

Poradnik wdrażania wymiany sygnałów bezpieczeństwa i ciągłej oceny dostępu

Rublon sp. z o.o.
ul. Stanisława Wyspiańskiego 11
65-036 Zielona Góra
NIP: 9730702133, KRS: 3011

www.rublon.pl

Firma Rublon sp. z o.o., NIP: 9730702133, KRS: 3011 (dalej Partner PWCyber), udziela Ministerstwu Cyfryzacji zgody na wykorzystanie i publikację materiałów przekazanych w ramach Programu PWCyber (zwanych dalej „Materiałami"), w szczególności: tekstów, grafik, diagramów, infografik, prezentacji oraz innych treści edukacyjnych.
Partner oświadcza, że materiały nie naruszają praw osób trzecich.

Spis treści

Spis ilustracji **5**

Spis tabel **6**

1. Wprowadzenie **7**

1.1. Cel poradnika 7

1.2. Dla kogo jest ten poradnik? 8

1.3. Główne wyzwanie: brak propagacji informacji o ryzyku 8

2. Czym są Shared Signals, SSF i CAEP? **9**

2.1. Shared Signals 9

2.2. OpenID Shared Signals Framework 10

2.3. CAEP jako profil ciągłej oceny dostępu 11

2.4. RISC jako profil pokrewny 12

3. Dlaczego temat wymiany sygnałów bezpieczeństwa jest ważny? **13**

3.1. Rozproszone środowiska IT 13

3.2. Problem „martwego czasu” między wykryciem a reakcją 14

3.3. Związek z podejściem Zero Trust 15

3.4. Tradycyjny model dostępu a model z CAEP 16

4. Podstawowe pojęcia **17**

4.1. Transmitter, Receiver i Subject 17

4.2. Security Event Token 17

4.3. Event Stream 18

4.4. Push i polling 18

5. Jakie zdarzenia może obejmować CAEP? **20**

5.1. Unieważnienie sesji 20

5.2. Zmiana deklaracji w tokenie 21

5.3. Zmiana danych uwierzytelniających 21

5.4. Zmiana poziomu pewności uwierzytelnienia 21

5.5. Zmiana zgodności urządzenia 22

5.6. Ustanowienie lub przedstawienie sesji 22
5.7. Zmiana poziomu ryzyka 23
6. Przykładowe scenariusze użycia 25
6.1. Konto użytkownika zostaje zablokowane 25
6.2. Urządzenie traci zgodność z polityką bezpieczeństwa 26
6.3. Wzrost ryzyka po stronie systemu detekcji zagrożeń 27
6.4. Zmiana ról lub przynależności do grup 28
7. Architektura referencyjna 29
7.1. Minimalny model integracji 29
7.2. Model organizacyjny dla większego środowiska 29
7.3. Separacja odpowiedzialności 31
8. Dobre praktyki wdrożeniowe 32
8.1. Zacznij od jednego problemu 32
8.2. Zdefiniuj właścicieli zdarzeń i reakcji 32
8.3. Mapuj zdarzenia na konkretne reakcje 33
8.4. Projektuj reakcje proporcjonalnie do ryzyka 34
8.5. Monitoruj opóźnienia i błędy dostarczania 35
9. Bezpieczeństwo i prywatność 37
9.1. Zaufanie między systemami 37
9.2. Minimalizacja danych 37
9.3. Ochrona poufności sygnałów i ryzyko wycieku kontekstu 38
9.4. Audyt i rozliczalność 38
10. Plan wdrożenia krok po kroku 39
10.1. Inwentaryzacja systemów 39
10.2. Wybór pierwszego scenariusza 40
10.3. Projekt mapowania zdarzeń 41
10.4. Testy techniczne 42
10.5. Pilotaż i rozszerzanie zakresu 43

10.6 Utrzymanie i doskonalenie wymiany sygnałów 44

11. Lista kontrolna dla administratora 44

12. Najczęstsze błędy przy wdrażaniu Shared Signals i CAEP 46

12.1. Brak wspólnej identyfikacji podmiotów 46

12.2. Odbiór zdarzeń bez lokalnej polityki reakcji 46

12.3. Zbyt ogólne traktowanie poziomu ryzyka 47

12.4. Ignorowanie aktywnych sesji 47

12.5. Brak kontroli nad strumieniami zdarzeń 47

12.6. Brak testów zachowania przy błędach 47

12.7. Zbyt szeroki zakres pierwszego wdrożenia 48

13. Podsumowanie 48

Załącznik A. Słownik pojęć 49

Załącznik B. Przykładowa macierz wdrożeniowa 53

Załącznik C. Źródła i dokumenty referencyjne 55

Spis ilustracji

Rysunek 1. Ilustracja okładkowa – koncepcja „Sygnały między systemami”

Rysunek 2. Jak działa wymiana sygnałów bezpieczeństwa między systemami

Rysunek 3. „Martwy czas reakcji”

Rysunek 4. „Aktywna sesja po zmianie ryzyka”

Rysunek 5. Przykład propagacji zdarzenia: utrata zgodności urządzenia

Rysunek 6. Architektura referencyjna SSF i CAEP w organizacji publicznej

Rysunek 7. „Lista kontrolna administratora”

Spis tabel

Tabela 1. Tradycyjny model dostępu a model z CAEP

Tabela 2. Podstawowe pojęcia SSF i CAEP

Tabela 3. Typy zdarzeń CAEP i możliwe reakcje administracyjne

Tabela 4. Od zdarzenia do reakcji: przykładowa macierz decyzyjna

Tabela 5. Wybór pierwszego scenariusza Shared Signals i CAEP

Tabela 6. Lista kontrolna wdrożenia Shared Signals i CAEP

Tabela 7. Przykładowa macierz wdrożeniowa (Załącznik B)

1. Wprowadzenie

1.1. Cel poradnika

Współczesne środowiska informatyczne, określane dalej jako środowiska IT (*ang. Information Technology - IT*), składają się z wielu systemów, które odpowiadają za różne elementy bezpieczeństwa: tożsamość użytkowników, kontrolę dostępu, uwierzytelnianie, stan urządzeń, monitoring, wykrywanie zagrożeń oraz reakcję na incydenty. Każdy z tych systemów może zawierać informację istotną dla bezpieczeństwa dostępu, na przykład o użytkowniku, urządzeniu, sesji lub poziomie ryzyka.

Problem pojawia się wtedy, gdy taka informacja pozostaje zamknięta w jednym narzędziu. System wykrywający zdarzenie może wiedzieć o zmianie statusu użytkownika, incydencie lub podwyższonym ryzyku, ale pozostałe systemy nadal działają tak, jakby nic się nie zmieniło.

Niniejszy poradnik wyjaśnia, jak standardy z rodziny Shared Signals[1], w tym Continuous Access Evaluation Profile (CAEP)[2], czyli profil ciągłej oceny dostępu, mogą pomóc w przekazywaniu sygnałów bezpieczeństwa między systemami. Dokument koncentruje się na praktycznym wykorzystaniu tych standardów do skrócenia czasu między wykryciem zdarzenia a reakcją systemów odpowiedzialnych za dostęp.

W poradniku znaleźć można odpowiedzi na kluczowe pytania związane z planowaniem i wdrażaniem wymiany sygnałów bezpieczeństwa:

- Czym są Shared Signals, OpenID Shared Signals Framework (SSF)[3] i CAEP?
- Jaki problem rozwiązują w organizacji?
- Jakie zdarzenia mogą wpływać na bieżącą ocenę dostępu?
- Jak wybrać pierwszy scenariusz wdrożeniowy?
- Jak zaplanować reakcje systemów odbierających sygnały?
- Jak testować, audytować i utrzymywać wymianę sygnałów bezpieczeństwa?

Poradnik pokazuje również, jakie typy zdarzeń mogą być przekazywane między systemami oraz jak administratorzy powinni podejść do praktycznego wykorzystania tych mechanizmów w organizacji.

[1] Patrz: Załącznik A – Słownik pojęć
[2] tamże
[3] tamże

1.2. Dla kogo jest ten poradnik?

Poradnik jest przeznaczony dla osób i zespołów odpowiedzialnych za bezpieczeństwo, kontrolę dostępu oraz integrację systemów IT w administracji publicznej, sektorze prywatnym i innych organizacjach objętych wymaganiami cyberbezpieczeństwa.

W szczególności poradnik będzie przydatny dla:

- administratorów i architektów IT w administracji publicznej,
- zespołów cyberbezpieczeństwa,
- osób odpowiedzialnych za zarządzanie tożsamością i dostępem,
- dostawców IT integrujących systemy dla sektora publicznego,
- jednostek objętych wymaganiami Krajowego Systemu Cyberbezpieczeństwa[4].

1.3. Główne wyzwanie: brak propagacji informacji o ryzyku

W wielu organizacjach informacja o incydencie lub zmianie statusu użytkownika zatrzymuje się tam, gdzie została wykryta:

- System zarządzania tożsamością może wiedzieć, że konto zostało zablokowane.
- System ochrony punktów końcowych może wiedzieć, że urządzenie przestało spełniać wymagania bezpieczeństwa.
- Narzędzie monitorujące może oznaczyć aktywność użytkownika jako ryzykowną.

Wszystkie te fakty nie oznaczają jednak, że pozostałe systemy od razu wykorzystają tę informację przy podejmowaniu decyzji o dostępie, co jest szczególnie istotne w środowiskach, w których jeden użytkownik korzysta równocześnie z wielu aplikacji, usług i aktywnych sesji.

Decyzja dostępowa podjęta przy logowaniu może po kilku minutach przestać odpowiadać aktualnej sytuacji, ponieważ konto mogło zostać zablokowane, mogły zostać odebrane uprawnienia, urządzenie mogło utracić zgodność z polityką bezpieczeństwa albo mógł wzrosnąć poziom ryzyka. Mimo to część systemów nadal będzie działać tak, jakby warunki bezpieczeństwa nie uległy zmianie.

W praktyce prowadzi to do prostego, ale bardzo poważnego problemu: organizacja wie o zdarzeniu, lecz nie wszystkie systemy potrafią na nie zareagować, co kończy się następującymi nieprawidłowościami:

[4] Patrz: Załącznik A – Słownik pojęć

- Aktywna sesja w aplikacji może pozostać ważna po zablokowaniu konta.
- Użytkownik może nadal korzystać z zasobów przy użyciu urządzenia, które nie spełnia już wymagań bezpieczeństwa.
- Aplikacja biznesowa może utrzymywać dostęp na podstawie wcześniejszego tokena[5], mimo że w innym systemie odebrano użytkownikowi określone uprawnienia.

Powstaje w ten sposób luka między wykryciem zdarzenia a reakcją systemów odpowiedzialnych za dostęp. Jej długość zależy od architektury środowiska, sposobu integracji systemów, czasu odświeżania sesji oraz tego, czy administratorzy muszą wykonywać część działań ręcznie. Czas trwania tej luki działa na niekorzyść bezpieczeństwa, zwiększając ryzyko utrzymania nieautoryzowanego dostępu przez użytkownika, sesję lub urządzenie.

Standardy Shared Signals i CAEP odpowiadają właśnie na ten problem braku propagacji informacji o ryzyku. Celem jest umożliwienie przekazywania istotnych sygnałów bezpieczeństwa między systemami w ustandaryzowany sposób, tak aby informacja o zmianie ryzyka, statusu konta, sesji lub urządzenia mogła zostać wykorzystana przez inne elementy środowiska IT.

Dlaczego to ważne?

Samo wykrycie incydentu nie ogranicza dostępu, jeśli informacja nie dotrze do systemu, który ten dostęp kontroluje.

2. Czym są Shared Signals, SSF i CAEP?

2.1. Shared Signals

Shared Signals to otwarty standard, dzięki któremu systemy bezpieczeństwa i tożsamości wymieniają ustandaryzowane informacje o zdarzeniach, ryzyku i zmianach stanu. Pozwala to na błyskawiczne podjęcie właściwej decyzji: utrzymanie dostępu, jego ograniczenie, zakończenie sesji, wymuszenie ponownego uwierzytelnienia lub zapisanie zdarzenia do analizy.

[5] Patrz: Załącznik A – Słownik pojęć

Najważniejsza jest tu nie sama wymiana danych, lecz ich znaczenie operacyjne. Sygnał bezpieczeństwa powinien być zrozumiały dla systemu, który go odbiera, oraz wystarczająco precyzyjny, aby można było powiązać go z konkretnym użytkownikiem, urządzeniem, sesją, aplikacją lub innym obiektem.

Standardy z rodziny Shared Signals ograniczają asymetrię informacji między systemami. Gdy jeden komponent wykryje istotne zdarzenie, może przekazać ustandaryzowany sygnał zaufanym odbiorcom, którzy uwzględnią go zgodnie z własną polityką bezpieczeństwa.

2.2. OpenID Shared Signals Framework

Specyfikacja OpenID Shared Signals Framework Specification 1.0 opisuje techniczną strukturę wymiany sygnałów i zdarzeń między współpracującymi systemami. Specyfikacja została opracowana w ramach grupy roboczej Shared Signals organizacji OpenID Foundation[6] i umożliwia budowanie profili takich jak Risk Incident Sharing and Coordination (RISC)[7] oraz Continuous Access Evaluation Profile (CAEP).

Specyfikacja Shared Signals Framework (SSF) nie określa konkretnej aplikacji ani dostawcy technologii, tylko definiuje sposób, w jaki systemy mogą przekazywać sobie informacje o zdarzeniach bezpieczeństwa. Jest to jeden uniwersalny standard wymiany informacji, dzięki któremu organizacje nie muszą tworzyć i utrzymywać dziesiątek dedykowanych integracji między poszczególnymi systemami.

Specyfikacja SSF porusza wiele istotnych tematów:

- profile tokenów Security Event Tokens[8],
- sposób identyfikowania podmiotów zdarzeń,
- strukturę zdarzeń i typów zdarzeń,
- mechanizmy dostarczania zdarzeń,
- metadane konfiguracji nadajnika,
- zarządzanie strumieniami zdarzeń.

