IEC 62443-4-1:2018 Bezpieczny cykl życia rozwoju produktu dla automatyki przemysłowej

Bezpieczny cykl życia rozwoju, osiem praktyk

47 wymagań. Ta norma może zostać certyfikowana przez akredytowaną jednostkę. Stan na 07/2026.

IEC 62443-4-1 może być przedmiotem certyfikacji, ale przedmiot certyfikacji jest nietypowy: certyfikowany jest proces rozwoju konkretnej, nazwanej organizacji deweloperskiej, czyli jedna konkretna, udokumentowana wersja bezpiecznego cyklu życia. Nie certyfikuje się ani produktu, ani osoby. Ścieżki certyfikacji to ISASecure SDLA oraz IECEE CB Scheme. Obecnie taki certyfikat nie tworzy domniemania zgodności z unijnym Aktem o Cyberodporności (Cyber Resilience Act). Nie należy mylić go z IEC 62443-4-2, który stawia wymagania wobec samego komponentu. Niniejsza lista jest pomocą roboczą do samooceny, nie dowodem.

Firma	Data	Opracował

5 Praktyka 1: Zarządzanie bezpieczeństwem (SM) 13

SM-1 **Istnieje zdefiniowany cykl życia rozwoju produktu, który zapewnia bezpieczeństwo na każdym etapie, od koncepcji początkowej aż po wycofanie produktu z eksploatacji, i ten cykl życia jest rzeczywiście stosowany w praktyce.** Dokument

Jak to wykazać: Opis procesu lub instrukcja robocza wymieniająca etapy, wyniki dla każdego etapu oraz punkty przekazania, wraz z dowodami z bieżącego projektu pokazującymi, że etapy zostały faktycznie zrealizowane. Mała organizacja może poprzestać na jednej stronie na etap oraz liście kontrolnej w systemie zgłoszeń; liczy się to, że udokumentowany proces i codzienna praktyka się pokrywają.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-2 **Każde zadanie w bezpiecznym cyklu życia rozwoju ma przypisanego właściciela, a to przypisanie jest znane osobom zaangażowanym.** Dokument

Jak to wykazać: Macierz ról i odpowiedzialności przypisująca każdy krok procesu do konkretnej, nazwanej roli, uzupełniona o aktualną obsadę tych ról. Przy zaledwie kilku osobach wystarczy tabela z rolą, zadaniem i osobą; ważna jest zasada zastępstw na czas urlopu i choroby.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-3 **Jest w sposób możliwy do prześledzenia określone, które produkty, warianty, wydania i komponenty podlegają bezpiecznemu cyklowi życia rozwoju, a które nie.** Dokument

Jak to wykazać: Lista produktów i stanów wersji objętych zakresem wraz z uzasadnieniem włączeń i wyłączeń, aktualizowana przy każdym nowym wydaniu. W praktyce sprawdza się kolumna w przeglądzie produktów z wpisem tak lub nie w każdym wierszu oraz jednym zdaniem uzasadnienia.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-4 **Osoby podejmujące zadania z zakresu bezpieczeństwa posiadają wymaganą do tego kompetencję techniczną, a kompetencja ta jest celowo budowana i odświeżana.**

Jak to wykazać: Profil kompetencji dla każdej roli bezpieczeństwa, ewidencja kwalifikacji, plan szkoleń i listy obecności, uzupełnione o przegląd luk kompetencyjnych. Małe organizacje dokumentują to za pomocą certyfikatów, udziału w konferencjach lub webinarach oraz krótkiego rocznego przeglądu, kto i do kiedy zamyka jaką lukę, w razie potrzeby korzystając z zewnętrznej ekspertyzy.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-5 **Zakres bezpiecznego cyklu życia rozwoju jest wyznaczony i wskazuje zaangażowane lokalizacje, jednostki organizacyjne, wkład dostawców oraz środowiska rozwojowe, wraz z granicami tego zakresu.** Dokument

Jak to wykazać: Opis zakresu obejmujący lokalizacje, zespoły, elementy zlecone na zewnątrz i systemy, wraz ze szkicem interfejsów zewnętrznych. Podmiot prowadzący rozwój w jednej lokalizacji opisuje to w kilku zdaniach i wyraźnie wskazuje, co pozostaje poza zakresem, na przykład podzespoły opracowywane zewnętrznie lub hosting u strony trzeciej.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-6 **Dla każdego elementu dostarczanego użytkownikom, oprogramowania, oprogramowania układowego, konfiguracji oraz plików towarzyszących, możliwa jest weryfikacja integralności, tak aby odbiorcy mogli wykryć niezauważoną modyfikację.**

Jak to wykazać: Podpisy lub opublikowane sumy kontrolne dla każdego pakietu dostawy, opis metody oraz jeden przykład z rzeczywistego wydania, wraz z instrukcją dla klienta, jak przeprowadzić weryfikację. Dla małych zespołów wystarczy podpisany plik sumy kontrolnej obok pobierania oraz akapit w notatkach do wydania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-7 **Środowiska używane do rozwoju, budowania i testowania są chronione przed nieuprawnionym dostępem oraz przed manipulacją kodem źródłowym, narzędziami budowania i artefaktami.**

