseline dla krytycznych	Zdefiniować baseline, przeprowadzić audyt zgodności	Wysoki
IAM / MFA (uwierzytelnianie wieloskładnikowe) / PAM	IR – IAM i uwierzytelnianie wieloskładnikowe	MFA (uwierzytelnianie wieloskładnikowe) niepełne na kontach uprzywilejowanych	Włączyć MFA (uwierzytelnianie wieloskładnikowe)/PAM; wprowadzić cykl przeglądów/audytów kont	Wysoki
Segmentacja sieci	IR – segmentacja, ograniczenie przepływów	Brak mapy/specyfikacji stref i ACL dla stref	Zdefiniować strefy, wdrożyć ACL/NGFW; testy ruchu	Wysoki
Logowanie i monitorowanie	IR – logowanie, detekcja, retencja	Brak części źródeł w SIEM	Dodać źródła i ustalić retencję	Wysoki
Reagowanie na incydenty	IR – playbooki, komunikacja, zgłoszenia	Brak ćwiczeń, nieaktualna lista kontaktowa	Przeprowadzić ćwiczenia i aktualizować kontakty w zakresie monitorowania 24/7	Średni
Kryteria incydentu istotnego	IR – istotność, zgłaszanie	Brak progów istotności	Przyjąć progi zgodne z IR 2690 i dodać do IRP, przeprowadzić szkolenia	Wysoki
Vulnerability & patching	IR – podatności i łatki	Brak SLA patchy u dostawców	Wdrożyć SLA i automatyzować skany	Wysoki
Anti-malware / EDR	IR –EDR/AV	Brak EDR/AV na VDI	Rozszerzyć EDR/AV na VDI.	Średni
Kryptografia / klucze	IR – crypto, KMS/HSM	Brak centralnego rejestru kluczy krypto.	Utworzyć rejestr i ujednolicić polityki krypto.	Średni
Backup / odtwarzanie	IR – kopia zapasowa/odtworzenie i testy DR	Testy DR nie są prowadzone dla wszystkich krytycznych systemów	Zaplanować testy DR dla krytycznych systemów i raportować czasy.	Wysoki
ciągłość działania/odtworzenie / gotowość ICT	IR – ciągłość działania/odtworzenie	Brakuje BIA dla 2 usług krytycznych.	Wykonać BIA i uaktualnić BCP/DRP, przeprowadzić testy	Wysoki
Supply chain	IR – bezpieczeństwo dostawców	Brak klauzul NIS2 w 36% umów	Zaktualizować wzorce umów o prawa audytu i raportowanie	Wysoki
SBOM / komponenty	IR – oprogramowanie i SBOM	Brak procesu SBOM i SCA	Wdrożyć SCA i gromadzić dane SBOM	Średni
SSDLC	IR – secure SDLC, SAST/DAST	Nie wszystkie produkty objęte SAST/DAST	Rozszerzyć CI o SAST/DAST	Średni
Threat Intel	IR – wykorzystanie TI	Brak playbooka TI→detekcja	Sformalizować proces TI i przetestować sposób postępowania dla detekcji	Średni
Szkolenia	IR – program szkoleń	Brak pomiaru efektywności	Wprowadzić wskaźniki efektywności	Niski
Chmura	IR – podział odpowiedzialności (shared responsibility), logowanie	Niepełny model odpowiedzialności	Zdefiniować RACI, wprowadzić monitorowanie i retencję logów	Wysoki
Komunikacja kryzysowa	IR – komunikacja kryzysowa	Brak szablonów i zapasowych kanałów komunikacji	Przygotować szablony, przeprowadzić test łączności	Średni