Dla administratora najważniejsze jest to, że SSF wprowadza rozróżnienie między systemem wysyłającym sygnał a systemem, który go odbiera. System źródłowy zdarzenia, określany po angielsku jako *Transmitter*, informuje o zmianie stanu lub

[6] Patrz: Załącznik A – Słownik pojęć
[7] tamże
[8] tamże

ryzyka. System odbierający, określany jako *Receiver*, analizuje sygnał i reaguje zgodnie z własną polityką bezpieczeństwa.

Reakcja systemu odbierającego nie musi być zawsze taka sama. Ten sam typ zdarzenia może w jednym systemie zakończyć sesję, w drugim wymusić ponowne uwierzytelnienie, a w trzecim tylko utworzyć wpis audytowy. Standard SSF porządkuje wymianę informacji, ale decyzja o reakcji pozostaje po stronie systemu odbierającego.

Rysunek 2. Jak działa wymiana sygnałów bezpieczeństwa między systemami



2.3. CAEP jako profil ciągłej oceny dostępu

OpenID Continuous Access Evaluation Profile 1.0, czyli CAEP, to profil standardu Shared Signals przeznaczony do przekazywania zdarzeń, które mogą wpływać na bieżącą ocenę dostępu.

Profil CAEP odpowiada na bardzo praktyczne pytanie: co powinno się stać, gdy po rozpoczęciu sesji zmieni się poziom ryzyka, stan urządzenia, status poświadczeń albo warunki, na podstawie których wcześniej przyznano dostęp?

W tradycyjnym modelu wiele decyzji zapada głównie przy logowaniu. Użytkownik przechodzi przez proces uwierzytelniania, otrzymuje dostęp, a aplikacja działa dalej, dopóki sesja lub token nie wygaśnie. Profil CAEP wspiera inny model: dostęp może być ponownie oceniany także w trakcie korzystania z usługi, jeżeli inny system przekaże istotny sygnał bezpieczeństwa.

Specyfikacja CAEP definiuje zestaw typów zdarzeń zgodnych ze standardem SSF. Obejmują one między innymi unieważnienie sesji, zmianę informacji w tokenie, zmianę poświadczeń, zmianę poziomu pewności uwierzytelnienia, zmianę zgodności urządzenia oraz zmianę poziomu ryzyka.

W środowisku administracji publicznej taki mechanizm ma kluczowe znaczenie na przykład wtedy, gdy konto użytkownika zostanie zablokowane, urządzenie utraci zgodność z polityką bezpieczeństwa, a system monitorowania wykryje podwyższone ryzyko. Profil CAEP nie zastępuje co prawda lokalnych reguł dostępu, ale oferuje wspólny sposób przekazywania informacji, które mogą natychmiast uruchomić adekwatną reakcję po stronie innych systemów.

Warto zapamiętać

Profil CAEP nie zastępuje polityki bezpieczeństwa. Dostarcza tylko sygnał, który system odbierający może wykorzystać zgodnie z własnymi regułami.

2.4. RISC jako profil pokrewny

Risk Incident Sharing and Coordination, czyli RISC, to profil pokrewny profilowi CAEP. Dotyczy koordynacji i udostępniania informacji o incydentach ryzyka związanych z kontem. Są to sytuacje, w których jeden dostawca lub system posiada informację o zdarzeniu dotyczącym konta i może przekazać ją innym zaufanym stronom.

Profil RISC koncentruje się przede wszystkim na zdarzeniach związanych z ryzykiem konta, takich jak podejrzenie przejęcia konta, zmiana stanu konta lub inne zdarzenia, które mogą wymagać reakcji po stronie współpracujących systemów. Jego rola jest więc bliska CAEP, ale punkt ciężkości jest inny, gdyż CAEP odnosi się szerzej do ciągłej oceny dostępu, w tym sesji, urządzeń, poziomu ryzyka i warunków, które mogą zmienić się już po zalogowaniu użytkownika.

W praktyce oba profile można traktować jako elementy tego samego kierunku rozwoju architektury bezpieczeństwa: systemy nie powinny działać w izolacji, jeśli posiadają informacje istotne dla decyzji dostępowych. Profil RISC pokazuje ten mechanizm z perspektywy incydentów ryzyka związanych z kontem, a profil CAEP rozszerza go na bieżącą ocenę dostępu do usług i aplikacji.

3. Dlaczego temat wymiany sygnałów bezpieczeństwa jest ważny?

3.1. Rozproszone środowiska IT

Środowiska IT w administracji publicznej, sektorze prywatnym i organizacjach objętych wymaganiami cyberbezpieczeństwa rzadko składają się z jednego spójnego systemu. Najczęściej jest to zestaw wielu rozwiązań wdrażanych w różnym czasie, przez różnych dostawców i dla różnych potrzeb organizacyjnych. Obok systemów dziedzinowych lub biznesowych działają usługi katalogowe, poczta elektroniczna, aplikacje webowe, dostęp przez wirtualną sieć prywatną (VPN, ang. *Virtual Private Network)* oraz systemy zarządzania tożsamością.

Działają tam również narzędzia do wykrywania zagrożeń i reagowania na nie na punktach końcowych (EDR, ang. *Endpoint Detection and Response*), rozwiązania rozszerzonej detekcji i reakcji (XDR, ang. *Extended Detection and Response*) oraz systemy zarządzania urządzeniami mobilnymi (MDM, ang. *Mobile Device Management*). Środowisko uzupełniają rozwiązania klasy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM, ang. *Security Information and Event Management*) oraz orkiestracji, automatyzacji i reagowania na zdarzenia bezpieczeństwa (SOAR, ang. *Security Orchestration*, *Automation and Response*).

Każde z tych narzędzi ma własną rolę. Jedno odpowiada za tożsamość użytkownika, inne za stan urządzenia, kolejne za wykrywanie anomalii, a jeszcze inne za logowanie zdarzeń lub automatyzację reakcji. Problem nie polega więc na braku danych. Często jest odwrotnie: dane istnieją, ale są rozproszone i nie zawsze trafiają tam, gdzie mogłyby realnie wpłynąć na bezpieczeństwo dostępu.

Ma to szczególne znaczenie w organizacjach, których systemy obsługują procesy krytyczne, usługi publiczne, dane wrażliwe lub zadania istotne dla ciągłości działania. Dostęp do takich systemów powinien zależeć nie tylko od tego, czy użytkownik poprawnie zalogował się, ale również od tego, czy w trakcie pracy nie zmieniły się warunki bezpieczeństwa. Dotyczy to zarówno konta użytkownika, jak i urządzenia, sesji, lokalizacji, poziomu ryzyka oraz przyznanych uprawnień.

Administratorzy często muszą łączyć ze sobą rozwiązania o różnym wieku, różnej architekturze i różnym poziomie gotowości do integracji. Otwarte standardy wymiany sygnałów bezpieczeństwa są w takim środowisku szczególnie wartościowe, ponieważ pozwalają ograniczyć zależność od zamkniętych integracji tworzonych osobno dla każdej pary systemów.

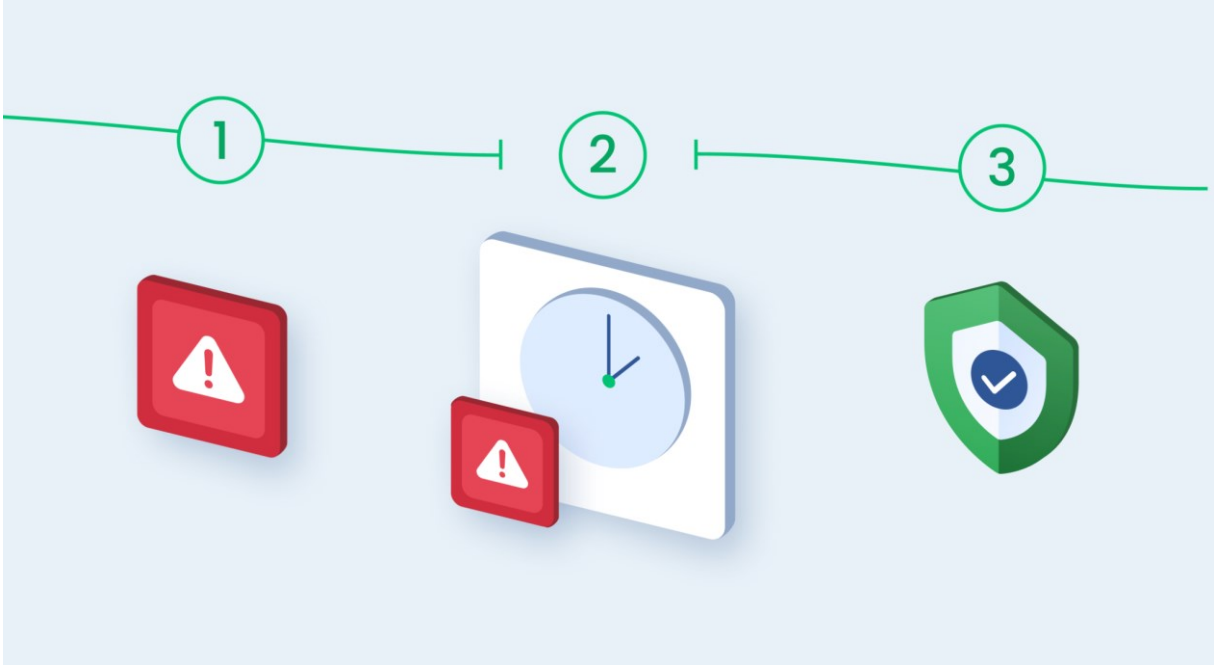
3.2. Problem „martwego czasu” między wykryciem a reakcją

W bezpieczeństwie dostępu liczy się nie tylko to, czy zdarzenie zostanie wykryte, ale również to, jak szybko inne systemy będą mogły na nie zareagować. Czas, jaki upływa od zidentyfikowania zagrożenia do faktycznego zablokowania dostępu, ma tu krytyczne znaczenie. W tym czasie użytkownik, sesja lub urządzenie mogą nadal korzystać z zasobów, mimo że warunki bezpieczeństwa uległy zmianie.

Ten okres można nazwać martwym czasem reakcji. Nie zawsze jest to awaria czy błąd pojedynczego systemu. Często wynika to po prostu z architektury: jeden system wykrywa zmianę, ale pozostałe dowiadują się o niej dopiero po odświeżeniu danych, wygaśnięciu tokena, zakończeniu sesji albo ręcznej interwencji administratora.

Najbardziej widoczne jest to w przypadku aktywnych sesji. Użytkownik może być już zalogowany do aplikacji, panelu administracyjnego, usługi pocztowej albo systemu dziedzinowego. Jeżeli po rozpoczęciu sesji pojawi się informacja o podwyższonym ryzyku, samo zablokowanie kolejnych logowań może nie wystarczyć. Istotne jest również to, czy systemy potrafią ocenić istniejący dostęp na nowo.

Rysunek 3. „Martwy czas reakcji”



Podobny problem dotyczy zmian organizacyjnych. Odebranie uprawnień, zmiana roli, wyłączenie konta lub utrata zgodności urządzenia z polityką bezpieczeństwa powinny możliwie szybko wpływać na decyzje dostępowe. Bez sprawnego przekazywania sygnałów część środowiska może przez pewien czas działać według poprzedniego stanu.

Dla administratora oznacza to konieczność myślenia o reakcji nie tylko w kategoriach logowania. Coraz ważniejsze staje się pytanie, co dzieje się po zalogowaniu: jak długo ważna jest sesja, kiedy aplikacja odświeża informacje o użytkowniku, czy potrafi przyjąć sygnał o zmianie ryzyka i czy ma jasno określoną reakcję na takie zdarzenie.

Shared Signals i CAEP warto rozważyć szczególnie wtedy, gdy:

- aktywne sesje pozostają ważne mimo zablokowania konta,
- zmiany ról lub grup nie są szybko widoczne w aplikacjach,
- system zarządzania urządzeniami zna status urządzenia, ale aplikacje go nie uwzględniają,
- system detekcji zagrożeń podnosi poziom ryzyka, ale nie wpływa to na dostęp,
- administratorzy muszą ręcznie ustalać, które systemy powinny zareagować po incydencie.

3.3. Związek z podejściem Zero Trust

Standardy Shared Signals i CAEP dobrze wpisują się w podejście Zero Trust[9], ale nie należy traktować ich jako hasła marketingowego. Ich znaczenie jest bardziej konkretne: pomagają budować środowisko, w którym decyzja o dostępie nie jest jednorazowym zdarzeniem podejmowanym wyłącznie przy logowaniu.

W modelu Zero Trust dostęp powinien zależeć od aktualnego kontekstu. Znaczenie mają tożsamość użytkownika, stan urządzenia, poziom ryzyka, rodzaj zasobu, siła uwierzytelnienia oraz inne warunki określone w politykach bezpieczeństwa. Jeżeli któryś z tych elementów zmieni się w trakcie sesji, systemy powinny mieć możliwość uwzględnienia tej zmiany.

Standardy SSF i CAEP wspierają właśnie taki model pracy. Umożliwiają przekazywanie sygnałów, które mogą doprowadzić do ponownej oceny dostępu już po rozpoczęciu sesji. Nie oznacza to, że każda zmiana musi automatycznie kończyć dostęp. W zależności od polityki organizacji reakcją może być zakończenie sesji, wymuszenie ponownego uwierzytelnienia, dodatkowa weryfikacja, ograniczenie zakresu dostępu albo utworzenie zdarzenia do dalszej analizy.

W organizacjach o rozproszonym środowisku IT takie podejście ma praktyczne znaczenie, ponieważ pozwala lepiej powiązać decyzje dostępowe z bieżącym stanem bezpieczeństwa. Nie zastępuje ono istniejących mechanizmów ochrony, takich jak

[9] Patrz: Załącznik A – Słownik pojęć

uwierzytelnianie wieloskładnikowe (MFA, ang. *Multi-Factor Authentication*), zarządzanie urządzeniami, monitoring czy obsługa incydentów. Może jednak sprawić, że informacje z tych mechanizmów szybciej trafią do systemów, które faktycznie kontrolują dostęp do zasobów.