Jak to wykazać: Koncepcja kontroli dostępu do repozytorium, serwera budowania i systemów testowych, listy dostępu z datą ostatniego przeglądu, ewidencja zmian istotnych dla bezpieczeństwa oraz dowody rozdzielenia dostępu produkcyjnego od dostępu rozwojowego. Bez własnego działu IT wystarczy logowanie dwuskładnikowe, chroniona gałąź główna z obowiązkowym przeglądem oraz półroczny przegląd, kto nadal ma dostęp.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-8 **Klucze prywatne używane do podpisywania dostaw są chronione przed ujawnieniem i nadużyciem, a ich użycie jest ograniczone do uprawnionych osób i systemów.**

Jak to wykazać: Opis przechowywania kluczy, dostępu do nich, ich odnawiania i unieważniania, dowody chronionego przechowywania, na przykład tokena sprzętowego lub usługi zarządzania kluczami, wraz z ewidencją operacji podpisywania. Mała organizacja przechowuje klucz podpisujący na tokenie sprzętowym, dokumentuje dwie osoby mające do niego dostęp i ma gotową procedurę na wypadek utraty.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-9 **Dla komponentów kupowanych lub przejmowanych, w tym oprogramowania open source, określone są oczekiwania bezpieczeństwa stawiane dostawcy i są one stosowane podczas wyboru.** Dokument

Jak to wykazać: Wymagania bezpieczeństwa w specyfikacjach lub umowach z dostawcami, kryteria wyboru komponentów zewnętrznych, inwentaryzacja wszystkich komponentów zewnętrznych z wersją i źródłem, wraz z oceną, czy dostawca spełnia oczekiwania. Bez działu zakupów wystarczy prowadzona lista komponentów z kolumną odnotowującą, czy sprawdzono aktualizacje bezpieczeństwa i kanały zgłoszeniowe dostawcy.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-10 **Komponenty opracowywane na zamówienie przez stronę trzecią podlegają tym samym wymaganiom bezpieczeństwa co rozwój własny, a ich spełnienie jest weryfikowane.**

Jak to wykazać: Zamówienie lub dokumenty umowne określające wymagane zobowiązania w zakresie bezpieczeństwa, dowody od usługodawcy dotyczące stosowanych praktyk, ewidencja odbioru oraz wyniki własnych kontroli dostarczonej pracy. Bez budżetu na audyt wystarczy zapewnienie umowne, przekazanie wyników testów dostawcy oraz jedna własna kontrola wyrywkowa przed odbiorem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-11 **Wyniki związane z bezpieczeństwem pochodzące ze wszystkich źródeł, testów, przeglądów, zgłoszeń użytkowników i powiadomień stron trzecich, są rejestrowane, oceniane pod kątem wpływu, przypisywane do właściciela i terminu, oraz śledzone aż do zamknięcia.** Dokument

Jak to wykazać: System defektów lub zgłoszeń z dedykowanym oznaczeniem dla tematów bezpieczeństwa, a dla każdego wpisu ocena wpływu, właściciel, termin i notatka zamykająca, wraz z raportem otwartych pozycji. Mały zespół używa etykiety w istniejącym systemie zgłoszeń oraz stałego punktu na cotygodniowym spotkaniu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-12 **Przed wydaniem produktu weryfikuje się i dokumentuje, że przewidziane kroki bezpiecznego cyklu życia rozwoju zostały rzeczywiście zrealizowane oraz że powstały związane z nimi zapisy.** Dokument

Jak to wykazać: Przegląd wydania dla każdej wersji, porównujący ją z krokami procesu, odniesienia do odpowiednich zapisów oraz udokumentowana decyzja o wydaniu z datą i podpisem. W praktyce sprawdza się lista kontrolna wydania, która nie dopuszcza wysyłki bez kompletu zaznaczeń; otwarte pozycje są uzasadniane i otrzymują termin.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SM-13 **Sam bezpieczny cykl życia rozwoju jest regularnie kwestionowany i doskonalony, na podstawie wniosków z incydentów, wyników testów, informacji zwrotnych od klientów oraz zmieniającego się krajobrazu zagrożeń.**

Jak to wykazać: Zapisy z przeglądu procesu, na przykład przeglądu zarządczego lub retrospektywy, wraz z wywołanymi zmianami procesu, ich statusem wdrożenia oraz odniesieniem do przyczyny źródłowej. Podmiot stosujący poziomy dojrzałości normy odnotowuje stan bieżący i docelowy dla każdej praktyki; poziom dojrzałości 4 wymaga właśnie takiego dowodu ciągłego doskonalenia. Dla małej organizacji wystarczy jedno spotkanie rocznie z protokołem i trzema konkretnymi usprawnieniami.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

6 Praktyka 2: Specyfikacja wymagań bezpieczeństwa (SR) 5

SR-1 **Opisany jest zamierzony kontekst produktu: oczekiwane środowisko eksploatacji, środki bezpieczeństwa zakładane jako zapewniane przez to środowisko, przewidziane grupy użytkowników i role, przyjęte granice zaufania oraz zastosowania, do których produkt wyraźnie nie jest przeznaczony.** Dokument