Przykładowa lista kontrolna CISO

1. Zakres, klasyfikacja informacji, usług i systemów krytycznych (w tym usługi mieszczące się w IR 2024/2690).
2. Ocena Gap – w zakresie UoKSC oraz ew. 2024/2690 w stosunku do SoA/Załącznik A.
3. Plan zgodności z kamieniami milowymi oraz wskaźnikami KRI.
4. Governance – uchwała zarządu, wskazanie role i odpowiedzialności, ustalenie cyklu przeglądów.
5. Zarządzanie ryzykiem – metodologia, apetyt na ryzyko, rejestr ryzyka, przypisanie właścicieli.
6. IRP/SOC – CIRP, playbooki, kryteria incydentu istotnego, informowanie CSIRT, 24/7.
7. Łańcuch dostaw – audyty, klauzule w umowach, ciągłość usług.
8. BCP/DRP – BIA, strategia, RTO/RPO, testy odtworzeniowe.
9. Narzędzia – MFA, segmentacja, hardening, XDR/AV, logowanie (retencja), kryptografia.
10. Podatności i patchowanie – zasady, SLA, wskaźniki (np. krytyczne/o niskim wpływie), dowody.
11. Szkolenia i świadomość z mierzeniem efektywności.
12. Dowody – mapa wymagań → kontrolka → dowód, repozytorium dowodów.

Jak monitorować wdrożenie/wpięcie NIS2/IR 2024/2690 w istniejący SZBI (ISO/IEC 27001:2022)

Obszar	Status (przykład)	KPI/KRI (przykład docelowych)	Właściciel	Dowód
Governance i przeglądy	Żółty	Przeglądy kwartalne 100%, decyzje ≤ 30 dni	CISO / Zarząd	Protokoły, KRI
Zarządzanie ryzykiem	Żółty	Pokrycie ryzyk ≥ 95%, plany ≥ 90%	CISO / Właściciele	Polityka, rejestr ryzyka
Zgodność (NIS2/IR 2690)	Żółty	Pokrycie dowodami ≥ 95%, raporty w terminach	CISO / Compliance	Matryca, repozytorium dowodów
Gotowość do reagowania na incydenty	Żółty	MTTD ≤ 15 min, MTTR ≤ 4 h, 2 ćwiczenia/rok	CISO / SOC	CIRP, playbooki
MSSP/MSP	Żółty	Przeglądy kwartalne = 100%, niezgodności ≤ 30 dni	CISO / Opiekun dostawcy	Przeglądy kwartalne, zapisy zadań
Metryki i raportowanie	Żółty	Raportowanie w terminie; KPI zgodne z progami	CISO	Wyniki, źródła danych
Szkolenia i świadomość	Zielony	Pokrycie ≥ 98%, CTR ≤ 3%	CISO / HR	Plany szkoleń, wyniki szkoleń i testów
Repozytorium dowodów	Żółty	Aktualność ≤ 90 dni, pokrycie ≥ 95%	CISO / ?	Repozytorium artefaktów

Monitorowanie procesów

Skuteczność kontroli i decyzje o ryzyku

Właściciele, pomiary, dowody

Architektura pomiaru

Warstwa	Przykład: odebranie dostępów
Cel i ryzyko	Były pracownik nie ma aktywnego dostępu
Kontrola i właściciel	Offboarding w HR/ITSM, wykonanie przez IAM
Źródła i obliczenie	HR + IAM, czas do blokady wszystkich kont
Próg i decyzja	Przekroczenie SLA uruchamia eskalację do właściciela
Dowód i weryfikacja	Zgłoszenie, log blokady, test logowania, przegląd CISO

Każdy wskaźnik potrzebuje czasu pomiaru i osoby odpowiedzialnej

Rejestr zgodności

Pole rejestru	Przykład MON-01
Wymóg i zakres	Art. 8 ust. 1 pkt 2 lit. g, krytyczne usługi w CMDB
Kontrola i właściciel	Odbiór i kontrola jakości logów, SOC Manager
Miara i próg	100% krytycznych źródeł spełnia warunki jakości
Dowód i wynik testu	Lista źródeł, raport aktualności, test alarmu utraty logów
Odchylenie i działanie	Brak logów, właściciel i termin

Macierz KPI/KRI procesów

Obszar i ID matrycy	KPI (wykonanie)	KRI (ekspozycja)	Przykładowy cel
Dostępy • REQ-04	Przeglądy w terminie	Konta bez wznowienia	Cykl $\leq$ 90 dni
Podatności • REQ-09	Czas usunięcia podatności	Krytyczne po SLA	Średnio $\leq$ 7 dni
Odtwarzanie • REQ-12	Udane testy / wykonane	Usługi bez testu RTO/RPO	Sukces $\geq$ 95%
Dostawcy • REQ-14	Oceny w terminie	Krytyczni bez oceny	Zakres 100%
Szkolenia • REQ-18	Osoby przeszkolone / zakres	Role bez kompetencji	Pokrycie $\geq$ 98%