> Największą wartością Shared Signals i CAEP jest uporządkowanie komunikacji między systemami, które dotąd często działały osobno: tożsamością, kontrolą dostępu, zarządzaniem urządzeniami, detekcją zagrożeń i aplikacjami. Standard nie narzuca jednej reakcji, tylko daje wspólny język do przekazywania zdarzeń. Dzięki temu architekt może projektować środowisko, w którym decyzja dostępowa nie kończy się w momencie logowania.

3.4. Tradycyjny model dostępu a model z CAEP

Tabela 1. Tradycyjny model dostępu a model z CAEP

Aspekt	Tradycyjny model dostępu	Model z CAEP
Moment oceny dostępu	Głównie przy logowaniu.	Także po rozpoczęciu sesji, gdy zmieni się kontekst bezpieczeństwa.
Reakcja na zmianę ryzyka	Często po wygaśnięciu sesji, odświeżeniu danych albo ręcznej interwencji.	Po odebraniu sygnału od innego systemu.
Aktywne sesje	Mogą pozostać ważne mimo zmiany statusu konta, urządzenia lub poziomu ryzyka.	Mogą zostać ponownie ocenione przez system odbierający sygnał.
Integracja systemów	Często punktowa i zależna od konkretnej pary systemów.	Oparta na wspólnym standardzie wymiany zdarzeń.
Audyt reakcji	Zależny od lokalnych logów poszczególnych systemów.	Może obejmować wysłanie zdarzenia, odbiór, walidację i wykonaną reakcję.

4. Podstawowe pojęcia

4.1. Transmitter, Receiver i Subject

W specyfikacji SSF pojawiają się trzy pojęcia, które warto znać przed omówieniem konkretnych scenariuszy: Transmitter, Receiver i Subject. Te pojęcia opisują podstawowy układ wymiany sygnałów bezpieczeństwa.

Transmitter to system, który wysyła zdarzenie. Może to być na przykład system zarządzania tożsamością, narzędzie oceniające stan urządzeń albo system wykrywania zagrożeń. Jego zadaniem jest przekazanie informacji o zdarzeniu do innego zaufanego systemu.

Receiver to system, który odbiera zdarzenie. Po odebraniu sygnału może podjąć akcję zgodną z własną polityką bezpieczeństwa. Nie każda reakcja musi być natychmiastowa i nie każda musi oznaczać zablokowanie dostępu. Czasem właściwą reakcją będzie zakończenie sesji, czasem ponowne uwierzytelnienie, a czasem tylko zapis do audytu.

Subject to obiekt, którego dotyczy zdarzenie. Najczęściej będzie to użytkownik, ale nie zawsze. Subject może oznaczać także urządzenie, sesję, aplikację, grupę, tenant[10], jednostkę organizacyjną albo inny obiekt rozpoznawany przez systemy biorące udział w wymianie sygnałów.

Fundamentem całego procesu jest jednoznaczne określenie obiektu zdarzenia (*Subject*). System docelowy musi dokładnie wiedzieć, jakiego użytkownika, jakiej sesji lub jakiego urządzenia dotyczy otrzymany sygnał. W przeciwnym razie nie będzie w stanie adekwatnie zareagować, odciąć dostępu we właściwym miejscu ani podjąć akcji naprawczej.

4.2. Security Event Token

Security Event Token, często zapisywany skrótem SET, to ustandaryzowany sposób przekazywania informacji o zdarzeniu bezpieczeństwa. Zamiast wysyłać dowolnie zbudowany komunikat, system źródłowy przekazuje zdarzenie w formacie, który może zostać obsłużony przez system odbierający.

Dla administratora najważniejsze jest to, że SET przenosi informację o tym, co się wydarzyło, jakiego podmiotu dotyczy zdarzenie i kto je wysłał. Dzięki temu odbiorca

[10] Patrz: Załącznik A – Słownik pojęć

może sprawdzić, czy sygnał pochodzi z zaufanego źródła oraz czy powinien uruchomić określoną reakcję.

Istotne są również podpis i walidacja tokena. System odbierający nie powinien ufać sygnałowi tylko dlatego, że został dostarczony na właściwy adres. Musi mieć możliwość potwierdzenia, że zdarzenie pochodzi od uprawnionego nadawcy i nie zostało zmienione po drodze. W środowiskach, w których sygnały mogą wpływać na dostęp do systemów, jest to warunek podstawowy.

4.3. Event Stream

Event Stream to strumień zdarzeń między systemem wysyłającym a systemem odbierającym. Można go rozumieć jako uzgodniony kanał wymiany określonych typów sygnałów bezpieczeństwa.

Strumień nie oznacza, że każdy system wysyła wszystko do wszystkich. W dobrze zaprojektowanej integracji wiadomo, jakie typy zdarzeń są przekazywane, kto jest ich nadawcą, kto jest odbiorcą i czego dotyczy dana wymiana. Przykładowo, jeden strumień może służyć do przekazywania informacji o unieważnieniu sesji, a inny do zdarzeń związanych ze zmianą poziomu ryzyka.

Takie uporządkowanie ma znaczenie operacyjne. Administratorzy mogą łatwiej określić, które systemy współpracują ze sobą, jakie zdarzenia są obsługiwane i jakiego rodzaju reakcji należy oczekiwać po stronie odbiorcy. Strumień zdarzeń staje się więc zarówno elementem technicznym, jak i częścią modelu odpowiedzialności między systemami.

4.4. Push i polling

Standard SSF przewiduje dwa podstawowe sposoby dostarczania zdarzeń: **push** oraz **polling**. Oba modele służą temu samemu celowi, czyli przekazaniu tokenów Security Event Tokens między systemami, ale różnią się sposobem inicjowania komunikacji.

W modelu **push** system wysyłający przekazuje zdarzenie bezpośrednio do systemu odbierającego. Ten sposób jest stosowany tam, gdzie ważna jest szybka reakcja. Jeżeli zmiana ryzyka powinna możliwie szybko wpłynąć na aktywną sesję, model push powinien sprawdzić się najlepiej.

W modelu **polling** system odbierający okresowo sprawdza, czy są dostępne nowe zdarzenia. Takie podejście może być prostsze do wdrożenia w środowiskach, w których system odbierający nie potrafi łatwo wystawić punktu odbioru zdarzeń albo komunikacja przychodząca jest ograniczona przez architekturę sieci.

Wybór modelu zależy od wymagań organizacji, rodzaju zdarzeń i możliwości technicznych systemów. Dla zdarzeń wymagających szybkiej reakcji większe znaczenie będzie miał czas dostarczenia. Dla zdarzeń mniej krytycznych wystarczające powinno być okresowe pobieranie informacji.

Tabela 2. Podstawowe pojęcia SSF i CAEP

Pojęcie	Znaczenie	Przykład w środowisku administracji publicznej
Transmitter	System, który wysyła zdarzenie bezpieczeństwa do innego systemu.	System zarządzania tożsamością wysyła informację o zablokowaniu konta użytkownika.
Receiver	System, który odbiera zdarzenie i może wykonać reakcję zgodną z własną polityką bezpieczeństwa.	Aplikacja administracyjna odbiera sygnał i wymusza ponowne uwierzytelnienie użytkownika.
Subject	Użytkownik, urządzenie, sesja, aplikacja, grupa, tenant lub inny obiekt, którego dotyczy zdarzenie.	Zdarzenie dotyczy konkretnego użytkownika urzędu albo urządzenia, z którego uzyskano dostęp.
Security Event Token	Ustandaryzowany token zawierający informację o zdarzeniu bezpieczeństwa.	System wykrywania zagrożeń wysyła token informujący o podwyższonym poziomie ryzyka.
Event Stream	Uzgodniony strumień zdarzeń między systemem wysyłającym a systemem odbierającym.	Strumień służy do przekazywania zdarzeń o unieważnieniu sesji do aplikacji krytycznych.
Push	Model, w którym nadawca wysyła zdarzenie do odbiorcy.	System tożsamości natychmiast przekazuje informację o zablokowaniu konta do systemów odbierających.
Polling	Model, w którym odbiorca okresowo pobiera dostępne zdarzenia.	Aplikacja cyklicznie sprawdza, czy pojawiły się nowe sygnały dotyczące użytkowników lub sesji.

5. Jakie zdarzenia może obejmować CAEP?

Specyfikacja OpenID Continuous Access Evaluation Profile 1.0 definiuje typy zdarzeń, które mogą być przekazywane między współpracującymi systemami w celu bieżącej oceny dostępu. W przeciwieństwie do zwykłych logów, które służą głównie do zapisu historii, sygnały CAEP wymuszają działanie. Każdy z nich dostarcza odbiorcy informacje niezbędne do podjęcia natychmiastowej decyzji o utrzymaniu, ograniczeniu lub zablokowaniu dostępu dla danej sesji, użytkownika lub urządzenia.

Profil CAEP 1.0 obejmuje między innymi takie typy zdarzeń:

- Session Revoked (unieważnienie sesji)
- Token Claims Change (zmiana deklaracji w tokenie)
- Credential Change (zmiana danych uwierzytelniających)
- Assurance Level Change (zmiana poziomu pewności uwierzytelnienia)
- Device Compliance Change (zmiana zgodności urządzenia)
- Session Established & Session Presented (ustanowienie i przedstawienie sesji)
- Risk Level Change (zmiana poziomu ryzyka)

5.1. Unieważnienie sesji

Unieważnienie sesji oznacza, że system źródłowy informuje odbiorcę, iż określona sesja nie powinna być już traktowana jako ważna. Może chodzić o sesję konkretnego użytkownika, sesję powiązaną z danym urządzeniem albo szerszy zestaw sesji spełniających określone warunki.

Taki sygnał ma duże znaczenie wtedy, gdy samo zablokowanie kolejnego logowania nie wystarcza. Użytkownik może być już zalogowany do aplikacji, panelu administracyjnego lub usługi wewnętrznej. Jeżeli pojawi się powód do cofnięcia dostępu, odbiorca sygnału może zakończyć sesję, wymusić ponowne uwierzytelnienie albo ograniczyć dostęp do wybranych funkcji.

Przykładowym źródłem zdarzenia może być system zarządzania tożsamością, który wykrył konieczność odwołania sesji. Odbiorcą może być aplikacja biznesowa, usługa webowa albo system dostępu, który utrzymuje własną sesję użytkownika.

5.2. Zmiana deklaracji w tokenie

Zmiana deklaracji w tokenie dotyczy sytuacji, w której zmieniają się informacje używane do podejmowania decyzji o dostępie. Mogą to być atrybuty użytkownika, role, przynależność do grup, poziom uprawnień lub wszelkie inne parametry (tzw. *claims*) zaszyte w tokenie.

Zmiana deklaracji w tokenie to ważny typ zdarzenia, ponieważ wiele aplikacji opiera decyzje autoryzacyjne na wcześniej otrzymanych informacjach. Jeżeli użytkownik stracił rolę, zmienił jednostkę organizacyjną albo został usunięty z grupy dającej dostęp do określonego zasobu, aplikacja nie powinna bez końca działać na podstawie starego tokena.

Odbiorca zdarzenia może ponownie ocenić uprawnienia użytkownika, odświeżyć dane o jego dostępie, ograniczyć widoczne funkcje albo wymusić ponowne logowanie. W bardziej wrażliwych systemach taka zmiana może być także powodem do zakończenia aktywnej sesji.

5.3. Zmiana danych uwierzytelniających

Zmiana danych uwierzytelniających obejmuje zdarzenia związane z hasłem, kluczem, metodą uwierzytelniania albo innym elementem poświadczeń. Nie każda taka zmiana oznacza incydent, ale każda może mieć znaczenie dla oceny aktywnego dostępu.

Przykłady zmian danych uwierzytelniających to: reset hasła po zgłoszeniu użytkownika, zmiana metody uwierzytelniania, usunięcie starego klucza bezpieczeństwa albo dodanie nowego składnika uwierzytelniania. Jeżeli taka zmiana następuje w trakcie aktywnych sesji, część systemów może chcieć sprawdzić, czy te sesje powinny pozostać ważne.

Reakcja zależy od polityki organizacji. W jednym przypadku wystarczy zapis audytowy. W innym przypadku odbiorca wymusi ponowne uwierzytelnienie, zwłaszcza gdy zmiana poświadczeń wynika z podejrzenia przejęcia konta albo działań administratora po incydencie.

5.4. Zmiana poziomu pewności uwierzytelnienia

Poziom pewności uwierzytelnienia określa, jak silne uwierzytelnienie zostało zastosowane w danej sesji. Zdarzenie *Assurance Level Change* informuje, że od początkowego logowania zmieniła się metoda uwierzytelnienia, na przykład z jednoskładnikowej na silniejszą metodę wieloskładnikową albo odwrotnie.

Sygnał *Assurance Level Change* jest wysyłany, gdy to zaufanie rośnie (np. po pomyślnym uwierzytelnieniu wieloskładnikowym) lub nagle spada (np. z powodu zmiany ryzyka).

Dzięki temu mechanizmowi system odbierający może natychmiastowo i adekwatnie zareagować. Zamiast całkowicie odcinać użytkownika, można pozostawić mu dostęp do zwykłych funkcji, blokując jedynie operacje krytyczne (jak eksport danych czy modyfikacja uprawnień administracyjnych) do momentu ponownej weryfikacji tożsamości.

5.5. Zmiana zgodności urządzenia

Zdarzenie *Device Compliance Change* dotyczy zmiany statusu urządzenia. Urządzenie może przestać spełniać wymagania bezpieczeństwa, zostać uznane za zagrożone, utracić zarządzanie albo przestać odpowiadać polityce organizacji.

Dla sektora publicznego jest to szczególnie istotne w środowiskach, w których dostęp do systemów zależy nie tylko od tożsamości użytkownika, ale również od stanu urządzenia. Ten sam użytkownik może być uprawniony do pracy z danym systemem, ale niekoniecznie z każdego komputera, telefonu czy tabletu.