Jak to wykazać: Opis kontekstu bezpieczeństwa produktu, jako dokument samodzielny lub jako stała sekcja specyfikacji produktu, obejmujący środowisko sieciowe, zakładane zabezpieczenia zewnętrzne, na przykład zaporę sieciową lub kontrolę dostępu fizycznego, listę ról oraz wyraźną listę zastosowań poza zakresem. Mała organizacja ogranicza to do dwóch stron, dodaje prosty szkic środowiska zakładu i zapewnia, że właściciel produktu opatruje go datą i zatwierdza.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SR-2 **Dla produktu istnieje model zagrożeń, który odwzorowuje przepływy danych, interfejsy, granice zaufania i ścieżki ataku, nazywa wynikające z nich zagrożenia i ich możliwy wpływ oraz przypisuje środki zaradcze. Jest on przeglądany i aktualizowany przy istotnych zmianach oraz co najmniej raz na każde wydanie produktu, a otwarte pozycje są śledzone aż do zamknięcia.** Dokument

Jak to wykazać: Model zagrożeń z diagramem przepływu danych, listą zagrożeń dla każdego interfejsu, przypisanymi środkami zaradczymi oraz statusem otwartych pozycji, wraz z historią zmian z datą i autorem. Mała organizacja może pracować na jednej tabeli na interfejs, z kolumnami: co może pójść źle, jak poważne byłyby skutki, co się z tym robi i kto to przegląda.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SR-3 **Wymagania bezpieczeństwa dla produktu są zdefiniowane i udokumentowane. Obejmują one wyniki modelu zagrożeń, opisany kontekst bezpieczeństwa produktu, obowiązujące wymagania prawne i umowne oraz docelowy poziom bezpieczeństwa, i zawierają zdolności bezpieczeństwa, które musi zapewnić sam produkt.** Dokument

Jak to wykazać: Lista wymagań lub narzędzie do zarządzania wymaganiami z unikalnym identyfikatorem dla każdego wymagania, źródłem każdego wpisu, na przykład zagrożeniem, umową z klientem lub obowiązkiem prawnym, oraz docelowym poziomem bezpieczeństwa. Mała organizacja prowadzi to jako pojedynczą tabelę ze stałą kolumną identyfikatora, do której podpinają się później weryfikacja i testowanie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SR-4 **Każde pojedyncze wymaganie bezpieczeństwa jest sformułowane jednoznacznie, wolne od sprzeczności, weryfikowalne i możliwe do prześledzenia do konkretnej funkcji lub interfejsu produktu, i zawiera informacje potrzebne do jego późniejszej weryfikacji bez dodatkowych wyjaśnień.**

Jak to wykazać: Próbka z listy wymagań pokazująca, dla każdego wymagania, mierzalne kryterium akceptacji oraz dotkniętą funkcję lub interfejs, wraz z przypisaniem wymagania do przypadku testowego. Mała organizacja sprawdza to za pomocą ustalonego szablonu formułowania oraz pytania kontrolnego, czy na podstawie wymagania można napisać przypadek testowy bez konieczności dopytywania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SR-5 **Wymagania bezpieczeństwa są przeglądane przed użyciem w projektowaniu i implementacji, z udziałem zainteresowanych stron, takich jak zespół rozwoju, zespół testów, właściciel produktu oraz, gdy to przydatne, sprzedaż lub klient. Przegląd obejmuje kompletność względem modelu zagrożeń i kontekstu bezpieczeństwa produktu, poprawność oraz testowalność. Wyniki są rejestrowane i śledzone aż do zamknięcia.**

Jak to wykazać: Zapis przeglądu z datą, uczestnikami i ich rolami, przeglądaną wersją wymagań, listą wyników z właścicielem i statusem zamknięcia oraz notatką o zatwierdzeniu. Mała organizacja realizuje to jako przegląd dwuosobowy między zespołem rozwoju a zespołem testów, z krótkim zapisem i linią zatwierdzenia na liście wymagań.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

7 Praktyka 3: Bezpieczne projektowanie (SD) 4

SD-1 **Każdy produkt posiada opis projektu, który obejmuje istotne dla bezpieczeństwa aspekty architektury: jakie komponenty istnieją, jak komunikują się między sobą, gdzie przebiegają granice zaufania, jakie interfejsy zewnętrzne są udostępnione oraz za pomocą jakich mechanizmów w projekcie realizowane są wcześniej zdefiniowane wymagania bezpieczeństwa.** Dokument

Jak to wykazać: Dokument architektury lub specyfikacja projektowa zawierająca diagram pokazujący komponenty, przepływy danych i granice zaufania, wraz z tabelą przypisania każdego wymagania bezpieczeństwa do elementu projektu, który je realizuje. Małemu dostawcy wystarczy jeden aktualizowany diagram wraz z dwiema lub trzema stronami wyjaśnień; liczy się to, że jest on objęty kontrolą wersji w repozytorium i aktualizowany przy każdej zmianie architektury.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SD-2 **Projekt jest systematycznie analizowany pod kątem zagrożeń. Analiza wskazuje cele atakującego, dotknięte granice zaufania i interfejsy, wynikające z tego zagrożenia wraz z ich oceną oraz środki zaradcze zastosowane w projekcie. Jest ona powtarzana przy każdej istotnej zmianie architektury lub środowiska, a zidentyfikowane zagrożenia są śledzone aż do podjęcia decyzji w sprawie każdego z nich.** Dokument