Definicja wskaźnika i wiarygodność danych

Karta wskaźnika

Cel, właściciel i zakres usług

Licznik, mianownik, jednostka

Źródła, zapytanie i wersja reguły

Okno pomiaru, próg, reakcja

Pułapki interpretacji

Brak pomiaru oznaczony jako 0

Wyjątki usunięte z mianownika

Średnia ukrywająca skrajne wyniki

Ten sam incydent liczony wielokrotnie

Dowody działania

Warstwa	Co przechowujemy	Co sprawdza audytor
Zasady	Polityka, procedura, role, SLA	Czy określono wymaganie i odpowiedzialność?
Wykonanie	Log, ticket, przegląd, zapis szkolenia	Czy kontrola działała w badanym okresie?
Skuteczność	Wynik testu, próbka, analiza odchylenia	Czy osiągnięto cel zabezpieczenia?
Nadzór	Decyzja, plan naprawy, ponowny test	Czy organizacja usunęła przyczynę luki?

Raport CISO – podstawa decyzji kierownictwa

Wynik przykładowy	Znaczenie	Decyzja/dowód wykonania
2 usługi bez testu odtworzenia	Niepotwierdzona zdolność powrotu	Właściciel, termin testu, wynik
1 krytyczne źródło logów milczy	Luka w detekcji dostępu	Przywrócenie połączenia, test alertów
8 zaległych przeglądów dostępu/kont	Niepotwierdzone uprawnienia	Sprawdzenie, usunięte dostępy
3 eskalacje MSSP po SLA	Ryzyko spóźnionej reakcji	Plan naprawczy, test reakcji

Monitorowanie jakości MSSP

Uzgodnienia w SLA/OLA

Źródła/usługi/godziny obsługi

Początek i koniec każdego zdarzenia

Powiadomienie i akceptacja np. izolacji

Dostęp do logów oraz eksport przy wyjściu od danego dostawcy

Kontrola po stronie klienta

Test kontaktu poza godzinami pracy

Próbka alertów i jakości kwalifikacji

Niezależny pomiar braków logów

Przegląd działań i zaległości dostawcy

Audyt monitorowania procesów

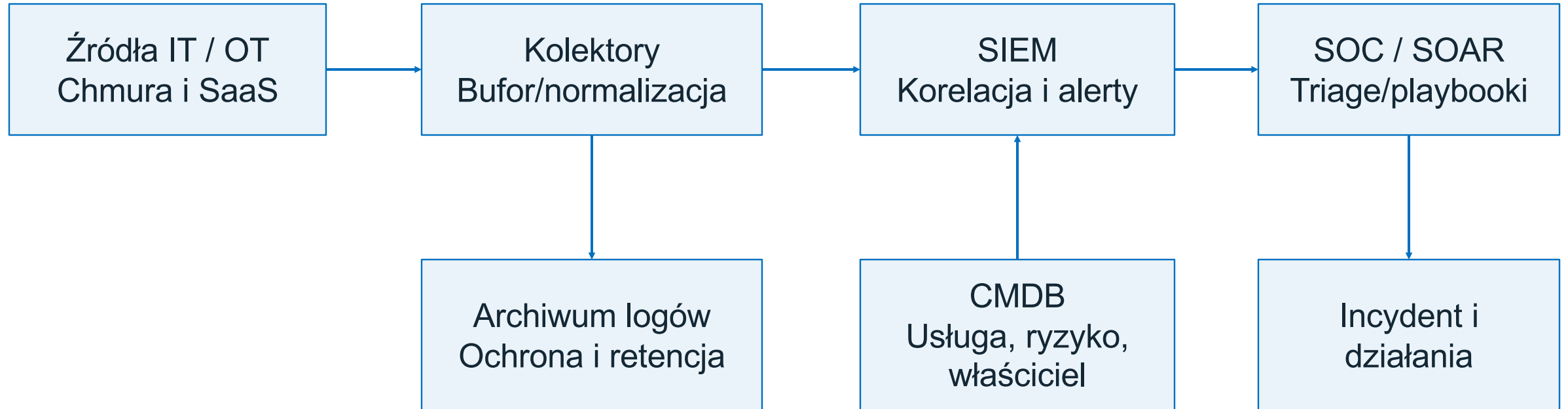
- | | | |
|-----------|----------------------------------|---|
| 01 | Zakres i odpowiedzialność | Czy każda krytyczna usługa ma właściciela kontroli? |
| 02 | Odtworzenie wyniku | Czy można ponownie policzyć wskaźnik z danych źródłowych? |
| 03 | Dowód skuteczności | Czy próbka potwierdza wykonanie i osiągnięcie celu? |
| 04 | Odchylenia i wyjątki | Czy decyzje mają termin, akceptację i szczególnie weryfikację wykonania? |
| 05 | Niezależny przegląd | Czy audytor ocenia także niewykonane i nieudane np. reakcje na incydenty? |