Jeżeli system zarządzania urządzeniami wykryje utratę zgodności, odbiorcy sygnału mogą ograniczyć dostęp z tego urządzenia, wymusić dodatkową weryfikację, zablokować dostęp do wybranych aplikacji albo przekazać zdarzenie do dalszej analizy. Nie musi to oznaczać natychmiastowego odcięcia użytkownika od wszystkich zasobów, ale powinno wpływać na ocenę ryzyka.

5.6. Ustanowienie lub przedstawienie sesji

Profil CAEP obejmuje także zdarzenia związane z ustanowieniem lub przedstawieniem sesji. Zdarzenie *Session Established* oznacza, że sesja została utworzona. Z kolei zdarzenie *Session Presented* oznacza, że sesja została przedstawiona systemowi, na przykład przy próbie dostępu do usługi.

Choć zdarzenia te nie stanowią bezpośredniego zagrożenia, są niezwykle cennym źródłem danych do audytu, korelacji logów i analizy behawioralnej. Informacje o czasie i źródle nawiązania sesji pozwalają skutecznie śledzić i powiązać aktywność użytkownika w różnych, niezależnych od siebie systemach.

W środowisku administracji publicznej ułatwia to analizę nietypowej aktywności na koncie, wykrywanie równoległych sesji z podejrzanych lokalizacji oraz weryfikację poprawności samego procesu uwierzytelnienia. Skorelowanie tych informacji z innymi sygnałami pozwala na znacznie szybsze i bardziej precyzyjne rozpoznanie anomalii.

5.7. Zmiana poziomu ryzyka

Zdarzenie *Risk Level Change* informuje, że zmienił się poziom ryzyka powiązany z użytkownikiem, urządzeniem, sesją lub aplikacją. Źródłem takiej informacji może być system analizujący zachowanie użytkowników, narzędzie wykrywania zagrożeń, system zarządzania tożsamością albo inny komponent bezpieczeństwa.

Zmiana poziomu ryzyka nie musi od razu oznaczać naruszenia bezpieczeństwa. Może jednak wskazywać, że bieżący dostęp powinien zostać oceniony ostrożniej. Przykładem jest nietypowe zachowanie użytkownika, dostęp z nowego urządzenia, próba wykonania operacji wykraczającej poza normalny profil pracy albo korelacja kilku sygnałów ostrzegawczych.

Odbiorca może zareagować na kilka sposobów. Może wymusić dodatkowe uwierzytelnienie, ograniczyć dostęp do funkcji administracyjnych, zakończyć sesję, podnieść poziom monitorowania albo przekazać zdarzenie do systemu obsługi incydentów. Najważniejsze jest to, aby poziom ryzyka nie pozostawał informacją dostępną wyłącznie w jednym narzędziu.

Tabela 3. Typy zdarzeń CAEP i możliwe reakcje administracyjne

Typ zdarzenia	Co oznacza	Przykładowy system źródłowy	Przykładowy system odbierający	Możliwa reakcja
Session Revoked	Sesja została unieważniona lub nie powinna być dalej akceptowana.	System zarządzania tożsamością	Aplikacja administracyjna	Zakończenie sesji albo wymuszenie ponownego logowania.
Token Claims Change	Zmieniły się informacje w tokenie, które mogą wpływać na dostęp.	System katalogowy lub system zarządzania tożsamością	Aplikacja biznesowa	Ponowna ocena uprawnień użytkownika.

Typ zdarzenia	Co oznacza	Przykładowy system źródłowy	Przykładowy system odbierający	Możliwa reakcja
Credential Change	Zmieniono hasło, klucz, metodę uwierzytelniania albo inny element poświadczeń.	System tożsamości	Usługa webowa lub system dostępu	Ponowne uwierzytelnienie albo zapis zdarzenia do audytu.
Assurance Level Change	Zmienił się poziom pewności uwierzytelnienia.	System uwierzytelniania	Aplikacja wymagająca silnej weryfikacji	Wymuszenie dodatkowej weryfikacji przed operacją wrażliwą.
Device Compliance Change	Zmienił się status zgodności urządzenia z polityką bezpieczeństwa.	System zarządzania urządzeniami	System dostępu do aplikacji	Ograniczenie dostępu z danego urządzenia.
Session Established	Sesja została ustanowiona.	System uwierzytelniania	System audytu lub korelacji zdarzeń	Zapis informacji o rozpoczęciu sesji.
Session Presented	Sesja została przedstawiona przy dostępie do usługi.	Aplikacja lub system dostępu	System monitorowania bezpieczeństwa	Korelacja użycia sesji z innymi zdarzeniami.
Risk Level Change	Zmienił się poziom ryzyka użytkownika, urządzenia, sesji lub aplikacji.	System wykrywania zagrożeń	Aplikacja krytyczna lub system dostępu	Dodatkowe uwierzytelnienie, ograniczenie dostępu albo eskalacja alertu.

6. Przykładowe scenariusze użycia

6.1. Konto użytkownika zostaje zablokowane

Jednym z najbardziej oczywistych scenariuszy jest zablokowanie konta użytkownika. Może to być działanie administratora, reakcja na odejście pracownika, wynik procedury po incydencie albo automatyczna decyzja systemu, który wykrył podejrzenie przejęcia konta.

Bez wymiany sygnałów bezpieczeństwa taka zmiana nie zawsze od razu wpływa na wszystkie aktywne sesje. Konto może być już zablokowane w systemie tożsamości, ale użytkownik nadal korzysta z aplikacji, do których zalogował się wcześniej. Część systemów dowie się o zmianie dopiero po wygaśnięciu sesji, odświeżeniu tokena albo ręcznej interwencji.

W modelu opartym na SSF i CAEP system tożsamości może wysłać zdarzenie do aplikacji i usług, które utrzymują sesje użytkownika. Odbiorcy sygnału mogą zakończyć aktywne sesje, wymusić ponowne uwierzytelnienie lub ograniczyć dostęp do czasu ponownej oceny sytuacji.

Typowy przebieg wygląda następująco:

1. Administrator blokuje konto lub system wykrywa podejrzenie przejęcia konta.
2. System tożsamości wysyła zdarzenie do zaufanych odbiorców.
3. Aplikacje i usługi odbierające kończą sesje albo wymagają ponownej weryfikacji użytkownika.

Taki scenariusz jest szczególnie ważny dla kont uprzywilejowanych, kont administracyjnych oraz użytkowników mających dostęp do systemów przetwarzających dane wrażliwe.

Rysunek 4. „Aktywna sesja po zmianie ryzyka”



6.2. Urządzenie traci zgodność z polityką bezpieczeństwa

Dostęp do systemów organizacji coraz częściej zależy nie tylko od tożsamości użytkownika, ale również od stanu urządzenia. Komputer lub telefon może być dopuszczony do pracy, dopóki spełnia wymagania polityki bezpieczeństwa, czyli ma aktualne zabezpieczenia, jest zarządzany przez organizację, nie wykazuje oznak naruszenia i korzysta z wymaganej konfiguracji.

Sytuacja zmienia się, gdy urządzenie traci zgodność, bo nie otrzymało aktualizacji, zostało wyłączone z zarządzania, utraciło wymagane zabezpieczenia albo zostało oznaczone jako potencjalnie zagrożone. Jeżeli informacja o tym fakcie pozostaje wyłącznie w systemie zarządzania urządzeniami, inne systemy nadal będą traktować dostęp z tego urządzenia jako prawidłowy.

W takim scenariuszu system zarządzania urządzeniami pełni rolę źródła sygnału. Po wykryciu braku zgodności wysyła zdarzenie do systemów, które kontrolują dostęp do aplikacji lub usług. Odbiorcy mogą ograniczyć dostęp z danego urządzenia, wymusić dodatkowe uwierzytelnienie albo dopuścić tylko mniej wrażliwe operacje.

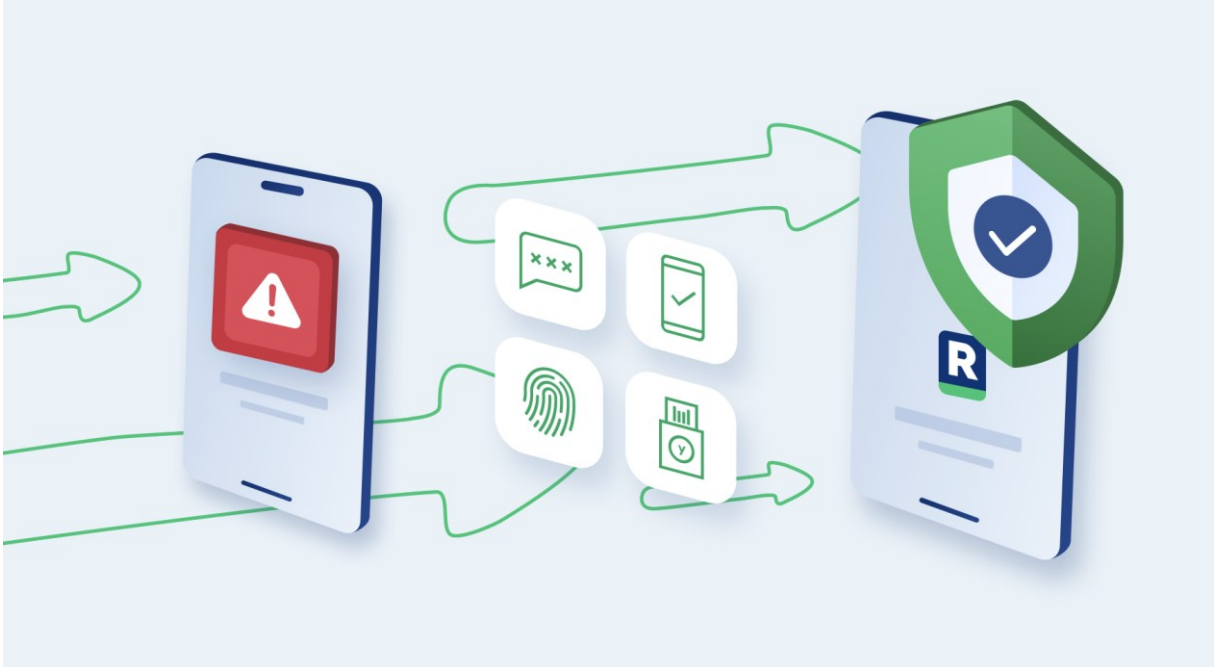
Typowy przebieg wygląda następująco:

1. System zarządzania urządzeniami wykrywa brak zgodności z polityką bezpieczeństwa.
2. Zdarzenie trafia do systemów odpowiedzialnych za kontrolę dostępu.

3. Dostęp z tego urządzenia zostaje ograniczony zgodnie z polityką organizacji.

Nie w każdym przypadku reakcją musi być całkowita blokada. Dla części organizacji właściwe będzie stopniowanie reakcji, na przykład ograniczenie dostępu do systemów krytycznych przy pozostawieniu dostępu do usług podstawowych.

Rysunek 5. Przykład propagacji zdarzenia: utrata zgodności urządzenia



6.3. Wzrost ryzyka po stronie systemu detekcji zagrożeń

Systemy bezpieczeństwa czasem wykrywają sygnały, które same w sobie nie przesądzają jeszcze o incydencie, ale wskazują na podwyższone ryzyko. Może to być nietypowa aktywność użytkownika, dostęp o nietypowej godzinie, próba wykonania operacji odbiegającej od normalnego profilu pracy albo korelacja kilku słabszych sygnałów ostrzegawczych.

Problem pojawia się wtedy, gdy informacja o wzroście ryzyka pozostaje wyłącznie w narzędziu detekcyjnym. System widzi anomalię, lecz aplikacje nadal obsługują użytkownika na dotychczasowych zasadach. W środowisku, w którym użytkownik ma aktywne sesje w kilku systemach, każde opóźnienie reakcji ma istotne znaczenie.

Dzięki profilowi CAEP informacja o zmianie poziomu ryzyka może zostać przekazana do systemów, które podejmują decyzje dostępowe. Taki mechanizm nie narzuca jednak radykalnego odcinania użytkownika. Często właściwą reakcją będzie dodatkowa weryfikacja (np. *step-up MFA*), ograniczenie dostępu do wrażliwych funkcji albo zapis zdarzenia do audytu. Przykładem praktycznego zastosowania takiego

podejścia w aplikacjach webowych jest możliwość dodania step-up MFA lub blokowania wybranych działań wysokiego ryzyka.

Typowy przebieg wygląda następująco:

1. System bezpieczeństwa wykrywa nietypowe zachowanie.
2. Informacja o podwyższonym ryzyku trafia do systemów decydujących o ostępie.
3. Systemy wymuszają step-up MFA, ograniczają dostęp albo zapisują zdarzenie do audytu.

Ten scenariusz pokazuje, że wymiana sygnałów nie musi służyć wyłącznie blokowaniu dostępu. Jej wartość polega także na tym, że pozwala dostosować reakcję do poziomu ryzyka.

6.4. Zmiana ról lub przynależności do grup

Mechanizmy autoryzacji w dużej mierze opierają się na atrybutach, rolach i przynależności do grup. To one decydują o tym, czy użytkownik ma dostęp do konkretnych funkcji, wrażliwych danych czy uprawnień administracyjnych.

Problem polega na tym, że modyfikacja tych informacji po stronie dostawcy tożsamości nie zawsze jest od razu widoczna dla aplikacji docelowej. Jeśli użytkownik zostanie usunięty z grupy, jego wciąż aktywny token sesyjny zachowa stare, zdezaktualizowane deklaracje. W efekcie aplikacja może nadal przyznawać mu nieuprawniony dostęp.

Sygnał o zmianie deklaracji w tokenie (*Token Claims Change*) pozwala ograniczyć to opóźnienie. System źródłowy może poinformować odbiorców, że dane wpływające na dostęp uległy zmianie. Dzięki temu aplikacja może szybciej ponownie ocenić uprawnienia, ograniczyć zakres dostępu lub zażądać ponownego uwierzytelnienia.

Typowy przebieg wygląda następująco:

1. Dochodzi do zmiany roli lub przynależności grupowej użytkownika.
2. System tożsamości emituje sygnał o aktualizacji kluczowych atrybutów.
3. Aplikacja natychmiast odświeża decyzję autoryzacyjną, odrzucając historyczny stan tokena.