Jak to wykazać: Model zagrożeń dla produktu lub dla każdego istotnego wydania, na przykład tabela z kolumnami: zagrożenie, dotknięty interfejs, ocena, środek zaradczy i status, wraz z protokołem sesji modelowania z listą uczestników i datą. Mały zespół modeluje w sposób pragmatyczny podczas warsztatu trwającego dwie do trzech godzin wzdłuż diagramu architektury i rejestruje otwarte punkty jako zgłoszenia, dzięki czemu dowód śledzenia powstaje bez dodatkowego wysiłku.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SD-3 **Projekt w sposób możliwy do wykazania stosuje uznane zasady bezpiecznego projektowania, między innymi zasadę minimalnych uprawnień, minimalną powierzchnię ataku, obronę wielowarstwową, bezpieczne ustawienia domyślne, bezpieczne zachowanie w razie awarii oraz mechanizmy bezpieczeństwa tak proste i weryfikowalne, jak to możliwe. Zastosowanie tych zasad jest widoczne w projekcie i uzasadnione.**

Jak to wykazać: Sekcja w opisie projektu lub wewnętrzne wytyczne projektowe wymieniające te zasady, wraz z konkretnymi dowodami dla każdej zasady w produkcie, na przykład macierzą uprawnień usług, listą otwartych portów z uzasadnieniem, ustawieniami domyślnymi w stanie dostawy lub udokumentowanym zachowaniem w przypadku błędów. Mały dostawca wykorzystuje krótką listę kontrolną tych zasad jako stały punkt przeglądu projektu i archiwizuje wypełniony arkusz razem z projektem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SD-4 **Projekt jest przeglądany przez wykwalifikowanych specjalistów, zanim rozpocznie się implementacja. Przegląd obejmuje kompletność względem wymagań bezpieczeństwa, poprawność i skuteczność mechanizmów bezpieczeństwa oraz wyniki analizy zagrożeń. Udział biorą osoby o wystarczającej kompetencji w zakresie bezpieczeństwa, wyniki są rejestrowane i śledzone aż do zamknięcia.** Dokument

Jak to wykazać: Zapis przeglądu z datą, przeglądanym elementem wraz z jego wersją, uczestnikami i ich rolami, listą wyników ze statusem oraz decyzją o wydaniu. Mały zespół dołącza przegląd do pull requestu dokumentów projektowych i pozostawia wyniki jako komentarze z notatką zamykającą, co dokumentuje śledzenie bez dodatkowych narzędzi. Tam, gdzie brakuje wewnętrznej kompetencji w zakresie bezpieczeństwa, pragmatycznym rozwiązaniem jest zaangażowanie zewnętrznego recenzenta rozliczanego godzinowo do krytycznych projektów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

8 Praktyka 4: Bezpieczna implementacja (SI) 2

SI-1 **Istnieje zdefiniowany proces weryfikacji rzeczywistej implementacji względem bezpiecznego projektu: przegląd potwierdza, że środki ochronne przewidziane w projekcie są faktycznie obecne i skuteczne w kodzie, że zachowana jest obrona wielowarstwowa oraz że podczas implementacji nie wprowadzono nowych podatności. Przegląd przeprowadza odpowiednio wykwalifikowany personel, a wszelkie stwierdzone odchylenia są rejestrowane i śledzone aż do zamknięcia.**

Jak to wykazać: Pisemna procedura przeglądu implementacji wraz z zapisami przeglądów dla każdego komponentu lub wydania: przeglądany moduł, odniesienie do dokumentu projektowego, data, recenzent, wyniki i status ich rozwiązania. Odpowiednim dowodem są przeglądy pull requestów z obowiązkową listą kontrolną bezpieczeństwa, wyniki statycznej analizy kodu wraz z udokumentowaną oceną każdego wyniku oraz protokoły sesji przeglądowych. Mały zespół pokrywa to zasadą czterech oczu, szablonem przeglądu przechowywanym w repozytorium, w którym każdy środek projektowy jest odznaczany indywidualnie, oraz jednym zgłoszeniem na każdy otwarty wynik. Kluczowe jest to, że autor kodu nigdy nie jest recenzentem tego samego kodu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SI-2 **Wiążące zasady bezpiecznego kodowania obowiązują we wszystkich pracach rozwojowych związanych z bezpieczeństwem i obejmują co najmniej unikanie znanych niebezpiecznych konstrukcji i funkcji, obsługę danych wejściowych i błędów, zarządzanie pamięcią i zasobami oraz stosowanie zweryfikowanego kodu bezpieczeństwa zamiast implementacji własnych. Zasady obowiązują dla każdego używanego języka programowania, są znane wszystkim programistom i są aktualizowane w razie potrzeby, na przykład gdy pojawiają się nowe wzorce ataków lub nowe narzędzia.** Dokument

Jak to wykazać: Zatwierdzony standard bezpiecznego kodowania ze statusem wersji, zakresem dla każdego języka i datą zatwierdzenia, uzupełniony o dowody, że jest on stosowany w codziennej pracy: konfiguracja linterów i narzędzi analitycznych w repozytorium, reguła budowania ujawniająca naruszenia oraz lista obecności na szkoleniu wprowadzającym. Małe organizacje nie piszą standardu od podstaw; uznają ustalony, publicznie dostępny zestaw reguł za wiążący, dodają krótką listę własnych reguł uzupełniających i osadzają kontrolę w pipeline, tak aby zgodność była wykazywana automatycznie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