Próbka audytowa obejmuje wynik poprawny, przekroczenie progu, brak danych

Monitorowanie infrastruktury

Źródła danych, detekcja, przegląd logów, triage, reakcja, zgłoszenie incydentu

Architektura monitoringu



Rejestr i raport KPI/KRI korzystają z CMDB, SIEM

Należy pamiętać o dopływie logów, czasie, kolejkach, dostępności SIEM, kanałach alarmowania

Źródła danych według scenariusza ryzyka

Scenariusz	Źródła	Kontekst do decyzji
Przejęcie konta	AD, VPN, PAM, audyt SaaS	Rola, uprawnienia, urządzenie, właściciel
Ransomware	EDR, serwery, DNS, backup	Krytyczności, segmenty, możliwość izolacji segmentów/hostów
Wyciek danych	Proxy, DNS, DLP, audyt aplikacji	Klasa danych, odbiorca, normalny profil
Zmiana w OT	Dostęp serwisowy, pasywna sieć, stacja inżynierska	Bezpieczny tryb reakcji
Utrata monitoringu	Heartbeat, kolejki, parser, czas	Lista wymaganych źródeł, stan kolektora

Zakres logów wynika z ryzyka i potrzeb detekcji. W OT plan testów uzgadnia się z właścicielem procesu.

Pokrycie i telemetria

Miara	Sposób pomiaru	Cel przykładowy
Pokrycie efektywne	Źródła spełniające wszystkie warunki / wymagane źródła	100% krytycznych
Świeżość logów	Czas od ostatniego oczekiwanego zdarzenia	Według profilu źródła
Opóźnienie dopływu	Czas odbioru – czas zdarzenia	≤ 5 min
Poprawność parsera	Rekordy z wymaganymi polami / rekordy odebrane	Próg lokalny
Skuteczność detekcji	Udane testy / wykonane testy + zakres planu	Każdy scenariusz krytyczny

Progi alarmowania i detekcja

Przykładowy sygnał	Warunek alarmowania	Triage
Nadanie roli administratora	Zmiana poza zatwierdzonym procesem	ITSM, sprawca, konto, zakres roli
Seria błędów logowania	≥ 10 błędów / 5 min i sukces w 10 min	AD, VPN, urządzenie i profil
Wyłączenie ochrony EDR	Nieplanowana zmiana lub brak heartbeat	Serwis? Uprawnienia? Inne alerty?
Usunięcie kopii zapasowych	Operacja konta poza uprawnionym scenariuszem	PAM, konfiguracja, integralność kopii

hipoteza, źródła, reguła, próg, wyjątki, właściciel, playbook, test

MSP: progi poważnego incydentu

Usługi zarządzane. Wystarczy jedno kryterium z art. 10.