Taki scenariusz jest krytyczny z punktu widzenia bezpieczeństwa, zwłaszcza przy zmianie stanowiska, zakończeniu współpracy (*offboarding*), transferach między działami czy operacjach na czasowych uprawnieniach administracyjnych.

7. Architektura referencyjna

7.1. Minimalny model integracji

Najprostszy model integracji SSF i CAEP powinien być możliwie wąski. Na początku nie trzeba obejmować całego środowiska, wszystkich aplikacji i wszystkich możliwych zdarzeń. Wystarczy jeden dobrze zdefiniowany przepływ, który rozwiązuje konkretny problem bezpieczeństwa.

Minimalny układ składa się z pięciu elementów:

- jednego systemu wysyłającego zdarzenie,
- jednego systemu odbierającego zdarzenie,
- jednego typu zdarzenia,
- jednego strumienia zdarzeń,
- jednej zdefiniowanej reakcji.

> **Przykład:** Integracja systemu tożsamości z aplikacją administracyjną. System tożsamości pełni rolę *Transmitter* i wysyła zdarzenie o unieważnieniu sesji. Aplikacja pełni rolę *Receiver* i po odebraniu sygnału kończy sesję użytkownika albo wymaga ponownego uwierzytelnienia.

Choć taki model jest prosty, to ma dużą wartość wdrożeniową. Pozwala sprawdzić, czy systemy poprawnie identyfikują użytkownika lub sesję, czy zdarzenie dociera do odbiorcy, czy odbiorca potrafi je zweryfikować i czy reakcja następuje zgodnie z założeniami. Dopiero po takim sprawdzeniu warto rozszerzać zakres o kolejne typy zdarzeń i kolejnych odbiorców.

Przy małej integracji pilotażowej łatwiej też ustalić odpowiedzialności. Wiadomo, który system jest źródłem informacji, który system podejmuje decyzję po odebraniu sygnału i jak administratorzy mogą sprawdzić, czy cały przepływ zadziałał poprawnie.

7.2. Model organizacyjny dla większego środowiska

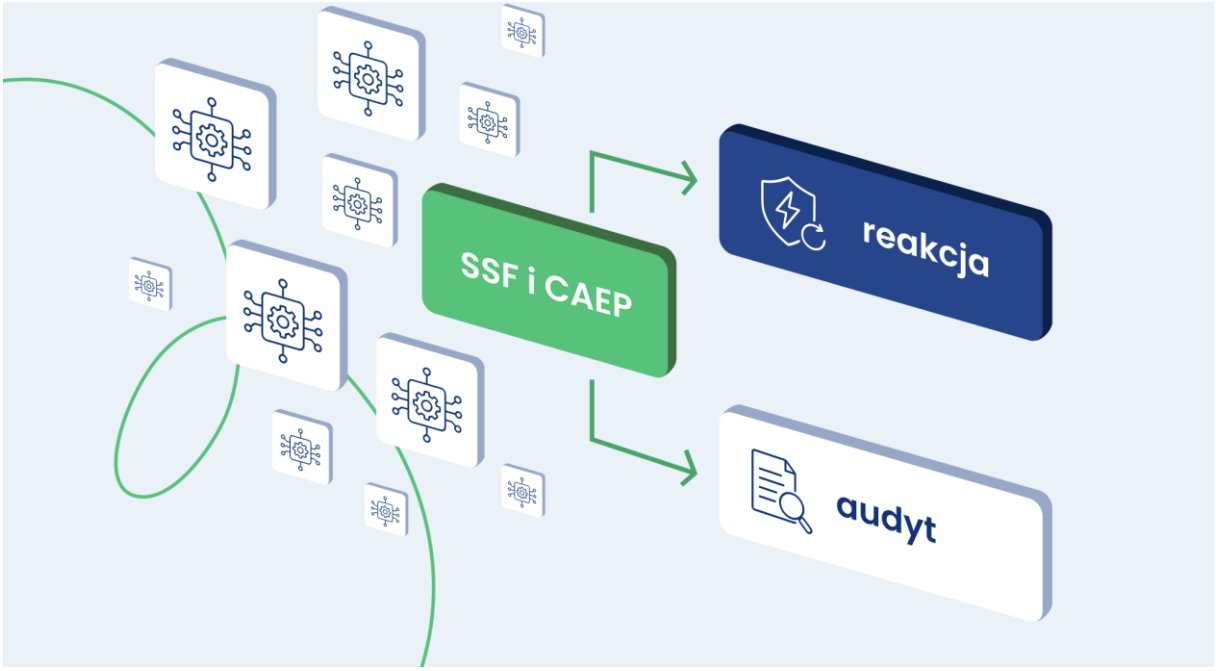
W rozbudowanych organizacjach architektura wymiany sygnałów obejmuje zazwyczaj kilka klas systemów. Nie wszystkie pełnią tę samą funkcję. Kluczowy jest jasny podział na narzędzia dostarczające informacje o ryzyku oraz na te, które egzekwują na ich podstawie kontrolę dostępu.

Typowy model opiera się na współpracy następujących elementów:

- **Dostawca tożsamości (*IdP*, *ang. Identity Provider*):** działa jako główne źródło danych o koncie, sesji, użytych metodach uwierzytelniania i modyfikacjach uprawnień.
- System zarządzania urządzeniami mobilnymi (*MDM*, *ang. Mobile Device Management*) lub ujednoliconego zarządzania punktami końcowymi (*UEM*, *ang. Unified Endpoint Management*): raportuje wszelkie naruszenia i utratę zgodności sprzętu z polityką bezpieczeństwa.
- **System detekcji zagrożeń:** Ostrzega o anomaliach i nagłych skokach poziomu ryzyka.
- **Systemy dostępu i aplikacje krytyczne:** Przechwytują powyższe sygnały i natychmiast stosują adekwatne reakcje (np. blokadę lub wymuszenie MFA).
- **SIEM i SOAR:** Stanowią warstwę audytu i korelacji. Choć nie odcinają dostępu bezpośrednio, agregują dane o wyemitowanych i odebranych zdarzeniach. Dzięki temu analitycy centrum operacji bezpieczeństwa (*SOC*, *ang. Security Operations Center*) widzą nie tylko sam incydent, ale także to, czy mechanizmy obronne faktycznie zadziałały.

W tak zaprojektowanym środowisku funkcjonują trzy niezależne strumienie danych: **przepływ decyzyjny** (wpływający bezpośrednio na dostęp użytkownika), **przepływ audytowy** (rejestrujący historię zdarzeń) oraz **przepływ operacyjny** (wykorzystywany przez analityków do obsługi incydentów).

Rysunek 6. Architektura referencyjna SSF i CAEP w organizacji publicznej



7.3. Separacja odpowiedzialności

W architekturze opartej na wymianie sygnałów bezpieczeństwa system wysyłający zdarzenie nie musi wiedzieć, jak dokładnie zareaguje każdy odbiorca. Jego zadaniem jest przekazanie wiarygodnej, poprawnie opisanej informacji. To odbiorca decyduje, co z tą informacją zrobić.

Takie rozdzielenie odpowiedzialności jest korzystne. System tożsamości może poinformować, że sesja została unieważniona, ale nie musi znać wewnętrznej logiki każdej aplikacji. Aplikacja może zakończyć sesję, wymusić ponowne uwierzytelnienie albo ograniczyć dostęp do wybranych funkcji. Decyzja zależy od charakteru systemu, rodzaju danych, poziomu ryzyka i lokalnej polityki bezpieczeństwa.

Podobnie system zarządzania urządzeniami może przekazać informację, że urządzenie utraciło zgodność. Nie musi jednak wskazywać każdej aplikacji, które przyciski ma ukryć albo które operacje zablokować. To system odbierający powinien mieć własną, jasno opisaną politykę reakcji.

Dobrze zaprojektowana architektura powinna więc odpowiadać na kilka pytań:

- które systemy mogą wysyłać zdarzenia,
- które systemy mogą je odbierać,
- jakie typy zdarzeń są obsługiwane,
- jak identyfikowany jest użytkownik, sesja lub urządzenie,

- jaka reakcja jest oczekiwana po stronie odbiorcy,
- gdzie zapisywana jest informacja o dostarczeniu i obsłudze zdarzenia.

Bez takiego podziału łatwo stworzyć integrację, która działa technicznie, ale jest trudna do utrzymania. Jeden system zaczyna zakładać zbyt wiele na temat działania drugiego, reakcje są niejednolite, a administratorom trudno ustalić, dlaczego w jednej aplikacji dostęp został odebrany, a w drugiej pozostał aktywny.

Separacja odpowiedzialności pozwala uniknąć tego problemu. *Transmitter* odpowiada za jakość i wiarygodność sygnału, a *Receiver* za jego walidację i reakcję. Warstwa monitorowania odpowiada za widoczność całego procesu. Dzięki temu wymiana sygnałów staje się częścią architektury bezpieczeństwa, a nie tylko pojedynczą integracją między dwoma systemami.

8. Dobre praktyki wdrożeniowe

8.1. Zacznij od jednego problemu

Wdrożenie wymiany sygnałów bezpieczeństwa najlepiej rozpocząć od jednego dobrze rozpoznanego problemu. Nie powinien to być projekt, który od pierwszego dnia obejmuje wszystkie systemy, wszystkie aplikacje i wszystkie możliwe typy zdarzeń. Próba zrobienia wszystkiego naraz to prosta droga do utraty kontroli nad integracją, w której każdy błąd projektowy pociąga za sobą lawinowy wzrost kosztów.

Dobrym punktem startowym jest scenariusz, którego wartość można łatwo wyjaśnić i zmierzyć. Może to być zakończenie sesji po zablokowaniu konta, reakcja na utratę zgodności urządzenia albo wymuszenie dodatkowego uwierzytelnienia po wzroście poziomu ryzyka. Ważne, aby wybrany przypadek był konkretny: wiadomo, jaki system wysyła zdarzenie, jaki system je odbiera i jaka reakcja ma nastąpić.

Taki ograniczony pilotaż pozwala sprawdzić zarówno stronę techniczną, jak i organizacyjną. Administratorzy mogą ocenić, czy zdarzenia są właściwie rozumiane, czy reakcja nie jest zbyt agresywna, czy nie blokuje pracy użytkowników bez potrzeby i czy cały przepływ można później audytować.

Dopiero po udanym wdrożeniu pierwszego scenariusza warto rozszerzać zakres. Kolejnym krokiem może być dodanie kolejnych aplikacji odbierających, innych typów zdarzeń albo kolejnych źródeł sygnałów.

8.2. Zdefiniuj właścicieli zdarzeń i reakcji

Wymiana sygnałów bezpieczeństwa wymaga jasnego podziału odpowiedzialności. Sama integracja techniczna między dwoma systemami to dopiero połowa sukcesu.

Równie ważne jest ustalenie, kto odpowiada za jakość emitowanego sygnału, jego poprawny odbiór oraz egzekwowanie adekwatnej reakcji.

Dla każdego wdrażanego scenariusza należy wyznaczyć co najmniej cztery role:

- właściciela systemu źródłowego (emitującego zdarzenie),
- właściciela systemu docelowego (odbierającego sygnał i sterującego dostępem),
- decydenta (osobę lub zespół) zatwierdzającego reguły polityki bezpieczeństwa,
- zespół odpowiedzialny za monitorowanie błędów, opóźnień i wyjątków, na przykład centrum operacji bezpieczeństwa (SOC) lub zespół operacji bezpieczeństwa (SecOps, ang. *Security Operations*).

Bez takiego podziału ryzykujemy powstanie martwych punktów, czyli sytuacji, w których alarm został wysłany, ale nikt nie potrafi jednoznacznie potwierdzić, czy został obsłużony. Największe ryzyko biznesowe pojawia się, gdy reakcja systemu docelowego odcina dostęp użytkownikowi, a zespoły nie uzgodniły wcześniej, w jakich warunkach takie działanie jest dopuszczalne.

Warto również zdefiniować procedurę zarządzania takimi regułami. Jeśli aplikacja docelowa ma automatycznie kończyć sesje, ograniczać uprawnienia lub wymuszać MFA, modyfikacja tych reguł nigdy nie powinna być zmianą *ad hoc*. Musi podlegać ścisłemu procesowi zarządzania zmianą (*Change Management*), analogicznie jak wprowadzanie kluczowych modyfikacji w zaporach sieciowych czy systemach tożsamości.

> Wdrożenie Shared Signals i CAEP wymaga dobrego przygotowania operacyjnego. Kluczowe jest nie tylko samo wysłanie zdarzenia, ale też poprawne rozpoznanie użytkownika, urządzenia lub sesji po stronie odbiorcy, walidacja sygnału, obsługa błędów i audyt wykonanej reakcji. To właśnie te szczegóły decydują, czy wymiana sygnałów realnie skróci czas między wykryciem zdarzenia a reakcją systemów.

8.3. Mapuj zdarzenia na konkretne reakcje

Każde obsługiwane zdarzenie powinno mieć przypisaną reakcję. Nie wystarczy zapisać, że system odbiera sygnał o zmianie ryzyka albo zmianie statusu urządzenia. Trzeba określić, co odbiorca ma zrobić po odebraniu takiego sygnału.

Reakcje mogą być różne w zależności od typu zdarzenia i wagi systemu. Najczęściej będą to:

- zakończenie sesji,
- wymuszenie ponownego logowania,
- wymuszenie dodatkowego składnika MFA,
- ograniczenie dostępu,
- obniżenie poziomu uprawnień,
- utworzenie alertu,
- zapis do audytu.

Mapowanie powinno być możliwie jednoznaczne. Jeżeli konto użytkownika zostaje zablokowane, aplikacja administracyjna może zakończyć aktywną sesję. Jeżeli urządzenie traci zgodność z polityką bezpieczeństwa, system dostępu może ograniczyć dostęp z tego urządzenia. Jeżeli zmienia się rola użytkownika, aplikacja może ponownie ocenić uprawnienia przed wykonaniem kolejnej operacji.