9 Praktyka 5: Weryfikacja i walidacja bezpieczeństwa poprzez testy (SVV) 5

SVV-1 Dokument

Każde wymaganie produktu związane z bezpieczeństwem ma przypisany co najmniej jeden przypadek testowy, wykazujący, że funkcja ochronna działa zgodnie z zamierzeniem w normalnej eksploatacji, że zachowuje się zgodnie ze specyfikacją przy nieprawidłowych danych wejściowych lub nadużyciu, oraz że ustawienia domyślne dostarczane z produktem odpowiadają stanowi bezpiecznemu. Wykonanie i wynik są rejestrowane dla każdej testowanej wersji oprogramowania.

Jak to wykazać: Macierz identyfikowalności łącząca wymaganie, przypadek testowy i wynik, wraz z zapisami testów pokazującymi datę, testowaną wersję lub build oraz nazwisko osoby przeprowadzającej test. Mały dostawca po prostu dodaje kolumnę z identyfikatorem przypadku testowego do listy wymagań i archiwizuje log wyjściowy z automatycznego przebiegu testów z pipeline budowania jako plik dołączony do odpowiedniej wersji.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SVV-2

Środki zaradcze wynikające z modelu zagrożeń są celowo testowane w celu potwierdzenia, że rzeczywiście zamykają założoną ścieżkę ataku. Testowanie jest prowadzone wobec zidentyfikowanych zagrożeń, a nie tylko wobec poprawnego użycia, a otwarte pozycje trafiają do procesu obsługi defektów.

Jak to wykazać: Przypadki testowe odwołujące się bezpośrednio do wpisów modelu zagrożeń, na przykład jeden przypadek nadużycia na identyfikator zagrożenia wraz z oczekiwanym zachowaniem obronnym, wraz z zapisami tych przebiegów. Bez rozbudowanego zaplecza wystarczy dodać do modelu zagrożeń kolumnę odwołującą się do przypadku testowego oraz datę ostatniej pomyślnej kontroli.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SVV-3 Dokument

Produkt jest systematycznie badany pod kątem podatności przed wydaniem. Zakres obejmuje co najmniej: badanie interfejsów i usług dostępnych z zewnątrz, testowanie z użyciem danych wejściowych zniekształconych i losowo mutowanych, przegląd wykorzystywanych komponentów zewnętrznych pod kątem znanych, zgłoszonych podatności oraz kontrolę pod kątem znanych klas słabości we własnym kodzie dostawcy. Wyniki są rejestrowane wraz z ich oceną.

Jak to wykazać: Raporty z użytych narzędzi, wskazujące nazwę narzędzia, wersję oraz stan danych bazy podatności, zapisy fuzzingu, listę komponentów zewnętrznych z datą ostatniego porównania oraz listę wyników z oceną i decyzją. Mały dostawca łączy bezpłatne narzędzia standardowe, skan zależności oraz skan portów i usług przeciwko zainstalowanemu produktowi i archiwizuje wyniki dla każdej wersji w jednym folderze.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SVV-4

Kandydat do wydania jest poddawany próbie ataku w realistycznych warunkach, która aktywnie próbuje obejść mechanizmy ochronne, a nie tylko je odpytuje. Zakres, warunki brzegowe i granice testu są uzgadniane z wyprzedzeniem, a stwierdzone słabości są obsługiwane i śledzone jak defekty.

Jak to wykazać: Zlecenie lub zamówienie testu wskazujące zakres i środowisko testowe, raport obejmujący zastosowane podejście, wykorzystane słabości i ich ocenę, wraz z wpisami w systemie defektów lub zgłoszeń zawierającymi dowody usunięcia lub uzasadnionej akceptacji ryzyka. Mali dostawcy zwykle kupują taki test zewnętrznie w ramach ograniczonego budżetu czasowego lub zlecają go osobie, która nie tworzyła produktu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SVV-5

Niezależność personelu testującego jest zdefiniowana i odpowiednia do zamierzonego poziomu dojrzałości. Osoba, która opracowała komponent, nie wydaje go wyłącznie na podstawie własnych testów, a w miarę wzrostu poziomu dojrzałości testowanie należy do organizacyjnie odrębnej jednostki lub podmiotu zewnętrznego. Rzeczywiste przypisanie jest możliwe do prześledzenia dla każdego testu.

