

Co przygotować przed podłączeniem urzędu do SOC

[Read in English \(UK\)](#)

Inwentaryzacja, Źródła logów, upoważnienia i test reakcji przed odbiorem usługi.

Opracowanie DATPOL, 4 października 2026. Materiał pomaga przygotować rozmowę, zakres prac i odbiór; nie zastępuje projektu ani instrukcji konkretnego urzędu.

Opisz środowisko i właścicieli

Przygotuj listę lokalizacji, systemów, serwerów, stacji, urządzeń sieciowych i dostawców. Wskaż osoby odpowiedzialne oraz krytyczne usługi. Ustal Źródła logów, synchronizację czasu i bezpieczny sposób przekazywania danych. Brak zdarzeń może oznaczać brak integracji, a nie brak zagrożenia.

Uzgodnij zakres reakcji

Zapisz kanały kontaktu, godziny obsługi, priorytety i czynności wymagające akceptacji. Automatyczna blokada może zakłócić pracę, dlatego potrzebuje zatwierdzonej reguły, wyjątków, planu działania i procedury odblokowania. Nie utożsamiaj alertu z potwierdzonym zagrożeniem.

Sprawdź cały obieg zdarzenia

W uzgodnionym scenariuszu przetestuj dostarczenie zdarzenia, wykrycie, powiadomienie i udokumentowanie reakcji. Odbierz listę aktywnych integracji oraz braków. SOC wspiera wykrywanie i reagowanie; nie zastępuje zarządzania ryzykiem, backupu ani całości obowiązków jednostki.

Checklista do wykorzystania

- Inwentaryzacja i krytyczne usługi.
- Źródła logów i test dostarczania.
- Kontakty, eskalacje i zatwierdzone działania.
- Protokół odbioru i lista braków.

Dalsze kroki i materiały

[Zakres usługi i materiały DATPOL](#)

[CISA — Use Logging on Business Systems](#)

Zgłoszenia serwisowe: [DATPOL24](#). Nie przesyłaj haseł ani sekretów w formularzu.

Powiązane poradniki

- [Jak przygotować firmę do audytu bez zakłócania pracy](#)
- [Jak porównać serwerownię w budynku i kontenerów?](#)
- [Jak udokumentować test odtworzenia kopii zapasowej](#)

Wersja #2

Utworzono 2026-10-04 14:56:33 UTC przez Administrator DATPOL

Zaktualizowano 2026-10-04 14:56:35 UTC przez Administrator DATPOL