Dobrze przygotowana mapa zdarzeń i reakcji zmniejsza ryzyko niespójnego działania systemów. Administratorzy wiedzą, czego oczekiwać, a zespół bezpieczeństwa może później sprawdzić, czy reakcja faktycznie nastąpiła.

8.4. Projektuj reakcje proporcjonalnie do ryzyka

Nie każde zdarzenie powinno powodować natychmiastowe odcięcie dostępu. Zbyt agresywne reakcje mogą zakłócić pracę użytkowników, zwiększyć liczbę zgłoszeń do wsparcia i doprowadzić do obchodzenia procedur. Równocześnie zbyt łagodne reakcje nie rozwiązują problemu bezpieczeństwa.

Właściwa reakcja powinna zależeć od poziomu ryzyka, krytyczności systemu i rodzaju operacji, którą wykonuje użytkownik. W systemie zawierającym dane wrażliwe podwyższony poziom ryzyka może uzasadniać zakończenie sesji. W mniej krytycznej aplikacji wystarczające może być wymuszenie dodatkowego uwierzytelnienia albo ograniczenie dostępu do funkcji administracyjnych.

Warto odróżnić zdarzenia informacyjne od zdarzeń wymagających działania. Ustanowienie sesji jest potrzebne głównie do audytu i korelacji. Natomiast utrata zgodności urządzenia może już wymagać ograniczenia dostępu. Zablokowanie konta powinno zwykle prowadzić do bardziej zdecydowanej reakcji.

Proporcjonalność jest szczególnie ważna w sektorze publicznym, gdzie systemy IT obsługują procesy administracyjne, usługi dla obywateli i zadania wewnętrzne.

Mechanizmy bezpieczeństwa muszą chronić dostęp, ale nie powinny niepotrzebnie zatrzymywać pracy całej jednostki.

8.5. Monitoruj opóźnienia i błędy dostarczania

Korzyść z wymiany sygnałów bezpieczeństwa zależy od tego, czy zdarzenia są dostarczane szybko, poprawnie i w sposób dający się zweryfikować. Jeżeli sygnał dociera z dużym opóźnieniem, trafia do niewłaściwego odbiorcy lub nie wywołuje żadnej reakcji, cały mechanizm traci swoją wartość.

Dlatego należy monitorować nie tylko moment wykrycia zagrożenia, ale każdy kolejny etap jego przepływu. Istotne jest śledzenie całej osi czasu: wygenerowania zdarzenia, jego wysyłki, odbioru oraz ostatecznej reakcji systemu docelowego. W przypadku zdarzeń krytycznych to właśnie czas od detekcji do faktycznego odcięcia dostępu jest najważniejszą metryką.

Konieczne jest także przewidzenie scenariuszy awaryjnych. System odbierający może być chwilowo niedostępny, a samo zdarzenie może zostać odrzucone z powodu błędów walidacji. Mogą wystąpić duplikaty komunikatów albo problemy z właściwą identyfikacją użytkownika, sesji czy urządzenia. Takie sytuacje muszą być od razu widoczne na pulpitach administratorów, a nie chować się w technicznych logach pojedynczego systemu.

System monitorowania powinien obejmować co najmniej:

- liczbę wysłanych i odebranych zdarzeń,
- opóźnienia w dostarczaniu,
- błędy walidacji danych,
- błędy w identyfikacji podmiotu zdarzenia,
- konkretne reakcje wykonane po stronie odbiorcy,
- zdarzenia, które nie wyzwoliły żadnej akcji,
- przypadki wyjątkowe wymagające ręcznej interwencji.

Tabela 4. Od zdarzenia do reakcji: przykładowa macierz decyzyjna

Zdarzenie	Warunek lub kontekst	Zalecana reakcja	Priorytet	Co monitorować
Konto użytkownika zostaje zablokowane	Użytkownik ma aktywną sesję w aplikacji krytycznej.	Zakończenie sesji albo wymuszenie ponownego logowania.	Wysoki	Czas od blokady konta do zakończenia sesji.
Urządzenie traci zgodność z polityką bezpieczeństwa	Dostęp następuje z urządzenia zarządzanego wcześniej przez organizację.	Ograniczenie dostępu z tego urządzenia lub dodatkowa weryfikacja.	Wysoki	Status urządzenia, czas dostarczenia sygnału, wykonana reakcja.
Zmienia się rola użytkownika	Zmiana wpływa na dostęp do funkcji administracyjnych.	Ponowna ocena uprawnień przed kolejną operacją.	Średni	Czy aplikacja odświeżyła decyzję autoryzacyjną.
Wzrasta poziom ryzyka użytkownika	System wykrywa nietypowe zachowanie, ale nie potwierdza incydentu.	Step-up MFA, alert lub ograniczenie dostępu do operacji wrażliwych.	Średni lub wysoki	Poziom ryzyka, reakcja odbiorcy, dalsze zdarzenia powiązane.
Sesja zostaje ustanowiona	Sesja dotyczy systemu przetwarzającego dane wrażliwe.	Zapis do audytu i korelacja z innymi zdarzeniami.	Niski lub średni	Czas, źródło sesji, użytkownik, urządzenie.
Zdarzenie nie przechodzi walidacji	Odbiorca nie może potwierdzić zaufanego źródła.	Odrzucenie zdarzenia i alert administracyjny.	Wysoki	Przyczyna odrzucenia, nadawca, liczba podobnych błędów.

9. Bezpieczeństwo i prywatność

9.1. Zaufanie między systemami

Wymiana sygnałów bezpieczeństwa ma sens tylko wtedy, gdy system odbierający może ufać źródłu zdarzenia. Nie powinno się przyjmować sygnału wyłącznie dlatego, że ma poprawny format albo został dostarczony pod właściwy adres. Odbiorca musi potwierdzić, że zdarzenie pochodzi od uprawnionego nadawcy i nie zostało zmienione po wysłaniu.

Podstawowe znaczenie mają tu podpisy tokenów, konfiguracja kluczy oraz walidacja nadawcy. Jeżeli zdarzenie może prowadzić do zakończenia sesji, ograniczenia dostępu albo wymuszenia dodatkowej weryfikacji, jego autentyczność musi być sprawdzana konsekwentnie. Fałszywy lub błędnie zaakceptowany sygnał mógłby spowodować zakłócenie działania systemów albo nieuzasadnione odcięcie użytkowników od zasobów.

Istotna jest również autoryzacja strumieni zdarzeń. Nie każdy system powinien móc wysyłać każdy typ sygnału do każdego odbiorcy. Systemy powinny mieć uzgodnione, jakie zdarzenia są obsługiwane, przez kogo mogą być wysyłane i w jakim celu są odbierane. Takie ograniczenie zmniejsza ryzyko błędnej konfiguracji i ułatwia późniejszy audyt.

9.2. Minimalizacja danych

Sygnał bezpieczeństwa powinien zawierać tylko te dane, które są potrzebne do identyfikacji podmiotu i obsługi zdarzenia. Jeżeli odbiorca musi wiedzieć, którego użytkownika, urządzenia lub sesji dotyczy zdarzenie, komunikat powinien umożliwiać taką identyfikację. Nie oznacza to jednak, że należy dołączać pełny zestaw danych osobowych, opis incydentu albo informacje organizacyjne, które nie są potrzebne do wykonania reakcji.

Minimalizacja danych jest szczególnie ważna w środowiskach publicznych, gdzie systemy przetwarzają informacje dotyczące pracowników, obywateli, kontrahentów i jednostek organizacyjnych. Im więcej danych trafia do strumieni zdarzeń, tym większe znaczenie mają kontrola dostępu do tych strumieni, retencja danych i sposób ich późniejszego wykorzystania.

Warto oddzielić informację potrzebną do reakcji od informacji potrzebnej do analizy incydentu. System odbierający sygnał nie zawsze musi znać pełny kontekst zdarzenia. Czasem wystarczą stabilny identyfikator podmiotu, typ zdarzenia, czas wystąpienia

i zaufane źródło. Szczegółowa analiza może pozostać w systemie bezpieczeństwa lub w narzędziu obsługi incydentów.

9.3. Ochrona poufności sygnałów i ryzyko wycieku kontekstu

Sygnały bezpieczeństwa mogą ujawniać istotny kontekst działania organizacji, nawet jeśli nie zawierają bezpośrednich danych osobowych. Informacja o zablokowaniu konta, utracie zgodności urządzenia, unieważnieniu sesji lub podwyższonym poziomie ryzyka może mieć znaczenie nie tylko dla systemu odbierającego, ale również dla osoby próbującej rozpoznać sposób działania zabezpieczeń.

Nadmierna ekspozycja takich metadanych może ułatwić atakującemu rekonesans. Nieuprawniony dostęp do strumienia zdarzeń mógłby pokazać, które systemy wymieniają sygnały, jakie typy zdarzeń są obsługiwane, które zasoby podlegają ściślejszej kontroli oraz jak szybko organizacja reaguje na określone sytuacje. Taka wiedza może zostać wykorzystana do lepszego zaplanowania ataku oraz ominięcia wybranych mechanizmów ochronnych.

Z tego powodu strumienie sygnałów należy traktować jako element infrastruktury bezpieczeństwa, a nie zwykły kanał integracyjny. Dostęp do nich powinien być ograniczony zgodnie z zasadą najmniejszych uprawnień, monitorowany i uzasadniony rolą konkretnego systemu. Należy również kontrolować, gdzie zdarzenia są zapisywane, jak długo są przechowywane i kto może je przeglądać.

Ochrona poufności powinna być uwzględniona już na etapie projektowania integracji. Obejmuje to dobór przekazywanych danych, kontrolę dostępu do strumieni zdarzeń, zasady retencji, monitorowanie użycia oraz sposób obsługi informacji o podmiotach zdarzeń przed uruchomieniem integracji w środowisku produkcyjnym.

9.4. Audyt i rozliczalność

Wymiana sygnałów bezpieczeństwa powinna być możliwa do odtworzenia po fakcie. Jeżeli zdarzenie wpłynęło na dostęp użytkownika, administratorzy powinni móc sprawdzić, co dokładnie się stało, kiedy i w którym systemie. Dotyczy to zarówno reakcji automatycznych, jak i działań wymagających obsługi ręcznej.

Dla każdego istotnego scenariusza warto zapewnić odpowiedzi na następujące pytania:

- kto wysłał zdarzenie,
- kiedy zostało wysłane,
- czy zostało odebrane,

- jaka reakcja została wykonana,
- czy reakcja była automatyczna czy ręczna,
- jak długo trwała propagacja.

Audyt nie powinien ograniczać się do informacji, że zdarzenie istnieje. Ważny jest cały przebieg: wygenerowanie sygnału, dostarczenie, walidacja, decyzja odbiorcy i wykonana reakcja. Dopiero taki zapis pozwala ocenić, czy mechanizm działa zgodnie z polityką bezpieczeństwa.

Rozliczalność ma znaczenie także przy incydentach i reklamacjach użytkowników. Jeżeli dostęp został zakończony, ograniczony albo wymagał ponownej weryfikacji, administrator powinien móc ustalić, czy była to prawidłowa reakcja na sygnał, błąd konfiguracji, opóźnienie w dostarczeniu zdarzenia czy działanie ręczne. Bez tej widoczności wymiana sygnałów może stać się trudna do utrzymania, mimo że technicznie działa poprawnie.

> Shared Signals i CAEP pokazują, w jakim kierunku powinny rozwijać się nowoczesne architektury cyberbezpieczeństwa: od izolowanych systemów do środowisk, które potrafią wymieniać informacje o ryzyku i szybciej reagować na zmianę sytuacji. Dla administracji publicznej szczególnie ważne jest to, że mówimy o otwartych standardach, a więc o podejściu wspierającym interoperacyjność, przewidywalność i długofalowe bezpieczeństwo.

10. Plan wdrożenia krok po kroku

10.1. Inwentaryzacja systemów

Pierwszym krokiem jest ustalenie, które systemy mogą wysyłać sygnały bezpieczeństwa, a które powinny je odbierać. Warto zacząć od systemów, które już dziś mają wpływ na decyzje dostępowe albo posiadają informacje o poziomie ryzyka, stanie kont użytkowników, stanie urządzeń lub aktywnych sesjach.

Po stronie źródeł zdarzeń mogą znaleźć się między innymi:

- system zarządzania tożsamością,
- usługa katalogowa,
- system zarządzania urządzeniami,

- system wykrywania zagrożeń,
- system uwierzytelniania,
- system zarządzania uprawnieniami,
- narzędzie obsługi incydentów.

Po stronie odbiorców warto wskazać systemy, które faktycznie mogą zmienić dostęp użytkownika. Będą to na przykład aplikacje krytyczne, systemy dostępu, panele administracyjne, usługi webowe, systemy pocztowe albo rozwiązania pośredniczące w dostępie do zasobów.

Inwentaryzacja nie powinna ograniczać się do listy nazw systemów. Dla każdego z nich należy ustalić, jakie informacje posiada, czy potrafi wysłać lub odebrać zdarzenie, jakie identyfikatory użytkowników, urządzeń i sesji stosuje oraz kto odpowiada za jego konfigurację. Dopiero wtedy można ocenić, które integracje są realne, a które wymagają dodatkowych zmian organizacyjnych lub technicznych.

10.2. Wybór pierwszego scenariusza

Po inwentaryzacji należy wybrać pierwszy scenariusz wdrożeniowy. Najlepiej, aby był ważny z punktu widzenia bezpieczeństwa, ale jednocześnie możliwy do kontrolowanego przetestowania. Próba wdrożenia zbyt wielu elementów naraz drastycznie podnosi ryzyko pomyłek i utrudnia mierzalność całego projektu.

Dobry scenariusz startowy powinien spełniać kilka warunków. Musi mieć jasno określone źródło zdarzenia, znanego odbiorcę, zrozumiałą reakcję oraz możliwość sprawdzenia, czy cały przepływ zadziałał poprawnie. Powinien też dotyczyć problemu, który administratorzy już znają w swoim środowisku.