Jak to wykazać: Definicja ról w procesie rozwoju pokazująca rozdzielenie tworzenia i testowania, a ponadto dla każdego przebiegu testu lub raportu testowego zarejestrowane nazwisko i rola osoby przeprowadzającej test. Dwuosobowa firma realizuje to poprzez wzajemny przegląd z udokumentowaną notatką o zasadzie czterech oczu i angażuje osobę zewnętrzną do pogłębionych testów bezpieczeństwa.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

10 Praktyka 6: Zarządzanie defektami bezpieczeństwa (DM) 6

DM-1 **Istnieje zdefiniowany kanał, przez który przyjmowane i rejestrowane są zgłoszenia słabości bezpieczeństwa w produkcie z każdego kierunku: od samego zespołu rozwoju, z testów i przeglądów, od klientów i integratorów, od zgłaszających zewnętrznych oraz z powiadomień dotyczących wykorzystywanych komponentów zewnętrznych i open source. Kanał zgłoszeniowy jest możliwy do odnalezienia przez strony zewnętrzne, a każde zgłoszenie jest rejestrowane z datą wpływu i źródłem.** Dokument

Jak to wykazać: Opis kanału zgłoszeniowego, publicznie dostępny punkt kontaktowy (strona bezpieczeństwa, plik security.txt lub skrzynka pocztowa taka jak security@), oraz rejestr wpływu zawierający dla każdego zgłoszenia datę, źródło i krótki opis. Mała organizacja może pracować ze współdzieloną skrzynką pocztową i jednym arkuszem kalkulacyjnym lub etykietą zgłoszenia, pod warunkiem że wszystkie zgłoszenia tam trafiają, w tym te zgłaszane na wewnętrznym czacie programistów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

DM-2 **Każde przychodzące zgłoszenie jest poddawane triage i badane w celu ustalenia, czy jest istotne dla bezpieczeństwa oraz których produktów, wersji i komponentów dotyczy. Zgłoszenia, które okazują się nieistotne dla bezpieczeństwa lub niemające zastosowania, są również zamykane z podaniem powodu, a nie po cichu odrzucane.**

Jak to wykazać: Notatka z triage dla każdego zgłoszenia wskazująca wynik (istotne dla bezpieczeństwa: tak lub nie), dotknięte wersje oraz powód odrzucenia, gdy ma to zastosowanie, widoczna w zgłoszeniu lub na liście wpływu. Zespoły o niskiej liczbie zgłoszeń mogą przeprowadzać triage w krótkiej, cyklicznej sesji i rejestrować wynik w dwóch zdaniach na wpis.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

DM-3 **Potwierdzone defekty bezpieczeństwa są oceniane spójną metodą: przyczyna źródłowa, dotknięte wersje i konfiguracje, potencjalny wpływ na eksploatację i bezpieczeństwo, możliwość wykorzystania oraz istotność względem zdefiniowanej skali. Wynik oceny jest rejestrowany i możliwy do prześledzenia.** Dokument

Jak to wykazać: Zapis oceny lub zestaw pól zgłoszenia dla każdego defektu obejmujący przyczynę źródłową, istotność oraz zastosowaną skalę (na przykład powszechny system punktacji z udokumentowanym wektorem), wraz z listą dotkniętych wersji. Małe zespoły mogą oprzeć się na stałym szablonie pól w systemie zgłoszeń oraz pół strony opisującej skalę i progi wywołujące natychmiastowe działanie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

DM-4 **Dla każdego ocenionego defektu bezpieczeństwa podejmowana jest decyzja o sposobie postępowania: usunięcie, środek kompensujący lub uzasadniona akceptacja ryzyka. Decyzja wynika z istotności, jest przypisana do osoby odpowiedzialnej i terminu, a defekt jest śledzony aż do zamknięcia.** Dokument

Jak to wykazać: Lista działań lub status zgłoszenia pokazujący właściciela, termin docelowy, rodzaj środka oraz notatkę zamykającą, powiązaną z bazą kodu lub wydaniem, w którym poprawka staje się skuteczna. Zaakceptowane ryzyka szczątkowe wymagają krótkiego pisemnego uzasadnienia zatwierdzonego przez właściciela produktu. Mała organizacja może prowadzić to na tablicy zgłoszeń z terminami, bez dodatkowych narzędzi.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

DM-5 **Dotknięci użytkownicy, integratorzy i inne zainteresowane strony są informowani o defektach bezpieczeństwa, gdy tylko wymaga tego ocena, ze wskazaniem dotkniętych wersji, wpływu oraz dostępnej poprawki lub środka kompensującego. Ramy czasowe i zakres odbiorców takiego ujawnienia są ustalone z wyprzedzeniem, podobnie jak podejście do zgłoszeń stron trzecich, które przychodzą z własnym terminem ujawnienia.**

Jak to wykazać: Opublikowane powiadomienia lub biuletyny bezpieczeństwa opatrzone datą i odniesieniem do wersji, lista dystrybucyjna lub kanał subskrybentów oraz pisemna reguła dotycząca ram czasowych i skoordynowanego ujawniania. Dostawcy mający niewielu klientów mogą posłużyć się jednorazową wysyłką do prowadzonej listy klientów wraz z opatrzoną datą stroną biuletynów, której zmiany są wersjonowane.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

DM-6 **Sposób obsługi defektów bezpieczeństwa jest przeglądany w ustalonych odstępach czasu. Przegląd obejmuje przypadki otwarte i przeterminowane, czas od zgłoszenia do usunięcia, powtarzające się przyczyny źródłowe oraz skuteczność zastosowanych środków. Usprawnienia procesu wynikające z przeglądu są wdrażane, a ich wdrożenie jest śledzone.** Dokument

Jak to wykazać: Protokół cyklicznego przeglądu z datą, uczestnikami, danymi liczbowymi dotyczącymi przypadków otwartych i przeterminowanych oraz listą uzgodnionych usprawnień z właścicielem i terminem. Mała organizacja może dołączyć ten punkt do istniejącego spotkania kwartalnego i prowadzić dane liczbowe i decyzje na jednej stronie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

