

Bezpieczeństwo operacyjne

Tożsamości, sekrety i pochodzenie artefaktu

mgr inż. Jakub Woźniak

Zarządzanie Systemami Rozproszonymi · Semestr zimowy 2026/27



Punkt	Zagrożenie	Możliwy skutek
CI	Wykonanie kodu niezaufanego PR	Kradzież uprawnień wydania
Rejestr	Podmiana wskazania tagu	Uruchomienie innego obrazu
Worker	Przejęcie procesu	Dostęp do danych z jego rolą

Granice zaufania wyznaczają osobne tożsamości i zasady dostępu.

Pytanie	Mechanizm	Przykład
Kto wykonuje operację?	Token / certyfikat / tożsamość	worker-prod
Co może zrobić?	Rola i zakres	Odbiór z kolejki orders
Czy było dozwolone?	Log audytowy i decyzja polityki	Receive: allow; Delete: deny

- Dostęp sieciowy do endpointu nie nadaje uprawnień do danych.
- Wspólna tożsamość wszystkich usług zwiększa zasięg przejęcia.

Podmiot	Uprawnienie	Zakres
API / publisher	Wysyłanie wiadomości	Kolejka orders
Worker	Odbiór i potwierdzenie	Kolejka orders
Potok IaC	Zarządzanie zasobem	Wybrane środowisko

- Worker nie potrzebuje usuwania kolejki ani zarządzania rolami.
- Rozdzielenie control plane i data plane.

Microsoft — Service Bus managed identities



- Token w obrazie lub repozytorium pozostaje w historii artefaktów.
- Base64 w Kubernetes Secret jest kodowaniem, nie szyfrowaniem.
- Potrzebne kontrola odczytu, szyfrowanie magazynu i ograniczenie montowania.
- Odczyt Secret i możliwość uruchomienia Poda wymagają wspólnej analizy uprawnień.

Kubernetes — Secrets good practices



- Sprawdzić, czy proces odczytuje sekret ponownie, czy tylko przy starcie.
- Okno zgodności ograniczone; pomiar użycia starego poświadczenia.
- Przy kompromitacji: pilne unieważnienie i analiza użycia; płynna rotacja może nie wystarczyć.

Tokeny krótkotrwałe ograniczają czas użycia, ale nie usuwają potrzeby kontroli ról.

Artefakt	Odpowiada na pytanie	Nie dowodzi
SBOM	Jakie składniki zadeklarowano?	Braku podatności
Skan	Jakie znane problemy wykryto?	Braku błędów nieznanых
Podpis	Czy treść pasuje do podpisu i zaufania?	Bezpieczeństwa kodu
Provenance	Z czego i gdzie wykonano build?	Poprawności funkcjonalnej

SLSA 1.2 — Specification

Wyciąg dydaktyczny, format tabelaryczny

COMPONENT	VERSION	SOURCE
libexample	2.4.0	image layer sha256:aaa...

FINDING	FIXED IN	REACHABILITY
DEMO-2026-001	2.4.1	wymaga sprawdzenia

- Identyfikator podatności fikcyjny. Dopasowanie pakietu nie dowodzi wykorzystania błędu.
- Priorytet: ekspozycja, osiągalność kodu, skutek i dostępność poprawki.
- Wyjątek od polityki: właściciel, powód, termin i działanie ograniczające ryzyko.

```
subject:  
  name: worker  
  digest: sha256:abc...  
buildDefinition:  
  resolvedDependencies:  
    - uri: git+https://example.test/orders  
      digest: {gitCommit: "9c81..."}  
runDetails:  
  builder: https://ci.example.test/trusted-builder
```

Schemat poglądowy, nie pełna atestacja SLSA. Wielokropki zastępują pełne identyfikatory.

- Sprawdzić digest wyniku, oczekiwany builder, repozytorium i rewizję.

SLSA 1.2 — Provenance

```
cosign verify \  
  --certificate-identity "$EXPECTED_IDENTITY" \  
  --certificate-oidc-issuer "$EXPECTED_ISSUER" \  
  "$IMAGE_BY_DIGEST"
```

- Zmienne ustala polityka wydania; nie dane dostarczone przez autora obrazu.
- Podpis zgodny kryptograficznie, lecz nieoczekiwany signer → odrzucenie.
- Zaufany signer z przejętym buildem nadal może podpisać szkodliwy obraz.



- Rola na konkretnej kolejce zamiast całej subskrypcji.
- Brak współdzielonego hasła w konfiguracji aplikacji.
- Przejęty proces nadal działa z uprawnieniami swojej tożsamości.

Microsoft — Service Bus managed identities

Żądanie wdrożenia



Polityka admission



Dopuszczenie / odmowa

- Sprawdzenie dozwolonego rejestru, digestu i wymaganych poświadczeń.
- Polityka wymaga wdrożonego kontrolera weryfikacji; Kubernetes nie robi tego automatycznie.
- Awaria weryfikatora: jawna decyzja o dostępności i zachowaniu fail-closed.

Kubernetes — Admission controllers

Warunek polityki	Odczyt z atestacji
Repozytorium: org/orders	org/orders
Builder: trusted-prod	personal-runner
Commit: zatwierdzony 9c81...	9c81...
Podpis	Poprawny, tożsamość innego workflow

Decyzja

Dopuszczyć obraz? Które kontrole przechodzą, które zawodzą? Czy czysty skan zmienia decyzję?

- NIST SP 800-190 — Application Container Security Guide
- Kubernetes — Secrets good practices
- SLSA 1.2 — Specification
- Sigstore — Verifying signatures
- Microsoft — Service Bus managed identities

Dokumentacja sprawdzona: 26.09.2026. Dane przypadków: przykłady dydaktyczne.