W celu wyboru scenariusza startowego warto rozważyć jeden z następujących przypadków:

- zablokowanie konta,
- unieważnienie sesji,
- utrata zgodności urządzenia,
- wzrost poziomu ryzyka,
- zmiana ról lub grup.

Każdy z tych scenariuszy ma bezpośredni związek z dostępem. Nie chodzi więc tylko o przesłanie informacji do kolejnego systemu, ale o skrócenie czasu między zmianą stanu a reakcją po stronie usług, z których korzysta użytkownik.

Tabela 5. Wybór pierwszego scenariusza Shared Signals i CAEP

Pytanie kontrolne	Dlaczego jest ważne
Czy scenariusz rozwiązuje konkretny problem bezpieczeństwa?	Pierwsze wdrożenie powinno dotyczyć realnego ryzyka, a nie abstrakcyjnej integracji systemów.
Czy znany jest system źródłowy zdarzenia?	Trzeba wiedzieć, który system wykrywa zmianę statusu, ryzyka, sesji lub urządzenia.
Czy wskazano system odbierający sygnał?	Odbiorca musi być przygotowany do walidacji zdarzenia i wykonania reakcji.
Czy typ zdarzenia jest jednoznaczny?	Scenariusz powinien odpowiadać konkretnemu typowi zdarzenia, na przykład Session Revoked, Device Compliance Change albo Risk Level Change.
Czy odbiorca potrafi rozpoznać podmiot zdarzenia?	System odbierający musi jednoznacznie powiązać sygnał z użytkownikiem, urządzeniem lub sesją.
Czy reakcja jest jasno określona?	Należy ustalić, czy odbiorca zakończy sesję, wymusi ponowne uwierzytelnienie, ograniczy dostęp albo zapisze zdarzenie do audytu.
Czy reakcja jest proporcjonalna do ryzyka?	Pierwszy scenariusz nie powinien powodować niepotrzebnych blokad ani zbyt szerokich skutków ubocznych.
Czy można łatwo sprawdzić wynik testu?	Administratorzy powinni móc potwierdzić, że zdarzenie zostało wysłane, odebrane, walidowane i obsłużone.

10.3. Projekt mapowania zdarzeń

Dla wybranego scenariusza należy przygotować mapowanie zdarzenia na reakcję. To jeden z najważniejszych elementów wdrożenia, ponieważ przekłada ogólną ideę wymiany sygnałów na konkretne działanie systemów.

Dla każdego scenariusza należy określić:

- źródło zdarzenia,
- odbiorców zdarzenia,
- typ zdarzenia,
- identyfikator podmiotu,
- oczekiwaną reakcję,
- wymagany czas reakcji,
- sposób audytu.

Szczególną uwagę trzeba poświęcić identyfikatorom. System wysyłający i system odbierający muszą jednoznacznie rozumieć, którego użytkownika, urządzenia lub sesji dotyczy zdarzenie. Jeżeli jeden system używa adresu e-mail, drugi wewnętrznego identyfikatora, a trzeci nazwy konta, konieczne może być dodatkowe mapowanie.

Oczekiwana reakcja powinna być dokładnie opisana. Zamiast ogólnego zapisu „ograniczyć dostęp" lepiej wskazać, czy system ma zakończyć sesję, wymusić ponowne logowanie, zablokować funkcje administracyjne, wymagać dodatkowego składnika MFA czy tylko zapisać zdarzenie do audytu.

Warto również określić dopuszczalny czas reakcji. Dla zdarzeń krytycznych, takich jak zablokowanie konta uprzywilejowanego, oczekiwany czas może być bardzo krótki. Dla zdarzeń informacyjnych wystarczające może być późniejsze przetworzenie i korelacja.

Uwaga administracyjna

Najtrudniejszą częścią wdrożenia często nie jest wysłanie zdarzenia, ale jednoznaczne powiązanie go z użytkownikiem, urządzeniem lub sesją po stronie odbiorcy.

10.4. Testy techniczne

Testy powinny potwierdzić, że mechanizm działa nie tylko w idealnym scenariuszu, ale również w sytuacjach granicznych. Samo wysłanie przykładowego zdarzenia nie wystarczy, jeżeli nie sprawdzono walidacji, identyfikacji podmiotu, reakcji odbiorcy i zachowania przy awarii.

Zakres testów powinien obejmować co najmniej:

- poprawność podpisu i walidacji tokena,
- poprawność identyfikacji użytkownika, urządzenia lub sesji,
- obsługę niedostępności odbiorcy,
- ponowienie dostarczenia,
- reakcję na duplikaty,
- opóźnienie od zdarzenia do reakcji.

W testach warto uwzględnić także przypadki negatywne. Odbiorca powinien odrzucić zdarzenie z niepoprawnym podpisem, zdarzenie od nieuprawnionego nadawcy albo zdarzenie dotyczące podmiotu, którego nie potrafi rozpoznać. Takie zachowanie powinno być widoczne dla administratorów, ponieważ błędy walidacji mogą wskazywać zarówno na problem konfiguracji, jak i na próbę nadużycia.

Należy też sprawdzić, czy reakcja systemu odbierającego jest zgodna z założeniami. Jeżeli zdarzenie ma zakończyć sesję, trzeba potwierdzić, że faktycznie tak się dzieje. Jeżeli reakcją jest dodatkowe uwierzytelnienie, użytkownik powinien zostać przeprowadzony przez właściwy proces w sposób zrozumiały i możliwy do odtworzenia w audycie.

10.5. Pilotaż i rozszerzanie zakresu

Pilotaż najlepiej rozpocząć w środowisku testowym albo w ograniczonym zakresie produkcyjnym. Może to być jedna aplikacja krytyczna, jedna grupa użytkowników, jeden typ zdarzenia lub jeden zespół administracyjny. Celem jest potwierdzenie, że mechanizm działa stabilnie i nie powoduje niezamierzonych blokad dostępu.

W trakcie pilotażu należy obserwować zdarzenia techniczne oraz wpływ na użytkowników i administratorów. Ważne jest, czy reakcje są zrozumiałe, czy nie pojawia się nadmierna liczba zgłoszeń, czy zespoły wiedzą, gdzie szukać informacji o wykonanej reakcji i czy da się szybko wyjaśnić przypadki sporne.

Po zakończeniu pilotażu można stopniowo rozszerzać zakres. Najbezpieczniejsza kolejność to dodawanie jednego elementu naraz: kolejnego odbiorcy, kolejnego typu zdarzenia albo kolejnej grupy użytkowników. Dzięki temu łatwiej ustalić przyczynę ewentualnych problemów.

Rozszerzanie wdrożenia powinno być prowadzone wraz z aktualizacją dokumentacji operacyjnej. Każdy nowy scenariusz powinien mieć opis źródła zdarzenia, odbiorców, oczekiwanej reakcji, zasad audytu i osób odpowiedzialnych. Bez tego mechanizm

wymiany sygnałów może z czasem stać się trudny do kontrolowania, nawet jeśli jego pierwszy etap został wdrożony poprawnie.

10.6. Utrzymanie i doskonalenie wymiany sygnałów

Po uruchomieniu pierwszych scenariuszy wymiana sygnałów bezpieczeństwa powinna zostać objęta bieżącym utrzymaniem. Administratorzy powinni okresowo przeglądać obsługiwane typy zdarzeń, reakcje systemów odbierających, błędy walidacji, niedostarczone zdarzenia oraz mapowanie identyfikatorów użytkowników, urządzeń i sesji.

Warto również sprawdzać, czy zasady retencji i dostępu do strumieni zdarzeń pozostają aktualne, a reakcje systemów nadal są proporcjonalne do ryzyka. Zmiany w aplikacjach, systemach tożsamości, urządzeniach i politykach bezpieczeństwa mogą sprawić, że wcześniej poprawne mapowanie zdarzeń będzie wymagało aktualizacji.

11. Lista kontrolna dla administratora

Poniższa lista kontrolna pomaga sprawdzić, czy organizacja jest przygotowana do wdrożenia wymiany sygnałów bezpieczeństwa oraz czy wybrane scenariusze mają jasno określony zakres. Warto wykorzystać ją przed pilotażem, po testach technicznych oraz przy rozszerzaniu integracji na kolejne systemy.

Choć spełnienie wszystkich punktów z listy nie gwarantuje całkowitego braku problemów wdrożeniowych, to drastycznie minimalizuje ryzyko rozmycia odpowiedzialności, niespójnego egzekwowania polityk oraz nieuzasadnionych blokad dostępu.

Tabela 6. Lista kontrolna wdrożenia Shared Signals i CAEP

Pytanie kontrolne	Dlaczego jest ważne
Czy wskazano systemy źródłowe zdarzeń?	Bez tego nie wiadomo, które systemy mają dostarczać informacje o zmianach statusu kont, sesji, urządzeń lub ryzyka.
Czy wskazano systemy odbierające zdarzenia?	Odbiorcy muszą być znani, zaufani i przygotowani do walidacji sygnałów.

Pytanie kontrolne	Dlaczego jest ważne
Czy określono typy zdarzeń CAEP i RISC potrzebne w organizacji?	Nie każda organizacja musi obsługiwać wszystkie typy zdarzeń. Zakres powinien wynikać z realnych potrzeb bezpieczeństwa.
Czy zdefiniowano reakcje na każde zdarzenie?	Sam odbiór sygnału nie wystarcza. System musi wiedzieć, co zrobić po jego otrzymaniu.
Czy reakcje są proporcjonalne do ryzyka?	Nie każde zdarzenie wymaga natychmiastowego zablokowania dostępu. Czasem lepsza jest dodatkowa weryfikacja lub ograniczenie uprawnień.
Czy istnieje audyt odbioru i obsługi zdarzeń?	Administratorzy powinni móc sprawdzić, czy zdarzenie dotarło, zostało zweryfikowane i wywołało oczekiwaną reakcję.
Czy określono wymagany czas propagacji?	Dla zdarzeń krytycznych opóźnienie między wykryciem a reakcją może mieć bezpośredni wpływ na bezpieczeństwo.
Czy określono zachowanie systemów przy błędach dostarczenia i obsługi zdarzeń?	Należy określić reakcję systemów na niedostępność odbiorcy, duplikaty zdarzeń, błędy walidacji, opóźnienia oraz problemy z identyfikacją podmiotu.
Czy ograniczono zakres przekazywanych danych?	Sygnały powinny zawierać wyłącznie informacje potrzebne do identyfikacji podmiotu i obsługi zdarzenia.
Czy użytkownicy i administratorzy wiedzą, czego się spodziewać?	Reakcje takie jak zakończenie sesji, dodatkowe uwierzytelnienie lub ograniczenie dostępu powinny być zrozumiałe dla zespołów obsługujących środowisko.

Rysunek 7. „Lista kontrolna administratora”



12. Najczęstsze błędy przy wdrażaniu Shared Signals i CAEP

12.1. Brak wspólnej identyfikacji podmiotów

Jedną z najważniejszych pułapek jest założenie, że systemy w taki sam sposób rozpoznają użytkownika, urządzenie lub sesję. W rzeczywistości jeden system może używać adresu e-mail, drugi identyfikatora konta, trzeci identyfikatora urządzenia, a aplikacja własnego identyfikatora sesji.

Jeżeli te identyfikatory nie są jednoznacznie mapowane, odbiorca może nie wiedzieć, którego podmiotu dotyczy zdarzenie. Wtedy nawet poprawnie dostarczony sygnał nie doprowadzi do właściwej reakcji.

12.2. Odbiór zdarzeń bez lokalnej polityki reakcji

Sam profil CAEP nie określa, co dokładnie ma zrobić każda aplikacja po odebraniu sygnału. To musi wynikać z lokalnej polityki systemu odbierającego.

Błędem jest wdrożenie integracji, w której odbiorca przyjmuje zdarzenia, ale nie ma jasnych reguł reakcji. W takim przypadku organizacja uzyskuje nowy kanał informacji, lecz nie skraca realnego czasu reakcji na zmianę ryzyka.

12.3. Zbyt ogólne traktowanie poziomu ryzyka

Sygnał o zmianie poziomu ryzyka powinien być powiązany z konkretną reakcją i kontekstem systemu. Samo nadanie statusu podwyższonego ryzyka nie wystarczy, jeśli odbiorca nie wie, czy ma zakończyć sesję, wymusić dodatkowe uwierzytelnienie, ograniczyć dostęp czy tylko zapisać zdarzenie do audytu.

Szczególnie problematyczne jest stosowanie jednego typu reakcji dla wszystkich przypadków. Ten sam sygnał może mieć inne znaczenie w systemie obsługującym dane wrażliwe, a inne w aplikacji pomocniczej.

12.4. Ignorowanie aktywnych sesji

Skupienie integracji wyłącznie na kolejnych logowaniach przy pominięciu sesji, które już trwają, podważa sens ciągłej oceny dostępu. Profil CAEP ma największą wartość wtedy, gdy warunki bezpieczeństwa zmieniają się już po rozpoczęciu sesji.

Samo zabezpieczenie przyszłych logowań nie wystarcza w sytuacjach, gdy konto zostaje zablokowane, urządzenie traci zgodność z polityką albo system wykrywa anomalię. System odbierający sygnał powinien wiedzieć, co zrobić z dostępem już przyznanym: zakończyć sesję, wymusić ponowne uwierzytelnienie, ograniczyć zakres dostępu albo przekazać zdarzenie do dalszej obsługi.

12.5. Brak kontroli nad strumieniami zdarzeń

Strumienie zdarzeń pokazują więcej niż sam fakt wystąpienia incydentu lub zmiany stanu. Można z nich odczytać, które systemy wymieniają sygnały, jakie typy zdarzeń organizacja obsługuje, które konta, urządzenia lub sesje są objęte reakcją oraz jak szybko poszczególne systemy odpowiadają na zmianę ryzyka.

Dlatego strumieni zdarzeń nie należy traktować jak zwykłej integracji technicznej. Częste błędy to: nadawanie zbyt szerokiego dostępu do strumieni, zapisywanie nadmiarowych danych, brak kontroli retencji oraz brak monitorowania tego, które systemy i osoby korzystają z informacji przekazywanych w ramach integracji.