Przesłanka	Próg kwalifikacji	Art. 10
Całkowita niedostępność usługi	Ponad 30 minut.	lit. a
Ograniczona dostępność usługi	Ponad 1 godz. i liczba dotkniętych użytkowników > min(5% użytkowników usługi w UE, 1 mln).	lit. b
Naruszenie danych wskutek podejrzanego działania złośliwego	Bez minimalnego czasu i bez progu liczby użytkowników.	lit. c
Naruszenie danych niezależnie od przyczyny	Liczba dotkniętych użytkowników > min(5% użytkowników usługi w UE, 1 mln). Bez minimalnego czasu.	lit. d

Naruszenie danych: integralności, poufności lub autentyczności danych związanych z usługą.

Niezależnie oceniamy kryteria ogólne (art. 3) i powtarzalność (art. 4).

min = niższa wartość. Użytkownicy według art. 3 ust. 3. Szczegóły i źródło w notatkach.

MSSP: progi poważnego incydentu

Usługi zarządzane w zakresie bezpieczeństwa. Progi są takie same jak dla MSP.

Przesłanka	Próg kwalifikacji	Art. 10
Całkowita niedostępność usługi	Ponad 30 minut.	lit. a
Ograniczona dostępność usługi	Ponad 1 godz. i liczba dotkniętych użytkowników > min(5% użytkowników usługi w UE, 1 mln).	lit. b
Naruszenie danych wskutek podejrzanego działania złośliwego	Bez minimalnego czasu i bez progu liczby użytkowników.	lit. c
Naruszenie danych niezależnie od przyczyny	Liczba dotkniętych użytkowników > min(5% użytkowników usługi w UE, 1 mln). Bez minimalnego czasu.	lit. d

Naruszenie danych: integralności, poufności lub autentyczności danych związanych z usługą.

Niezależnie oceniamy kryteria ogólne (art. 3) i powtarzalność (art. 4).

min = niższa wartość. Użytkownicy według art. 3 ust. 3. Szczegóły i źródło w notatkach.

Przykład MSP: ograniczenie usługi

Usługa zdalnej administracji IT.

Element oceny	Ustalenia
Zdarzenie	Błąd aktualizacji blokuje zdalne wykonywanie zadań u części użytkowników. Pozostałe funkcje działają.
Pomiar	08:00–09:20, czyli 80 minut ograniczenia. Dotkniętych 1 200 z 20 000 użytkowników usługi w UE.
Porównanie z progiem	$5\% \times 20\,000 = 1\,000$. Niższy próg to 1 000 użytkowników. $1\,200 > 1\,000$ oraz $80\text{ min} > 60\text{ min}$.
Dowody	Testy dostępności funkcji, logi zadań i czas przywrócenia. Wykaz użytkowników usługi oraz rejestr zmiany.

Poważny incydent: art. 10 lit. b.

Przykład MSSP: manipulacja logami

Usługa monitorowania SOC.

Element oceny	Ustalenia
Zdarzenie	Atakujący używa przejętego konta administratora MSSP. Zmienia wpisy w logach jednego klienta w zarządzanym SIEM.
Pomiar	Potwierdzono zmianę treści logów bez uprawnienia. Aktywność trwała 12 minut. Usługa pozostawała dostępna.
Porównanie z kryterium	Naruszono integralność danych związanych z usługą w wyniku podejrzanego działania złośliwego.
Dowody	Ślad sesji administratora i audyt zmian. Porównanie logów w SIEM z chronioną kopią źródłową.

Poważny incydent: art. 10 lit. c.

Operacyjny przegląd logów

Kiedy	Co analizujemy	Jaki zapis pozostaje
Ciągle	Alerty i kondycję dopływu danych	Alert, ticket, eskalacja
Na zmianie / codziennie	Kolejkę, luki źródeł, konta uprzywilejowane	Co sprawdzone i przekazanie zmiany
Co tydzień	Trendy, powtarzalne zdarzenia, strojenie reguł	Raport analizy, zmiana reguły
Po zmianie / incydencie	Nowe ryzyko, luki detekcji, kompletność śladów	Test i działania naprawcze

Częstotliwość dobiera się do ryzyka i obowiązku monitorowania ciągłego.

Retencja i klasyfikacja danych w logach

Klasa / zastosowanie	Reguła przechowywania	Kontrola
Indeks SIEM do analizy	Okno szybkiego wyszukiwania według potrzeb SOC	Koszt, dostępność zapytań
Log jako dokumentacja	Art. 10 ust. 4 i 7 UoKSC, polityka archiwizacji	Kwalifikacja i termin usunięcia
Materiał konkretnego incydentu	Zabezpieczenie na potrzeby obsługi i postępowań	Wstrzymanie usuwania, integralność
Pozostała telemetria	Cel, ryzyko, właściwe przepisy, minimalizacja danych	Maskowanie, ograniczony dostęp

Ochrona logów i odporność monitoringu

Wiarygodność śladu

Spójny czas i strefa czasowa

Kontrola dostępu oraz rejestr odczytów

Ochrona przed zmianą i usunięciem

Łańcuch przekazania dowodu

Dostępność monitoringu

Buforowanie i kontrola utraty rekordów

Redundancja, kopie i test odtworzenia

Alarm o awarii poza SIEM

Monitoring pojemności

Triage i granice automatyzacji SOAR

Etap	Działanie	Decyzja
Wzbogacenie	CMDB, właściciel, konto, zmiana ITSM	Czy zagrożona jest usługa krytyczna?
Weryfikacja	Korelacja śladów i ocena hipotezy	Zdarzenie poprawne, fałszywy alert czy incydent?
Ograniczenie skutków	Zatwierdzony playbook i ślad działania	Automatycznie czy po akceptacji?
Kwalifikacja prawna	Wpływ, skala, czas, straty, odbiorcy	Czy to incydent poważny?
Zamknięcie	Przyczyna, korekta, test po zmianie	Czy ryzyko i luka zostały ograniczone?

Dla systemów krytycznych i OT izolacja wymaga wcześniej uzgodnionych warunków oraz odpowiedzialności.

MTTD i czas reakcji

10:00	Pierwszy obserwowalny ślad
10:03	Odbiór w SIEM
10:08	Detekcja przez regułę
10:12	Rozpoczęcie triage
10:25	Ograniczenie skutków

W tym przypadku: detekcja 8 min, reakcja analityka 4 min, ograniczenie skutków 17 min od detekcji

MTTD i czas reakcji

Miara	Co oznacza	Na co odpowiada
MTTD — średnia	Suma czasów wykrycia podzielona przez liczbę przypadków.	Ile przeciętnie zajmuje nam wykrycie incydentu?
Mediana — p50	Połowa przypadków ma czas wykrycia nie większy od tej wartości.	Jak szybko wykrywamy typowy incydent?
p95 — 95. percentyl	Próg, w którym mieści się około 95% czasów wykrycia. Pozostałe około 5% jest dłuższe.	Jak długo trwa wykrycie w wolniejszych przypadkach, poza skrajnymi 5%?
n — liczba przypadków	Liczba incydentów uwzględnionych w obliczeniach.	Na ilu obserwacjach opieramy wynik?

Fałszywe alarmy i incydenty

Miara	Przykład	Interpretacja
Udział fałszywych alertów	$30 \text{ FP} / 100 \text{ zamkniętych alertów} = 30\%$	Jakość alertów ocenionych w triage
Konwersja alert-to-incident	$10 \text{ alertów powiązanych z incydem} / 100 = 10\%$	Odsetek alertów potwierdzających incydent
Klasyczny FPR	$\text{FP} / (\text{FP} + \text{TN})$	Udział fałszywych alertów w rozpatrzonych alarmach
Niewykryte scenariusze	$2 \text{ niewykryte} / 10 \text{ testów} = 20\%$	Luka wykryta w kontrolowanym teście

Audyt monitorowania infrastruktury

- | | | |
|-----------|-------------------------------|--|
| 01 | Pełna ścieżka | Czy testowe zdarzenie trafia do SIEM, analityka i ITSM? |
| 02 | Pokrycie rzeczywiste | Czy wymagane źródła i pola działają dla usług krytycznych? |
| 03 | Awaria monitoringu | Czy utrata źródła lub SIEM wyzwala niezależny alarm? |
| 04 | Dowody i retencja | Czy można odtworzyć chroniony log oraz jego pochodzenie? |
| 05 | Eskalacja i zgłoszenie | Czy dyżurny potrafi działać i wysłać pakiet właściwym kanałem? |

Weryfikacja

Priorytet	Kryterium ukończenia
Zakres usług, rejestr, właściciele, definicje	Znany mianownik i najważniejsze luki
Źródła krytyczne, przypadki detekcji, retencja	Przejście testu od logu do reakcji
Ćwiczenie, przegląd CISO, korekta SLA, audyt próbki	Decyzje, działania naprawcze

Zgłoszenie incydentu i współpraca z CSIRT

Etap	Termin ogólny	Zakres informacji (skrót)
Wczesne ostrzeżenie	Niezwłocznie ≤ 24 h	Podejrzenie przyczyny, zasięg i wpływ
Zgłoszenie incydentu poważnego	Niezwłocznie ≤ 72 h	Ocena incydentu, dotknięta usługa, wskaźniki
Sprawozdanie okresowe	Na wniosek CSIRT	Stan obsługi i nowe ustalenia
Sprawozdanie końcowe	≤ 1 miesiąc od zgłoszenia	Przyczyna, skutki, działania naprawcze

Pytania i dyskusja

Którą lukę sprawdzisz jako pierwszą?

Czy znamy zakres usług i źródeł?

Czy potrafimy udowodnić skuteczność detekcji?

Czy wiemy, kto podejmuje decyzję?

Karta wskaźnika

Pole	Wzór do uzupełnienia
ID, cel i właściciel	[ID] [ryzyko / cel] [osoba lub rola]
Zakres i definicja	[usługi] [licznik] / [mianownik] [jednostka]
Dane i odtwarzalność	[systemy] [klucze łączenia] [wersja zapytania]
Pomiar i interpretacja	[okno] [częstotliwość] [n] [braki] [wyjątki]
Próg i działanie	[zielony / żółty / czerwony] [eskalacja] [termin]
Dowód i przegląd	[URI dowodu] [data] [weryfikator] [kolejny przegląd]

Macierz KPI/KRI infrastruktury

Wskaźnik	Źródło i definicja	Właściciel / przegląd
Efektywne pokrycie	CMDB, SIEM, źródła spełniające warunki / wymagane	Właściciel SIEM / codziennie
TTD, MTDD, mediana, p95	Oś czasu incydentu, detekcja – pierwszy ślad	SOC / miesięcznie
Udział FP	FP / zamknięte alerty	Odpowiedzialny za wykrywanie / tygodniowo
Konwersja alertów	Alerty związane z incydemem / zamknięte alerty	SOC / miesięcznie
Opóźnienie logów	Odbiór – czas zdarzenia, p95 oraz ubytki	Właściciel SIEM / ciągle
Eskalacje w SLA	Eskalacje w terminie / wymagane eskalacje	SOC Manager / miesięcznie

Wykaz mierników

Grupa pól	Pola wymagane w rejestrze
Identyfikacja	ID, wersja, zakres podmiotowy, usługa, zasób / zbiór
Podstawa	Przepis i jednostka redakcyjna, wymaganie, mapowanie ISO
Realizacja	Cel, opis kontroli, częstotliwość, właściciel/zastępca
Pomiar	ID KPI/KRI, definicja, źródło, próg, bieżący wynik
Dowód	Lokalizacja, okres, data, klasa danych, retencja, wynik testu
Nadzór	RAG, odchylenie, zadanie, termin, wyjątek, akceptacja
Zamknięcie	Weryfikator, wynik ponownego testu, data przeglądu

Przykładowe wskaźniki

Aneks G. Źródła i materiały

UoKSC po nowelizacji

Dz.U. 2026 poz. 252, art. 8, 8c–8e, 10–12b, 15 i przepisy przejściowe

Harmonogram wdrożenia

Ministerstwo Cyfryzacji, komunikat z 5 czerwca 2026 r.

Rozporządzenie (UE) 2024/2690

Zakres adresatów oraz załącznik pkt 2.2, 2.3, 3.2–3.6 i 7

Praktyki wdrożeniowe i mapowanie

ENISA Technical Implementation Guidance, 2025, Mapping table v1.2