11 Praktyka 7: Zarządzanie aktualizacjami bezpieczeństwa (SUM) 5

SUM-1 **Każda aktualizacja bezpieczeństwa produktu jest weryfikowana względem obsługiwanych wersji produktu i środowisk eksploatacji przed udostępnieniem klientom, i istnieje zapis wykazujący, że aktualizacja usuwa podatność bez zakłócania zamierzonej funkcji produktu.** Dokument

Jak to wykazać: Zapis testu dla każdej poprawki obejmujący testowaną wersję produktu, platformę, przypadki testowe (skuteczność wobec podatności oraz regresję funkcji podstawowych) oraz zatwierdzenie wydania. Mały dostawca może posłużyć się krótkim wpisem zatwierdzenia poprawki w zgłoszeniu: identyfikator zgłoszenia, zweryfikowane przez, zweryfikowane dnia, wynik, wraz z dołączonym logiem z automatycznego przebiegu testów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SUM-2 **Dla wszystkich komponentów produktu, które nie zostały opracowane wewnętrznie (biblioteki zewnętrzne, system operacyjny, środowiska uruchomieniowe), jest określone i udokumentowane, w jaki sposób oceniane są ich aktualizacje bezpieczeństwa oraz w jaki sposób są one przyjmowane do produktu lub odrzucane z udokumentowanym uzasadnieniem.** Dokument

Jak to wykazać: Inwentaryzacja komponentów części zewnętrznych z wersją i źródłem, wraz z jednym wpisem oceny dla każdej zgłoszonej podatności komponentu zewnętrznego, wskazującym decyzję (przyjęcie, brak wpływu, objęte środkiem kompensującym) oraz uzasadnienie. Małe zespoły stosują automatyczny skan zależności w procesie budowania i prowadzą decyzje jako komentarze do wyniku skanu lub w prostej liście wyjątków.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SUM-3 **Dla każdej wydanej aktualizacji bezpieczeństwa użytkownicy otrzymują zrozumiałą informację towarzyszącą: które wersje produktu są dotknięte, jaka podatność jest usuwana, jak duża jest jej istotność, czy należy uwzględnić skutki uboczne lub środki kompensujące, oraz jak instalowana jest aktualizacja.** Dokument

Jak to wykazać: Opublikowane powiadomienia bezpieczeństwa lub notatki do wydania wskazujące identyfikator podatności, dotknięte wersje, ocenę istotności, kroki instalacji oraz wskazówki dotyczące powrotu do poprzedniego stanu. Mali dostawcy prowadzą jedną publiczną stronę z chronologiczną listą powiadomień bezpieczeństwa i odsyłają do niej z poziomu produktu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SUM-4 **Istnieje zdefiniowana i chroniona przed manipulacją droga, przez którą użytkownicy uzyskują aktualizacje bezpieczeństwa, a autentyczność i integralność aktualizacji można zweryfikować po stronie użytkownika przed jej zainstalowaniem.**

Jak to wykazać: Opis kanału dostawy (obszar pobierania, serwer aktualizacji, nośnik fizyczny) wraz z jego środkami ochronnymi, podpis cyfrowy lub suma kontrolna dla każdego pakietu oraz instrukcja informująca użytkownika, jak ją zweryfikować. Mali dostawcy osiągają to poprzez podpisywanie na serwerze budowania, publikowanie sumy kontrolnej obok pobierania oraz wskazanie jednego jasnego miejsca przechowywania klucza publicznego.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SUM-5 **Istnieją zdefiniowane cele czasowe udostępniania aktualizacji bezpieczeństwa, zróżnicowane według istotności podatności; rzeczywiście osiągane czasy są śledzone, a każdy niedotrzymany cel jest uzasadniany i zabezpieczany środkiem tymczasowym dla użytkowników.** Dokument

Jak to wykazać: Wewnętrzna specyfikacja z oknem czasowym dla każdej kategorii istotności (na przykład krytyczna <= 30 dni, wysoka <= 90 dni) oraz ocena dla każdej podatności: data zgłoszenia, data wydania poprawki, liczba dni, które upłynęły, powód odchylenia. Mali dostawcy prowadzą to jako dwa pola daty w zgłoszeniu podatności i przeglądają listę raz na kwartał, zamiast budować dedykowany system metryk.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

12 Praktyka 8: Wytyczne bezpieczeństwa dotyczące wdrożenia i eksploatacji produktu (SG) 7

SG-1 **Każdy produkt jest dostarczany wraz z opisem swojej strategii obrony wielowarstwowej: wymienia warstwy ochronne wbudowane w sam produkt, odwzorowuje je na zagrożenia, którym przeciwdziałają, oraz pokazuje, jaki efekt ochronny wynika dopiero ze współdziałania kilku warstw.** Dokument