12.6. Brak testów zachowania przy błędach

Wymiana sygnałów powinna działać przewidywalnie również w sytuacjach problemowych. Odbiorca bywa niedostępny, zdarzenie może zostać dostarczone

więcej niż raz, token może nie przejść walidacji, a system może nie rozpoznać użytkownika, urządzenia lub sesji.

Takie przypadki trzeba przetestować przed uruchomieniem integracji produkcyjnej. Organizacja powinna wiedzieć, czy błąd spowoduje brak reakcji, opóźnienie, alert administracyjny, odrzucenie zdarzenia czy nieuzasadnione ograniczenie dostępu.

12.7. Zbyt szeroki zakres pierwszego wdrożenia

Próba objęcia pierwszym wdrożeniem wszystkich systemów, aplikacji i typów zdarzeń znacząco zwiększa ryzyko niepowodzenia. Trudniej wtedy diagnozować błędy, ustalać zakresy odpowiedzialności i mierzyć efekty.

Lepszym podejściem jest wybór jednego scenariusza, który ma jasną wartość bezpieczeństwa. Dopiero po jego przetestowaniu warto dodawać kolejnych odbiorców, kolejne źródła zdarzeń i następne typy sygnałów.

13. Podsumowanie

Standardy Shared Signals i CAEP odpowiadają na problem, który w wielu organizacjach przez długi czas pozostawał ukryty w architekturze systemów: informacja o ryzyku, zmianie statusu konta, sesji lub urządzenia nie zawsze dociera tam, gdzie podejmowane są decyzje o dostępie.

Ich znaczenie nie polega na zastąpieniu istniejących mechanizmów bezpieczeństwa. Chodzi raczej o połączenie ich w bardziej spójny sposób. System, który wykrywa istotne zdarzenie, może przekazać je innym systemom w ustandaryzowanej formie, a te mogą zareagować zgodnie z własną polityką.

Największą wartością wynikającą z wdrożenia standardu Shared Signals jest skrócenie czasu między wykryciem zdarzenia a reakcją dostępową. Dotyczy to zwłaszcza aktywnych sesji, zmian uprawnień, utraty zgodności urządzenia i wzrostu poziomu ryzyka. W takich przypadkach decyzja podjęta przy logowaniu może nie wystarczyć.

Dobrze zaprojektowana wymiana sygnałów bezpieczeństwa pozwala przejść od modelu, w którym systemy działają osobno, do modelu, w którym mogą szybciej uwzględniać zmiany zachodzące w całym środowisku IT. Mimo iż nie eliminuje to potrzeby dobrych polityk, audytu i testów, daje administratorom lepszą podstawę do egzekwowania dostępu w oparciu o aktualny stan bezpieczeństwa.

Załącznik A. Słownik pojęć

- **Assurance Level Change** — typ zdarzenia CAEP informujący o zmianie poziomu pewności uwierzytelnienia. Taki sygnał może oznaczać, że bieżąca sesja wymaga ponownej oceny, dodatkowej weryfikacji albo ograniczenia dostępu do operacji wrażliwych.
- **CAEP (Continuous Access Evaluation Profile)** — profil Shared Signals służący do przekazywania zdarzeń, które mogą wpływać na bieżącą ocenę dostępu. Profil CAEP obejmuje między innymi zdarzenia dotyczące sesji, poświadczeń, poziomu ryzyka, zgodności urządzenia i zmian informacji wpływających na dostęp.
- **Claim** — deklaracja lub informacja przekazywana w tokenie, na przykład identyfikator użytkownika, rola, grupa albo inny atrybut wykorzystywany przez system do podejmowania decyzji o dostępie.
- **Credential Change** — typ zdarzenia CAEP informujący o zmianie danych uwierzytelniających, takich jak hasło, klucz, metoda uwierzytelniania albo inny element poświadczeń użytkownika.
- **Device Compliance Change** — typ zdarzenia CAEP informujący o zmianie zgodności urządzenia z polityką bezpieczeństwa. Może dotyczyć na przykład urządzenia, które przestało być zarządzane, utraciło wymagane zabezpieczenia albo zostało oznaczone jako niespełniające wymagań organizacji.
- **Event Stream** — strumień zdarzeń, czyli uzgodniony kanał przekazywania określonych typów sygnałów bezpieczeństwa między systemem wysyłającym a systemem odbierającym.
- **Krajowy System Cyberbezpieczeństwa (KSC)** — system określony w ustawie o krajowym systemie cyberbezpieczeństwa, którego celem jest zapewnienie cyberbezpieczeństwa na poziomie krajowym. Obejmuje między innymi podmioty kluczowe i podmioty ważne, właściwe organy oraz zespoły reagowania na incydenty bezpieczeństwa komputerowego, a także określa obowiązki związane z zarządzaniem ryzykiem i obsługą incydentów.
- **MFA (Multi-Factor Authentication)** — uwierzytelnianie wieloskładnikowe, czyli mechanizm wymagający użycia co najmniej dwóch składników uwierzytelniania potwierdzających tożsamość użytkownika.

- **OpenID Foundation (OIDF) —** organizacja non-profit rozwijająca otwarte standardy i specyfikacje dotyczące tożsamości cyfrowej i bezpieczeństwa. W ramach OpenID Foundation rozwijane są między innymi standardy z rodziny Shared Signals, w tym SSF, CAEP i RISC.
- **Polling** — model dostarczania zdarzeń, w którym system odbierający okresowo sprawdza, czy są dostępne nowe zdarzenia do pobrania.
- **Push** — model dostarczania zdarzeń, w którym system wysyłający przekazuje zdarzenie bezpośrednio do systemu odbierającego.
- **Receiver** — system, który odbiera zdarzenie bezpieczeństwa i może podjąć działanie zgodne z własną polityką. Może to być na przykład zakończenie sesji, wymuszenie ponownego uwierzytelnienia, ograniczenie dostępu albo zapis zdarzenia do audytu.
- **RISC (Risk Incident Sharing and Coordination)** — profil Shared Signals dotyczący koordynacji i udostępniania informacji o incydentach ryzyka związanych z kontem. Jest pokrewny profilowi CAEP, ale koncentruje się przede wszystkim na zdarzeniach dotyczących ryzyka konta.
- **Risk Level Change** — typ zdarzenia CAEP informujący o zmianie poziomu ryzyka związanego z użytkownikiem, urządzeniem, sesją lub aplikacją. Odbiorca takiego sygnału może wymusić dodatkową weryfikację, ograniczyć dostęp albo przekazać zdarzenie do dalszej analizy.
- **Security Event Token (SET)** — ustandaryzowany token zdarzenia bezpieczeństwa. Zawiera informacje niezbędne do opisania zdarzenia, wskazania jego źródła i identyfikacji podmiotu, którego zdarzenie dotyczy.
- **Session Established** — typ zdarzenia CAEP informujący, że sesja została ustanowiona. Może wspierać audyt, korelację zdarzeń oraz analizę użycia kont i aplikacji.
- **Session Presented** — typ zdarzenia CAEP informujący, że sesja została przedstawiona systemowi przy próbie dostępu do usługi lub zasobu.
- **Session Revoked** — typ zdarzenia CAEP informujący, że sesja została unieważniona albo nie powinna być dalej akceptowana. Odbiorca może zakończyć sesję, wymusić ponowne logowanie lub ograniczyć dostęp.

- **Shared Signals** — podejście do wymiany ustandaryzowanych sygnałów bezpieczeństwa między współpracującymi systemami. Celem jest szybsze przekazywanie informacji o zdarzeniach, ryzyku i zmianach stanu, które mogą wpływać na decyzje dostępowe.
- **SIEM (Security Information and Event Management)** — klasa systemów służących do zbierania, korelacji i analizy zdarzeń bezpieczeństwa z różnych źródeł. W kontekście Shared Signals może wspierać audyt, analizę incydentów i monitorowanie reakcji systemów.
- **SOAR (Security Orchestration, Automation and Response)** — klasa systemów wspierających automatyzację i koordynację reakcji na zdarzenia bezpieczeństwa. Może pomagać w obsłudze incydentów, eskalacji oraz wykonywaniu zaplanowanych działań operacyjnych.
- **SSF (Shared Signals Framework)** — techniczna rama wymiany zdarzeń bezpieczeństwa opracowana przez OpenID Foundation. Standard SSF opisuje między innymi sposób przekazywania Security Event Tokens, zarządzanie strumieniami zdarzeń oraz role systemów wysyłających i odbierających sygnały.
- **Step-up MFA** — wymuszenie dodatkowego lub silniejszego uwierzytelnienia w odpowiedzi na podwyższone ryzyko, próbę dostępu do wrażliwej funkcji albo zmianę kontekstu bezpieczeństwa.
- **Subject** — podmiot, którego dotyczy zdarzenie. Może to być użytkownik, urządzenie, sesja, aplikacja, grupa, tenant, jednostka organizacyjna albo inny obiekt rozpoznawany przez systemy uczestniczące w wymianie sygnałów.
- **Tenant** — logicznie wydzielone środowisko organizacji, klienta lub jednostki w systemie wielodostępnym. Tenant może mieć własnych użytkowników, konfigurację, polityki i dane.
- **Token** — ustandaryzowany nośnik informacji przekazywany między systemami. W kontekście tożsamości token może zawierać dane o użytkowniku, sesji, czasie ważności, rolach oraz innych atrybutach istotnych dla decyzji dostępowej.
- **Token Claims Change** — typ zdarzenia CAEP informujący, że zmieniły się informacje w tokenie, które mogą wpływać na decyzję o dostępie. Może dotyczyć na przykład roli użytkownika, przynależności do grupy albo innych atrybutów autoryzacyjnych.

- **Transmitter** — system, który wysyła zdarzenie bezpieczeństwa do innego systemu. Może to być na przykład system tożsamości, system zarządzania urządzeniami albo system detekcji zagrożeń.
- **Zero Trust** — model bezpieczeństwa zakładający, że dostęp do zasobów powinien być stale oceniany na podstawie aktualnego kontekstu, a nie tylko jednorazowo przy logowaniu. Standardy Shared Signals i CAEP mogą wspierać ten model, ponieważ umożliwiają przekazywanie sygnałów o zmianie ryzyka, sesji, urządzenia lub konta.

Załącznik B. Przykładowa macierz wdrożeniowa

Macierz wdrożeniowa pomaga uporządkować najważniejsze decyzje przed uruchomieniem wymiany sygnałów bezpieczeństwa.

Tabela 7. Przykładowa macierz wdrożeniowa (Załącznik B)

Scenariusz	System źródłowy	System odbierający	Oczekiwana reakcja
Zablokowanie konta użytkownika	System tożsamości	Aplikacja krytyczna	Zakończenie aktywnej sesji lub wymuszenie ponownego logowania.
Utrata zgodności urządzenia	System zarządzania urządzeniami	System kontroli dostępu	Ograniczenie dostępu z danego urządzenia.
Wzrost poziomu ryzyka	System detekcji zagrożeń	Aplikacja administracyjna	Dodatkowa weryfikacja, ograniczenie dostępu albo alert administracyjny.
Zmiana roli lub grupy	System katalogowy lub system tożsamości	Aplikacja biznesowa	Ponowna ocena uprawnień użytkownika.
Zmiana danych uwierzytelniających	System uwierzytelniania	Usługa webowa	Ponowne uwierzytelnienie albo zapis zdarzenia do audytu.
Ustanowienie sesji w systemie krytycznym	System uwierzytelniania	System audytu lub korelacji zdarzeń	Zapis informacji o sesji i korelacji z innymi zdarzeniami.

Scenariusz	System źródłowy	System odbierający	Oczekiwana reakcja
Błąd walidacji zdarzenia	System odbierający	Zespół administracyjny lub system monitorowania	Odrzucenie zdarzenia i utworzenie alertu administracyjnego.

Dla każdego scenariusza należy dodatkowo określić:

- **typ zdarzenia**, na przykład Session Revoked, Device Compliance Change, Risk Level Change, Token Claims Change albo Credential Change,
- **identyfikator podmiotu**, na przykład identyfikator użytkownika, urządzenia lub sesji,
- **właściciela scenariusza**, czyli zespół odpowiedzialny za konfigurację i utrzymanie integracji,
- **wymagany czas reakcji**, zależny od krytyczności zdarzenia i systemu,
- **sposób audytu** obejmujący zapis wysłania zdarzenia, jego odbioru, walidacji i wykonanej reakcji.

Tak przygotowana macierz jest łatwa do utrzymania, a jednocześnie wystarczająco konkretna, aby służyć jako punkt wyjścia do projektu technicznego i rozmów między właścicielami systemów.

Załącznik C. Źródła i dokumenty referencyjne

- OpenID Shared Signals Framework Specification 1.0: końcowa specyfikacja OpenID Foundation opisująca techniczną ramę wymiany sygnałów i zdarzeń między współpracującymi systemami. Dokument definiuje między innymi role systemów wysyłających i odbierających zdarzenia, Security Event Tokens, podmioty zdarzeń, typy zdarzeń, metadane konfiguracyjne oraz zarządzanie strumieniami zdarzeń.
- OpenID Continuous Access Evaluation Profile 1.0: finalna specyfikacja profilu CAEP. Dokument definiuje typy zdarzeń zgodne ze standardem SSF, które mogą wspierać ciągłą ocenę dostępu, w tym zdarzenia dotyczące sesji, poświadczeń, zgodności urządzenia, poziomu pewności uwierzytelnienia i poziomu ryzyka.
- OpenID RISC Profile Specification 1.0: finalna specyfikacja profilu RISC. Dokument opisuje typy zdarzeń związanych z koordynacją i udostępnianiem informacji o incydentach ryzyka dotyczących kont.
- Shared Signals Working Group: strona grupy roboczej OpenID Foundation odpowiedzialnej za rozwój standardów z rodziny Shared Signals. Zawiera informacje o celu grupy, zakresie prac oraz powiązanych specyfikacjach.
- Shared Signals Working Group Specifications: strona zbierająca specyfikacje rozwijane przez grupę roboczą Shared Signals, w tym SSF, CAEP i RISC.