Jak to wykazać: Sekcja w dostarczanej dokumentacji produktu lub odrębna koncepcja bezpieczeństwa, wskazująca dla każdej warstwy ochronnej mechanizm, zagrożenie, przed którym chroni, oraz granice jej skuteczności. Mała organizacja prowadzi to jako dwustronicową tabelę: kolumna warstwa ochronna, kolumna zagrożenie zaczerpnięte z własnego modelu zagrożeń, kolumna ryzyko szczątkowe. Wystarczy odniesienie krzyżowe do modelu zagrożeń z SR-2, treść nie musi być prowadzona podwójnie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SG-2 **Dokumentacja wskazuje środki bezpieczeństwa, których produkt sam nie zapewnia, lecz oczekuje ich od środowiska wdrożenia, na przykład segmentacji sieci, zapór sieciowych po stronie infrastruktury, kontroli dostępu fizycznego lub zewnętrznej usługi czasu, i jasno stwierdza, że zapewniony poziom bezpieczeństwa nie zostaje osiągnięty bez tych środków.** Dokument

Jak to wykazać: Rozdział wymagań wstępnych wdrożenia w instrukcji lub rysunek architektury referencyjnej ze strefami i kanałami, w którym środki wymagane od właściciela zasobu są wyraźnie oznaczone. W praktyce sprawdza się lista założeń dotyczących środowiska, wyprowadzona bezpośrednio z kontekstu bezpieczeństwa produktu i ponownie sprawdzana przy każdej wersji produktu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SG-3 **Istnieje przewodnik bezpiecznej konfiguracji bazowej, który wymienia wszystkie istotne dla bezpieczeństwa ustawienia, usługi, porty i interfejsy, wskazuje zalecany stan dostawy oraz opisuje skutki odstąpienia od tego zalecenia.** Dokument

Jak to wykazać: Przewodnik hartowania z tabelą ustawień: parametr, wartość zalecana, efekt, skutek uboczny odstępstwa. Wraz z listą usług i portów aktywnych w konfiguracji domyślnej, wraz z uzasadnieniem, dlaczego pozostają włączone. Mały zespół prowadzi tę tabelę bezpośrednio obok pliku konfiguracyjnego w repozytorium i eksportuje ją do dokumentacji dostawy, dzięki czemu pozostaje zgodna z produktem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SG-4 **Dla bieżącej eksploatacji istnieje przewodnik opisujący, jak produkt jest eksploatowany w sposób bezpieczny, monitorowany i utrzymywany w stanie bezpiecznym, w tym tworzenie i odtwarzanie kopii zapasowych, rejestrowanie zdarzeń oraz postępowanie z komunikatami zdarzeń istotnymi dla bezpieczeństwa.** Dokument

Jak to wykazać: Przewodnik eksploatacji z sekcjami dotyczącymi rejestrowania zdarzeń, kopii zapasowych, ponownego uruchamiania oraz komunikatów zdarzeń. Jako dodatkowy dowód, lista istotnych dla bezpieczeństwa komunikatów emitowanych przez produkt, każdy z krótkim zalecanym działaniem, tak aby właściciel zasobu nie musiał interpretować ich samodzielnie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

SG-5 **Dokumentacja wyjaśnia, w jaki sposób konfigurowane i utrzymywane są konta użytkowników, role i uprawnienia produktu, w szczególności rozdzielenie ról, zmiana domyślnych danych uwierzytelniających oraz usuwanie kont, które nie są już potrzebne.** Dokument

Jak to wykazać: Rozdział zarządzania kontami z przeglądem ról i uprawnień przypisanych każdej roli, wraz z wyraźną wzmianką o domyślnych danych uwierzytelniających i ich zmianie podczas uruchamiania. W praktyce sprawdza się krótka lista kontrolna uruchamiania w instrukcji, którą właściciel zasobu może odznaczyć i zarchiwizować.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

SG-6 **Istnieje przewodnik bezpiecznego wycofania z eksploatacji, który opisuje całkowite usunięcie danych wrażliwych z produktu, takich jak dane uwierzytelniające, klucze, dane konfiguracyjne i dzienniki zdarzeń, zanim urządzenie zostanie przekazane dalej, ponownie wykorzystane lub zutylizowane.** Dokument

Jak to wykazać: Sekcja wycofania z eksploatacji wymieniająca każde miejsce przechowywania danych wrażliwych wewnątrz produktu oraz odpowiadającą mu procedurę usuwania, w tym przypadki, w których usunięcie jest technicznie niemożliwe i sprzęt musi zostać fizycznie zniszczony. Pomocna jest tu lista pamięci trwałej zaczerpnięta z opisu architektury, która zapobiega pominięciu jakiegoś miejsca przechowywania.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

SG-7 **Dokumentacja bezpieczeństwa dostarczana użytkownikom jest przeglądana przed wydaniem: jest technicznie poprawna, spójna z dostarczaną wersją produktu, kompletna względem zamierzonej treści oraz zrozumiała dla docelowych odbiorców, i jest aktualizowana przy każdej zmianie produktu.**

Jak to wykazać: Zapis przeglądu dla każdego dokumentu i wersji produktu z recenzentem, datą, wynikami i ich zamknięciem, powiązany z zatwierdzeniem wydania. Mała organizacja rozwiązuje to zasadą czterech oczu w pull requeście dokumentacji: jeden programista sprawdza treść techniczną, druga osoba sprawdza zrozumiałość, a zatwierdzenie jest rejestrowane w zgłoszeniu. Wersję można wydać dopiero po udokumentowaniu przeglądu.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie