MC

Tłumaczenie standardów i rekomendacji
w zakresie cyberbezpieczeństwa

Wsparcie automatyzacji w zakresie oceny środków bezpieczeństwa

Tom 1: **Przegląd**

NIST IR 8011 vol. 1_wer. 1.0_PL

NIST IR 8011 vol. 1_wer. 1.0_PL

Tom 1

18 września 2025

Wsparcie automatyzacji w zakresie oceny środków bezpieczeństwa

Tom 1: Przegląd

Publikacja dostępna pod adresem:

Tłumaczenia zaleceń w zakresie cyberbezpieczeństwa

NISTIR 8011
Volume 1

Automation Support for Security Control Assessments

Volume 1: Overview

Kelley Dempsey
Paul Eavy
George Moore

This publication is available free of charge from:

https://doi.org/10.6028/NIST.IR.8011-1

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8011
Volume 1

Automation Support for Security Control Assessments

Volume 1: Overview

Kelley Dempsey
Computer Security Division
Information Technology Laboratory

Paul Eavy
Federal Network Resilience Division
Department of Homeland Security

George Moore
Johns Hopkins University
Applied Physics Laboratory

This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8011-1

June 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

O PUBLIKACJI

Niniejsze opracowanie **NIST IR 8011 vol. 1 wer. 1.0_PL, *Wsparcie automatyzacji w zakresie oceny środków bezpieczeństwa. Tom 1: Przegląd***, stanowi tłumaczenie publikacji NISTIR 8011, *Automation Support for Security Control Assessments. Volume 1: Overview,* i zostało opracowane za zgodą National Institute of Science and Technology.

Przytaczane i cytowane w publikacji przepisy, okólniki, rozporządzenia wykonawcze, dyrektywy, normy, standardy, polityki, memoranda itp. odnoszą się, o ile nie zaznaczono inaczej, do prawodawstwa i rynku amerykańskiego. Jeżeli cytowany fragment ma przełożenie lub odpowiednik w polskim porządku prawnym lub normalizacyjnym, wówczas informacje te wskazane są bezpośrednio w tekście lub w przypisach.

W publikacji posłużono się pojęciami zdefiniowanymi w oryginalnej (angielskiej) wersji dokumentu, na podstawie którego powstały niniejsze zalecenia.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim[1]. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.**

Podmioty, urządzenia lub materiały o charakterze komercyjnym prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie. Taka identyfikacja nie stanowi rekomendacji, poparcia ani nie ma na celu sugerowania, że dane podmioty, materiały lub urządzenia są bezwzględnie najlepsze z dostępnych dla osiągnięcia danego celu.

[1] Kluczowi uczestnicy zarządzania ryzykiem – patrz: Narodowe Standardy Cyberbezpieczeństwa

STRESZCZENIE

W niniejszym tomie przedstawiono koncepcje ułatwiające zautomatyzowaną ocenę większości środków bezpieczeństwa opisanych w publikacji NSC[2] 800-53. Nawiązując do NSC 800-53A, środki te są podzielone na bardziej szczegółowe części (wymogi dla zabezpieczenia), które podlegają ocenie. Części składowe środka bezpieczeństwa oceniane w ramach każdego wymogu dla zabezpieczenia nazywane są elementami zabezpieczenia. Elementy zabezpieczenia są następnie grupowane w celu uzyskania odpowiednich funkcjonalności zabezpieczeń. Jak podano w NSC 800-53A, zdolności do ochrony (*ang. security capability*) są grupami środków bezpieczeństwa, które służą wspólnemu celowi. W celu skutecznej zautomatyzowanej oceny definiowane są testowalne kontrole defektów (*ang. defect checks*) łączące wymogi dla zabezpieczeń z szerszymi zdolnościami do ochrony, które mają być osiągnięte, oraz z samymi środkami bezpieczeństwa opisanymi w NSC 800-53. Kontrole defektów odpowiadają elementom zdolności do ochrony, nazywanym elementami zdolności, ponieważ każda z nich jest częścią większej zdolności. Zdolności i elementy zdolności są opracowywane z myślą o przeciwdziałaniu serii etapów ataku. Zautomatyzowane oceny (w formie kontroli defektów) są wykonywane przy użyciu testowej metody oceny zdefiniowanej w NSC 800-53A poprzez porównanie stanu (lub zachowania) pożądanego i rzeczywistego.

[2] NSC – Narodowy Standard Cyberbezpieczeństwa – wykaz publikacji NSC: patrz Załącznik A.

SŁOWA KLUCZOWE

stan rzeczywisty (*ang. actual state*); ocena (*ang. assessment*); granica oceny (*ang. assessment boundary*); metoda oceny (*ang. assessment method*); granica autoryzacji (*ang. authorization boundary*); zautomatyzowana ocena środków bezpieczeństwa (*ang. automated security control assessment*); automatyzacja (ang. a*utomation*); zdolność (*ang. capability*); program ciągłej diagnostyki i mitygacji skutków (*ang. continuous diagnostics and mitigation – CDM*); strategia ciągłego monitorowania bezpieczeństwa informacji (*ang. information security continuous monitoring – ISCM*); pulpit nawigacyjny (*ang. dashboard*); defekt (*ang. defect*); kontrola defektu (*ang. defect check*); specyfikacja stanu pożądanego (*ang. desired state specification*); pulpit nawigacyjny ISCM (*ang. ISCM dashboard*); łagodzenie skutków (*ang. mitigation*); bieżąca ocena (*ang. ongoing assessment*); analiza przyczyn źródłowych (*ang. root cause analysis*); automatyzacja bezpieczeństwa (*ang. security automation*); zdolność do ochrony (*ang. security capability*); środek bezpieczeństwa (*ang. security control*); ocena zabezpieczeń (*ang. security control assessment*); element zabezpieczenia (*ang. security control item*)

PODSUMOWANIE

Ewoluujące zagrożenia stanowią wyzwanie dla organizacji, które projektują, wdrażają i obsługują złożone systemy obejmujące wiele zmiennych elementów. Dokonywanie oceny wszystkich wdrożonych środków bezpieczeństwa informacji tak często, jak jest to konieczne, przy użyciu ręcznych metod proceduralnych, jest niepraktyczne i nierealistyczne dla większości organizacji ze względu na sam rozmiar, złożoność i zakres wykorzystywanych technologii informacyjnych. Dodatkowo, szybkie wdrażanie nowych technologii, takich jak urządzenia mobilne, chmury obliczeniowe i media społecznościowe, niesie ze sobą nowe zagrożenia, które sprawiają, że bieżąca ręczna ocena proceduralna wszystkich środków bezpieczeństwa jest niemożliwa w przypadku zdecydowanej większości organizacji. Obecnie w społeczności zajmującej się bezpieczeństwem informacji panuje powszechna zgoda co do tego, że gdy system jest już eksploatowany, konieczna jest automatyzacja oceny środków bezpieczeństwa[3] w celu wsparcia i ułatwienia realizacji strategii ciągłego monitorowania bezpieczeństwa informacji (*ang. Information Security Continuous Monitoring – ISCM*)[4] w czasie zbliżonym do rzeczywistego.

Niniejsza publikacja wspiera trzy podejścia do ISCM: 1) opracowanie własnego programu ISCM; 2) wykorzystanie programu CDM opracowanego przez DHS (Department of Homeland Security USA); lub 3) stworzenie programu hybrydowego. Rekomendacje te powstały w celu zapewnienia operacyjnego podejścia do automatyzacji oceny wybranych i wdrożonych środków bezpieczeństwa zawartych w NSC 800-53, w sposób zgodny z zaleceniami z NSC 800-53A.

Organizacje wdrażające ISCM i automatyzujące oceny środków bezpieczeństwa za pomocą opisanych tu metod są zachęcane do dzielenia się uzyskanymi wynikami, aby można było udostępnić zdobyte doświadczenia wszystkim zainteresowanym. W razie potrzeby niniejszy dokument zostanie zmieniony i/lub uzupełniony w celu udokumentowania takich najlepszych praktyk.

---

[3] Definicja *oceny bieżącej* znajduje się w Załączniku B.

[4] Patrz: NSC 800-137. Publikacja przedstawia wskazówki dla kadry zarządzającej dotyczące opracowania strategii ISCM i wdrażania programu ISCM.

SPIS TREŚCI

SPIS ILUSTRACJI

SPIS TABEL

1. WPROWADZENIE

1.1 *Cel i zakres*

Celem niniejszej publikacji NISTIR 8011 jest przedstawienie podejścia do automatyzacji oceny środków bezpieczeństwa w systemach i organizacjach, aby ułatwić ciągłe monitorowanie bezpieczeństwa informacji, bieżącą oceną i bieżące autoryzacje bezpieczeństwa.

Automatyzacja oceny środków bezpieczeństwa jest niezbędna, ponieważ zagrożenia bezpieczeństwa materializują się w coraz szybszym tempie. Zautomatyzowane oceny mogą zapewniać bardziej aktualne dane na temat defektów środków bezpieczeństwa (tj. o braku lub nieskuteczności takich środków), co umożliwia organizacjom skuteczniejsze reagowanie, zanim podatności na zagrożenia zostaną wykorzystane. Dodatkowo, zautomatyzowana ocena środków bezpieczeństwa może być potencjalnie tańsza i wymagająca mniejszej ilości zasobów ludzkich niż ręczne testy proceduralne. Wszelkie uzyskane w ten sposób oszczędności mogą uwolnić zasoby, które można wykorzystać na inne działania, np. inwestowanie w dodatkowe zabezpieczenia lub środki przeciwdziałania albo szybsze reagowanie na defekty i incydenty związane z bezpieczeństwem.

Istnieje wiele sposobów na zautomatyzowanie oceny środków bezpieczeństwa w celu określenia ich skuteczności. Podejście opisane w niniejszej publikacji, choć nie jest obowiązkowe, zapewnia kompleksową metodę zautomatyzowanej oceny środków bezpieczeństwa.

Przejście z ręcznej oceny środków bezpieczeństwa na proces zautomatyzowany wymaga czasu i przygotowania do wdrożenia systemu gromadzenia danych, który ułatwia jego realizację, a także panelu nawigacyjnego do ciągłego monitorowania bezpieczeństwa informacji, który umożliwia wizualizację wyników oceny. Zautomatyzowana ocena środków bezpieczeństwa wymaga również zasobów do modyfikacji i aktualizacji procesu oceny. Niniejsza publikacja ułatwia przejście na zautomatyzowaną ocenę środków bezpieczeństwa poprzez przedstawienie podejścia do tego procesu, które można dostosować do własnych potrzeb, oraz opracowanie planu oceny bezpieczeństwa, który jest zgodny zarówno z rekomendacjami NIST, jak i programem CDM DHS.

Organizacje mają swobodę wprowadzania innowacji i poszukiwania ulepszonych metod automatycznej oceny środków bezpieczeństwa. W przypadku opracowania nowych metod oceny, zachęca się organizacje do dzielenia się nimi z innymi organizacjami. Takie informacje są wykorzystywane do doskonalenia publikacji NISTIR 8011.

W niniejszym dokumencie, tomie 1 publikacji NISTIR 8011, przedstawiono przegląd metod automatyzacji ocen środków bezpieczeństwa. W kolejnych tomach, które będą wydawane oddzielnie, zostaną przedstawione i omówione wszystkie zdolności do ochrony określone poniżej.

Zdolności do ochrony ISCM zdefiniowane w niniejszej publikacji to zbiory środków bezpieczeństwa logicznie pogrupowane pod kątem spełnienia określonego celu w zakresie bezpieczeństwa oraz ułatwienia zautomatyzowanej oceny środków bezpieczeństwa. Zdolności ISCM nie stanowią ostatecznego zestawu zdolności do ochrony i w żaden sposób nie mają na celu ograniczenia elastyczności organizacji w zakresie definiowania innych lub dodatkowych zdolności[5]. Poniżej znajduje się lista zdolności do ochrony ISCM, dla których zostaną opublikowane dodatkowe tomy[6]:

Tom 2 Zarządzanie zasobami sprzętu komputerowego

Tom 3 Zarządzanie zasobami oprogramowania

Tom 4 Zarządzanie ustawieniami konfiguracyjnymi

Tom 5 Zarządzanie podatnościami na zagrożenia

Tom 6 Zarządzanie granicami (granice fizyczne, filtry i inne)

Tom 7 Zarządzanie zaufaniem

Tom 8 Zarządzanie zachowaniami związanymi z bezpieczeństwem

Tom 9 Zarządzanie poświadczeniami i uwierzytelnianiem

[5] W niniejszej publikacji zdolności do ochrony zostały zdefiniowane bardziej szczegółowo, jednak są zgodne z programem CDM DHS. Ponadto zdolności te zostały zaprojektowane w taki sposób, aby uwzględnić bazowe środki bezpieczeństwa opisane w NSC 800-53B.

[6] Opis wszystkich zdolności do ochrony ISCM znajduje się w podrozdziale 3.3.5.

Tom 10 Zarządzanie przywilejami i kontami

Tom 11 Zarządzanie przygotowaniem do zdarzeń (incydentów i sytuacji kryzysowych)

Tom 12 Zarządzanie wykrywaniem nietypowych zdarzeń

Tom 13 Zarządzanie reagowaniem na nietypowe zdarzenia i usuwaniem ich skutków

Niniejszy Tom 1 zawiera definicje terminów i ogólnych procesów, które są wspólne dla zautomatyzowanej oceny środków bezpieczeństwa dla zdolności do ochrony ISCM. Szczegółowe informacje dotyczące zautomatyzowanych ocen zdolności i powiązanych środków bezpieczeństwa znajdują się w tomach dotyczących zdolności do ochrony ISCM.

1.2 *Docelowi odbiorcy*

Dokument NISTIR 8011 jest przeznaczony dla osób związanych z projektowaniem, rozwojem, wdrażaniem, obsługą, utrzymaniem i audytowaniem programów ciągłego monitorowania bezpieczeństwa informacji w organizacjach oraz programów oceny i autoryzacji środków bezpieczeństwa, w tym dla osób o następujących obowiązkach:

- rozwój i integracja systemów (np. menedżerowie programów, twórcy produktów informatycznych, twórcy systemów, integratorzy systemów, projektanci korporacyjni, projektanci bezpieczeństwa informacji);
- zarządzanie/nadzór nad systemem lub bezpieczeństwem (np. starsi liderzy, osoby zarządzające ryzykiem, osoby autoryzujące, CIO, SISO);
- ocena i monitorowanie systemu i środków bezpieczeństwa (np. osoby przeprowadzające ocenę systemów, oceniający/zespół oceniający, osoby przeprowadzające niezależną weryfikację i walidację, audytorzy, właściciele systemów);
- wdrożenia i operacje związane z bezpieczeństwem informacji (np. właściciele systemu, dostawcy zabezpieczeń wspólnych, właściciele/zarządcy informacji, właściciele misji/biznesu, architekci bezpieczeństwa informacji, inżynierowie/urzędnicy ds. bezpieczeństwa systemu, administratorzy systemów/sieci/baz danych).

Należy podkreślić, że w niniejszym dokumencie przyjęto założenie, że czytelnik posiada ogólną, praktyczną wiedzę na temat ram zarządzania ryzykiem (*ang. Risk Management Framework – RMF*), a w szczególności tematyki zawartej w rekomendacjach: NSC 800-30, NSC 800-39, NSC 800-37, NSC 800-53, NSC 800-53A i NSC 800-137.

W niniejszej publikacji założono, że docelowi odbiorcy znają terminologię i najlepsze praktyki z zakresu technologii informacyjnych i bezpieczeństwa informacji. Definicje kluczowych terminów można znaleźć w załączniku B do niniejszego tomu lub w publikacji NSC 7298.

1.3 *Organizacja Tomu 1*

Dalsza część niniejszej publikacji ma następującą strukturę:

W rozdziale 2, Przegląd zautomatyzowanego procesu oceny środków bezpieczeństwa, opisano, w jaki sposób istniejące ręczne metody oceny środków bezpieczeństwa można dostosować do zautomatyzowanego procesu, a także omówiono obawy dotyczące automatyzacji metod oceny środków bezpieczeństwa.

W rozdziale 3, Ukierunkowanie ocen środków bezpieczeństwa na wyniki w zakresie bezpieczeństwa, opisano grupowanie środków bezpieczeństwa według celu (zdolności do ochrony ISCM), które ułatwia ich zautomatyzowaną ocenę.

W rozdziale 4, Wykorzystywanie specyfikacji stanu rzeczywistego i stanu pożądanego do wykrywania wad, określono wymagane przygotowanie do zautomatyzowanej oceny środków bezpieczeństwa i opisano, w jaki sposób w ramach tego procesu można określić specyfikację stanu rzeczywistego i stanu pożądanego, aby móc je porównać.

W rozdziale 5, Kontrola defektów, opisano koncepcję kontroli defektów.

W rozdziale 6, Dokumentacja planu oceny, przedstawiono dokumentację sporządzaną dla każdej zdolności do ochrony.

W rozdziale 7, Analiza przyczyn źródłowych, opisano analizę przyczyn źródłowych problemu ze środkiem bezpieczeństwa, niepowodzenia kontroli defektu lub nieskuteczności zdolności do ochrony na pożądanym ogólnym poziomie bezpieczeństwa.

W rozdziale 8, Role i obowiązki, opisano role i obowiązki operacyjne oraz porównano je z rolami i obowiązkami kadry kierowniczej ds. bezpieczeństwa systemu opisanymi w publikacjach NSC.

W rozdziale 9, Związek zautomatyzowanej oceny środków bezpieczeństwa z ramami zarządzania ryzykiem, opisano zadania i funkcję zautomatyzowanego procesu ISCM w ramach fazy oceny RMF.

2. PRZEGLĄD ZAUTOMATYZOWANEGO PROCESU OCENY ŚRODKÓW BEZPIECZEŃSTWA

Ataki na systemy dokonywane są coraz częściej. Defekt zabezpieczeń (tj. uszkodzenie lub wada środka bezpieczeństwa), który jest użyteczny dla atakującego, prawdopodobnie zostanie wykorzystany bardzo szybko, ponieważ większość atakujących stosuje *zautomatyzowane metody ataku*. Jednocześnie wiele organizacji, przynajmniej w niektórych przypadkach, stosuje ręczne metody wykrywania defektów (czyli ręczne metody oceny środków bezpieczeństwa) oraz ręczne metody analizy informacji związanych z bezpieczeństwem (tj. danych o defektach). W rezultacie wiele organizacji prawdopodobnie nigdy nie będzie miało zdolności do wykrywania dużej liczby defektów zabezpieczeń i reagowania na nie szybciej niż napastnicy mogą wykryć i wykorzystać jeden lub więcej z tych defektów.

W tym rozdziale opisano, jak istniejące metody ręcznej oceny środków bezpieczeństwa można dostosować do potrzeb zautomatyzowanego procesu. Zawarte są również rozwiązania potencjalnych problemów związanych z automatyzacją metod oceny środków bezpieczeństwa.

2.1 *Warunki wstępne zautomatyzowanej oceny środków bezpieczeństwa*

Proces oceny środków bezpieczeństwa przedstawiony w niniejszej publikacji jest przeznaczony do stosowania po zakończeniu wstępnej oceny i autoryzacji (*ang. Assessment and Authorization – A&A*)[7]. Niektóre wyniki zautomatyzowanych ocen środków bezpieczeństwa mogą mieć zastosowanie do wstępnej oceny systemu, jednak w niniejszym dokumencie skoncentrowano się na kolejnych tego typu ocenach, które są częścią strategii ciągłego monitorowania bezpieczeństwa informacji (*ang. Information Security Continuous Monitoring – ISCM*) realizowanej w fazie eksploatacji i utrzymania cyklu życia systemu.

Jako następstwo założenia, że wstępny proces A&A został przeprowadzony zgodnie z opisem w publikacji NSC 800-37 i powiązanymi rekomendacjami, zakłada się, że

[7] Więcej informacji na temat procesu RMF dotyczącego bezpieczeństwa informacji, w tym A&A, można znaleźć w publikacji NSC 800-37.

oceniany system (systemy) posiada standardowy zestaw dokumentów dotyczących bezpieczeństwa, w tym plan bezpieczeństwa systemu, wstępny (lub najbardziej aktualny) raport z oceny bezpieczeństwa oraz dokumenty pomocnicze, takie jak plan awaryjny systemu.

W niniejszej publikacji skupiono się na automatyzacji oceny środków bezpieczeństwa wybranych dla każdego poziomu wpływu zabezpieczeń bazowych, zgodnie z definicją zawartą w publikacji NSC 800-53B. Więcej informacji na temat automatycznej oceny poszczególnych środków bezpieczeństwa można znaleźć w tomach poświęconych zdolności do ochrony. Jeżeli *dostosowany* zestaw bazowych zabezpieczeń systemu zawiera dodatkowe środki bezpieczeństwa, które nie zostały wybrane jako bazowe w publikacji NSC 800-53B (tj. uzupełniono zestaw środków bezpieczeństwa), to te środki bezpieczeństwa mogą nie być uwzględnione w niniejszej publikacji. Do oceny takich środków stosowane są metody ręczne/proceduralne, a ręcznie generowane informacje związane z bezpieczeństwem są uwzględniane przy podejmowaniu decyzji opartych na ryzyku.

2.2 *Automatyzacja testowej metody oceny*

Po wstępnej autoryzacji bezpieczeństwa systemu, oceny środków bezpieczeństwa są przeprowadzane na bieżąco, aby zapewnić, że są one skuteczne i nadal będą skuteczne w środowisku operacyjnym. Metoda oceny opiera się na strategii ciągłego monitorowania opracowanej przez organizację, właściciela systemu i/lub dostawcę zabezpieczeń wspólnych i jest zatwierdzona przez osobę autoryzującą. Szczegółowe informacje na temat planowania oceny środków bezpieczeństwa znajdują się w publikacji NSC 800-53A.

Metody oceny określają specyfikę działań osoby oceniającej i obejmują badanie, wywiad i test. W tabeli 1: *Metody oceny z publikacji NSC 800-53A*, znajdują się definicje wszystkich metod oceny. Organizacja wykorzystuje wyniki każdej z metod oceny, aby określić, czy środki bezpieczeństwa istnieją, są funkcjonalne, poprawne i kompletne[8] oraz czy istnieje możliwość ich poprawy w czasie.

[8] Definicja kompletności oceny *(ang. assessment completeness)* znajduje się w glosariuszu.

Tabela 1: Metody oceny zawarte w publikacji NSC 800-53A

Metoda	Definicja [a)]
Badanie	Proces sprawdzania, kontroli, przeglądu, obserwacji, studiowania lub analizowania jednego lub więcej obiektów oceny w celu łatwiejszego zrozumienia, uzyskania wyjaśnienia lub uzyskania dowodów.
Wywiad	Proces prowadzenia rozmów z osobami lub grupami w organizacji w celu łatwiejszego zrozumienia, uzyskania wyjaśnień lub doprowadzenia do zlokalizowania dowodów.
Test	Proces wykorzystania jednego lub więcej obiektów oceny w określonych warunkach w celu porównania rzeczywistego zachowania z oczekiwanym.

[a)] Publikacja NSC 800-53A wer. 2, załącznik C; NSC 800-53A wer. 1, załącznik D

Testowa metoda oceny zwykle najłatwiej i najskuteczniej poddaje się automatyzacji, a po zautomatyzowaniu dostarcza dokładniejszych wyników.

W ramach technicznego wdrożenia programu ISCM, stosuje się testową metodę oceny wszędzie tam, gdzie można ją wykorzystać. Ocena poprzez test jest generalnie metodą, której automatyzacja jest najłatwiejsza i najskuteczniejsza. Ponadto zastosowanie zautomatyzowanej metody testowej może zapewnić dokładniejsze i bardziej powtarzalne wyniki, jeśli zostanie ona prawidłowo opracowana i wdrożona. Dlatego właściwe może być zastosowanie testowej metody oceny jako jedynej metody oceny dla wielu środków bezpieczeństwa. Trudniej jest zautomatyzować metody oceny oparte na badaniu i wywiadzie, ponieważ wymagają one udziału ludzi. Organizacje mogą jednak stosować metody oparte na badaniu i wywiadzie do analizy przyczyn źródłowych niepowodzeń w stosowaniu środków bezpieczeństwa (zagadnienie omówione w podrozdziale 7.2, Analiza przyczyn źródłowych) lub jeśli potrzebna jest większa pewność, szczegółowość lub zakres oceny.

2.2.1 *Terminy odnoszące się do obiektów oceny*

W niniejszym dokumencie powszechnie używa się terminu *obiekt oceny (ang. assessment object)*. Znaczenie terminu *obiekt oceny* użyte w niniejszym dokumencie jest zgodne z definicją słownikową, ale skupia się na tym, co potencjalnie może mieć defekt zabezpieczeń. Stąd też, w rozumieniu niniejszej publikacji, termin *obiekt oceny* odnosi się bardziej szczegółowo do:

> *Wszystkiego, co może mieć defekt zabezpieczeń (tj. nieskuteczny środek bezpieczeństwa lub jego brak). Przykłady obejmują urządzenia, oprogramowanie, osoby, dane uwierzytelniające, konta, przywileje oraz obiekty, w odniesieniu do których przyznawane są przywileje (w tym dane i obiekty fizyczne).*

Obiekt oceny jest pojęciem ogólnym i stosowany jest tam, gdzie tekst odnosi się do kwestii ogólnych. Natomiast w kontekście konkretnej zdolności (lub grupy zdolności) bardziej zrozumiałe może być użycie bardziej szczegółowego terminu. Wiele zdolności skupia się na obiektach oceny z defektami. Zarządzanie zasobami sprzętowymi (*ang. Hardware Asset Management – HWAM*) i zarządzanie zasobami programowymi (*ang. Software Asset Management – SWAM*) to przykłady takich zdolności. W odniesieniu do takich obiektów oceny można użyć terminu *zasób*[9] (np. zasoby z defektami).

Większość specyficznych zdolności koncentruje się na konkretnych typach obiektów oceny. Na przykład zdolność HWAM skupia się wyłącznie na defektach w urządzeniach i wokół nich. Ponieważ w tym tomie często wykorzystuje się przykłady z tomu o zdolności HWAM, często używa się terminu *urządzenia*, odnosząc się do defektów w tym kontekście.

Na potrzeby niniejszej publikacji wszystkie *zasoby sprzętowe*[10] (obiekty oceny) są urządzeniami, ale nie wszystkie urządzenia są obiektami oceny. Na przykład chip na płytce drukowanej jest urządzeniem i zasobem, ale w kontekście HWAM nie znajduje się na odpowiednim poziomie abstrakcji. Podobnie, zautomatyzowana ocena środków bezpieczeństwa nie skupia się na klawiaturze, myszy i monitorze urządzenia,

[9] *ang. asset*

[10] *ang. hardware assets*

ponieważ elementy te są tylko częścią większego urządzenia (lub obiektu oceny) podlegającego ocenie. W ramach systemów własności mogą być jednak klasyfikowane jako odrębne zasoby.

2.3 *Czynniki pozwalające określić, kiedy należy zaufać bieżącym automatycznym ocenom*

Zautomatyzowany wariant odpowiedniej metody oceny powinien być stosowany w przypadku danego środka bezpieczeństwa, jeśli jest on równie lub bardziej skuteczny w wykrywaniu defektów w porównaniu z tradycyjnymi metodami, które są stosowane. Dwa czynniki, które najbardziej przyczyniają się do wykrywania defektów to:

- kompletność zautomatyzowanej oceny środków bezpieczeństwa;
- terminowość stosowania zautomatyzowanej oceny środków bezpieczeństwa.

Kompletność oznacza, że zautomatyzowana ocena środków bezpieczeństwa obejmuje *wszystkie* kontrole defektów[11] i jest przeprowadzana na wszystkich obiektach oceny, które mogą mieć defekt. Stuprocentowa kompletność może nie zostać osiągnięta, jednak im bardziej zbliża się do niej zautomatyzowana ocena środków bezpieczeństwa, tym mniejsze prawdopodobieństwo niewykrycia wad.

Terminowość oznacza, że każdy cykl testów na ocenianych kombinacjach obiektów oceny defektów występuje co najmniej z częstotliwością określoną w strategii ISCM. Początkowo określona częstotliwość może być jedynie szybsza lub większa niż w przeszłości. Jednak w miarę rozwoju funkcjonalności automatycznej oceny środków bezpieczeństwa, częstotliwość powinna być na tyle duża, aby system automatycznej oceny środków bezpieczeństwa wykrywał (i dawał czas na reakcję na) duży odsetek wad, zanim przeciwnik zdąży je wykorzystać.

W związku z tym, jako część procesu zarządzania ryzykiem oraz strategii ISCM, organizacja określa wymagany stopień kompletności i terminowości, zanim zastąpi ręczne/proceduralne oceny zautomatyzowanym systemem oceny środków

[11] „Wszystkie kontrole defektów” ograniczają się do tych, które są niezbędne do zbadania wybranych środków bezpieczeństwa (patrz podrozdział 5.3).

bezpieczeństwa. Pulpit nawigacyjny ISCM[12](omówiony w następnym rozdziale) zapewnia wskaźniki dojrzałości, które pomagają ocenić tę gotowość.

Zautomatyzowana ocena środków bezpieczeństwa jest wystarczająca, aby zastąpić ręczną/proceduralną ocenę tych środków, jeśli tylko jest:

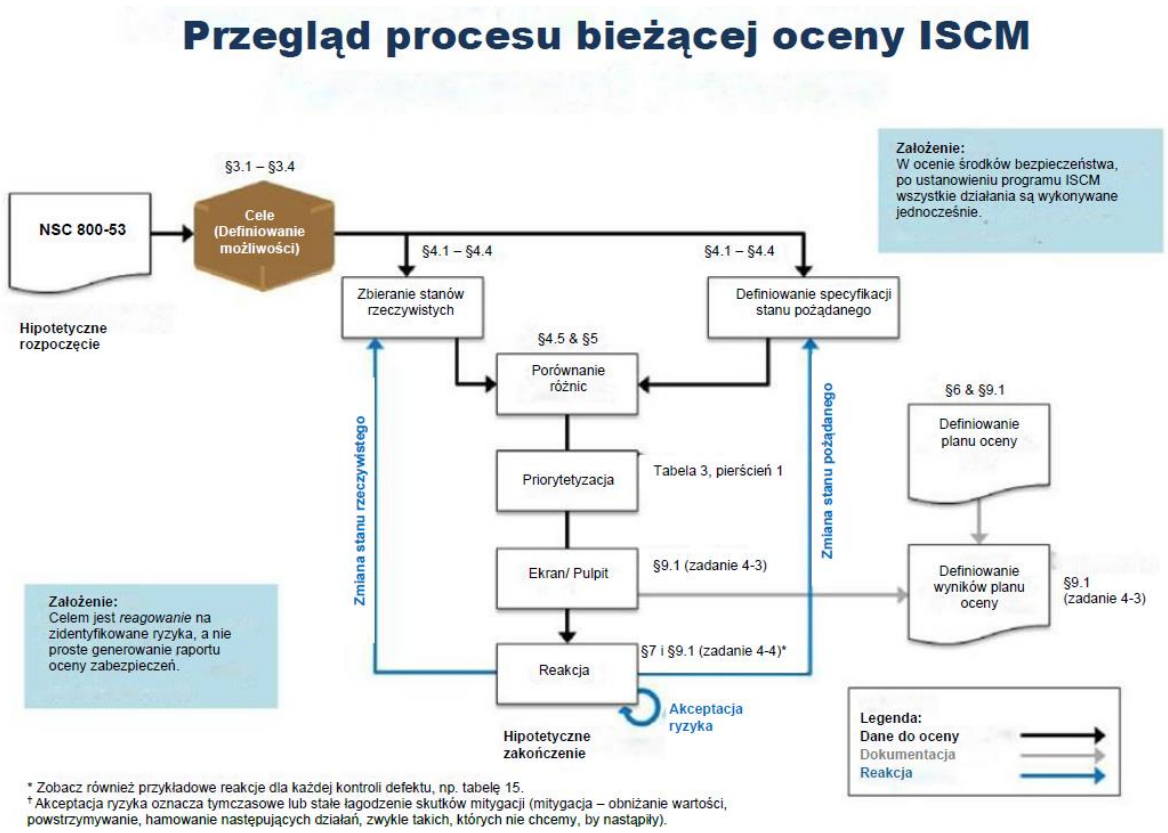
- co najmniej równie terminowa; oraz
- co najmniej równie kompletna,

co oceny manualne/proceduralne objętych nimi zdolności (i związanych z nimi środków bezpieczeństwa).

2.4 *Program zautomatyzowanej oceny środków bezpieczeństwa: ISCM*

Rysunek 1: *Przegląd zautomatyzowanego procesu oceny środków bezpieczeństwa*, to schemat działania zautomatyzowanego procesu oceny środków bezpieczeństwa. Na schemacie tym przedstawiono główne kroki wdrażania zautomatyzowanego procesu oceny środków bezpieczeństwa ISCM. Jak opisano w podrozdziale 1.3, Organizacja Tomu 1, poszczególne podrozdziały niniejszego dokumentu są uporządkowane w taki sposób, aby objaśniać wszystkie kolejne części schematu.

[12] *ang. ISCM dashboard*



Rysunek 1: Przegląd zautomatyzowanej oceny środków bezpieczeństwa

2.5 *Przygotowanie do zautomatyzowanych ocen środków bezpieczeństwa*

Aby skutecznie zautomatyzować oceny środków bezpieczeństwa, muszą być spełnione następujące warunki wstępne:

- odczytywalny maszynowo stan rzeczywisty i rzeczywiste zachowanie są zapisywane w postaci danych;
- odczytywalne maszynowo specyfikacje pożądanego/oczekiwanego stanu/zachowania (łatwo porównywalne ze stanem rzeczywistym) są określane i zapisywane w postaci danych;
- określono metodę obliczania/identyfikowania wad (różnic między stanem/zachowaniem pożądanym a rzeczywistym);
- określono metodę tworzenia czytelnego dla człowieka raportu oceny bezpieczeństwa w celu ułatwienia analizy i podejmowania decyzji opartych na ryzyku;
- ustalono organizacyjny próg *kompletności* kontroli defektów;
- ustalono organizacyjny próg *terminowości* kontroli defektów.

Jeśli warunki wstępne są spełnione, system automatycznej oceny kontroli bezpieczeństwa (jako część pulpitu nawigacyjnego ISCM) może automatycznie określić:

- czy występują różnice między specyfikacją stanu pożądanego a stanem rzeczywistym (wady);
- priorytet każdej wady[13];
- przypisanie wad do odpowiedniego zespołu operacyjnego w celu podjęcia reakcji[14].

Konkretne wytyczne dotyczące oceny ryzyka i reakcji na ryzyko są poza zakresem niniejszej publikacji, jednak konieczne jest określenie następujących kwestii w celu najbardziej efektywnego wykorzystania wyników/rezultatów zautomatyzowanej oceny bezpieczeństwa:

- metoda przypisywania wartości/oceny ryzyka (tj. priorytetu) do każdej zidentyfikowanego defektu;
- metoda określania operacyjnej odpowiedzialności za reagowanie na zidentyfikowane defekty.

[13] Do zautomatyzowanego określania priorytetów niezbędna jest metodologia oceny ryzyka, ale nie wchodzi ona w zakres niniejszej publikacji.

[14] Obowiązki są specyficzne dla danej zdolności do ochrony, dlatego są zdefiniowane i opisane w podrozdziałach 3.2, 3.3 i 3.4 w każdym tomie dotyczącym zdolności.

3. UKIERUNKOWANIE OCENY ZABEZPIECZEŃ NA WYNIKACH W ZAKRESIE BEZPIECZEŃSTWA

W niniejszym rozdziale wprowadzono trzy warstwy abstrakcji, które koncentrują się na osiąganiu wyników w zakresie bezpieczeństwa (jako zdolności do ochrony) wykraczających poza poziom poszczególnych środków bezpieczeństwa/elementów zabezpieczeń (patrz podrozdział 3.5).

Wprowadzono następujące warstwy abstrakcji zdolności do ochrony, które można powiązać[15] z wymaganiami bezpieczeństwa i realizującymi je poszczególnymi środkami bezpieczeństwa/elementami zabezpieczeń:

1. Warstwa etapu ataku — pożądany rezultat: zablokowanie lub opóźnienie ataku (patrz podrozdział 3.2).
2. Warstwa zdolności funkcjonalnych — każda zdolność jest grupą środków bezpieczeństwa i elementów zabezpieczenia opisanych w publikacji NSC 800-53. Pożądany rezultat: Zwiększenie bezpieczeństwa rozległego systemu (patrz podrozdział 3.3).
3. Warstwa elementów zdolności — każda zdolność jest podzielona na elementy niezbędne i wystarczające do wspomagania realizacji celu większej zdolności. Każdy element zdolności jest testowany z wykorzystaniem jednej odpowiadającej mu kontroli defektów. Pożądane rezultaty:
    a. wspieranie blokowania etapów ataku i zapewnienie funkcjonalnej zdolności do ochrony; oraz
    b. zapewnienie możliwych do jednoznacznego przetestowania wyników (patrz podrozdział 3.4).

Czwartą warstwę abstrakcji stanowią same elementy zabezpieczeń:

4. Warstwa elementów zabezpieczeń — patrz podrozdział 3.5.

[15] Możliwość powiązania wymagań została szczegółowo omówiona w publikacji SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*.

Cztery warstwy abstrakcji służą następującym celom:

- wspieranie silnej inżynierii systemowej w zakresie zdolności do ochrony;
- zapewnianie pomocniczych wskazówek dotyczących doboru środków bezpieczeństwa;
- uproszczenie zrozumienia całego procesu ochrony;
- umożliwienie oceny wyników w zakresie bezpieczeństwa na poziomie wyższym niż poszczególne zabezpieczenia;
- usprawnienie zarządzania ryzykiem poprzez określenie wyników w zakresie bezpieczeństwa, które są lepiej dopasowane do pożądanych wyników biznesowych.

Aby uwzględnić te cele, w publikacji NSC 800-53 wprowadzono koncepcję zdolności do ochrony informacji. *Zdolności do ochrony informacji* (omówione bardziej szczegółowo poniżej) to grupy środków, które współpracują ze sobą w celu osiągnięcia celu w zakresie bezpieczeństwa informacji i umożliwiają/zabezpieczają zdolność organizacji do realizacji jej misji.

Warstwy abstrakcji powstały na podstawie zabezpieczeń i analizy elementów niezbędnych do ograniczenia udanych ataków. Warstwy abstrakcji zostały udokumentowane, aby pokazać, w jaki sposób środki bezpieczeństwa z publikacji NSC 800-53 mogą oddziaływać na siebie, aby osiągnąć kluczowe wyniki w zakresie bezpieczeństwa informacji, co z kolei wspiera inżynierię systemów skoncentrowaną na bezpieczeństwie.

3.1 *Zastosowanie zdolności do ochrony do zautomatyzowanej oceny*

Przedstawienie zdolności do ochrony jako warstw abstrakcji powyżej poziomu środków bezpieczeństwa zapewnia kilka korzyści.

3.1.1 *Wspieranie solidnej inżynierii systemowej w zakresie zdolności do ochrony*

W przypadku normalnej inżynierii systemów proces rozpoczyna się od ogólnych wymagań biznesowych na dość wysokim poziomie abstrakcji. Następnie na podstawie wymagań biznesowych określa się bardziej szczegółowe wymagania techniczne. Procesy inżynierii bezpieczeństwa informacji na ogół przebiegają w inny sposób. Stosuje się określone zestawy zabezpieczeń w celu spełnienia szczegółowych wymagań technicznych bez udokumentowania powiązania elementów zabezpieczeń z bardziej ogólnymi wymaganiami[16].

[16] Dla zainteresowanych - NIST opublikował wytyczne dotyczące inżynierii systemów bezpieczeństwa informacji mające na celu realizację misji (SP 800-160).

Niezamierzonym i niepożądanym skutkiem tego jest fakt, że wiele programów bezpieczeństwa koncentruje się na poszczególnych środkach bezpieczeństwa w formie listy kontrolnej, nie zwracając uwagi na to, jak środki te współpracują ze sobą w celu ochrony poufności, integralności i dostępności informacji i systemów.

Cztery warstwy abstrakcji wspierają zintegrowaną inżynierię systemów poprzez sprawienie, że pożądane rezultaty programu bezpieczeństwa są jasne i mierzalne na konkretnym poziomie. To z kolei sprawia, że wyniki są bardziej zrozumiałe dla osób niebędących ekspertami w dziedzinie bezpieczeństwa, a tym samym łatwiejsze do powiązania z pożądanymi wynikami biznesowymi/w zakresie realizacji misji.

Świadomość wyników docelowych ułatwia inżynierię bezpieczeństwa, umożliwiając projektantom środków bezpieczeństwa postrzeganie ich jako części systemu zaprojektowanego w celu osiągnięcia ogólnego celu, co umożliwia im podejmowanie lepszych decyzji dotyczących projektowania i planowania zabezpieczeń.

3.1.2 *Zapewnianie pomocniczych wskazówek dotyczących doboru środków bezpieczeństwa*

Świadome i rozważne podejmowanie decyzji w zakresie doboru środków bezpieczeństwa wymaga zrozumienia, jak współpracują one ze sobą w celu osiągnięcia szerokiej ochrony. Określenie i udokumentowanie, w jaki sposób grupy środków współpracują ze sobą w celu zablokowania etapów ataku i wspierania szerokich funkcji bezpieczeństwa, ułatwia wybór zestawu uzupełniających się zabezpieczeń, które współpracują ze sobą w celu osiągnięcia pożądanych rezultatów (tj. zapewnienia ochrony współmiernej do ryzyka). W ramach koncepcji zdolności do ochrony uznaje się, że ochrona informacji przetwarzanych, przechowywanych lub przekazywanych przez systemy rzadko wynika z pojedynczego zabezpieczenia lub środka przeciwdziałania (tj. środka bezpieczeństwa). W większości przypadków taka ochrona wynika z doboru i wdrożenia zestawu wzajemnie wzmacniających się środków bezpieczeństwa.

3.1.3 *Uproszczenie zrozumienia całego procesu ochrony*

Szczegółowe zrozumienie setek poszczególnych elementów środków bezpieczeństwa jest trudnym zadaniem, dlatego zdefiniowanie zdolności do ochrony może uprościć koncepcyjne podejście do problemu ochrony. Wykorzystanie koncepcji zdolności do ochrony zapewnia skróconą metodę grupowania środków bezpieczeństwa, które mają to samo zadanie lub służą osiągnięciu wspólnego celu.

Podział środków na grupy wspierające powstrzymywanie etapów ataku, zdolności i składniki zdolności ułatwia lepsze zrozumienie wymagań i wdrożeń w zakresie bezpieczeństwa informacji. Pogrupowanie środków bezpieczeństwa w zdolności zwiększa świadomość oczekiwanych wyników.

3.1.4 *Umożliwienie oceny wyników w zakresie bezpieczeństwa na poziomie wyższym niż poszczególnych zabezpieczeń*

Wybór najbardziej odpowiedniego poziomu abstrakcji do oceny skuteczności implementacji środków bezpieczeństwa wiąże się z kompromisami. Jeśli ocena jest przeprowadzana na zbyt szczegółowym poziomie, można stwierdzić, że wszystkie części działają, ale jednocześnie przeoczyć fakt, że suma części nie działa. Z drugiej strony, jeśli wyniki są oceniane na wyższym poziomie abstrakcji i na tym poziomie wykryto nieprawidłowe działanie środka bezpieczeństwa, konieczna jest analiza pierwotnej przyczyny, aby określić, który element (elementy) wspierający działanie zabezpieczeń nie działa. Ponadto, jak zaznaczono w publikacji NSC 800-53A:

> *Staje się to istotną kwestią, na przykład podczas oceny środków bezpieczeństwa pod kątem skuteczności. Tradycyjnie przeprowadza się kolejno ocenę wszystkich środków, uzyskując dla nich wynik pozytywny (tj. środek jest wystarczający) lub negatywny (tj. środek nie jest wystarczający). Jednakże nieprawidłowe działanie pojedynczego środka lub, w niektórych przypadkach, wielu środków może nie mieć wpływu na ogólną zdolność do ochrony potrzebną organizacji. Nie oznacza to, że takie środki nie przyczyniają się do zapewnienia danego poziomu bezpieczeństwa lub ochrony prywatności systemu i/lub organizacji (określonego w wymaganiach bezpieczeństwa i wymaganiach dotyczących ochrony prywatności podczas fazy inicjacji cyklu życia systemu), ale raczej, że takie środki mogą nie wspierać realizacji danej funkcji*

> *bezpieczeństwa lub funkcji ochrony prywatności. Ponadto każdy wdrożony środek bezpieczeństwa lub ochrony prywatności niekoniecznie wspiera lub musi wspierać zdolność zdefiniowaną przez organizację.*

Warstwa abstrakcji elementów zdolności jest najwłaściwszym poziomem dla zautomatyzowanej oceny. Warstwa elementów zdolności jest bliższa wynikom i łatwiejsza do zautomatyzowania. Dlatego kontrole defektów zostały opracowane w taki sposób, aby testować skuteczność w warstwie elementów zdolności. W przypadku wykrycia niepowodzeń można zastosować analizę przyczyn źródłowych, aby znaleźć konkretny element lub elementy środka bezpieczeństwa powodujące niepowodzenie. (Patrz podrozdział 7.2, Analiza przyczyn źródłowych).

3.1.5 *Usprawnienie zarządzania ryzykiem poprzez określenie wyników (w zakresie bezpieczeństwa) lepiej dopasowanych do pożądanych wyników biznesowych*

W zaleceniach zawartych w NSC dotyczących ryzyka związanego z bezpieczeństwem informacji podkreśla się potrzebę skupienia się nie tylko na zagrożeniach na poziomie systemu, ale także na zagrożeniach na poziomie misji (NSC 800-30 oraz NSC 800-39).

W publikacjach NSC 800-37, NSC 800-53 oraz NIST SP 800-115 położono większy nacisk na ocenę wyników, a nie tylko na skuteczność środków. Ponadto, w publikacji NSC 800-39 zaleca się „trzypoziomowe podejście do zarządzania ryzykiem, które uwzględnia problemy związane z zagrożeniami na: (I) poziomie organizacji; (II) poziomie misji/procesu biznesowego; oraz (III) poziomie systemu". Środki bezpieczeństwa są w większości stosowane na poziomie systemu, a wyniki (rezultaty) biznesowe i dotyczące bezpieczeństwa są najbardziej widoczne na poziomie organizacji i misji/procesu biznesowego. Ponadto, jak zaznaczono w publikacji NSC 800-53:

> *Ostatecznie decyzje autoryzacyjne (tj. decyzje o akceptacji ryzyka) podejmowane są w oparciu o stopień, w jakim pożądane zdolności do ochrony zostały skutecznie osiągnięte i spełniają wymagania bezpieczeństwa zdefiniowane przez organizację. Te decyzje oparte na ryzyku są bezpośrednio związane z tolerancją ryzyka organizacji, która jest określona w ramach strategii zarządzania ryzykiem.*

Wartością warstw abstrakcji jest ścisłe dopasowanie do misji biznesowej organizacji, co ułatwia analitykom w danej organizacji powiązanie wymagań z misją. Jednakże warstwy abstrakcji opisane w tym dokumencie nie mogą odnosić się do misji konkretnej organizacji (ponieważ został on napisany w taki sposób, aby można go było zastosować w każdej organizacji). W razie potrzeby każda organizacja może dodać warstwy specyficzne dla danej misji, na podstawie wkładu zarządzanych systemów we wspieranie realizacji konkretnej misji organizacji. Warstwy abstrakcji związane z etapami ataku i zdolnościami do ochrony zostały przewidziane w celu ułatwienia powiązania środków bezpieczeństwa z misją organizacji.

W poniższych podrozdziałach opisano, jak koncepcja zdolności do ochrony z publikacji NSC 800-53 może być wykorzystana do pogrupowania środków bezpieczeństwa według wyników w zakresie ochrony, które każda zdolność ma osiągnąć. Dzięki wykorzystaniu odpowiednich wskaźników umożliwia to osobom zarządzającym ryzykiem podejmowanie lepszych decyzji w zakresie zarządzania ryzykiem poprzez ocenę stopnia realizacji celów wyższego poziomu.

3.2 *Etapy ataku*

Ostatecznie bezpieczeństwo informacji zależy od zablokowania lub ograniczenia szkód w zakresie poufności, integralności i dostępności informacji i systemów.

Takie szkody są spowodowane przez jedno lub więcej z następujących źródeł zagrożeń (NSC 800-30):

- wrogie cyberataki lub ataki fizyczne,
- błąd człowieka,
- uszkodzenia strukturalne zasobów kontrolowanych przez organizację (np. sprzętu, oprogramowania, kontroli środowiska),
- klęski żywiołowe i katastrofy spowodowane przez człowieka, wypadki i awarie będące poza kontrolą organizacji.

3.2.1 *Model etapów ataku adwersarza*

Opracowano różne modele opisujące sposób przeprowadzania wrogich ataków. Modele etapów ataku uwzględniają punkt widzenia złośliwego atakującego. Modele

etapów ataku nie odnoszą się bezpośrednio do zdarzeń niemających charakteru wrogiego ataku (tj. zdarzeń, które występują bez złych intencji, takich jak klęski żywiołowe, awarie sprzętu, błędy ludzkie itp.). Jednak opisany poniżej model etapów ataku i związane z nim działania atakującego i obrońcy mogą być stosowane do zdarzeń niemających charakteru wrogiego ataku, ponieważ istnieje wiele podobieństw między nimi. W każdym przypadku organizacje pozostają odpowiedzialne za uwzględnienie zarówno zdarzeń o charakterze wrogich ataków, jak i nie mających takiego charakteru, a także za wdrożenie zdolności do ochrony / środków bezpieczeństwa w celu osiągnięcia całościowego sposobu zarządzania ryzykiem oraz w ramach kompleksowego programu bezpieczeństwa informacji.

Etapy ataku i zdolności do ochrony. Ponieważ konkretne środki bezpieczeństwa potrzebne do zablokowania lub opóźnienia etapów ataku mogą być mapowane, kroki ataku odpowiadają zdolnościom do ochrony zaprojektowanym do zablokowania lub opóźnienia atakującego na każdym kroku. Model etapów ataku przedstawiono na rysunku 2. Model etapów ataku składa się z sześciu etapów, a każdemu z nich odpowiadają określone zdolności i elementy zdolności do ochrony określone w niniejszej publikacji. Należy zauważyć, że opisane tutaj etapy ataku nie są ostatecznym zestawem takich etapów i w żaden sposób nie ograniczają możliwości organizacji w zakresie określania innych lub dodatkowych etapów ataku i związanych z nimi zdolności do ochrony na potrzeby własnej sytuacji.

Etapy ataku	
1)	Uzyskanie dostępu do systemu
2)	Zainicjowanie ataku wewnątrz sieci
3)	Uzyskanie punktu zaczepienia
4)	Zdobycie trwałego punktu zaczepienia
5)	Rozszerzenie nielegalnie uzyskanej kontroli – eskalacja lub propagacja
6)	Osiągnięcie celu ataku

Rysunek 2: Model etapów ataku.

Obrona w głąb. Z perspektywy etapów ataku, koncepcja dogłębnej obrony oznacza, że wprowadza się środki bezpieczeństwa dla wszystkich etapów, aby w przypadku złamania zabezpieczeń w ramach jednego z nich, dla kolejnego etapu istniały środki bezpieczeństwa, które nadal będą chronić system. Przykłady i/lub opisy sześciu etapów ataku oraz potencjalnych przeciwdziałających im środków bezpieczeństwa przedstawiono w tabeli 2: Opis etapów ataku.

Tabela 2: Opis etapów ataku.

Etap ataku	Działanie atakującego	Działanie obrońcy
1) Uzyskanie dostępu do systemu	Atakujący znajduje się poza granicami celu i szuka wejścia do systemu. Przykłady: wysłanie wiadomości e-mail ze spersonalizowaną próbą wyłudzenia informacji; zainicjowanie ataku DDoS przeciwko danej domenie; próba uzyskania przez nieupoważnioną osobę fizycznego dostępu do obiektu o ograniczonym dostępie. *Uwaga:* W przypadku ataku DDoS wygenerowany w jego ramach ruch przedostaje się jedynie do zapory sieciowej lub innego urządzenia granicznego. Mimo to ruch ten zakłóca połączenie z Internetem, które znajduje się wewnątrz granicy oceny.	1) Przeciwdziałanie atakom lub negatywnym zdarzeniom przed ich zainicjowaniem lub możliwością wywarcia wpływu na lokalne środowisko. Przykłady: uwierzytelnianie wieloskładnikowe; filtry antyspamowe; listy kontroli dostępu dla routerów/ zapór sieciowych; zabezpieczenia fizyczne, takie jak blokady lub osłony; szyfrowanie łączy i wirtualne sieci prywatne (ang. *Virtual Private Network – VPN*); autorytatywna usługa nazw domen (DNS) w celu zapobiegania atakom przez skażenie (*ang. poisoning*); aplikacje antywirusowe na poziomie bramy. 2) Wykrywanie włamania; reagowanie i odzyskiwanie. Przykłady: systemy wykrywania włamań do sieci; sprzęt do nadzoru nad obiektem fizycznym, który identyfikuje próby nieautoryzowanego

Etap ataku	Działanie atakującego	Działanie obrońcy
		fizycznego dostępu do obiektu.
2) Zainicjowanie ataku wewnątrz sieci.	Atakujący znajduje się w granicach sieci i inicjuje atak na jakiś wewnętrzny obiekt oceny. Przykłady: użytkownik[a] otwiera wiadomość e-mail ze spersonalizowaną próbą wyłudzenia informacji lub klika załącznik; zgubienie lub kradzież laptopa; użytkownik instaluje nieautoryzowane oprogramowanie lub sprzęt; nieautoryzowany personel uzyskuje fizyczny dostęp do obiektu o ograniczonym dostępie.	1) Przeciwdziałanie wystąpieniu warunku inicjującego w środowisku lokalnym. Przykłady: edukowanie użytkowników, aby nie klikali załączników; utrzymywanie skutecznej kontroli nad aktywami; ograniczanie uprawnień do instalacji oprogramowania lub nośników wymiennych. 2) Ograniczenie zdarzenia powodującego atak. Przykłady: zapobieganie automatycznemu wykonywaniu kodu na nośnikach wymiennych; umieszczanie autoryzowanego oprogramowania do wykonania na białej liście; edukowanie użytkowników, aby nie udostępniali haseł; edukowanie użytkowników, aby nie wysyłali niezaszyfrowanych danych osobowych (*ang*. *Personally Identifiable Information – PII*) poza organizacje; aplikacje zwalczające złośliwe oprogramowanie na poziomie hosta, które blokują wykonanie kodu. 3) Wykrywanie włamania, reagowanie i odzyskiwanie.

Etap ataku	Działanie atakującego	Działanie obrońcy
		Przykłady: systemy wykrywania włamań opartych na hoście; sprzęt do nadzoru nad obiektem fizycznym, który identyfikuje nieautoryzowany fizyczny dostęp do obiektu.
3) Uzyskanie punktu zaczepienia.	Atakujący uzyskał dostęp do obiektu oceny i w takim stopniu pokonał zabezpieczenia, aby zdobyć punkt zaczepienia, ale bez możliwości utrzymania się. Przykłady: nieautoryzowanemu użytkownikowi udaje się zalogować przy użyciu autoryzowanych danych uwierzytelniających; kod wykorzystujący luki przeglądarki zostaje pomyślnie wykonany w pamięci i inicjuje połączenie zwrotne; włamywacz uzyskuje nieautoryzowany dostęp do serwerowni.	1) Ograniczanie podatności, które wykorzystują ataki/zagrożenia. Przykłady: instalowanie poprawek; wdrażanie standardowych bezpiecznych konfiguracji. 2) Przeciwdziałanie skutecznemu wykorzystaniu podatności. Przykłady: zapobieganie wykonywaniu danych (*ang. Data Execution Prevention – DEP*); techniki rekompilacji; usuwanie domyślnych haseł i kont; uwierzytelnianie wieloskładnikowe; wyłączanie kont; redundantne ścieżki komunikacji; ograniczanie fizycznego dostępu do krytycznych zasobów. 3) Przeciwdziałanie pomyślnemu zajęciu punktu zaczepienia w ocenianym obiekcie. Przykłady: wykrywanie prób; blokowanie prób dostępu do znanych złośliwych domen DNS; przeglądanie dzienników audytu i zdarzeń. 4) Wykrywanie punktu zaczepienia, reagowanie i odzyskiwanie. Przykłady: systemy wykrywania

Etap ataku	Działanie atakującego	Działanie obrońcy
		włamań oparte na hoście; analiza behawioralna; sprzęt do nadzoru obiektów fizycznych, który identyfikuje próby nieautoryzowanego fizycznego dostępu do wewnętrznych lokalizacji lub zasobów.
4) Zdobycie trwałego punktu zaczepienia.	W ramach ataku udało się uzyskać punkt zaczepienia w ocenianym obiekcie oraz udaje się go utrzymać. Przykłady: złośliwe oprogramowanie zainstalowane na hoście, które przetrwało ponowne uruchomienie lub wylogowanie; modyfikacja BIOS-u lub jądra; nowe/uprzywilejowane konto utworzone dla nieautoryzowanego użytkownika[a)]; nieautoryzowana osoba wydała dane uwierzytelniające / pozwolenie na dostęp; nieautoryzowany personel dodany do listy kontroli dostępu (*ang. Access Control List – ACL*) do serwerowni.	1) Przeciwdziałanie stałemu narażeniu zasobów. Przykłady: umieszczanie aplikacji na białej liście; narzędzia do zapobiegania złośliwemu oprogramowaniu / włamaniom; wirtualizacja i sandboxing; systemy haseł jednorazowych; wymaganie tokenów sprzętowych do uwierzytelniania; ograniczanie dostępu fizycznego za pomocą czytników kart. 2) Wykrywanie możliwości pozostania włamywacza w systemie, reagowanie i odzyskiwanie. Przykłady: usługi oceny reputacji plików; sprawdzanie integralności plików; blokowanie znanych złośliwych kanałów sterowania i kontroli; przeglądanie dzienników audytu i zdarzeń; zaawansowane techniki analizy behawioralnej; sprzęt do nadzoru nad fizycznym obiektem, który identyfikuje udany nieautoryzowany fizyczny dostęp do wewnętrznych lokalizacji lub zasobów.

Etap ataku	Działanie atakującego	Działanie obrońcy
5) Rozszerzenie nielegalnie uzyskanej kontroli – eskalacja lub propagacja.	Atakujący ma stałą kontrolę nad obiektem oceny i stara się rozszerzyć kontrolę poprzez podniesienie uprawnień na obiekcie oceny lub propagację do innego obiektu oceny Przykłady: przejęcie lub kradzież uprawnień administratora; wykorzystanie hasła administratora przez nieupoważnioną osobę; zmiana konfiguracji zabezpieczeń i/lub wyłączenie funkcji audytu; autoryzowani użytkownicy uzyskują dostęp do zasobów, których nie potrzebują do wykonywania pracy; proces lub program uruchamiany jako główny jest zagrożony lub przejęty.	1) Przeciwdziałanie eskalacji uprawnień lub propagacji dostępu do innych zasobów. Przykłady: ograniczanie uprawnień dla kont, programów i procesów; wdrażanie i przestrzeganie procesów kontroli zmian w konfiguracji; stosowanie tokenów sprzętowych lub uwierzytelniania wieloskładnikowego dla działań uprzywilejowanych; ograniczanie fizycznego dostępu do serwerowni. 2) Wykrywanie działań zmierzających do eskalacji lub propagacji, reagowanie i odzyskiwanie. Przykłady: wykorzystanie narzędzi systemu wykrywania włamań (*ang. Intrusion Detection System – IDS*); przeglądanie dzienników audytów i zdarzeń.
6) Osiągnięcie celu ataku.	Atakujący osiąga swój cel. Utrata poufności, integralności lub dostępności danych lub zdolności systemu. Przykłady: eksfiltracja plików; modyfikacja wpisów w bazie danych; udany atak DDoS; usunięcie pliku lub aplikacji; odmowa świadczenia usługi;	1) Minimalizacja skutków udanego ataku. Przykłady: wykorzystanie narzędzi do zapobiegania utracie danych; szyfrowanie laptopów i nośników; filtrowanie granic zewnętrznych; edukowanie użytkowników w zakresie ochrony informacji krytycznych; ograniczanie dostępu do informacji i zasobów

Etap ataku	Działanie atakującego	Działanie obrońcy
	ujawnienie danych osobowych.	krytycznych; szyfrowanie plików i operacji (np. poczty elektronicznej); szyfrowanie łączy/VPN. 2) Wykrywanie skutków udanego ataku, reagowanie i odzyskiwanie. Przykładowe metody: wykorzystanie narzędzi do audytu i zapobiegania zagrożeniom wewnętrznym; narzędzia do analizy i badania zdarzeń sieciowych.

[a)] W całej treści publikacji NISTIR 8011 termin *użytkownik* może oznaczać osobę, proces lub urządzenie, w zależności od kontekstu.

Uwaga do tabeli 2: Działania obrońcy (tj. środki bezpieczeństwa) to w większości zabezpieczenia bazowe opisane w publikacji NSC 800-53B, a zatem mogą być już wdrożone. Tabela ta nie ma na celu zasugerowania potrzeby wdrożenia środków bezpieczeństwa, które nie zostały dobrane jako zabezpieczenia bazowe, ale po prostu ma pomóc w powiązaniu środków bezpieczeństwa z przykładowymi etapami ataku.

3.3 *Zdolności do ochrony*

Z uwagi na fakt, że środki bezpieczeństwa współdziałają ze sobą w celu osiągnięcia określonych rezultatów, przyjęta została poniższa definicja zdolności do ochrony.

Zdolność do ochrony to połączenie wzajemnie wzmacniających się środków bezpieczeństwa (tj. zabezpieczeń i środków zaradczych) wdrażanych za pomocą środków technicznych (tj. funkcjonalności sprzętu, aplikacji i oprogramowania układowego), fizycznych (tj. urządzeń fizycznych i środków ochronnych) oraz proceduralnych (tj. procedur wykonywanych przez personel). Zdolności takie są zwykle wyznaczane w celu osiągnięcia wspólnego celu związanego z bezpieczeństwem informacji.

3.3.1 *Kategorie środków bezpieczeństwa z publikacji NSC 800-53 a zdolności do ochrony*

Środki niezbędne do wsparcia danej zdolności mogą pochodzić z więcej niż jednej kategorii opisanej w publikacji NSC 800-53. Często zdarza się, że jeden środek bezpieczeństwa jest elementem wielu zdolności do ochrony. Kategorie środków bezpieczeństwa nie mają stanowić zdolności do ochrony. Są to raczej ogólne kategorie używane do logicznego grupowania poszczególnych środków bezpieczeństwa w ramach katalogu środków.

Kategorie środków bezpieczeństwa zostały opracowane w taki sposób, że każdy ze środków znajduje się tylko w jednej z nich. Pojedynczy środek bezpieczeństwa może być jednak elementem wielu zdolności do ochrony. Sprawia to, że kategorie środków bezpieczeństwa nie są wykorzystywane jako zdolności do ochrony.

3.3.2 *Domeny automatyki zabezpieczeń z publikacji NSC 800-137 a zdolności do ochrony*

W załączniku do publikacji NSC 800-137 zdefiniowano zestaw domen automatyki zabezpieczeń[17] jako „obszar bezpieczeństwa informacji, który obejmuje grupę narzędzi, technologii i danych”[18]. Domeny automatyki zabezpieczeń nie są analogiczne do zdolności do ochrony, ponieważ nie są zbiorem środków bezpieczeństwa służących wspólnemu celowi.

3.3.3 *Wykorzystanie zdolności do ochrony w ocenie środków bezpieczeństwa*

Termin *zdolność do ochrony* został zdefiniowany w publikacji NSC 800-53, jednak nie określono w niej szczegółowych zdolności, co umożliwia organizacjom ich zdefiniowanie zgodnie z celami ochrony. W kolejnym podrozdziale zdefiniowano stosowane tu zdolności do ochrony jako zdolności ISCM. Zdolności ISCM opisują cele wszystkich środków bezpieczeństwa z publikacji NSC 800-53, wybranych w ramach zabezpieczeń bazowych o niskim i wysokim poziomie wpływu[19].

[17] NSC 800-137.

[18] *Tamże.*

[19] NSC 800-53B.

3.3.4 *Zdolności do ochrony a strategia ISCM*

Aby ułatwić wdrożenie zautomatyzowanych ocen środków bezpieczeństwa, w programie ISCM określa się konkretne zdolności do ochrony, aby pokierować wdrożeniem i skoncentrować je na określonych celach. Każda zdolność ma jasno określony skutek, dzięki czemu działania oceniające mogą dostarczać lepszych informacji dotyczących analizy ryzyka i reagowania na nie.

Zdolność do ochrony ISCM składa się ze środków bezpieczeństwa z publikacji NSC 800-53 niezbędnych do osiągnięcia celu tej zdolności. Zdolność ISCM ma następujące dodatkowe cechy:

- Cel (pożądany rezultat) każdej zdolności to przeciwdziałanie określonym rodzajom scenariuszy ataków lub wykorzystaniu podatności.
- Każda zdolność skupia się na atakach na określone *obiekty oceny*.
- Istnieje realny sposób na zautomatyzowanie oceny wielu środków bezpieczeństwa, składających się na zdolność do ochrony.

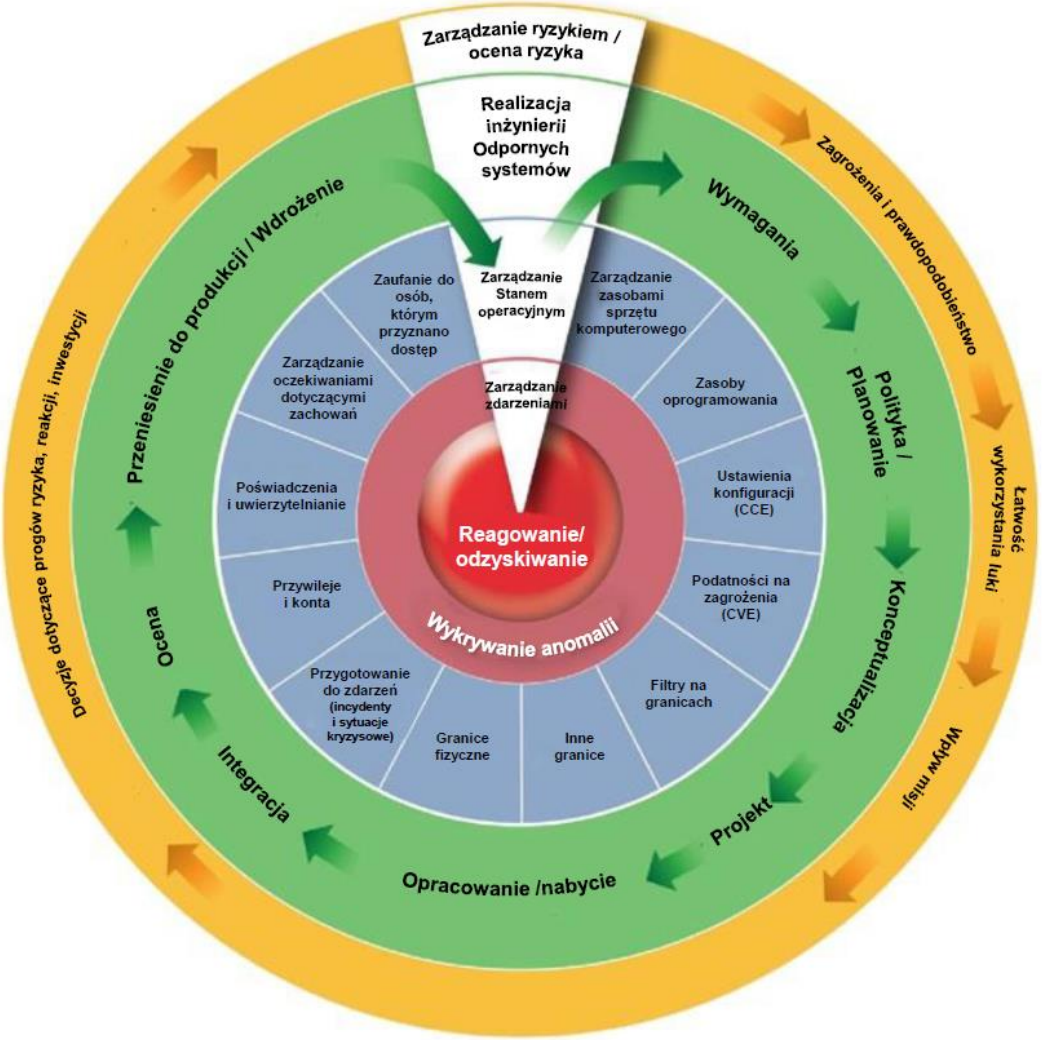
Kompleksowy zestaw zdolności do ochrony, opisany w podrozdziale 3.3.5, zapewnia zabezpieczenie przed aktualnymi i niebezpiecznymi scenariuszami ataków/ próbami wykorzystania podatności, a zatem obejmuje wszystkie bazowe zabezpieczenia o wysokim poziomie wpływu z publikacji NSC 800-53B.

Należy zauważyć, że kiedy organizacje wdrażają środki bezpieczeństwa, które nie zostały określone w publikacji NSC 800-53B jako zabezpieczenia bazowe o wysokim poziomie wpływu (czyli dostosowują je lub uzupełniają), ważne jest, aby wszelkie takie dodatkowe środki były również oceniane z odpowiednią częstotliwością (określoną w strategii ISCM organizacji). W razie potrzeby do istniejących zdolności można dodać dodatkowe zabezpieczenia lub utworzyć nowe zdolności.

W miarę pojawiania się zupełnie nowych scenariuszy ataków/ prób wykorzystania podatności, może być konieczne rozszerzenie zestawu zdolności do ochrony.

3.3.5 *Lista i definicje przykładowych zdolności do ochrony*

W publikacji NISTIR 8011 przedstawiono zestaw zdolności do ochrony obejmujący zabezpieczenia bazowe o wysokim poziomie wpływu z publikacji NSC 800-53B oraz skutecznie ukazujący interakcje pomiędzy różnymi zdolnościami do ochrony. Rysunek 3: *Zdolności do ochrony ISCM*, to schemat ukazujący zdolności do ochrony wykorzystane w tym dokumencie. Opisy w tabeli 3: *Zdolności do ochrony ISCM*, zawierają informacje na temat każdej zdolności przedstawionej na rysunku 3. Ponieważ w programie CDM DHS określono podobne, ale nie dokładnie takie same zdolności do ochrony (można je znaleźć na ich stronie internetowej), różnice między tymi dwoma zestawami zdolności zostały odnotowane w przypisach do tabeli 3.



Rysunek 3: Zdolności do ochrony ISCM

Tabela 3: Zdolności do ochrony ISCM

Pierścień 1: Zarządzanie ryzykiem i jego ocena (żółty pierścień plus klin przechodzący przez wszystkie pozostałe pierścienie na rysunku 3)
Zarządzanie ryzykiem (i jego ocena) jest ogólnym celem strategii ISCM i jest oparte na wszystkich wewnętrznych pierścieniach, tj. wszystkich innych zdolnościach ISCM.

Nazwa zdolności do ochrony	Cel (pożądany rezultat)	Uwagi
Zarządzanie ryzykiem i jego ocena (RISK)	Zmniejszenie liczby przypadków znaczącego wykorzystania podatności, które mogą mieć miejsce w innych zdolnościach, ponieważ w procesie zarządzania ryzykiem nie udało się prawidłowo zidentyfikować i ustalić priorytetów działań i inwestycji niezbędnych do obniżenia profilu ryzyka.	Należy dążyć do tego, aby pulpity ISCM zapewniały ocenę i metrykę dojrzałości dla każdej zdolności w celu ustalenia priorytetów reagowania na ryzyko nie tylko na poziomie operacyjnym (administracja systemem) i taktycznym (rola SSO), ale także na poziomie strategicznym (role: CISO, CIO, CEO)

Pierścień 2: Realizacja inżynierii odpornych systemów[a)] (zielony pierścień na rysunku 3)
Inżynieria odporności systemów koncentruje się na zastosowaniu ogólnego procesu inżynierii systemów do kształtowania ich odporności. Inżynieria systemów jest stosowana we wszystkich wewnętrznych pierścieniach koła. Czerpie informacje z zarządzania ryzykiem i jego oceny oraz z wniosków wyciągniętych z realizacji strategii ISCM w wewnętrznych pierścieniach koła. Etapy inżynierii systemów mogą być dostosowane na wiele sposobów i mogą być wykonywane w sposób zwinny (ang. *agile*) lub (*ang. spiral*) spiralny. Opisy na rysunku

2 mają charakter poglądowy, a nie normatywny. Więcej wskazówek dotyczących inżynierii odporności systemów i skutecznych działań można znaleźć w publikacji NIST SP 800-160.

Wyniki zastosowania inżynierii systemów powinny być wstępnie ocenione poza programem ISCM, zanim trafią do eksploatacji. Dlatego niniejsza publikacja nie zawiera wytycznych dotyczących zautomatyzowanej oceny faz inżynierii systemów, poza tym, co można zaadaptować z testów operacyjnych innych zdolności.

Nazwa zdolności do ochrony	**Cel (pożądany rezultat)**	**Uwagi**
Realizacja inżynierii odpornych systemów (SE)[20]	Ograniczenie udanych prób wykorzystania podatności, które występują w zdolnościach z niebieskiego i czerwonego pierścienia, ponieważ niewłaściwie określono politykę, wymagania, plany lub inne kwestie związane z zarządzaniem podczas projektowania, wdrażania i/lub monitorowania środków bezpieczeństwa w ramach danej zdolności.	Wymagania i polityka są udokumentowane w specyfikacji stanu pożądanego dla każdej z pozostałych zdolności. Jeśli powtarzają się udane próby wykorzystania podatności, można wprowadzić dodatkowe środki w celu ich zablokowania poprzez bardziej kompleksowe wymagania, politykę i planowanie. Monitorowanie zabezpieczeń, które składają się na zdolności z niebieskiego i czerwonego pierścienia, umożliwia ujawnienie udanych prób

[20] Definicja: patrz Załącznik B.

Nazwa zdolności do ochrony	Cel (pożądany rezultat)	Uwagi
		wykorzystania podatności. Analiza przyczyn źródłowych może umożliwić ustalenie, czy próby wykorzystania podatności na etapie projektu przedoperacyjnego w cyklu życia systemu wynikają z defektów.

Pierścień 3: Zarządzanie stanem operacyjnym (niebieski pierścień na rysunku 3)
Zdolności do ochrony w pierścieniu 3 mogą być w dużej mierze oceniane za pomocą środków automatycznych i zapewniają podstawową ochronę informacji i systemów w fazie eksploatacji i utrzymania SDLC. Pełnią one również funkcję identyfikowania systemowych problemów w działaniu, które mogą zostać naprawione dzięki ulepszonej inżynierii.

Nazwa zdolności do ochrony	Cel (pożądany rezultat)	Uwagi
Zarządzanie zasobami sprzętu komputerowego (*ang. Hardware Asset Management - HWAM*)	Zapewnienie, że nieautoryzowane i niekontrolowane urządzenia są identyfikowane, aby umożliwić organizacji zapobieganie ich użyciu przez atakujących jako platformy, z której można naruszyć bezpieczeństwo systemów.	Prowadzenie ewidencji (np. listy)[b)] autoryzowanego sprzętu i osób nim zarządzających. Traktowanie innego ujawnionego sprzętu w ramach oceny jako defektu.

Nazwa zdolności do ochrony	**Cel (pożądany rezultat)**	**Uwagi**
Zarządzanie zasobami oprogramowania (*ang. Software Asset Management - SWAM*)	Zapewnienie, że nieautoryzowane oprogramowanie jest identyfikowane, aby zapobiec jego wykorzystaniu przez atakujących jako platformy, z której można naruszyć bezpieczeństwo systemów.	Prowadzenie ewidencji (np. listy)[b)] autoryzowanego oprogramowania zarówno na poziomie produktów[c)], jak i plików wykonywalnych. Traktowanie innego ujawnionego oprogramowania w ramach oceny jako defektu.
Zarządzanie ustawieniami konfiguracyjnymi (*ang. Configuration Settings Management - CSM*)	Zapewnienie, że powszechne bezpieczne konfiguracje (*ang. Common Configuration Enumeration – CCE*) zostały określone i są stosowane w celu uniemożliwienia atakującym naruszenia bezpieczeństwa systemu lub urządzenia, które z kolei może być wykorzystane jako platforma do ataku na inne systemy lub urządzenia.	Prowadzenie rejestru autoryzowanych ustawień. Traktowanie odstępstw od nich wykrytych w ramach oceny jako defektów.
Zarządzanie poprawkami podatności (*ang. Vulnerability (Patch) Management* - VULN)	Zapewnienie, że podatności oprogramowania i sprzętu (*ang. Common Vulnerabilities and Exposures – CVE*) są identyfikowane i naprawiane w celu uniemożliwienia atakującym naruszenia bezpieczeństwa systemu lub urządzenia, które z kolei może być wykorzystane do ataku na inne systemy lub urządzenia.	Krajowa baza danych dotyczących podatności na zagrożenia (*ang. National Vulnerability Database – NVD*) zawiera bibliotekę podatności przypisanych do podatnego oprogramowania. Reakcje mogą obejmować

Nazwa zdolności do ochrony	Cel (pożądany rezultat)	Uwagi
		zastosowanie poprawek, zainstalowanie bardziej bezpiecznych wersji lub zaakceptowanie ryzyka. Narzędzia skanujące powszechne enumeracje słabości (*ang. Common Weakness Enumeration – CWE*) mogą zidentyfikować złe praktyki programowania, które są bezpośrednio związane z warunkami, które często objawiają się jako luki wykrywane i przypisywane CVE.
Zarządzanie zaufaniem do osób z przyznanym dostępem (*ang. Manage Trust for Persons Granted Access - TRUST*)	Zapewnienie, że osobom nieupoważnionym/niesprawdzonym nie powierza się dostępu do systemu.	Monitorowanie realizacji procesów kontroli personelu (takich jak wydawanie zezwoleń, sprawdzanie przeszłości, kontrole danych osobowych itp.) mających na celu identyfikację dowodów braku wiarygodności.

Nazwa zdolności do ochrony	**Cel (pożądany rezultat)**	**Uwagi**
Zarządzanie oczekiwaniami dotyczącymi zachowań (*ang. Manage Behavioral Expectations - BEHAVE*)	Zapewnienie, że autoryzowani użytkownicy w trakcie wykonywania swoich obowiązków są świadomi oczekiwanych zachowań związanych z bezpieczeństwem i rozumieją, jak unikać i/lub zapobiegać celowym i nieumyślnym zachowaniom, które mogą narazić bezpieczeństwo informacji.	Zbieranie dowodów (takich jak szkolenia, zasady zachowania/ umowy o dostępie i użytkowaniu, certyfikaty dotyczące kursów i umiejętności itp.) mających na celu określenie i umożliwienie bezpiecznego zachowania.
Zarządzanie poświadczeniami i uwierzytelnianiem (*ang. Manage Credentials and Authentication - CRED*)	Zapewnienie, że autoryzowani użytkownicy posiadają poświadczenia i metody uwierzytelniania niezbędne do wykonywania swoich obowiązków, przy jednoczesnym ograniczeniu dostępu tylko do tych zasobów, które są im niezbędne.	Konieczne poświadczenia i metody uwierzytelniania należy wywnioskować na podstawie ról przypisanych użytkownikom i sprawdzić, czy nie zostały zapewnione żadne dodatkowe poświadczenia/metody.
Zarządzanie przywilejami i kontami (*ang. Manage Privileges and Accounts - PRIV*)	Zapewnienie, że autoryzowani użytkownicy mają przywileje niezbędne do wykonywania swoich obowiązków; dostęp jest ograniczony tylko do tych zasobów, które są im niezbędne.	Konieczne przywileje należy wywnioskować na podstawie ról przypisanych użytkownikom i sprawdzić, czy nie zostały zapewnione żadne dodatkowe przywileje.

Nazwa zdolności do ochrony	**Cel (pożądany rezultat)**	**Uwagi**
Zarządzanie fizycznymi granicami[c)] (*ang. Manage Physical Boundaries - BOUND-P*)	Zapewnienie, że ruch (osób, nośników, sprzętu itp.) do i z obiektu fizycznego nie zagraża bezpieczeństwu.	Należy ograniczyć i monitorować dostęp fizyczny przy użyciu zautomatyzowanych narzędzi i modułów zbierających dane, które umożliwiają śledzenie i kontrolowanie ruchu.
Zarządzanie granicami sieci informatycznej[d)] (*ang. Manage Network Boundaries - BOUND-N*)	Zapewnienie, że ruch do i z sieci (a więc poza zasięgiem ochrony fizycznej obiektu) nie narusza bezpieczeństwa. To samo dotyczy enklaw wydzielonych w ramach sieci.	Należy skonfigurować bezpieczny przepływ informacji i inne zabezpieczenia granic dotyczące ruchu w celu monitorowania i kontrolowania wewnętrznych i zewnętrznych granic sieci.
Zarządzanie pozostałymi granicami[c)] (*ang. Manage Other Boundaries - BOUND-O*)	Zapewnienie, że poufność i integralność informacji są chronione w trakcie ich tranzytu i przechowywania. Jest to szczególnie ważne, gdy informacje są narażone na ujawnienie (np. podczas przesyłania przez Internet lub łącze bezprzewodowe) lub znajdują się na sprzęcie, który może znajdować się poza bezpiecznym miejscem (np. w laptopie lub urządzeniu przenośnym). Szyfrowanie jest najczęściej stosowaną techniką ochrony poufności i integralności informacji.	Należy zadbać, aby środki bezpieczeństwa na granicach, które nie są związane z granicami fizycznymi i sieciowymi (np. szyfrowanie ruchu sieciowego, szyfrowanie przechowywanych danych oraz zarządzanie pasmem radiowym) zapewniały poziom bezpieczeństwa odpowiedni do ochrony danych w ruchu i podczas przechowywania.

Nazwa zdolności do ochrony	**Cel (pożądany rezultat)**	**Uwagi**
Zarządzanie przygotowaniem do zdarzeń (incydentów i sytuacji kryzysowych) (*ang. Manage Preparation for Events (Incidents and Contingencies) - PREP*)	Zapewnienie procedur i zasobów umożliwiających reagowanie zarówno na rutynowe, jak i nieoczekiwane zdarzenia, które mogą zagrozić bezpieczeństwu. Potencjalne reakcje obejmują szeroki zakres możliwych działań, między innymi kontynuowanie operacji, odzyskiwanie i badania kryminalistyczne. Nieoczekiwane zdarzenia obejmują rzeczywiste ataki i klęski żywiołowe, takie jak powodzie, trzęsienia ziemi, tsunami itp.	Należy określić pożądane przygotowania (np. dodatkowe zasoby, kopie zapasowe, zasilacze bezprzerwowe, generatory, zapasowe centra danych, dodatkowe miejsca pracy) i sprawdzić, czy przygotowania te zostały zrealizowane i czy działają zgodnie z przeznaczeniem.

Pierścień 4: Zarządzanie zdarzeniami nietypowymi (czerwony pierścień na rysunku 3)
Niezależnie od wszelkich starań w zakresie wdrażania zdolności z otaczających pierścieni zarządzania ryzykiem i jego oceny, inżynierii odpornych systemów oraz zarządzania stanem operacyjnym, nadal istnieje prawdopodobieństwo, że pewne udane ataki oraz szkodliwe zdarzenia będą miały negatywny wpływ na system. Zdolności do ochrony w pierścieniu 4 mają na celu wykrywanie takich zdarzeń i dostarczanie informacji koniecznych do reagowania na nie. Działania w zakresie wykrywania i reagowania muszą odnosić się do poszczególnych sekcji niebieskiego pierścienia. Oznacza to, że nietypowe zdarzenia mogą pojawić się w ramach każdej ze zdolności z niebieskiego pierścienia. W rzeczywistości większość ataków lub sytuacji awaryjnych dotyczy wielu zdolności związanych ze stanem operacyjnym i/ lub zachowaniem obiektów oceny objętych zdolnościami z niebieskiego pierścienia.

Nazwa zdolności do ochrony	**Cel (pożądany rezultat)**	**Uwagi**
Zarządzanie wykrywaniem zdarzeń nietypowych (*ang. Manage Anomalous Event Detection - DETECT*)	Zapewnienie, że rutynowe i nieoczekiwane zdarzenia, które zagrażają bezpieczeństwu, mogą być zidentyfikowane w określonych ramach czasowych, tak aby ich wpływ został ograniczony w jak największym stopniu.	Należy stosować różne metody korelacji zapisów audytu, zdarzeń systemowych, logów IDPS itp. oraz monitorować wzorce w celu zidentyfikowania nieoczekiwanych wzorców lub wskaźników szkodliwych działań. Należy wyznaczyć pożądane wartości progowe wpływu (np. serwery nigdy nie mogą być wyłączone na dłużej niż 24 godziny) i wykrywać, gdy wartości progowe nie są przestrzegane.
Zarządzanie reagowaniem na zdarzenia nietypowe i usuwaniem ich skutków (*ang. Manage Anomalous Event Response and Recovery - RESPOND*)	Zapewnienie, że rutynowe i nieoczekiwane zdarzenia, które wymagają reakcji w celu utrzymania funkcjonalności i bezpieczeństwa, spotykają się z reakcją (po ich zidentyfikowaniu) w określonych ramach czasowych, tak aby ograniczyć ich wpływ w jak największym stopniu.	Należy wdrożyć odpowiednie procedury reagowania i sprawdzić, czy działają one zgodnie z założeniami.

[a] W programie CDM DHS niektóre zdolności zostały nazwane nieco inaczej niż w publikacji NISTIR 8011, a mianowicie: a) projektowanie i wdrażanie w wymaganiach, polityce i planowaniu; b) projektowanie i wdrażanie jakości; c) zarządzanie informacjami z audytu; oraz d) zarządzanie bezpieczeństwem operacyjnym. W niniejszej publikacji uwzględniono: a) i b) w inżynierii systemów (zielony pierścień); c) w zarządzaniu zdarzeniami – wykrywanie anomalii (czerwony pierścień); oraz d) w zarządzaniu stanem operacyjnym (jako część ogólnego niebieskiego pierścienia).

[b] Wykazy HWAM/SWAM mogą mieć dowolny format nadający się do odczytu maszynowego. Mogą one być prowadzone w sposób ręczny lub zautomatyzowany, w zależności od potrzeb organizacji.

[c] Definicja produktu będącego oprogramowaniem obejmuje jego wersję, wydanie, poziom poprawek i inne wyróżniki.

[d] Trzy wyszczególnione tu zdolności związane z granicami (fizycznymi, filtrami, pozostałymi) zostały potraktowane jako jedna zdolność w programie CDM. Zostały one rozdzielone w oparciu o bardziej szczegółową ocenę odpowiadających im środków bezpieczeństwa.

3.3.6 *Wymogi dotyczące śledzenia: Powiązanie zdolności z etapami ataku*

Każdy tom niniejszej publikacji, poświęcony konkretnym zdolnościom, zawiera bardziej szczegółowy opis sposobu, w jaki zdolności te odpowiadają etapom ataku opisanym w rozdziale 3.2, Etapy ataku. Na przykład tom poświęcony HWAM zawiera tabelę 4: *Powiązanie zdolności HWAM z blokowaniem etapów ataku*, w której pokazano, jak cel zdolności służy blokowaniu lub opóźnianiu powodzenia określonych etapów ataku istotnych dla HWAM.

Tabela 4: Powiązanie zdolności HWAM z blokowaniem etapów ataku

Nazwa etapu ataku	Cel etapu ataku	Przykłady wpływu HWAM
2) Zainicjowanie ataku wewnątrz sieci.	Atakujący znajduje się w granicach sieci i inicjuje atak na jakiś wewnętrzny obiekt oceny. Przykłady:	Blokowanie lub ograniczanie dostępu wewnątrz: Zapobieganie lub

Nazwa etapu ataku	Cel etapu ataku	Przykłady wpływu HWAM
	Użytkownik otwiera wiadomość e-mail ze spersonalizowaną próbą wyłudzenia informacji lub klika załącznik; zgubienie lub kradzież laptopa; użytkownik instaluje nieautoryzowane oprogramowanie lub sprzęt; nieautoryzowany personel uzyskuje fizyczny dostęp do obiektu o ograniczonym dostępie.	minimalizowanie dostępu do zaufanych zasobów sieciowych przez potencjalnie nieautoryzowane/zainfekowane urządzenia. Ograniczenie czasu obecności nieautoryzowanych urządzeń przed ich wykryciem.
3) Uzyskanie punktu zaczepienia.	Atakujący uzyskał dostęp do obiektu oceny i pokonał zabezpieczenia w takim stopniu, aby zdobyć punkt zaczepienia, ale bez możliwości utrzymania się. Przykłady: Nieautoryzowanemu użytkownikowi udaje się zalogować przy użyciu autoryzowanych danych uwierzytelniających; kod wykorzystujący luki przeglądarki zostaje pomyślnie wykonany w pamięci i inicjuje połączenie zwrotne; osoba uzyskuje nieautoryzowany dostęp do serwerowni.	Zablokowanie punktu zaczepienia: Zmniejszenie liczby nieautoryzowanych i/lub łatwych do zainfekowania urządzeń, które nie są aktywnie administrowane.
6) Osiągnięcie celu ataku.	Atakujący osiąga swój cel. Utrata poufności, integralności lub dostępności danych albo możliwości systemu. Przykłady: eksfiltracja plików;	Zablokowanie fizycznej eksfiltracji: Zapobieganie lub minimalizowanie kopiowania informacji na nieautoryzowane urządzenia.

Nazwa etapu ataku	Cel etapu ataku	Przykłady wpływu HWAM
	modyfikacja wpisów w bazie danych; usunięcie pliku lub aplikacji; odmowa świadczenia usługi (DoS); ujawnienie danych osobowych.	

3.4 *Zdolności do ochrony definiowane przez organizację*

Zdolności do ochrony opisane w niniejszej publikacji nie stanowią ostatecznego zestawu takich zdolności. Zdefiniowane zdolności w żaden sposób nie ograniczają możliwości organizacji w zakresie definiowania innych lub dodatkowych zdolności do ochrony.

Organizacje mogą dokonywać rewizji istniejących lub definiować nowe zdolności/ składniki zdolności bezpieczeństwa, a następnie realizować ogólny model automatycznej oceny środków bezpieczeństwa opisany w niniejszej publikacji na poziomie organizacji. Należy jednak pamiętać, że wymagałoby to opracowania kompleksowego podejścia do zautomatyzowanej oceny środków bezpieczeństwa specyficznego dla danej organizacji oraz planu uwzględniającego stworzone przez nią zdolności. Zaleca się, aby organizacje zautomatyzowały swoje podejście do oceny środków bezpieczeństwa, początkowo korzystając z funkcjonalnych zdolności do ochrony, aby zdobyć doświadczenie, a następnie zdecydować w późniejszym czasie, czy takie dostosowanie jest konieczne.

3.5 *Składniki zdolności*

Zdolności składają się ze składników zdolności.

Kluczową cechą zdefiniowanych w tej publikacji składników zdolności jest to, że zostały one opracowane w taki sposób, aby można je było testować za pomocą środków automatycznych. W niniejszej publikacji dla każdego składnika zdolności określono jedną *kontrolę defektu*, która jest wykorzystywana do oceny, czy cel tego składnika jest spełniany, co z kolei przyczynia się do ogólnego określenia skuteczności programu bezpieczeństwa (elementów zabezpieczeń, zabezpieczeń, składników zdolności i zdolności do ochrony)[21].

[21] Odnalezienie defektów elementów środków bezpieczeństwa może wymagać analizy przyczyn źródłowych, jak opisano w rozdziale 8.2, Analiza przyczyn źródłowych.

Na przykład, zdolność HWAM związana z usuwaniem sprzętu wysokiego ryzyka może mieć składniki związane z:

- usuwaniem nieautoryzowanego sprzętu;
- zapewnieniem zarządzania całym sprzętem; oraz
- potwierdzeniem, że łańcuch dostaw sprzętu jest bezpieczny.

W przypadku HWAM, takie składniki zdolności wspierają realizację szerszego celu, jakim jest wyeliminowanie podatności sprzętu wysokiego ryzyka, ponieważ urządzenia nieautoryzowane, niezarządzane oraz urządzenia o niezatwierdzonych łańcuchach dostaw zwiększają ryzyko dla organizacji.

W tomach publikacji NISTIR 8011 poświęconych konkretnym zdolnościom, w ramach każdej szerszej zdolności zidentyfikowano składniki, aby zilustrować sposób, w jaki elementy środków w ramach zdolności współdziałają ze sobą w celu osiągnięcia jej ogólnego celu.

Składniki zdolności do ochrony opisane w niniejszej publikacji nie stanowią ostatecznego zestawu takich składników. W żaden sposób nie ograniczają one możliwości organizacji w zakresie definiowania innych lub dodatkowych składników zdolności do ochrony.

Ponieważ składniki zdolności są definiowane w ramach poszczególnych zdolności, każdy z nich należy do dokładnie jednej (i tylko jednej) zdolności. Należy jednak pamiętać, że dla różnych zdolności często identyfikuje się *podobne* składniki.

3.5.1 *Przykłady składników zdolności do ochrony (w ramach HVAM)*

Jak opisano w *tabeli 4: Powiązanie zdolności HWAM z blokowaniem etapów ataku*, HWAM zapewnia wysoce skuteczną metodę blokowania lub opóźniania etapów ataku związanych z wykorzystaniem urządzeń. Po przyporządkowaniu odpowiednich środków bezpieczeństwa do tej zdolności (patrz *podrozdział 3.5.2, Powiązanie elementów środków bezpieczeństwa ze zdolnościami*), określono składniki zdolności, aby dokładniej zademonstrować, w jaki sposób środki HWAM współpracują ze sobą w celu osiągnięcia celów HWAM (patrz podrozdział 3.5.3, *Powiązanie elementów zabezpieczeń ze składnikami zdolności*). Podobne analizy przedstawiono w każdym tomie publikacji NISTIR 8011 poświęconych konkretnej zdolności. Tabela 5: *Wybrane przykłady składników zdolności (HWAM)*, zaczerpnięta

z tomu poświęconego zdolności HWAM, zawiera definicje przykładowych składników tej zdolności.

Tabela 5: Wybrane przykłady składników zdolności (HWAM)

Nazwa składnika zdolności	Identyfikator kontroli defektu	Cel składnika zdolności
Przeciwdziałanie stosowaniu nieautoryzowanych urządzeń.	HWAM-F01	Zapobieganie lub ograniczanie obecności nieautoryzowanych urządzeń, a tym samym zmniejszenie liczby urządzeń potencjalnie złośliwych lub stanowiących wysokie ryzyko.
Zmniejszenie liczby urządzeń bez przypisanego menedżera urządzeń.	HWAM-F02	Zapobieganie używaniu lub zmniejszenie liczby urządzeń bez przypisanego menedżera urządzeń w ramach granicy oceny, a tym samym zmniejszenie opóźnienia w łagodzeniu skutków wad urządzeń (w przypadku ich wykrycia).
Ograniczenie możliwości wykorzystania podatności urządzeń przed ich usunięciem, podczas użytkowania w innym miejscu i po zwrocie.	HWAM-L01	Zapobieganie wykorzystaniu podatności urządzeń przed ich usunięciem, podczas używania w innym miejscu i po zwrocie (lub innym mobilnym wykorzystaniu) poprzez a) wzmocnienie zabezpieczeń urządzenia przed usunięciem z przestrzeni chronionych; b) sprawdzenie pod kątem obecności danych organizacji przed usunięciem z przestrzeni chronionych; oraz c) sanityzacja urządzenia przed wprowadzeniem lub ponownym wprowadzeniem w granice oceny.
Ograniczenie zagrożenia wewnętrznego związanego	HWAM-L02	Wymaganie od wielu osób zgody na dodanie urządzenia do granicy autoryzacji (tj. stosowanie zasady rozdziału

Nazwa składnika zdolności	Identyfikator kontroli defektu	Cel składnika zdolności
z nieautoryzowanym urządzeniem.		obowiązków) w celu ograniczenia możliwości autoryzacji urządzeń przez jedną nieostrożną lub mającą złe zamiary osobę z organizacji. Uwaga 1: Organizacja może zdecydować się na zastosowanie ograniczeń dostępu w celu wymuszenia rozdziału obowiązków. W takim przypadku składnik byłby oceniany w ramach zdolności PRIV. To, co jest oceniane dla tego składnika, to fakt, że rozdział obowiązków ma miejsce. Uwaga 2: Odnośnie granicy autoryzacji, patrz HWAM-L11.
Ograniczenie podatności na ataki metodą DoS wynikającej z braku wymaganych urządzeń i/lub podzespołów urządzenia.	HWAM-L03	Zapobieganie lub ograniczenie liczby ataków metodą DoS i/lub ataków na odporność poprzez zapewnienie, że wszystkie wymagane urządzenia i określone przez organizację podzespoły urządzeń są obecne w granicy oceny.
Ograniczenie liczby nieautoryzowanych podzespołów urządzenia.	HWAM-L06	Wykrywanie i usuwanie nieautoryzowanych podzespołów urządzenia w celu wdrożenia zasady najmniejszej możliwej liczby funkcjonalności, aby zapobiec lub ograniczyć wprowadzanie podzespołów, które mogłyby umożliwić ataki.
Weryfikacja bieżącej potrzeby biznesowej obecności urządzenia.	HWAM-L07	Wymóg okresowej lub zależnej od wystąpienia zdarzenia weryfikacji, czy dane urządzenie jest nadal potrzebne do

Nazwa składnika zdolności	Identyfikator kontroli defektu	Cel składnika zdolności
		działania systemu w celu spełnienia wymagań misji (w ramach realizacji zasady najniższej funkcjonalności). Uwaga: Dobra praktyka nakazuje, aby menedżerowie urządzeń dokonywali przeglądu zarządzanych urządzeń, a właściciele systemów dokonywali przeglądu funkcjonalności urządzeń wymaganych w ramach granicy autoryzacji, jak również w odpowiednim czasie identyfikowali urządzenia nieobsługiwane lub o kończącym się okresie eksploatacji.
Zapewnienie zbierania wymaganych danych o urządzeniach.	HWAM-L08	Zapewnienie, że dane wymagane do oceny ryzyka są gromadzone. Takie dane mogą odnosić się do innego problemu niż defekt HWAM, ale mogą wymagać wygenerowania przez moduł zbierający dane HWAM. Na przykład urządzenia z pamięcią niewystarczającą do obsługi bazowego systemu operacyjnego, a także defensywne urządzenia zabezpieczające, mogą wymagać identyfikacji podczas zbierania danych, aby takie problemy mogły zostać wykryte jako defekty.

3.5.2 *Powiązanie składników zdolności do ochrony z etapami ataku*

Dzięki powiązaniu składników zdolności do ochrony z etapami ataku staje się jasne, w jaki sposób dana zdolność chroni przed określonym etapem ataku. Na przykład, każdy tom dotyczący konkretnej zdolności zawiera tabelę z podobnymi kolumnami jak tabela 5 powyżej, w której znajdują się tylko etapy ataku związane z danym składnikiem zdolności.

3.6 *Elementy zabezpieczeń*

W wielu przypadkach środki bezpieczeństwa z publikacji NSC 800-53 i NSC 800-53B obejmują wiele wymagań – zarówno w przypadku zabezpieczeń bazowych jak i rozszerzonych. Niektóre wymagania dotyczące środków mogą wspierać jedną zdolność ISCM lub zdolność zdefiniowaną przez organizację, podczas gdy inne wymagania dla tego samego środka mogą wspierać inną zdolność lub wiele zdolności.

W związku z tym, aby wyodrębnić wymagania dla celów planowania automatycznej oceny środków bezpieczeństwa, stosuje się pojęcie *elementu zabezpieczenia*.

Elementy zabezpieczeń są określone w następujący sposób:

1. **Każde zabezpieczenie bazowe** jest osobnym elementem zabezpieczenia (niezależnie od jego rozszerzeń). Jeżeli zabezpieczenia bazowego dotyczą wymagań cząstkowych oznaczonych w publikacji NSC 800-53, NSC 800-53B literami a), b), c) itd., to każde wymaganie cząstkowe jest również oddzielnym elementem zabezpieczenia.
2. **Każde zabezpieczenie rozszerzone** jest oddzielnym elementem zabezpieczenia (niezależnie od innych zabezpieczeń rozszerzonych i podstawowych). Tak jak w przypadku zabezpieczenia bazowego, jeśli dotyczą go wymagania cząstkowe oznaczone literami a), b), c) itd., to każde wymaganie cząstkowe jest również oddzielnym elementem zabezpieczenia.

Środki bezpieczeństwa z publikacji NSC 800-53, NSC 800-53B zostały podzielone na elementy zabezpieczeń, tak aby:

- każdy wymóg dotyczący środka mógł być testowany indywidualnie.
- uprościć określanie zdolności do ochrony.

Dzięki temu elementy zabezpieczeń są bardziej zbliżone do indywidualnych wymogów dla zabezpieczeń opisanych w publikacji NSC 800-53A, z tą różnicą, że zidentyfikowane tutaj elementy są w niektórych przypadkach dodatkowo podzielone w publikacji NSC 800-53A. W celu uzyskania informacji o odpowiednich elementach zabezpieczeń, należy zapoznać się z podrozdziałem 3.3 tomu poświęconemu danej zdolności.

3.6.1 *Powiązanie elementów zabezpieczeń z etapami ataku*

Składniki zdolności do ochrony są powiązane z etapami ataku i elementami zabezpieczeń. Umożliwia to stworzenie listy elementów zabezpieczeń, które są powiązane z etapami ataku (tj. elementów, które wspierają blokowanie lub opóźnianie etapu ataku). Przykład znajduje się w Tabeli 6*: Przykład powiązania elementów zabezpieczeń HWAM z etapami ataku*, w którym przedstawiono tylko jeden etap ataku i związane z nim elementy zabezpieczeń HWAM. Pełna lista elementów zabezpieczeń dla danej zdolności powiązanych z etapami ataku znajduje się w załączniku B do każdego tomu publikacji NISTIR 8011 poświęconego konkretnej zdolności.

Tabela 6: Przykład powiązania elementów zabezpieczeń HWAM z etapami ataku

Przykładowy etap ataku	**Sortowalny kod elementu zabezpieczenia**[a)]	**Kod elementu zabezpieczenia z publikacji NSC 800-53; NSC 800-53B**
2) Zainicjowanie ataku wewnątrz sieci.	AC-19-a	AC-19(a)
2) Zainicjowanie ataku wewnątrz sieci.	AC-19-b	AC-19(b)
2) Zainicjowanie ataku wewnątrz sieci.	AC-19-z-05-z	AC-19(5)
2) Zainicjowanie ataku wewnątrz sieci.	AC-20-z-02-z	AC-20(2)
2) Zainicjowanie ataku wewnątrz sieci.	CM-02-z-07-a	CM-2(7)(a)

Przykładowy etap ataku	**Sortowalny kod elementu zabezpieczenia**[a)]	**Kod elementu zabezpieczenia z publikacji NSC 800-53; NSC 800-53B**
2) Zainicjowanie ataku wewnątrz sieci.	CM-02-z-07-b	CM-2(7)(b)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-b	CM-3(b)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-c	CM-3(c)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-d	CM-3(d)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-f	CM-3(f)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-g	CM-3(g)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-z-01-a	CM-3(1)(a)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-z-01-b	CM-3(1)(b)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-z-01-c	CM-3(1)(c)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-z-01-d	CM-3(1)(d)
2) Zainicjowanie ataku wewnątrz sieci.	CM-03-z-01-f	CM-3(1)(f)
2) Zainicjowanie ataku wewnątrz sieci.	CM-08-a	CM-8(a)

Przykładowy etap ataku	**Sortowalny kod elementu zabezpieczenia**[a)]	**Kod elementu zabezpieczenia z publikacji NSC 800-53; NSC 800-53B**
2) Zainicjowanie ataku wewnątrz sieci.	CM-08-b	CM-8(b)
2) Zainicjowanie ataku wewnątrz sieci.	CM-08-z-01-z	CM-8(1)
2) Zainicjowanie ataku wewnątrz sieci.	CM-08-z-03-b	CM-8(3)(b)
2) Zainicjowanie ataku wewnątrz sieci.	MA-03-z-01-z	MA-3(1)
2) Zainicjowanie ataku wewnątrz sieci.	MA-03-z-03-a	MA-3(3)(a)
2) Zainicjowanie ataku wewnątrz sieci.	MA-03-z-03-b	MA-3(3)(b)
2) Zainicjowanie ataku wewnątrz sieci.	MP-07-z-01-z	MP-7(1)
2) Zainicjowanie ataku wewnątrz sieci.	PS-04-d	PS-4(d)
2) Zainicjowanie ataku wewnątrz sieci.	SC-15-a	SC-15(a)

a) Sortowalny kod elementu zabezpieczenia jest używany do zarządzania i sortowania elementów zabezpieczenia w bazie danych. Jest on zawsze podawany wraz z powiązanym kodem elementu zabezpieczenia z publikacji NSC 800-53, NSC 800-53B.

3.6.2 *Powiązanie elementów zabezpieczeń ze zdolnościami do ochrony*

Przy definiowaniu poszczególnych elementów zabezpieczeń w publikacji NSC 800-53, NSC 800-53B opracowano reguły wyszukiwania za pomocą słów kluczowych, które zostały wykorzystane do automatycznego przyporządkowania elementów zabezpieczeń do zdolności. W celu walidacji przyporządkowania reguł słów kluczowych zastosowano

systematyczny proces – testowanie pod kątem pominiętych elementów zabezpieczeń oraz ocenę wyników fałszywie pozytywnych i fałszywie negatywnych.

Tabela 7: *Przykładowe reguły słów kluczowych umożliwiające powiązanie ze zdolnościami*, zawiera dwa przykłady reguł słów kluczowych wykorzystywanych do przyporządkowywania elementów zabezpieczeń do zdolności.

Tabela 7: Przykładowe reguły słów kluczowych umożliwiające powiązanie ze zdolnościami

Element zabezpieczenia jest powiązany ze zdolnością zarządzania zasobami sprzętowymi (HWAM), jeżeli spełniony jest jeden lub więcej z poniższych warunków:
Zawiera słowo „magazyn”
Zawiera słowo „łańcuch dostaw”, ale NIE „monitoring”
.... Oraz wiele innych warunków...

3.6.3 *Powiązanie elementów zabezpieczeń ze składnikami zdolności do ochrony*

Każdy tom publikacji NISTIR 8011 jest poświęcony konkretnej zdolności. W każdym tomie udokumentowano zarówno (1) zasady wyszukiwania według słów kluczowych stosowane (przez odniesienie) do przeszukiwania tekstów środków bezpieczeństwa i identyfikacji zabezpieczeń/ elementów zabezpieczeń, które wspierają zdolność; jak i (2) wykaz zabezpieczeń/ elementów zabezpieczeń. Dzięki temu nie ma potrzeby, aby organizacje powtarzały prace związane z przyporządkowywaniem, jeśli stosują zdefiniowane zdolności. Reguły wyszukiwania według słów kluczowych znajdują się w załączniku B do każdego z tomów dotyczących zdolności (tomy od 2 do 13). Jeśli jednak organizacja zdecyduje się na opracowanie nowych zdolności lub zmieni zdefiniowane tu zdolności, mogą być konieczne dodatkowe prace nad przyporządkowywaniem.

W tabeli 8: *Przykład powiązania elementów zabezpieczeń ze zdolnością HWAM* zawiera przykładowe elementy zabezpieczeń, które można powiązać ze zdolnością HWAM.

Tabela 8: Przykład powiązania elementów zabezpieczeń ze zdolnością HWAM

Zdolność do ochrony	Poziom zabezpieczeń bazowych	Sortowalny kod elementu zabezpieczenia	Kod elementu zabezpieczenia z publikacji NSC 800-53; NSC 800-53B
HWAM	Niski	AC-19-a	AC-19(a)
HWAM	Niski	CM-08-b	CM-8(b)
HWAM	Niski	PS-04-d	PS-4(d)
HWAM	Niski	SC-15-b	SC-15(b)
HWAM	Umiarkowany	AC-19-z-05-z	AC-19(5)
HWAM	Umiarkowany	CM-02-z-07-a	CM-2(7)(a)
HWAM	Umiarkowany	CM-03-a	CM-3(a)
HWAM	Umiarkowany	CM-03-d	CM-3(d)
HWAM	Umiarkowany	CM-08-z-03-b	CM-8(3)(b)
HWAM	Umiarkowany	MA-03-z-01-z	MA-3(1)
HWAM	Umiarkowany	MP-07-z-01-z	MP-7(1)
HWAM	Wysoki	CM-03-z-01-a	CM-3(1)(a)
HWAM	Wysoki	CM-03-z-01-e	CM-3(1)(e)
HWAM	Wysoki	CM-03-z-01-f	CM-3(1)(f)
HWAM	Wysoki	CM-08-z-02-z	CM-8(2)
HWAM	Wysoki	MA-03-z-03-a	MA-3(3)(a)
HWAM	Wysoki	SA-12	SA-12

Elementy zabezpieczeń wspierające każdy składnik zdolności są wymienione w podrozdziale 3.2 każdego tomu publikacji NISTIR 8011 poświęconego konkretnej zdolności. W przypadku każdego składnika zdolności jest to udokumentowane w tabeli analogicznej do tabeli 9, która zawiera przykładowe

elementy zabezpieczeń powiązane ze składnikiem zdolności zapobiegania używaniu lub zmniejszania liczby autoryzowanych urządzeń bez przypisanego menedżera urządzeń w zakresie objętym oceną.

Tabela 9: Powiązanie elementów zabezpieczeń ze składnikami zdolności: wybrane przykłady dla składnika zdolności *Zapobieganie używaniu autoryzowanych urządzeń bez menedżera urządzeń*

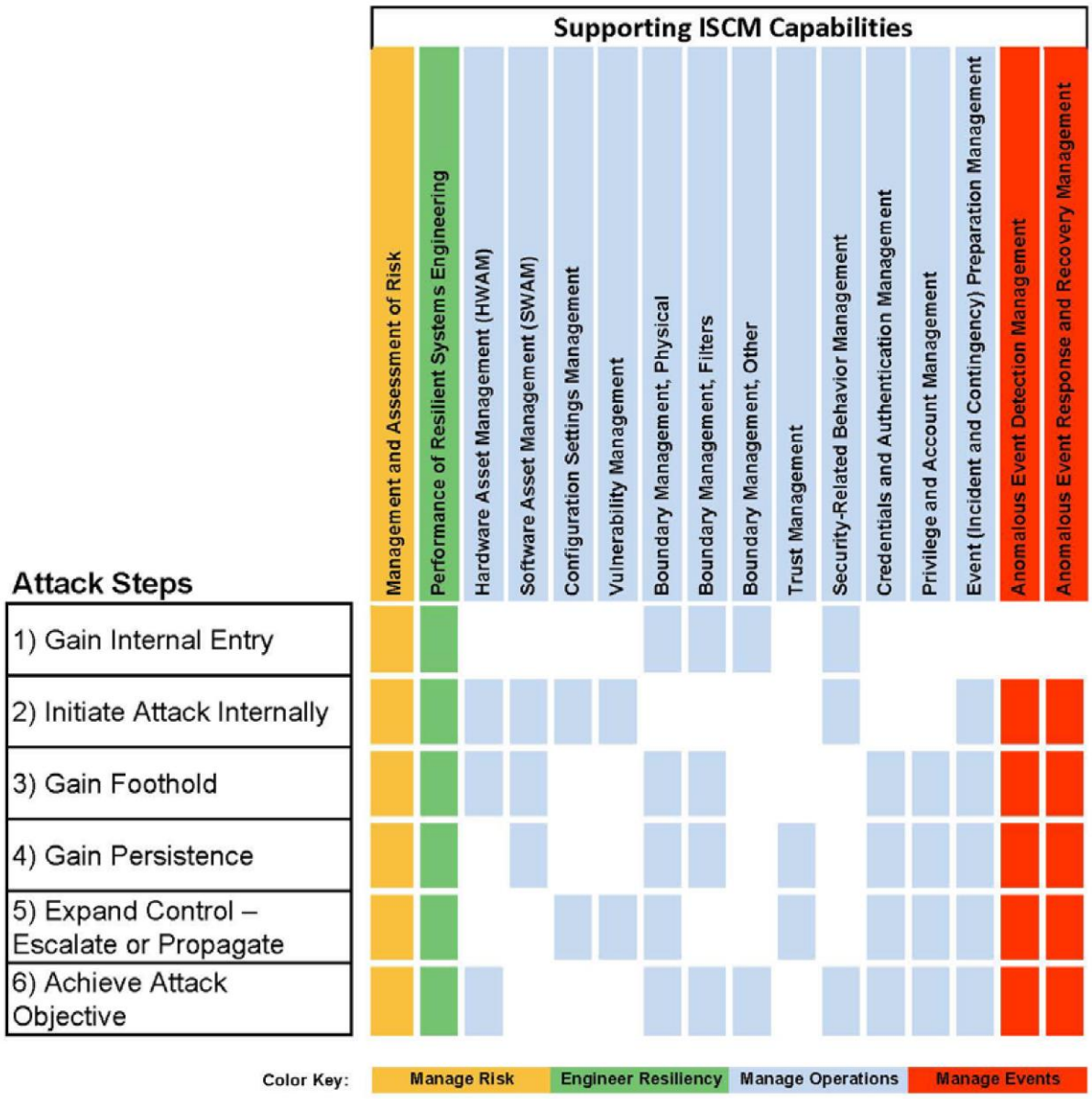
Identyfikator kontroli defektu	Poziom zabezpieczenia bazowego	Sortowalny kod elementu zabezpieczenia	Kod elementu zabezpieczenia z publikacji NSC 800-53; NSC 800-53B
HWAM-F02	Niski	AC-19-b	AC-19(b)
HWAM-F02	Niski	CM-08-z-04-z	CM-8(4)
HWAM-F02	Umiarkowany	CM-03-b	CM-3(b)
HWAM-F02	Umiarkowany	MA-03-z-01-z	MA-3(1)
HWAM-F02	Wysoki	CM-03-z-01-a	CM-3(1)(a)

3.7 *Współdziałanie na każdym poziomie abstrakcji*

Zdolności mogą się wzajemnie wspierać, ale ponieważ w publikacji NISTIR 8011 udokumentowano rodzaje powiązań w ramach zdefiniowanej zdolności do ochrony, współdziałanie między zdolnościami może nie być od razu widoczne. Istnieje wiele przykładów współdziałania zdolności do ochrony, które można zidentyfikować i które są przydatne w planowaniu programu bezpieczeństwa i w ogólnym zarządzaniu ryzykiem. Dwa takie przykłady przedstawiono poniżej.

3.7.1 *Wiele zdolności do ochrony wspiera przeciwdziałanie poszczególnym etapom ataku*

Pomiędzy zdolnościami do ochrony a etapami ataku istnieje relacja „wiele do wielu". Etapy ataku skupiają się na postrzeganiu systemu przez atakującego, czyli na sposobach znalezienia i wykorzystania podatności. Zdolności do ochrony skupiają się na postrzeganiu systemu przez obrońcę, czyli na sposobach zapobiegania atakom lub ograniczania wynikających z nich szkód. Na rysunku 4: *Zdolności współdziałające w celu zablokowania etapów ataku*, przedstawiono zdolności do ochrony, które wspierają przeciwdziałanie każdemu etapowi ataku.



Rysunek 4: Zdolności współdziałające w celu zablokowania etapów ataku

Legenda	
Attack Steps	Etapy ataku
1) Gain Internal Entry	1) Uzyskanie dostępu do systemu
2) Initiate Attack Internally	2) Zainicjowanie ataku wewnątrz sieci
3) Gain Foothold	3) Uzyskanie punktu zaczepienia
4) Gain Persistence	4) Zdobycie trwałego punktu zaczepienia
5) Expand Control - Escalate or Propagate	5) Rozszerzenie kontroli – eskalacja lub propagacja

Legenda	
6) Achieve Attack Objective	6) Osiągnięcie celu ataku
Supporting ISCM Capabilities	Wsparcie zdolności ISCM
Management and Assessment of Risk	Zarządzanie ryzykiem i ocena ryzyka
Performance of Resilient Systems Engineering	Wydajność inżynierii odpornych systemów
Hardware Asset Management (HWAM)	Zarządzanie zasobami sprzętowymi (HWAM)
Software Asset Management (SWAM)	Zarządzanie zasobami programowymi (SWAM)
Configuration Settings Management	Zarządzanie ustawieniami konfiguracyjnymi
Vulnerability Management	Zarządzanie podatnościami na zagrożenia
Boundary Management, Physical	Zarządzanie granicami (fizycznymi)
Boundary Management, Filters	Zarządzanie granicami (filtry)
Boundary Management, Other	Zarządzanie granicami (inne)
Trust Management	Zarządzanie zaufaniem
Security-Related Behavior Management	Zarządzanie zachowaniami związanymi z bezpieczeństwem
Credentials and Authentication Management	Zarządzanie poświadczeniami i uwierzytelnianiem
Privilege and Account Management	Zarządzanie przywilejami i kontami
Event (Incident and Contingency) Preparation Management	Zarządzanie przygotowaniem do zdarzeń (incydentów i sytuacji kryzysowych)
Anomalous Event Detection Management	Zarządzanie wykrywaniem nietypowych zdarzeń
Anomalous Event Response and Recovery Management	Zarządzanie reagowaniem na nietypowe zdarzenia i usuwaniem ich skutków
Color Key:	Klucz kolorów:
Manage Risk	Zarządzanie ryzykiem
Engineer Resiliency	Odporność inżynieryjna
Manage Operations	Zarządzanie operacjami
Manage Events	Zarządzanie zdarzeniami

Jako przykład mogą posłużyć trzy zdolności, które wspierają blokowanie lub opóźnianie zainicjowania ataku wewnątrz.

- Zdolność HWAM może zapobiegać wnikaniu złośliwego oprogramowania poprzez wykrywanie nieautoryzowanych/niezarządzanych urządzeń.

- Zdolność SWAM może odpowiadać za to samo poprzez tworzenie czarnych list i białych list oprogramowania.
- Zarządzanie zachowaniami związanymi z bezpieczeństwem może zablokować włamanie, pomagając użytkownikowi w uniknięciu wyłudzenia jego informacji oraz uniemożliwiając mu instalację nieautoryzowanego sprzętu i oprogramowania itp.

Odpowiednio połączone zdolności do ochrony zapewniają dogłębną obronę (lub dokładniej, obronę w szerokim zakresie), która umożliwia blokowanie ataków na każdym etapie.

3.7.2 *Obsługa różnorodnych zdolności przez wiele zabezpieczeń*

Większość elementów zabezpieczeń wspiera więcej niż jedną zdolność. Wynika to z faktu, że:

- Elementy zabezpieczeń nie uwzględniają zdolności.
- Niektóre elementy zabezpieczeń odzwierciedlają ogólne procesy (np. zarządzanie konfiguracją), które wspierają wiele zdolności.

W tabeli 10 przedstawiono przykład elementu zabezpieczenia, który wspiera różnorodne zdolności.

Tabela 10: Przykład elementu zabezpieczenia wspierającego wiele zdolności

Kod elementu zabezpieczenia z publikacji NSC 800-53; NSC 800-53B	**Wspierana zdolność do ochrony**	**Zastosowanie**
CM-3(b)	Granica sieci: Reguły zapory sieciowej i routingu; Reguły filtrowania treści	Weryfikacja zmian w regułach zapory sieciowej
CM-3(b)	Zarządzanie ustawieniami konfiguracyjnymi	Weryfikacja zmian w ustawieniach konfiguracyjnych
CM-3(b)	Ogólne audytowanie, rejestrowanie i monitorowanie w celu wykrycia incydentów	Weryfikacja zmian w zapisach audytów, dziennikach i regułach monitorowania

Kod elementu zabezpieczenia z publikacji NSC 800-53; NSC 800-53B	**Wspierana zdolność do ochrony**	**Zastosowanie**
	i sytuacji awaryjnych	
CM-3(b)	Zarządzanie zasobami sprzętowymi	Weryfikacja zmian w konfiguracji sprzętu
CM-3(b)	Planowanie i przygotowanie na wypadek incydentów i sytuacji kryzysowych	Weryfikacja zmian w wymaganych przygotowaniach
CM-3(b)	Reagowanie na incydenty i sytuacje awaryjne	Weryfikacja zmian w zaplanowanych reakcjach
CM-3(b)	Zarządzanie ryzykiem i budżetem na szczeblu zarządczym	Weryfikacja zmian w finansowaniu działań w zakresie zarządzania ryzykiem operacyjnym i ryzykiem wywołanym przez zdarzenia.
CM-3(b)	Zarządzanie zasobami oprogramowania	Weryfikacja zmian w autoryzowanych produktach programowych i plikach wykonywalnych
CM-3(b)	Inżynieria systemu	Weryfikacja zmian w wymaganiach, projektach itp.

4. WYKORZYSTANIE SPECYFIKACJI STANU RZECZYWISTEGO I STANU POŻĄDANEGO DO WYKRYWANIA WAD

W niniejszym rozdziale wyjaśniono wymagane przygotowanie do zautomatyzowanej oceny ISCM, aby następnie określić, w jaki sposób w ramach procesu oceny rozpoznaje się specyfikację stanu rzeczywistego i stanu pożądanego, aby móc je porównać. Ponieważ tworzenie zautomatyzowanego systemu oceny środków bezpieczeństwa dla każdego systemu osobno jest często nieefektywne, w niniejszym rozdziale wprowadzono pojęcie granicy oceny, która może się różnić (i być znacznie większa) od granicy autoryzacji zdefiniowanej w publikacji NSC 800-37. Ostatnia część tego rozdziału omawia kluczowy wymóg dotyczący zautomatyzowania oceny środków bezpieczeństwa – konieczność posiadania specyfikacji stanu pożądanego wyrażonej w obliczalnych danych (a nie w postaci dowolnego tekstu), które można porównać ze stanem rzeczywistym cyfrowo lub maszynowo.

4.1 *Specyfikacja stanu rzeczywistego i stanu pożądanego*

W publikacji NSC 800-53A zdefiniowano metodę testowania jako proces wykorzystania jednego lub więcej obiektów oceny (tj. działań lub mechanizmów) w określonych warunkach w celu porównania zachowania rzeczywistego z oczekiwanym. W pozostałej części niniejszego dokumentu zamiast terminów rzeczywiste zachowanie i oczekiwane zachowanie, stosuje się terminy *specyfikacja stanu rzeczywistego* i *specyfikacja stanu pożądanego*. Wyjaśnienie, dlaczego zamiast określenia *zachowanie* stosuje się *stan*, znajduje się w podrozdziale 4.4, Specyfikacja stanu pożądanego. W obecnym środowisku automatyzacji zabezpieczeń, stan rzeczywisty jest informacją związaną z bezpieczeństwem, która jest najprawdopodobniej dostępna. Model automatycznej oceny środków bezpieczeństwa zakłada, że dane o rzeczywistym stanie obiektów oceny mogą być gromadzone przez narzędzia zwane modułami zbierającymi dane.

4.2 *Moduły i system zbierania danych*

4.2.1 *Moduły zbierające dane o stanie rzeczywistym*

Moduły zbierające dane[22] są częścią systemu zbierania danych , która wchodzi w interakcje z obiektami oceny poddawanymi ocenie oraz z wszelkimi innymi obiektami oceny, które ustalają politykę dla obiektów oceny poddawanych ocenie. Modułami zbierającymi dane mogą być skanery, procesy wprowadzania danych, kanały danych z innych systemów itp. Sposób działania modułów zbierających dane jest nieistotny, o ile są one skonfigurowane i wdrożone tak, aby dostarczały wiarygodnych, prawidłowych (dokładnych) i kompletnych danych, dostarczanych na czas.

4.2.2 *Zbieranie danych specyfikacji stanu pożądanego*

System zbierania musi być w stanie zarządzać danymi specyfikacji stanu pożądanego dla każdego wdrożenia automatycznej oceny środków bezpieczeństwa.

Niektóre specyfikacje stanu są określane przez deweloperów (organizacyjne ustawienia konfiguracyjne, takie jak konfiguracja bazowa). Pulpit nawigacyjny organizacji może otrzymywać dane specyfikacji stanu pożądanego zdefiniowane przez dewelopera[23] z jego pulpitu nawigacyjnego. Inne specyfikacje stanu pożądanego są specyficzne dla organizacji (np. listy autoryzowanych urządzeń lub wymagania dotyczące częstotliwości szkoleń).

Sam system zbierania danych i pulpit nawigacyjny organizacji współpracują ze sobą w celu przedstawiania zdefiniowanych przez organizację specyfikacji stanu pożądanego. Na przykład:

- Spisy autoryzowanych urządzeń/oprogramowania są dostarczane przez system zbierania danych (który ma funkcję automatycznego importu lub wprowadzania danych związanych z ewidencją).
- Wartości dla ustawień konfiguracyjnych specyficznych dla organizacji są zarządzane (zbierane, przetwarzane, przechowywane, prezentowane itp.) na liście kontroli defektów w pulpicie nawigacyjnym organizacji.

[22] Moduły zbierające dane nazywane są również czujnikami.

[23] Dane specyfikacji stanu pożądanego są odbierane w postaci kontroli defektów. Patrz rozdział 5, Kontrole defektów.

4.2.3 *System zbierania danych*

System zbierania danych, przedstawiony na rysunku 5: *System zbierania danych ISCM*, zarządza modułami zbierającymi dane, generuje dane o stanie rzeczywistym, zbiera dane o stanie pożądanym i porównuje dane z modułu zbierającego dane (stan rzeczywisty) ze specyfikacją stanu pożądanego, aby wykryć defekty.

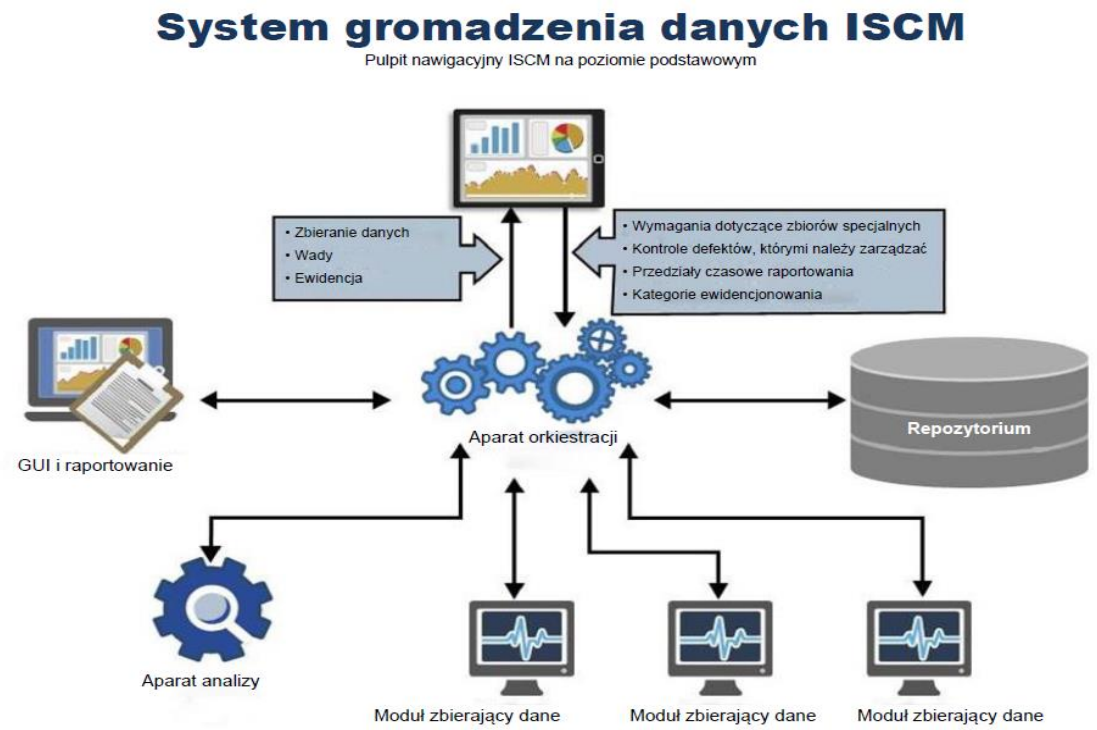
System zbierania ISCM może być wdrożony jako instancja architektury referencyjnej CAESARS (*ang. Continuous Asset Evaluation, Situational Awareness, and Risk Scoring*). W takim przypadku mogłoby to spowodować zamieszanie terminologiczne, ponieważ architektura CAESARS obejmuje podsystem do gromadzenia danych. Podsystem do gromadzenia danych CAESARS działa w sposób zbliżony do opisanych powyżej modułów zbierających dane. Co za tym idzie, system zbierania ISCM i podsystem gromadzenia CAESARS nie są tożsame. Ramy architektury CAESARS zostały opisane w publikacji NIST IR 7756[24].

System zbierania danych ISCM obejmuje:

- Funkcje modułów zbierających dane podsystemu gromadzenia danych CAESARS.
- Repozytorium do przechowywania danych.
- Mechanizm organizacyjny do koordynowania pracy modułów zbierających dane w celu gromadzenia danych w określonym czasie i w oparciu o określone zdarzenia oraz do koordynowania komunikacji w określonym czasie i w oparciu o określone zdarzenia.
- Mechanizm analityczny do wyszukiwania defektów i określania konieczności gromadzenia danych po określonych zdarzeniach.

Zazwyczaj graficzny interfejs użytkownika (*ang. Graphical User Interface – GUI*) systemu zbierania danych i funkcja raportowania są minimalne, ponieważ dane są przesyłane bezpośrednio do pulpitu nawigacyjnego organizacji w celu zapewnienia takich funkcji.

[24] Przykład podany dla zainteresowanych.



Rysunek 5: System zbierania danych ISCM

4.3 *Granica autoryzacji i granica oceny*

Aby informacje związane z bezpieczeństwem generowane przez moduły zbierające dane i przetwarzane przez system zbierania danych były maksymalnie użyteczne, należy zmapować wszystkie defekty systemu, które stanowią ryzyko dla tego systemu, w tym:

- defekty środków bezpieczeństwa wdrożonych na poziomie systemu;
- defekty zabezpieczeń wspólnych, które system dziedziczy;
- defekty w niepowiązanych obiektach oceny, umożliwiające stworzenie ścieżki ataku, który może zagrozić systemowi[25].

Aby moduły systemu zbierania danych mogły wykrywać i przetwarzać wszystkie trzy rodzaje wad, obiekty oceny są pogrupowane w następujące kategorie:

- obiekty oceny i wady w ramach granicy autoryzacji systemu;
- obiekty oceny i wady w ramach zabezpieczeń wspólnych, które system dziedziczy.

Dzięki temu pulpit nawigacyjny organizacji może obliczyć ryzyko z obu grup.

[25] Ponieważ granicą oceny jest zazwyczaj cała sieć, dane o najbardziej istotnych obiektach oceny (poza granicą autoryzacji) są zawarte w granicy oceny i mogą być brane pod uwagę.

4.3.1 *Granica autoryzacji systemu*

Koncepcja granicy autoryzacji systemu jest opisana w wielu publikacjach NIST. Poniżej znajduje się formalna definicja granicy autoryzacji z publikacji NISTIR 7298:

> *Wszystkie elementy systemu, które mają być dopuszczone do eksploatacji przez osobę autoryzującą i nie obejmują oddzielnie autoryzowanych systemów połączonych z zabezpieczanym systemem.*

Innymi słowy, granice autoryzacji są wykorzystywane do zapewnienia odrębności systemów w celu ułatwienia zarządzania bezpieczeństwem informacji i odpowiedzialnością za nie. W publikacji NSC 800-53, NSC 800-53B uwzględniono następujące środki bezpieczeństwa i zabezpieczenia rozszerzone, które wymagają, aby składniki systemu były przypisane do konkretnego systemu, i zapewniają, że nie są one powielane w innych ewidencjach składników systemu:

Środek bezpieczeństwa **CM-8**, INWENTARYZACJA KOMPONENTÓW SYSTEMU: Organizacja:

a. Opracowuje i dokumentuje inwentaryzację komponentów systemu, która:
   1. Dokładnie odzwierciedla system;
   2. Zawiera wszystkie komponenty systemu;
   3. Nie obejmuje podwójnego księgowania tych samych komponentów lub komponentów przypisanych do jakiegokolwiek innego systemu;
   4. Jest na poziomie szczegółowości uznanym za niezbędny do śledzenia i raportowania; oraz
   5. Zawiera następujące informacje umożliwiające rozliczalność komponentów systemu: [*Realizacja: informacje zdefiniowane przez organizację uznane za niezbędne do osiągnięcia skutecznej rozliczalności komponentów systemu teleinformacyjnego*]; oraz

b. Przegląda i aktualizuje spis komponentów systemu [*Realizacja: częstotliwość określona przez organizację*].

CM-8(5) INWENTARYZACJA KOMPONENTÓW SYSTEMU | BRAK DUPLIKACJI KOMPONENTÓW

[Włączone do CM-8]

Organizacja weryfikuje, czy wszystkie komponenty znajdujące się w granicy autoryzacji systemu nie są powielane w ewidencjach innych systemów.

4.3.2 *Granica oceny ISCM*

Gdy organizacje zaczną automatyzować ocenę środków bezpieczeństwa komponentów systemu, nie jest opłacalne wdrażanie oddzielnego, zautomatyzowanego procesu zbierania danych w ramach każdej granicy autoryzacji. Dlatego w ramach programu ISCM wprowadza się koncepcję granicy oceny (zazwyczaj szerszej i obejmującej więcej systemów i komponentów niż granica autoryzacji).

Ponieważ wdrożenie jednego centralnego systemu automatycznej oceny i zarządzanie nim jest najczęściej tańsze od wdrożenia wielu oddzielnych systemów tego typu w obrębie danej sieci, najbardziej opłacalna granica oceny obejmuje wszystkie urządzenia podłączone do sieci, która jest ograniczona filtrami ruchu (zaporami) i innymi zabezpieczeniami granicznymi (np. routerami, przełącznikami), aż po urządzenia internetowe zarządzane oddzielnie od samej sieci. Zazwyczaj granica ta obejmuje sieć obwodową lub *DMZ* (*ang. Demilitarized Zone*), ekstranet, intranet i ewentualne wewnętrzne enklawy. Granica z siecią zewnętrzną (zazwyczaj z Internetem) jest zabezpieczona przez zaufane połączenie internetowe (*ang. Trusted Internet Connection – TIC*), które stanowi zewnętrzną granicę sieci.

Ponieważ granica oceny jest kompleksowa, może być stosowana do oceny komponentów wielu systemów w jej obrębie. Ma to następujące zalety:

1. Stały koszt instalacji modułów oraz systemu zbierania danych i hierarchii pulpitów ISCM jest ponoszony tylko raz.
2. Wygenerowane informacje dotyczące bezpieczeństwa mogą być wykorzystane do analizy ryzyka we wszystkich systemach:

a. System może dziedziczyć środki bezpieczeństwa z innych systemów. Na przykład, większość systemów w organizacji prawdopodobnie odziedziczy zabezpieczenia graniczne z systemu sieciowego. Jest to zwykle objęte koncepcją dziedziczenia zabezpieczeń wspólnych.

b. System zapewniający zabezpieczenia wspólne może mieć wszystkie dziedziczone środki wdrożone prawidłowo, ale może mieć inne defekty, które zostaną wykorzystane podczas ataku do osłabienia zabezpieczeń wspólnych. Chociaż sprawozdania z oceny bezpieczeństwa oraz informacje z planu działania i kamieni milowych (*ang. Plan of Action and Milestones – POA&M*) dla systemów zapewniających wspólne (dziedziczone) zabezpieczenia mają być udostępnione personelowi dziedziczącego systemu, takie informacje nie zawsze są uwzględniane w tradycyjnej analizie oceny systemu. Możliwe jest jednak, aby informacje związane z bezpieczeństwem dotyczące systemu zapewniającego wspólne zabezpieczenia były wyświetlane automatycznie, wraz z informacjami dotyczącymi danego systemu, za pośrednictwem odpowiednio skonstruowanego pulpitu nawigacyjnego organizacji.

c. Komponenty (obiekty oceny) w danej sieci, które znajdują się w określonych granicach autoryzacji, mogą być podatne na atak i stać się jego wektorami, przez co zagrożone mogą być obiekty oceny w innych granicach autoryzacji. Ryzyko to nie jest oczywiste, jeżeli w ocenie uwzględnia się jedynie zagrożenia dotyczące w całości danej granicy autoryzacji. Innymi słowy, systemy poza granicą autoryzacji danego obiektu oceny mogą dziedziczyć związane z nim ryzyko, bez dziedziczenia zabezpieczeń tego obiektu oceny.

Dodatkowe informacje o dziedziczonym ryzyku opisane w punktach b) i c) powyżej są przydatne nie tylko na poziomie systemu. Stanowią one również cenne dane o zagregowanym ryzyku z punktu widzenia misji/ biznesu i organizacji, dotyczące tego, jak zagrożenia w jednym systemie mogą wpływać na całą organizację.

3. W dużych sieciach zazwyczaj występują komponenty, które nie są przypisane do żadnych granic autoryzacji. Takie komponenty w dużych sieciach mogą regularnie pojawiać się, znikać i pojawiać się ponownie, tworząc ciągły problem. Nieprzypisane komponenty mogą nie być widoczne, gdy szuka się tylko w granicach autoryzacji, ponieważ z definicji są one poza takimi granicami. Przeglądanie ewidencji komponentów w całym obszarze granic oceny i identyfikowanie nieprzypisanych komponentów sprawiają, że bardziej realne staje się ustrukturyzowanie procesu ich przypisywania do systemu w celu odpowiedniego zarządzania urządzeniami. Innymi słowy, kompleksowa granica oceny umożliwia zapewnienie, że wszystkie komponenty są już przypisane do granicy autoryzacji, oznaczone do przypisania do niej lub usunięte z sieci.

W całej treści publikacji NISTIR 8011 granica oceny ISCM jest określana jako sieć docelowa ISCM (*ang. ISCM Target Network – ISCM-TN*).

4.3.3 *Identyfikacja źródeł ryzyka dla systemu*

Aby zautomatyzowany system oceny środków bezpieczeństwa mógł dokładnie monitorować ryzyko związane z każdą granicą autoryzacji (systemem) w ramach granicy oceny, musi być w stanie zidentyfikować następujące źródła ryzyka (niezależne od atakującego):

1. komponenty (obiekty oceny) i zabezpieczenia wdrożone na poziomie systemu;
2. komponenty systemów, które zapewniają zabezpieczenia wspólne i wdrożone w nich środki bezpieczeństwa;
3. komponenty w granicach oceny, które są niezarządzane/nieprzypisane;
4. komponenty na potencjalnych ścieżkach ataku na system.

Odnośnie do punktu 1, identyfikacja komponentów wewnątrz granicy autoryzacji systemu może być procesem ręcznym. Często jednak możliwe jest określenie wskaźników (wpisów w rejestrze, określonych plików wykonywalnych itp.), które umożliwiają systemowi zarządzania zasobami zbierającymi dane o stanie rzeczywistym identyfikację urządzeń znajdujących się w granicach systemu. W miarę możliwości preferowane są wskaźniki identyfikacyjne, ponieważ istnieje większe prawdopodobieństwo, że są one aktualne i kompletne.

Odnośnie do punktu 2, identyfikacja obiektów oceny, z których system dziedziczy zabezpieczenia, może być równie prosta, jak identyfikacja systemów lub procesów biznesowych zapewniających wspólne zabezpieczenia, a następnie uwzględnienie wszystkich obiektów oceny przy ocenie skuteczności wspólnych zabezpieczeń. W innych przypadkach zakres zabezpieczeń wspólnych uwzględnionych w automatycznej ocenie środków bezpieczeństwa systemu jest zawężony, gdy system jest wspierany tylko przez jeden lub niektóre komponenty danego systemu z zabezpieczeniami wspólnymi.

Odnośnie do punktu 3, niezarządzane i/lub nieprzypisane urządzenia w granicach oceny stwarzają ryzyko dla wszystkich podłączonych komponentów. Punkt 4 może pomóc w określeniu, w jakim stopniu niezarządzane/ nieprzypisane komponenty wpływają na dany system.

Wreszcie, odnośnie do punktu 4, identyfikacja potencjalnych ścieżek ataku jest możliwa tylko wtedy, gdy dane i narzędzia są odpowiednio ustrukturyzowane, aby obliczyć prawdopodobne i możliwe do wykorzystania ścieżki ataku w granicach oceny, a następnie sprawdzić, które komponenty znajdują się na ścieżkach ataku stanowiących zagrożenie dla systemu. Komponenty na potencjalnych ścieżkach ataku mogą obejmować niezarządzane lub nieprzypisane urządzenia.

Po zidentyfikowaniu komponentów systemu, które mają być poddane ocenie, pulpit nawigacyjny organizacji powinien być w stanie przetworzyć wyniki oceny i określić znane zagrożenia dla systemu pochodzące z trzech źródeł wymienionych w podrozdziale 4.3, Granica autoryzacji i granica oceny. Pulpit nawigacyjny organizacji powinien być w stanie zapewnić obraz ryzyka dla systemu i bezzwłocznie ostrzegać osoby wyznaczone do pełnienia odpowiednich funkcji w przypadku zidentyfikowania:

- defektów komponentów systemu;
- defektów komponentów zapewniających zabezpieczenia wspólne;
- defektów innych komponentów w ramach granicy oceny.

4.4 *Specyfikacja stanu pożądanego*

Strategia zwiększenia liczby środków bezpieczeństwa, dla których monitorowanie skuteczności może być zautomatyzowane, opiera się na zdefiniowaniu specyfikacji stanu pożądanego i wyrażeniu go w formacie danych nadających się do odczytu maszynowego, które można porównać ze stanem rzeczywistym. Specyfikacja stanu pożądanego to zdefiniowana wartość (zestawienie), do której można porównać wartość stanu rzeczywistego. Rozbieżności tych dwóch wartości wskazują na istnienie defektu w skuteczności jednego lub większej liczby środków bezpieczeństwa. Na przykład w polityce organizacji określono, że konta użytkowników mają być blokowane po trzech nieudanych próbach logowania. Specyfikacja stanu pożądanego byłaby zatem taka, że odpowiednie urządzenia są skonfigurowane w sposób powodujący blokowanie konta po trzech nieudanych próbach logowania. Jeżeli podczas automatycznej oceny środków bezpieczeństwa zgromadzone informacje wykażą, że określone urządzenie jest skonfigurowane w sposób powodujący blokowanie konta po pięciu nieudanych próbach logowania, zidentyfikowano rozbieżność między specyfikacją stanu pożądanego (trzy dozwolone próby przed zablokowaniem) a stanem rzeczywistym (pięć dozwolonych prób przed zablokowaniem), co może świadczyć o problemie ze skutecznością środków bezpieczeństwa z publikacji NSC 800-53: AC-7, *Nieudane próby logowania*; AC-2, *Zarządzanie kontami*; CM-2, *Konfiguracja bazowa*; itp.

Posiadanie specyfikacji stanu pożądanego w postaci danych możliwych do odczytu maszynowego ma fundamentalne znaczenie dla automatyzacji ocen środków bezpieczeństwa.

Model systemu automatycznej oceny środków bezpieczeństwa zakłada, że dane o specyfikacji stanu pożądanego są przekazywane do systemu zbierania danych przez organizację zarządzającą systemem.

Specyfikacja stanu pożądanego może na przykład informować o:

- autoryzowanych urządzeniach;
- autoryzowanych rolach urządzeń;
- oprogramowaniu z białej listy i/lub autoryzowanemu dla każdej roli urządzenia;

- wymaganej częstotliwości szkoleń uświadamiających w zakresie bezpieczeństwa;
- autoryzowanych ustawieniach konfiguracyjnych dla każdej roli urządzenia;
- podatnych wersjach oprogramowania (dane z NVD);
- autoryzowanych użytkownikach i przywilejach; oraz
- wielu innych kwestiach.

4.4.1 *Rodzaje specyfikacji stanu pożądanego*

Specyfikacja stanu pożądanego może być taka, jak przedstawiono w dowolnym z poniższych przykładów. Dla uproszczenia stosuje się krótszy termin *specyfikacja stanu pożądanego*, zamiast bardziej kompletnego i jednoznacznego, ale kłopotliwego wyrażenia „specyfikacja stanu/zachowania pożądanego/dozwolonego/zakazanego".

Tabela 11: Rodzaje specyfikacji stanu pożądanego

Rodzaj specyfikacji stanu pożądanego	**Uproszczone przykłady** **(Rzeczywiste sytuacje mogą być bardziej złożone)**
Stan pożądany	Jeśli używany jest program X, ustawienie Z powinno mieć wartość Y.
Stan zakazany[a]	Jeśli używany jest program X, określone poziomy poprawek mają CVE, które powodują ryzyko i są zabronione.
Stan oczekiwany	Jeśli używany jest program X, urządzenie powinno posiadać parametr [lista plików wykonywalnych ze skrótami do ich identyfikacji]. Oczekiwany stan oprogramowania może być taki, że jest ono w pełni zainstalowane z poprawnymi skrótami, jednakże w rzeczywistym stanie niektóre pliki mają zmienione skróty.
Pożądane zachowanie	Użytkownicy otrzymujący wiadomości e-mail powinni sprawdzić ich pochodzenie przed użyciem zawartych w nich łączy lub załączników.
Zakazane zachowanie	Użytkownicy korzystający z kont uprawnionych do instalowania oprogramowania, czyli kont uprzywilejowanych, nie mogą przeglądać Internetu ani korzystać z poczty elektronicznej z takiego konta.

Rodzaj specyfikacji stanu pożądanego	**Uproszczone przykłady** **(Rzeczywiste sytuacje mogą być bardziej złożone)**
Oczekiwane zachowanie	Użytkownik B zwykle loguje się z urządzeń w [lokalizacja] w godzinach od 8.00 do 18.00. Stanowi to oczekiwane zachowanie. Inne wzorce aktywności logowania mogą wskazywać na włamanie na konto.

[a] Pożądane i zakazane stany oraz zachowania to zasady normatywne. Natomiast oczekiwane stany i zachowania nie są zasadami normatywnymi, lecz opisami wzorców. Oczekiwane stany i zachowania są wykorzystywane do wykrywania nietypowych (a więc anomalnych i podejrzewanych o złośliwość) stanów i zachowań, które mogą wymagać reakcji i usuwania skutków. Oczekiwane stany i zachowania zazwyczaj nie są wykorzystywane poza zdolnościami: zarządzanie wykrywaniem zdarzeń nietypowych oraz zarządzanie reagowaniem na zdarzenia nietypowe i usuwanie ich skutków. Należy zauważyć, że zakazany stan/zachowanie zawsze można przeformułować na pożądane zachowanie. W tabeli 12: *Równoważność specyfikacji stanu zabronionego i pożądanego – przykład*, przedstawiono takie przeformułowanie.

Tabela 12: Równoważność specyfikacji stanu zabronionego i pożądanego – przykład

Zakazane zachowanie	**Równoważne pożądane zachowanie**
Użytkownicy korzystający z kont uprawnionych do instalowania oprogramowania nie mogą przeglądać Internetu ani korzystać z poczty elektronicznej z takiego konta.	Użytkownicy korzystający z kont uprawnionych do instalowania oprogramowania nie przeglądają Internetu ani nie korzystają z poczty elektronicznej z takiego konta.

Oczekiwane zachowanie może czasami być przeformułowane na pożądane zachowanie, z tym że wtedy wskazuje ono na symptom możliwego problemu, a nie na definitywny problem

4.4.2 *Polityka uwzględniająca specyfikację stanu pożądanego*

Jak zaznaczono powyżej, specyfikacja stanu pożądanego jest wyrażeniem polityki w formie nadającej się do odczytu maszynowego (np. baza danych, plik XML, inny ustrukturyzowany format), którą można łatwo porównać z danymi dotyczącymi stanu rzeczywistego zebranymi za pomocą środków automatycznych.

Organizacje tworzą polityki, aby wspierać wdrażanie środków bezpieczeństwa i ogólnego bezpieczeństwa informacji. Jeśli polityki są wyrażone w formie nadającej się do odczytu maszynowego, a z formy wygenerowanej maszynowo można wygenerować formę możliwą do odczytania przez człowieka, to nie ma potrzeby oddzielnego tworzenia i utrzymywania polityk w tradycyjnej formie tekstowej (np. dokument Word lub PDF). Jeśli pojawi się konieczność wydrukowania tekstu, zawsze można go wygenerować z autorytatywnej, zautomatyzowanej specyfikacji.

4.4.3 *Polityka jako dowód wskazujący na istnienie specyfikacji stanu pożądanego*

Często zakłada się, że tylko techniczne środki bezpieczeństwa mogą być oceniane pod kątem skuteczności za pomocą metod automatycznych, a środki zarządcze i operacyjne nie mogą być oceniane w ten sposób. Jednak w wielu przypadkach możliwa jest ocena skuteczności środków zarządczych i operacyjnych za pomocą metod automatycznych poprzez wprowadzenie specyfikacji stanu pożądanego do danych.

Należy wziąć pod uwagę, że sama specyfikacja stanu pożądanego jest często polityką. Zatem jej istnienie jest dowodem na to, że organizacja posiada politykę w ramach danej zdolności do ochrony. W zakresie, w jakim organizacja może zautomatyzować zbieranie odpowiednich danych o stanie rzeczywistym, aby zidentyfikować, czy stan pożądany i rzeczywisty są zgodne, czy też nie, w sposób oczywisty wykorzystuje ona automatyzację do oceny, czy polityka jest stosowana.

Kiedy organizacja wykazuje, że ocenia czy polityka jest przestrzegana, udowadnia również, że polityka istnieje i jest udokumentowana w bazie danych specyfikacji stanu pożądanego. Aby zautomatyzować ten proces, system automatycznej oceny środków bezpieczeństwa musi być w stanie automatycznie porównać politykę ze stanem rzeczywistym.

Dobrym przykładem jest następujący środek bezpieczeństwa: okresowe szkolenie w zakresie świadomości bezpieczeństwa (AT-2 z publikacji NSC 800-53). Organizacja musi zdecydować, jak często takie szkolenie ma być przeprowadzane. Jeśli określony parametr ram czasowych to 360 dni, informacja ta jest przechowywana w danych jako „definicja polityki", tj. specyfikacja stanu pożądanego. Następnie parametr ten można porównać z rzeczywistym czasem, jaki upłynął od ostatniego odnotowanego zakończenia szkolenia w zakresie świadomości bezpieczeństwa, jaki został zapisany w systemie zarządzania nauką w organizacji. Jeśli szkolenie nie odbędzie się w określonym terminie, zostanie odnotowana to jako defekt.

Przykład ten pokazuje, że środki nietechniczne mogą być automatycznie testowane częściej, niż można by się tego spodziewać. Kluczowym działaniem jest opracowanie odpowiedniej specyfikacji stanu pożądanego, która wyraża politykę.

Uwaga

Mimo, że organizacje dążą do zautomatyzowania oceny środków bezpieczeństwa w jak największym stopniu przy użyciu metod opisanych w przykładzie, faktem jest, że podczas gdy ocena wielu środków może być w pełni zautomatyzowana, ocena niektórych z nich może być tylko częściowo zautomatyzowana lub może nie być zautomatyzowana w ogóle. Organizacje muszą dokładnie rozważyć podejście do oceny i konkretne metody oceny, które zostaną wykorzystane w ramach strategii ISCM.

4.5 *Wykorzystanie automatyzacji do porównywania specyfikacji stanu rzeczywistego i stanu pożądanego*

Przy dokonywaniu ręcznych/proceduralnych ocen środków bezpieczeństwa, plan oceny bezpieczeństwa, specyfikacje stanu rzeczywistego, stanu pożądanego i znalezione defekty są w dużej mierze prowadzone w formie dokumentów tekstowych. Takie dokumenty muszą być pisane i edytowane przez ludzi, co jest procesem powolnym i często kosztownym. Raport z oceny bezpieczeństwa może być nieaktualny do czasu jego ukończenia, z tej prostej przyczyny, że system zmienia się

tak szybko (wprowadzane/usuwane są urządzenia, instalowane poprawki itp.), że ręczna ocena nie jest w stanie za tym nadążyć. Dodatkowo, błędy ludzkie przy opracowywaniu raportu mogą skutkować zgłoszeniem nieistniejących defektów, które będą wymagały dalszego kosztownego, ręcznego sprawdzania.

Aby przedstawione tu podejście do automatycznej oceny środków bezpieczeństwa było skuteczne, zebrane wyniki stanu rzeczywistego i specyfikacja stanu pożądanego muszą być wyrażone w postaci danych, tak aby komputer mógł skutecznie analizować wyniki. Oznacza to, że mechanizm analityczny systemu zbierania danych musi być w stanie wykonać następujące czynności:

- Znaleźć specyfikacje stanu pożądanego dla każdego sprawdzanego defektu, mające zastosowanie do każdego obiektu podlegającego ocenie.
- Znaleźć odpowiednie wartości stanu rzeczywistego dla każdego ocenianego obiektu.
- Porównać stan rzeczywisty ze stanem pożądanym dla każdej kombinacji weryfikacji defektów i obiektu bez znaczącej interwencji człowieka.
- Wysłać listę wykrytych defektów do pulpitu nawigacyjnego organizacji w celu nadania priorytetów i podjęcia stosownej reakcji[26].

Aby zautomatyzowany system oceny środków bezpieczeństwa mógł generować użyteczne wyniki, musi być w stanie dopasować identyfikator obiektu oceny w stanie rzeczywistym do identyfikatora obiektu oceny w specyfikacji stanu pożądanego dla podobnych obiektów oceny (np. urządzeń, produktów programowych itp.).

Więcej informacji na ten temat można znaleźć w materiale dotyczącym kryteriów oceny zawartym w *podrozdziale 5.4, Dokumentacja kontroli defektów.*

[26] Do zautomatyzowanego określania priorytetów i reakcji niezbędna jest metodologia oceny ryzyka, ale nie wchodzi ona w zakres niniejszej publikacji.

5. KONTROLA DEFEKTÓW

W tym rozdziale opisano koncepcję kontroli defektów. Kontrole defektów umożliwiają zautomatyzowaną ocenę elementów zabezpieczeń w oparciu o wymogi stawiane zabezpieczeniom. Kontrole defektów umożliwiają sprawdzenie, czy warunki dla zabezpieczeń są spełniane przez obiekty oceny, które wspierają cel (zdolność do ochrony lub składnik zdolności) podlegający ocenie. Kontrole defektów są kluczowym elementem procesu zautomatyzowanej oceny środków bezpieczeństwa.

Kontrole defektów można również traktować jako stwierdzenie określające specyfikację stanu pożądanego danych poprzez znalezienie tego, czego NIE MA w specyfikacji stanu pożądanego.

5.1 *Kontrole defektów i wymogi dla zabezpieczeń*

W publikacji NSC 800-53A, która zawiera wytyczne dotyczące oceny środków bezpieczeństwa zawartych w dokumencie NSC 800-53, dla każdego z elementów zabezpieczenia określono cel oceny w postaci jednego lub większej liczby **wymogów dla zabezpieczeń (stwierdzeń ustalających)**. Wymogi dla zabezpieczeń zaczynają się od słów „Ustalić, czy". Aby ułatwić dokonanie szczegółowej oceny, elementy zabezpieczeń mogą być dodatkowo rozłożone na części podlegające ocenie. Celem oceny jest ustalenie, czy dany środek bezpieczeństwa jest skuteczny. Przykład znajduje się w tabeli 13: *Przykładowy środek bezpieczeństwa i wymogi dla zabezpieczenia*.

Tabela 13: Przykładowy środek bezpieczeństwa i wymogi dla zabezpieczenia

AC-2(2) – AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM | AWARYJNYM	
Wymóg dla środka bezpieczeństwa (NSC 800-53)	**Wymóg dla zabezpieczenia (NSC 800 53A wersja 1)**
Można automatycznie usuwać lub wyłączać konta tymczasowe i awaryjne po [*Przypisanie: zdefiniowany przez organizację okres dla każdego typu konta*].	CEL OCENY: *Ustalić, czy:* [1] *określono czas, po którym system automatycznie usuwa lub wyłącza konta*

AC-2(2) – AUTOMATYCZNE ZARZĄDZANIE KONTEM CZASOWYM | AWARYJNYM	
Wymóg dla środka bezpieczeństwa (NSC 800-53)	**Wymóg dla zabezpieczenia (NSC 800 53A wersja 1)**
	tymczasowe i awaryjne; oraz [2] k*onta tymczasowe i awaryjne są automatycznie usuwane lub wyłączane po upływie zdefiniowanego przez organizację czasu dla każdego typu konta.*

W tym przykładzie element zabezpieczenia został rozdzielony na dwa wymogi dla zabezpieczenia.

Wymóg [1] dla zabezpieczenia to pytanie, czy odpowiednia specyfikacja stanu pożądanego została określona. Wymóg [2] dla zabezpieczenia to pytanie, czy specyfikacja stanu pożądanego została wdrożona.

Kontrola defektu to sposób na weryfikację przestrzegania wymogu dla zabezpieczenia. Ma dodatkowe właściwości wymienione poniżej.

Kontrola defektu:

- jest przewidziana jako test (o ile ma to zastosowanie);
- może być zautomatyzowana[27];
- jednoznacznie określa specyfikację stanu pożądanego, która jest następnie porównywana z odpowiednim stanem rzeczywistym w celu określenia wyniku testu; oraz
- jest zwykle na wyższym poziomie abstrakcji niż pojedynczy wymóg dla zabezpieczenia (patrz następny podrozdział).

[27] W przypadku, gdy ocena elementu zabezpieczenia nie może być skutecznie zautomatyzowana, stosuje się ręczne/proceduralne podejścia do oceny (na przykład poprzez ręczny test, badanie lub wywiad). Kontrole defektów stanowią zautomatyzowane podejście do testowej metody oceny, natomiast ręczne/ proceduralne metody nimi nie są. Tabele kontroli defektów obejmują ręczne/proceduralne metody oceny, w sytuacjach, gdy automatyzacja nie uprościłaby kompleksowej oceny.

5.2 *Interpretowanie kontroli defektów jako testów elementów zabezpieczeń*

Kontrola defektu została pomyślana tak, aby koncentrować się na celu, jaki ma osiągnąć dany zestaw środków bezpieczeństwa. Ponieważ kontrola defektu służy do ustalania, czy zestaw środków bezpieczeństwa osiąga swój cel, znajduje się ona na wyższym poziomie abstrakcji niż wymogi dla pojedynczego elementu zabezpieczenia.

Na przykład, w ramach zdolności do ochrony HWAM zdefiniowano kontrolę defektu łańcucha dostaw w celu sprawdzenia, czy dostawca i/lub producent sprzętu znajdują się na zatwierdzonej liście. Ta kontrola defektu:

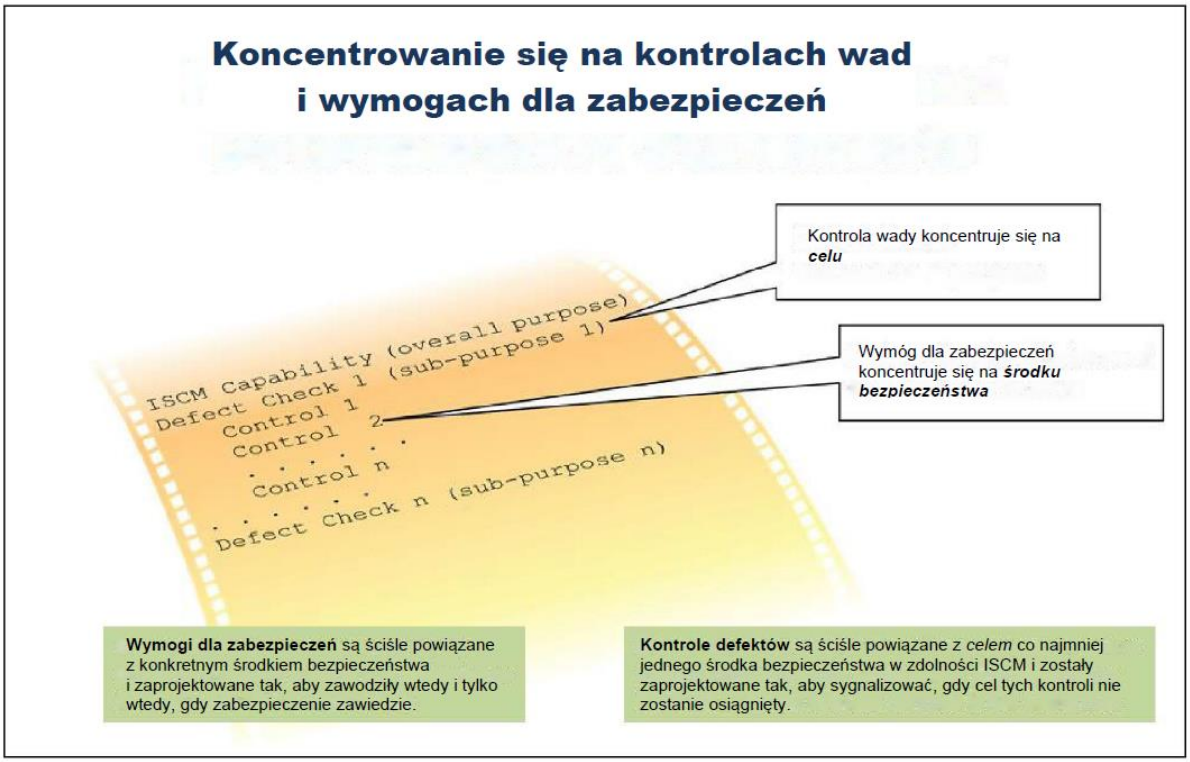
- jest bezpośrednio wspierana przez jeden środek bezpieczeństwa, SA-12, będący wymogiem uwzględnienia kwestii związanych z łańcuchem dostaw przy zatwierdzaniu urządzeń; oraz
- jest pośrednio wspierana przez inne środki, takie jak elementy CM-3, będące wymogami, aby proces zarządzania konfiguracją wyraźnie uwzględniał wpływ na bezpieczeństwo w procesie kontroli zmian (domyślnie włączając łańcuch dostaw, gdy jest to właściwe).

Ten związek kontroli defektów z elementami zabezpieczeń został zilustrowany na rysunku 6: *Koncentrowanie się na kontrolach defektów i wymogach dla zabezpieczeń*.

5.3 *Interpretowanie kontroli defektów jako testów składników zdolności do ochrony i elementów zabezpieczeń*

Jak omówiono w ostatniej sekcji, zbiór elementów zabezpieczeń ocenianych przez kontrolę defektów współdziała w celu osiągnięcia celu. W tym przykładzie celem jest zmniejszenie potencjalnych konsekwencji ataków na łańcuch dostaw – jest to część ogólnej zdolności zarządzania zasobami sprzętu i w efekcie składnik zdolności HWAM (patrz: podrozdział 3.4: *Składniki zdolności)*.

Kontrola defektu służy do oceny poszczególnych zabezpieczeń lub ich elementów, które współdziałają w celu osiągnięcia celu, a jednocześnie umożliwia testowanie ogólnej skuteczności zabezpieczeń współdziałających ze sobą jako składnik zdolności do ochrony. W publikacji NSC 8011 kontrole defektów zostały pomyślane w taki sposób, aby dla każdego zdefiniowanego składnika zdolności istniała jedna kontrola defektu.



Legenda do rysunku 6	
ISCM Capability (overall purpose)	Zdolność ISCM (ogólny cel)
Defect Check 1 (sub-purpose 1)	Kontrola defektu 1 (cel podrzędny 1)
Control 1	Środek bezpieczeństwa 1
Control 2	Środek bezpieczeństwa 2
Control n	Środek bezpieczeństwa n
Defect check n (sub-purpose n)	Kontrola n-tego defektu (cel podrzędny n)

Rysunek 6 : Koncentrowanie się na kontrolach defektów i wymogach dla zabezpieczeń

Różnica poziomu skupienia, między kontrolami defektów a wymogami dla zabezpieczeń, ma znaczący wpływ na to, jak interpretowane są wykryte defekty. Różnica dotyczy *czułości* i *swoistości* wyniku.

Czułość:

> *Czuły test to taki, który umożliwia znalezienie wszystkich przypadków, w których występuje defekt; to znaczy, że ma niski odsetek wyników fałszywie negatywnych.*

Kontrola defektu skoncentrowana na ustaleniu, czy cel zestawu zabezpieczeń został spełniony, wykazuje wysoki stopień czułości, jeśli umożliwia prawidłowe zgłoszenie wszystkich przypadków wystąpienia defektu.

W przykładzie z zabezpieczeniami łańcucha dostaw kontrola wady dla łańcucha dostaw sprzętu nie powiodłaby się, gdyby:

- wykaz zatwierdzonych dostawców i producentów nie został sporządzony zgodnie z zabezpieczeniem SA-12; lub
- urządzenie od dostawcy, który nie znajduje się na tej liście, zostało zatwierdzone w procesie kontroli zmian w ramach zabezpieczenia CM-3.

Ponieważ ta kontrola wady koncentruje się na zmniejszeniu potencjalnych konsekwencji ataków na łańcuch dostaw i umożliwia bezpośrednie wykrycie wszystkich przypadków, w których ten cel nie jest spełniony, można powiedzieć, że kontrola wady cechuje się wysoką czułością.

Swoistość:

> *Test swoisty to taki, który nie powoduje zgłoszenia wady, gdy ta nie występuje. Oznacza to, że cechuje go niski odsetek wyników fałszywie pozytywnych.*

Ponieważ kontrole defektów służą do testowania wyniku, który ma być osiągnięty przez zestaw zabezpieczeń, mogą one być bardzo swoiste na poziomie abstrakcji celu, w określaniu tego, czy wynik ten został osiągnięty. Jednakże nieosiągnięcie wyniku nie oznacza, że WSZYSTKIE zabezpieczenia lub ich elementy wspierające tę zdolność lub składnik zdolności do ochrony zawiodły. Tak więc, o ile kontrola defektu jest swoista na poziomie abstrakcji celu lub składniku celu, o tyle nie jest swoista na poziomie abstrakcji zabezpieczenia lub elementu zabezpieczenia.

W przykładzie z zabezpieczeniami łańcucha dostaw, niepowodzenie kontroli defektu nie pomaga w ustaleniu, czy dany środek zawiódł, ponieważ:

- wykaz zatwierdzonych dostawców i producentów nie został sporządzony zgodnie z zabezpieczeniem SĄ-12; lub
- urządzenie od dostawcy, który nie znajduje się na tej liście, zostało zatwierdzone w procesie kontroli zmian w ramach zabezpieczenia CM-3.

Defekt mógł wystąpić, ponieważ zawiódł jeden środek bezpieczeństwa lub oba. Jednakże niepowodzenie kontroli defektu NIE powinno być interpretowane w ten sposób, że wszystkie zabezpieczenia wspierające dany cel zawiodły.

Uwagi dotyczące czułości i swoistości zostały zebrane w poniższej tabeli:

Tabela 14: Uwagi dotyczące swoistości i czułości

Poziom oceny	**Stopień czułości (na określonym poziomie oceny)**	**Stopień swoistości (na określonym poziomie oceny)**
Cel składnika zdolności	WYSOKI	WYSOKI
Skuteczność elementu zabezpieczenia (wymogu dla zabezpieczenia)	WYSOKI	NISKI (wyższy w przypadku dokonania analizy przyczyn źródłowych)

Analiza przyczyn źródłowych zwiększa swoistość na poziomie środków bezpieczeństwa:

Powszechnie przyjmuje się, że trudno jest sprawić, aby jeden test był zarówno czuły, jak i swoisty. Wraz ze zmianą kryteriów w celu poprawy czułości, pogarsza się swoistość – i odwrotnie. Dlatego powszechną strategią jest użycie dwóch testów w fazach:

1. Stosuje się bardzo czuły test, aby uzyskać jak najwięcej pozytywnych wyników, wiedząc, że niektóre z nich mogą być fałszywie pozytywne.
2. Przypadki, które nie przeszły pierwszego testu, poddawane są testowi o wysokim poziomie swoistości, aby wyeliminować fałszywie pozytywne wyniki.

Taka kombinacja dwóch testów jest często najbardziej opłacalnym sposobem identyfikacji wszystkich prawdziwie pozytywnych wyników w danej populacji.

W przypadku oceny środków bezpieczeństwa, kontrola defektu działa podobnie jak przesiewowy test medyczny. Zapewnia ostrzeżenie, że jeden lub kilka środków wspierających dany cel zawiodło, ale ponieważ możliwe jest, że nie działa tylko jedno zabezpieczenie, nie można założyć, że dotyczy to wszystkich, ani określić, który środek bezpieczeństwa zawiódł.

Aby określić, który konkretnie środek (środki) bezpieczeństwa wspierający dany składnik zdolności zawiódł, stosuje się analizę przyczyn źródłowych. Patrz podrozdział 7.2, Analiza przyczyn źródłowych.

W przykładzie z zabezpieczeniami łańcucha dostaw, można wyobrazić sobie scenariusz, w którym analiza przyczyn źródłowych wykazała, że prowadzono listę zatwierdzonych producentów urządzeń, ale zainstalowano urządzenie zakupione od niezatwierdzonego producenta. Analiza przyczyn źródłowych mogłaby wykazać, że wada wynikała z problemu w ramach procesu zabezpieczania zmian w konfiguracji (zabezpieczenie CM-3).

Analiza trendów mogłaby dodatkowo wskazać, czy słabość procesu zabezpieczania zmian w konfiguracji była powtarzającym się problemem.

Ważne wnioski, które należy wyciągnąć, gdy wynik kontroli defektu nie mieści się w dopuszczalnym zakresie, to:

- jeden lub kilka środków bezpieczeństwa zawiodło;
- analiza przyczyn źródłowych jest wykorzystywana do określenia, które ze środków zawiodły;
- NIE jest przesądzone, że wszystkie wspierające środki zawiodły.

5.4 *Dokumentacja kontroli defektów*

Kontrole defektów są dokumentowane w postaci tabeli o następującej przykładowej formie:

Tabela 15: Przykładowe pozycje z opisem hipotetycznego składnika zdolności do ochrony i kontroli defektu[a)]

Składnik zdolności – przeciwdziałanie stosowaniu nieautoryzowanych urządzeń i kontrola defektu HWAM-F01

Cel tego składnika zdolności został zdefiniowany w następujący sposób:

Nazwa składnika zdolności	**Cel składnika zdolności**
Przeciwdziałanie stosowaniu nieautoryzowanych urządzeń.	Zapobieganie lub ograniczanie obecności nieautoryzowanych urządzeń, a tym samym zmniejszenie liczby urządzeń potencjalnie złośliwych lub stanowiących wysokie ryzyko.

Cel tego składnika zdolności został zdefiniowany w następujący sposób:

Identyfikator kontroli defektu	**Nazwa kontroli defektu**	**Podsumowanie kryteriów oceny**	**Uwagi dotyczące kryteriów oceny**	**Wybrana kontrola defektu**
HWAM-F01	Nieautoryzowane urządzenia	Urządzenie jest obecne w badanym obszarze ("stan rzeczywisty"), ale nie zostało autoryzowane do przebywania w nim ("stan pożądany") [Patrz kryteria uzupełniające w L02].	Uwagi dotyczące kryteriów oceny: Stan rzeczywisty to lista (ewidencja) wszystkich urządzeń (w ramach określonej przez organizację tolerancji) w granicy oceny, określona przez system ISCM. Specyfikacja stanu pożądanego to lista wszystkich urządzeń, których obecność w granicy oceny została autoryzowana. Defekt stanowi obecność urządzenia w stanie rzeczywistym, ale nie w stanie pożądanym, a więc nieautoryzowanym. Kontrola jest wykonywana poprzez proste porównanie zestawów.	Tak

Objaśnienia do[a)]:

- W kolumnie **Nazwa składnika zdolności** podaje się krótką nazwę określającą cel danego składnika zdolności.
- Kolumna **Cel składnika zdolności** zawiera pełny opis celu składnika zdolności.
- Kolumna Identyfikator kontroli defektu zawiera:
  - ✓ Skrót nazwy zdolności do ochrony ISCM (w przykładzie HWAM);
  - ✓ Literę F, L lub Q informującą o tym, czy wstępny poziom kontroli defektów można zakwalifikować jako:
    - Fundamentalny (F);
    - Lokalny (L) poziom kontroli defektu dotyczącej bezpieczeństwa (patrz podrozdział 5.9, Fundamentalne i lokalne kontrole defektów); lub
    - Kontrola jakości danych (Q) (patrz podrozdział 5.5 Wskaźniki jakości danych); oraz
  - ✓ Numer służący do jednoznacznej identyfikacji kontroli.
- Kolumna **Nazwa kontroli defektu** zawiera krótką nazwę służącą do identyfikacji kontroli defektu.
- Kolumna **Podsumowanie kryteriów oceny** zawiera krótki opis sposobu określania (obliczania) obecności defektu.
- Kolumna **Uwagi dotyczące kryteriów oceny** zawiera dodatkowe informacje na temat kryteriów oceny. Uwagi dotyczące kryteriów oceny określają przynajmniej:
  - ✓ Jakie dane są wykorzystywane, aby określić:
    - stan rzeczywisty; oraz
    - specyfikację stanu pożądanego; oraz
  - ✓ W jaki sposób zestawy danych specyfikacji stanu rzeczywistego i stanu pożądanego są wykorzystywane do identyfikacji wady.
- Kolumna **Wybrana** zawiera słowo „tak”, jeśli organizacja zdecydowała się na wybranie kontroli defektu do wdrożenia.

Potencjalne działania w zakresie reakcji na defekty oraz odpowiedzialne za to role zostały wymienione w dodatkowej tabeli. Na przykład:

Przykładowe środki zaradcze/reakcje: Następujące reakcje i/lub środki zaradcze (z przykładowymi przypisanymi rolami) są powszechne i właściwe w przypadku wykrycia defektu w składniku zdolności: *przeciwdziałanie stosowaniu nieautoryzowanych urządzeń*. Przedstawione przykładowe role nie zmieniają ogólnych obowiązków w zakresie zarządzania określonych w innych dokumentach NSC. Co więcej, obowiązki związane z zarządzaniem mogą być dostosowywane przez każdą organizację w celu jak najlepszego dopasowania do lokalnych warunków.

Identyfikator kontroli defektu	**Opis środków zaradczych/reakcji**	**Główna osoba odpowiedzialna**
HWAM-F01	Usunięcie urządzenia	DM
HWAM-F01	Autoryzacja urządzenia	DSM
HWAM-F01	Akceptacja ryzyka	RskEx
HWAM-F01	Zapewnienie odpowiedniej reakcji	DSM

W tej tabeli zasugerowano również *główną osobę odpowiedzialną*. Osoba pełniąca rolę, na której spoczywa główna odpowiedzialność, określa najbardziej odpowiednią reakcję i zapewnia, że działanie w ramach reakcji jest przypisane do odpowiedniej roli. Odpowiedzialność została określona zarówno na poziomie ról kierowniczych i/lub operacyjnych organizacji. Patrz rozdział 8, Role i obowiązki.

Uwagi dotyczące kryteriów oceny są celowo dość ogólne, aby zapewnić organizacjom elastyczność w ich wdrażaniu. Są one jednak na tyle szczegółowe, aby organizacja mogła zaprojektować wiarygodny (powtarzalny) test.

W tomach dotyczących poszczególnych zdolności do ochrony wyjaśniono konkretne cele, które mają być osiągnięte przez każdy składnik zdolności, i wspierające jego realizację środki bezpieczeństwa, ponieważ składniki i wspierające je środki są związane ze zdolnością objętą danym tomem. Kontrole defektów mają na celu zapewnienie wiarygodnej metody określania, czy (i w jakim stopniu) cel składnika zdolności jest osiągany.

5.5 *Wskaźniki jakości danych*

Opisane wcześniej środki mają znikomą wartość, jeśli zebrane dane nie są zarówno kompletne, jak i aktualne. Do oznaczenia kontroli jakości danych w ich kodzie identyfikacyjnym (ID) stosuje się przedrostek w postaci litery „Q".

Kompletność oznacza stopień, w jakim informacje związane z bezpieczeństwem obejmują wyniki oceny wszelkich istotnych defektów wszystkich obiektów oceny (w określonym zakresie, takim jak zdolność do ochrony). *Istotne defekty* to takie, które powodują znaczne ryzyko, np. dwa pierwsze rzędy wielkości. Niekompletne dane mają tendencję do zniekształcania wyników poprzez niedoszacowanie całkowitego ryzyka.

Aktualność oznacza stopień, w jakim informacje związane z bezpieczeństwem zostały odnowione w ciągu ostatnich X godzin lub dni (zgodnie z ustaleniami/wymaganiami organizacji). Dane muszą być zbierane (a defekty usuwane) szybciej niż atakujący może działać, aby wyprzedzić jego zdolność do naruszenia bezpieczeństwa systemu[28].

Jeśli wskaźniki kompletności i aktualności nie są odpowiednie, ocena nie jest wiarygodna, ponieważ wyniki mogą być niedokładne.

Tabela 16: Wskaźniki jakości danych

Rodzaj wskaźnika	Opis	Zakres stosowania tego wskaźnika
Wskaźniki kompletności i/lub aktualności	Procent urządzeń, dla których gromadzone są kompletne i aktualne dane.	Ustawienie zdefiniowanego przez organizację progu dla wskaźników kompletności i aktualności powoduje uruchomienie alarmu, gdy ogólny poziom kompletności i aktualności (odpowiednio) jest zbyt niski, aby zapewnić wiarygodne wyniki dotyczące wad.

5.6 *Grupy urządzeń, które należy wziąć pod uwagę przy tworzeniu kryteriów oceny*

W celu zarządzania ryzykiem dla systemów, zgodnie z definicją w publikacji NSC 800-37 urządzenia są grupowane według systemu (tj. granicy autoryzacji), aby umożliwić analizę ryzyka na poziomie systemu.

[28] Ocena oparta na zdarzeniach nie zawsze jest wykonalna, jednak umożliwia wykrycie defektów w momencie ich pojawienia się i zapewnia największą aktualność.

Jednak informacje dotyczące bezpieczeństwa uzyskane w wyniku zautomatyzowanej oceny zabezpieczeń w większej granicy oceny sprawiają, że osoba odpowiedzialna za zarządzanie ryzykiem ma możliwość przyjrzenia się ryzyku dla innych grup urządzeń w celu lepszego zidentyfikowania koncentracji ryzyka i zagregowanego ryzyka.

Grupy, które mogą być przydatne, obejmują urządzenia, które są:

- określone jako krytyczne dla misji;
- niezbędne dla zintegrowanej funkcji biznesowej;
- zarządzane przez oddzielnego partnera biznesowego;
- wsparciem określonej misji w całej organizacji; lub
- wsparciem dla konkretnego klienta.

Analiza ryzyka (z uwzględnieniem zdefiniowanych przez organizację progów) w tak dużych grupach urządzeń pomaga organizacji przeciwdziałać zagrożeniom dla całej organizacji i misji/biznesu, jak opisano w publikacji NSC 800-39.

5.7 *Grupy urządzeń, które należy wziąć pod uwagę przy tworzeniu kryteriów oceny*

Metody oceny mają na celu wykrycie nieprawidłowego działania lub braku środka bezpieczeństwa. W koncepcji inżynierii jakości nieprawidłowe działanie lub brak środków nazywa się zwykle *defektami*.

Na przykład, w terminologii dotyczącej metody Six Sigma, defekt to produkt (obiekt oceny) posiadający określoną cechę (stan rzeczywisty), która nie mieści się w granicach specyfikacji (stan pożądany).

Aby uniknąć nieporozumień, w publikacji NISTIR 8011 do opisu nieprawidłowego działania lub braku środka bezpieczeństwa używa się terminu *defekt*, oznaczającego defekt zabezpieczeń, a nie terminów *podatność* lub *słabość*. Stosowanie terminu *podatność* lub *słabość* mogłoby spowodować mylenie szerokiego pojęcia nieprawidłowego działania/ braku środka bezpieczeństwa ze znacznie bardziej precyzyjnymi pojęciami powszechnych *podatności* i zagrożeń (*ang. Common Vulnerabilities and Exposures – CVE*) oraz powszechnych enumeracji *słabości* (*ang.*

Common Weakness Enumerations – CWE). Należy jednak zaznaczyć, że chociaż w niniejszej publikacji unika się stosowania terminów *podatność* i *słabość*, uznaje się, że z perspektywy zarządzania ryzykiem defekt zabezpieczenia *stanowi* co najmniej jedną podatność lub słabość w systemie lub jego środowisku działania.

5.8 *Wybrane/niewybrane środki bezpieczeństwa i kontrole defektów*

Środki bezpieczeństwa, które należy ocenić w ramach programu ISCM, ograniczają się do tych zabezpieczeń z publikacji NSC 800-53, które są wskazane jako elementy zestawu zabezpieczeń bazowych o niskim, umiarkowanym i wysokim wpływie i zawarte są w publikacji NSC 800-53B.

Kontrole defektów są zorganizowane w taki sposób, aby można było łatwo określić, które z nich dotyczą danego zestawu zabezpieczeń bazowych.

Publikacja NSC 800-53 obejmuje również zabezpieczenia podstawowe i rozszerzone, które nie zostały wybrane do żadnego zestawu zabezpieczeń bazowych. Jeśli system został dostosowany poprzez wdrożenie jednego lub kilku środków niewymienionych pośród zabezpieczeń bazowych, organizacja może stworzyć zautomatyzowaną kontrolę defektów lub przeprowadzić ręczną/proceduralną ocenę skuteczności danego środka bezpieczeństwa. Każdy tom publikacji NISTIR 8011, dotyczący konkretnej zdolności, zawiera odnośniki do listy niewybranych środków bezpieczeństwa związanych z tą zdolnością.

5.9 *Fundamentalne i lokalne kontrole defektów*

W publikacji NSC 800-53A stwierdza się, że:

> *Nie oczekuje się, że organizacje będą stosować wszystkie metody i obiekty oceny ujęte w procedurach oceny opisanych w niniejszej publikacji dla powiązanych środków bezpieczeństwa wdrożonych w systemach organizacji lub przez nie dziedziczonych. Przeciwnie, organizacje mają zapewnioną elastyczność w określaniu poziomu nakładu środków koniecznych do przeprowadzenia danej oceny (np. tego, które metody oceny i obiekty oceny zostaną uznane za najbardziej przydatne do uzyskania pożądanych rezultatów). Określenie to jest dokonywane na podstawie ustalenia, co pozwoli osiągnąć cele oceny w sposób najbardziej opłacalny i zapewniający wystarczającą pewność, aby wesprzeć późniejsze określenie ryzyka związanego z misją lub działalnością.*

Podobnie, nie oczekuje się od organizacji stosowania wszystkich kontroli defektów (które same w sobie są metodami oceny) opisanych w niniejszej publikacji.

Kontrole defektów opisane w NISTIR 8011 zostały podzielone na trzy rodzaje – fundamentalne, lokalne oraz kontrole defektów jakości danych. Należy zwrócić uwagę, że kontrole defektów jakości danych zostały opisane w podrozdziale 5.5.

- **Fundamentalne kontrole defektów** – kontrole mające podstawowe znaczenie dla celów danej zdolności (np. HWAM, SWAM lub zarządzanie ustawieniami konfiguracyjnymi), w których pojawia się kontrola defektu.
- **Lokalne kontrole defektów** – kontrole, o których wdrożeniu decyduje dana organizacja. W odniesieniu do lokalnych kontroli defektów, organizacja:
  - ✓ Może nie wdrożyć danej kontroli, ponieważ dotyczy ona elementu zabezpieczenia, który znajduje się w zestawie zabezpieczeń bazowych niestosowanym w danej organizacji (np. element zabezpieczenia znajduje się w zestawie o wysokim wpływie, ale organizacja posiada tylko systemy o niskim i umiarkowanym wpływie) lub w określonym systemie organizacji.
  - ✓ Może nie wdrożyć kontroli, ponieważ służy ona do oceny elementu zabezpieczenia, który nie jest w ogóle wdrożony w organizacji lub w konkretnym systemie (tj. został on usunięty w ramach dostosowania, z odpowiednim uzasadnieniem).
  - ✓ Może wdrożyć kontrolę tylko dla określonych obiektów oceny w systemie, dla których został wdrożony powiązany środek bezpieczeństwa.
  - ✓ Może wdrożyć alternatywną wersję lokalnej kontroli defektów.
  - ✓ Może stosować ręczne/proceduralne metody oceny dla niektórych elementów zabezpieczeń.

Organizacja może dostosować tabele kontroli defektów poprzez zmianę opisu kontroli (dodanie kontroli, edycję kontroli, wyjaśnienie ról, cofnięcie wyboru kontroli). Tabela 15: Przykładowe wiersze z opisem hipotetycznego składnika zdolności do ochrony i kontroli defektu, zawiera przykład części tabeli kontroli defektów.

W celu zautomatyzowania oceny środków bezpieczeństwa w największym możliwym stopniu i wspierania bieżącej autoryzacji, konieczne jest wdrożenie odpowiednich fundamentalnych i lokalnych kontroli defektów zdefiniowanych w niniejszej publikacji dla *wszystkich* wdrożonych elementów zabezpieczeń.

5.10 *Dokumentowanie decyzji dotyczących dostosowywania*

Organizacje mogą podać uzasadnienie decyzji o wyborze kontroli defektu w kolumnie *Wybrana* tabeli kontroli defektów.

Organizacje mogą również dodawać lub edytować lokalne kontrole defektów, jeśli zachodzi taka potrzeba, w celu zarządzania własnym ryzykiem, np. kontrole defektów mogą być dodawane dla środków bezpieczeństwa wdrożonych jako uzupełniające.

Nazwy ról i/lub granic oceny mogą być również zmienione na bardziej konkretne, mające zastosowanie w organizacji.

6. DOKUMENTACJA PLANU OCENY

Bazując na definicjach stanu rzeczywistego, specyfikacji stanu pożądanego oraz kontroli defektów z poprzednich rozdziałów, w niniejszym rozdziale opisano dokumentację, która może być tworzona dla każdej zdolności do ochrony ISCM, oraz sposób, w jaki publikacja NISTIR 8011 ułatwia tworzenie dokumentacji planu oceny bezpieczeństwa.

W odniesieniu do planu oceny ISCM, organizacja może:

- Wykorzystać rządowy plan oceny ISCM, bez wprowadzania w nim zmian[29].
- Samodzielnie opracować własny plan oceny.
- Stworzyć rozwiązanie hybrydowe, które będzie łączyło elementy obu tych rozwiązań.

6.1 *Wprowadzenie do treści planu oceny bezpieczeństwa*

Tomy publikacji NISTIR dotyczące poszczególnych zdolności do ochrony zawierają treść planu oceny bezpieczeństwa, która może spełniać jego rolę, zgodnie z definicją zawartą w publikacji NSC 800-37 i NSC 800-53A. Treść planu oceny bezpieczeństwa, opracowana zgodnie z rekomendacjami NSC, może być przyjęta w obecnym kształcie lub z minimalnymi zmianami jako dokumentacja planu oceny bezpieczeństwa organizacji w celu opisu zastosowanych środków bezpieczeństwa/elementów zabezpieczeń ocenianych w ramach kontroli defektów. Ponadto, treść można dostosować do potrzeb organizacji. W rozdziale 6.8, Dokumentowanie wybranych środków bezpieczeństwa i decyzji o dostosowaniu opisano, w jaki sposób organizacja może zmienić treść planu oceny bezpieczeństwa. Przykład możliwego szablonu treści planu oceny bezpieczeństwa, opracowany na podstawie zdolności HWAM, znajduje się w rysunku 7: *Przykład treści planu oceny bezpieczeństwa*. Należy pamiętać, że organizacje mają możliwość modyfikacji treści planu oceny bezpieczeństwa, jeśli zachodzi taka potrzeba (np. poprzez wstawienie dodatkowych kolumn).

[29] W Polsce nie funkcjonuje regulacja, którą można by uznać za rządowy plan oceny ISCM. Przy opracowywaniu własnego planu można oprzeć się na planach innych krajów, o ile są dostępne i adekwatne dla organizacji.

Element zabezpieczenia CM-3(f): ZABEZPIECZANIE ZMIAN KONFIGURACJI

Tekst elementu zabezpieczenia:

Zabezpieczenie:

d. Audyt i przegląd działań związanych z kontrolowanymi przez konfigurację zmianami w {urządzeniach i podzespołach urządzeń w} systemie.

Wymóg dla zabezpieczenia 1: [patrz podrozdziały 6.2 i 6.3]

Identyfikator wymogu dla zabezpieczenia	**Tekst wymogu dla zabezpieczenia**
CM-3(f)(1)	Ustalić, czy: f. przeprowadza audyty i przeglądy dokonanych zmian w zabezpieczeniach systemu informacyjnego;

Role i metody oceny: [patrz podrozdział 6.4]

Identyfikator wymogu dla zabezpieczenia	**Wdrożone przez**	**Granica oceny**	**Obowiązek oceny**	**Metody oceny**	**Wybrana**	**Uzasadnienie akceptacji ryzyka**	**Częstotliwość oceny**	**Skutki braku wdrożeni**
CM-3(f)(1)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				

Tabela z uzasadnieniem stosowania kontroli defektów: [patrz podrozdział 6.5]

Brak skuteczności elementu zabezpieczenia skutkuje wykryciem defektu w jednej lub kilku z następujących kontroli defektów:

Identyfikator wymogu dla zabezpieczenia	**Identyfikator kontroli defektu**	**Nazwa kontroli defektu**	**Uzasadnienie** Jeżeli [wskaźnik zdefiniowany przez organizację] dla tej kontroli defektu przekracza [*wartość progowa* zdefiniowana przez organizację], **to defekty w ewidencji {urządzeń i podzespołów urządzeń} systemu, która obejmuje wszystkie składniki w ramach granicy autoryzacji opracowywanych/dokumentowanych lub bezpośrednio związanych z tym elementem zabezpieczenia**, mogą być przyczyną…
CM-3(f)(1)	HWAM-Q01	Brak zgłaszania urządzeń	Braku zgłoszenia urządzenia w określonych ramach czasowych.
CM-3(f)(1)	HWAM-Q02	Brak	Braku zgłoszenia konkretnych kontroli

		zgłaszania kontroli defektów	defektów.
CM-3(f)(1)	HWAM-Q03	Niski wskaźnik kompletności	Nieosiągnięcia progu ogólnej kompletności przez raporty ISCM.
CM-3(f)(1)	HWAM-Q04	Niski wskaźnik aktualności	Niedostateczna terminowość raportowania ISCM.

Należy pamiętać, że ten przykładowy szablon nie jest kompletny. Kompletna i miarodajna wersja znajduje się w odpowiednim tomie niniejszej publikacji NSC RT 8011.

Rysunek 7: Przykład treści planu oceny bezpieczeństwa

6.2 *Zakres oceny*

Należy pamiętać, że pojedynczy element zabezpieczenia może wspierać wiele zdolności do ochrony. W ramach danej zdolności brany jest pod uwagę tylko sposób, w jaki element zabezpieczenia wspiera tę zdolność. Sformułowanie „{urządzeń i podzespołów urządzeń}" wstawione w przykładzie na Rysunku 7: *Przykład treści planu oceny bezpieczeństwa*, dodano w celu wyjaśnienia jego zakresu w odniesieniu do zdolności HWAM i wymogu dla zabezpieczenia. Takie wstawki specyficzne dla danej zdolności zostały podane w każdym tomie dotyczącym konkretnej zdolności.

6.3 *Wymogi dla zabezpieczeń w treści planu*

Z wieloma elementami zabezpieczeń powiązany jest więcej niż jeden wymóg dla zabezpieczenia. Przykład na rysunku 7: Przykład treści planu oceny bezpieczeństwa, dotyczy pojedynczego elementu zabezpieczenia, CM-3(f), ale wymaga on dwóch wymogów dla zabezpieczenia, CM-3(f)(1) i CM-3(f)(2). W tabeli 17: *Przykład elementu zabezpieczenia* i dotyczących go wymogów dla zabezpieczenia pokazano tekst elementu zabezpieczenia i dwa wymogi dla zabezpieczenia. Należy zauważyć, że każdy wymóg dla zabezpieczenia ma swój własny opis metody oceny, chociaż na rysunku 7 został przedstawiony tylko jeden, CM-3(f)(1).

Tabela 17: Przykład elementu zabezpieczenia i dotyczących go wymogów dla zabezpieczenia

Tekst elementu zabezpieczenia	**CM-3(f)**: Audyt i przegląd działań związanych z kontrolowanymi przez konfigurację zmianami w {urządzeniach i podzespołach urządzeń w} systemie; oraz
Wymóg dla zabezpieczenia 1	**CM-3(f)(1): Ustalić, czy:** f. Działania dotyczące audytu związane z kontrolowanymi przez konfigurację zmianami w {urządzeniach i podzespołach urządzeń w} systemie są wykonywane.
Wymóg dla zabezpieczenia 2	**CM-3(f)(2): Ustalić, czy:** f. Działania dotyczące przeglądu związane z kontrolowanymi przez konfigurację zmianami w {urządzeniach i podzespołach urządzeń w} systemie są wykonywane.

Oznaczenie wymogu dla zabezpieczenia zawiera identyfikator elementu zabezpieczenia z publikacji NSC 800-53. W tym przypadku jest to CM-3(f), po którym następuje numer zabezpieczenia w nawiasie (jak pokazano w tabeli 17). Każdy wymóg dla zabezpieczenia zawiera takie same wyrażenia kwalifikujące, jakie zastosowano dla elementu zabezpieczenia (zgodnie z opisem w podrozdziale 6.2, Zakres oceny).

6.4 *Role i metody oceny w treści planu*

Do każdego wymogu dla zabezpieczenia dołączona jest tabela, w której dokumentowane są role i metody oceny. W tej części treści planu oceny bezpieczeństwa określa się:

- Rolę odpowiedzialną[30] za wdrożenie elementu zabezpieczenia (w celu sprecyzowania odpowiedzialności za defekty).
- Granicę oceny (aby sprecyzować zakres oceny, patrz podrozdział 4.3, Granica autoryzacji i granica oceny).

[30] Określone role to role kierownicze (podrozdział 8.1) lub role operacyjne (podrozdział 8.2).

- Rolę odpowiedzialną[31] za ocenę środków bezpieczeństwa.
- Metody oceny do zastosowania (patrz podrozdział 2.2, Automatyzacja testowej metody oceny).

6.5 *Tabela z uzasadnieniami stosowania kontroli defektów*

W ramach treści planu oceny bezpieczeństwa, tabela z uzasadnieniami stosowania kontroli defektów umożliwia powiązanie kryteriów oceny dla każdej stosowanej kontroli defektu z wymogiem dla zabezpieczenia. W tabeli tej określa się, które kontrole defektów kończą się niepowodzeniem, jeżeli dany wymóg dla zabezpieczenia nie został spełniony, oraz (w kolumnie uzasadnienia) w jaki sposób stosuje się kontrolę defektu (patrz przykład na rysunku 7: Przykład treści planu oceny bezpieczeństwa). W tabeli z uzasadnieniem stosowania kontroli defektów określa się, w jaki sposób kontrola defektów w rzeczywistości ocenia spełnianie wymogu danego elementu zabezpieczenia i zawiera wszystkie stosowne kontrole defektów dla każdego wymogu. W kolumnach *Kontrola defektu* i *Uzasadnienie* tabeli kryteriów oceny znajdują się następujące informacje:

- Kolumny kontroli defektów – *Identyfikator kontroli defektu* i *Nazwa kontroli defektu* – identyfikują w tabelach kontrole *defektów*, które służą do oceny danego środka bezpieczeństwa/elementu zabezpieczenia. Opisy sposobu stosowania kontroli *defektów* do danego elementu zabezpieczenia znajdują się w tabelach kontroli *defektów* w tomach dotyczących poszczególnych zdolności.
- Kolumna *Uzasadnienie* zawiera opis warunków, w których niepowodzenie kontroli *defektu* może być spowodowane nieskutecznością środka bezpieczeństwa. Co więcej, jeśli dany środek zawodzi zbyt często (względem zdefiniowanego przez organizację progu), może spowodować nieskuteczność kryteriów testu bezpieczeństwa dla kontroli *defektu*.

Należy pamiętać, że kontrola *defektu* może zakończyć się niepowodzeniem również dlatego, że inna powiązana z nią kontrola nie powiodła się (patrz rozdział 5.2, Interpretowanie kontroli *defektów* jako testów elementów zabezpieczeń). Samo niepowodzenie kontroli *defektu* nie dowodzi, że dany środek bezpieczeństwa jest

[31] Tamże.

nieskuteczny, ponieważ kontrola *defektu* nie jest swoista na poziomie środka bezpieczeństwa lub elementu zabezpieczenia. Kryteria oceny są raczej zaprojektowane w taki sposób, aby w przypadku nieskuteczności elementu zabezpieczenia kryteria oceny kontroli *defektu* elementu zabezpieczenia - wymogu dla zabezpieczenia (*ang. control item-determination statement - CI-DS*) - wskazywały na jego nieskuteczność. Informacje o tym, jak ustalić, które elementy zabezpieczenia spowodowały niepowodzenie kontroli defektu, znajdują się w podrozdziale 7.2 dotyczącym analizy przyczyn źródłowych. W przypadku ustalenia, że dany element zabezpieczenia nie działa, całe zabezpieczenie jest przynajmniej częściowo nieskuteczne.

6.6 *Dostosowywanie treści planu oceny bezpieczeństwa*

Jak zaznaczono wcześniej, konieczne jest stosowanie tylko tych kontroli defektów, które służą do oceny wdrożonych środków bezpieczeństwa. Lokalne kontrole defektów zapewniają większą szczegółowość oceny i mogą być wybrane przez organizację w oparciu o jej tolerancję ryzyka i potrzebę większej pewności przy wdrażaniu odpowiednich środków bezpieczeństwa. Ponadto, każda organizacja ma możliwość elastycznego wykorzystania treści planu w obecnej formie lub zmodyfikowania go w celu zapewnienia spójności ze swoimi wymogami, politykami i procedurami dotyczącymi zarządzania ryzykiem. Modyfikacje mogą obejmować między innymi:

- Usuwanie lub dodawanie lokalnych kontroli defektów.
- Podanie specyficznej dla danej organizacji definicji takich terminów jak systemy oceniane w ramach ISCM, sieć docelowa ISCM itp.
- Dodawanie, modyfikowanie lub usuwanie potencjalnych opcji reakcji.
- Wyjaśnienie specyficznych dla organizacji procesów, które towarzyszą każdej potencjalnej opcji reakcji.
- Stosowanie specyficznej dla danej organizacji terminologii w odniesieniu do działań związanych z reagowaniem, ról i obowiązków.
- Odnotowanie, które kontrole defektów zostały wybrane.

Decyzje dotyczące dostosowywania mogą być udokumentowane w tabelach alokacji środków bezpieczeństwa opisanych w podrozdziale 6.7, zgodnie z metodami opisanymi w podrozdziale 6.8.

6.7 Tabele alokacji środków bezpieczeństwa

Tabele alokacji środków bezpieczeństwa (*ang. Control Allocation Table – CAT*) zostały opracowane w celu dokumentowania planów oceny bezpieczeństwa dla zabezpieczeń bazowych o wysokim, umiarkowanym i niskim poziomie wpływu w ramach każdej zdolności do ochrony.

Tabele CAT mają stanowić podsumowanie treści planu oceny bezpieczeństwa i są wykorzystywane do wskazania, które środki bezpieczeństwa zostały wybrane. Ułatwia to określenie, które kontrole defektów są wymagane.

Tabela CAT znajduje się w każdym tomie publikacji NISTIR 8011 dotyczącym konkretnej zdolności. Tabele CAT zawierają podsumowanie treści planu oceny bezpieczeństwa przedstawionej powyżej. Tabela 18: *Wyjaśnienie kolumn tabeli alokacji środków bezpieczeństwa*, zawiera definicje kolumn w CAT. Tabela 19: Tabela alokacji hipotetycznych środków bezpieczeństwa – przykład, zawiera przykład tabeli alokacji środków bezpieczeństwa. Przykład ten ilustruje, w jaki sposób w tabeli podsumowuje się treść planu: Opisy w rysunku 7: Przykład treści planu oceny bezpieczeństwa, można porównać z odpowiednim wierszem w tabeli 19: Tabela alokacji hipotetycznych środków bezpieczeństwa – przykład, aby sprawdzić, jak można podsumować treść planu. Jeśli organizacja zdecyduje się na dostosowanie treści planu oceny bezpieczeństwa, należy zmodyfikować tabele alokacji środków bezpieczeństwa w celu zachowania spójności.

Należy zwrócić uwagę, że tabela nie zawiera wyjaśnienia, w jaki sposób każda kontrola defektu wspomaga ocenę środka bezpieczeństwa. Takie informacje znajdują się w tabelach kryteriów oceny w treści planu oceny bezpieczeństwa.

Tabela 18: Wyjaśnienie kolumn tabeli alokacji środków bezpieczeństwa

Kolumna	Wyjaśnienie
Identyfikator wymogu dla zabezpieczenia	Umożliwia powiązanie z elementem zabezpieczenia z publikacji NSC 800-53, który jest testowany.

Kolumna	Wyjaśnienie
Wdrożone przez	Rola lub system, na którym spoczywa główna odpowiedzialność za wdrożenie ocenianego zabezpieczenia i jego elementów.
Granica oceny	Granica oceny ISCM, w której znajduje się środek bezpieczeństwa.
Obowiązek oceny	Podmiot dokonujący oceny.
Metoda oceny	Ogólnie – „Test” w przypadku oceny automatycznej i „TBD” w przypadku oceny ręcznej.
Wybrano?	Służy do udokumentowania, czy dana organizacja lub system wybiera i stosuje test.
Uzasadnienie akceptacji ryzyka	Umożliwia udokumentowanie uzasadnienia dla niewybrania lub akceptacji ryzyka dla wybranego środka bezpieczeństwa, gdy wyniki oceny są inne niż zadowalające.
Częstotliwość monitoringu[a]	Minimalna częstotliwość, z jaką ma być przeprowadzany test.
Skutki braku wdrożenia	Skutki dla obiektów oceny organizacji, osób fizycznych, innych organizacji i państwa, jakie może mieć nieskuteczność tego środka bezpieczeństwa.

[a] Częstotliwości określone w tej kolumnie są co najmniej równe częstotliwościom określonym w strategii ciągłego monitorowania organizacji.

6.8 *Dokumentowanie wybranych środków bezpieczeństwa i decyzji dotyczących dostosowywania*

Oprócz podsumowania treści planu oceny bezpieczeństwa, w kilku kolumnach tabeli CAT znajduje się miejsce na udokumentowanie, w jaki sposób i dlaczego organizacja dostosowała zestaw zabezpieczeń bazowych. Dzięki temu tabela może pomóc w udokumentowaniu planu bezpieczeństwa systemu na następujące sposoby:

- Kolumna *Wybrano* może być wykorzystana do udokumentowania, które środki bezpieczeństwa zostały wybrane do wdrożenia.
- Jeśli w ramach dostosowywania usunięto niektóre środki z odpowiedniego zestawu zabezpieczeń bazowych:
  - ✓ Kolumna *Skutki* może być wykorzystana do udokumentowania zakładanych skutków braku wyboru.
  - ✓ Kolumna *Akceptacja ryzyka* może być wykorzystana do udokumentowania uzasadnienia akceptacji ryzyka (np. uzasadnienie decyzji o dostosowaniu zestawu środków bezpieczeństwa).

Tabela 19: Tabela alokacji hipotetycznych środków bezpieczeństwa – przykład

Identyfikator wymogu dla zabezpieczenia	Wdrożone przez	Granica oceny	Obowiązek oceny	Metody oceny	Wybrano[a]	Uzasadnienie akceptacji ryzyka[a]	Częstotliwość oceny[a]	Skutki braku wdrożenia[a]
CM-8(a)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-8(a)(2)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-8(a)(3)	ISCM-Sys	ISCM-TN	ISCM-Sys	Test				
CM-8(b)(1)	DM	ISCM-TN	ISCM-Sys	Test				
CM-8(b)(2)	DSM	ISCM-TN	ISCM-Sys	Test				
CM-8(4)(1)	DSM	ISCM-TN	ISCM-Sys	Test				
PS-4(d)(1)	DM	ISCM-TN	ISCM-Sys	Test				
SC-15(a)(1)	DM	ISCM-TN	ISCM-Sys	Test				
SC-15(b)(1)	MAN	ISCM-TN	ISCM-Sys	TBD				

[a] Wypełnia organizacja. Należy pamiętać, że ta tabela stanowi jedynie przykład. Autorytatywne tabele dotyczące alokacji środków bezpieczeństwa znajdują się w odpowiednich tomach NISTIR 8011.

7. ANALIZA PRZYCZYN ŹRÓDŁOWYCH

Reagowanie na kontrole defektów odbywa się przy użyciu typowych reakcji w ramach zarządzania ryzykiem określonych w publikacji NSC 800-39. W ramach programu ISCM odpowiedzialność za reagowanie na ryzyko ponosi organizacja, która jest jego właścicielem.

7.1 *Wiedza o tym, kto jest odpowiedzialny*

Aby pulpit nawigacyjny organizacji mógł generować efektywne listy zadań do wykonania w celu reagowania na defekty, wymaga on funkcji identyfikacji konkretnej roli operacyjnej (osoby lub grupy) odpowiedzialnej za reagowanie na każdy defekt (utrzymywanej jako część specyfikacji stanu pożądanego). W zależności od wielkości i złożoności systemu role operacyjne mogą być realizowane:

- przez określoną osobę; lub
- przez grupę z wyznaczonym przełożonym.

Aby właściwe zadanie związane z reagowaniem zostało wykonane i aby dalsze kroki w celu przydzielenia odpowiedzialności za reakcję nie były konieczne (lub były minimalne), niezbędne jest, aby grupy odpowiedzialne były wystarczająco małe, aby umożliwić wyraźne przydzielenie obowiązków.

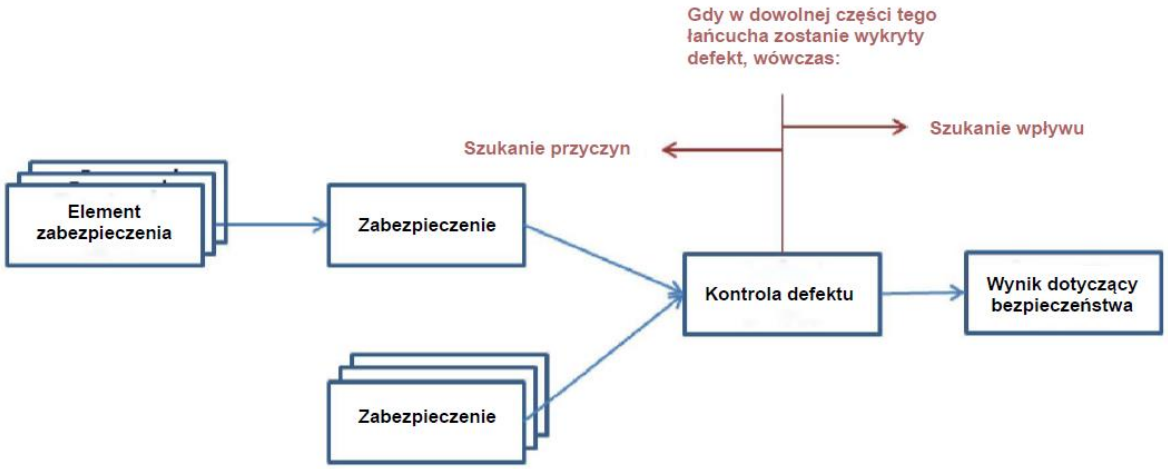
Ponieważ wyniki kontroli defektów mogą być symptomami nieskuteczności jednego lub kilku środków bezpieczeństwa, reakcja będzie prawdopodobnie obejmować pewien zakres analizy przyczyn źródłowych w celu znalezienia przyczyny defektu.

7.2 *Analiza przyczyn źródłowych*

Jak zauważono powyżej, analiza przyczyn źródłowych jest często niezbędna do ustalenia, które zabezpieczenia lub ich elementy zawiodły, jeśli w ramach danej zdolności wykryto defekt.

Analiza przyczyn źródłowych opiera się na logicznym łańcuchu przyczynowo-skutkowym od elementów zabezpieczeń do rezultatu w zakresie bezpieczeństwa, który jest celem zdolności do ochrony (Rysunek 8: *Łańcuch przyczynowo-skutkowy od elementów zabezpieczeń do rezultatów w zakresie bezpieczeństwa*). Pożądanym rezultatem w zakresie bezpieczeństwa jest utrudnienie realizacji scenariuszy ataków

i/lub wykorzystania podatności poprzez zmniejszenie liczby defektów, które mogą być wykorzystane, oraz prawdopodobieństwa, że tak się stanie. Pożądane rezultaty w zakresie bezpieczeństwa są określone dla każdej zdolności do ochrony w kolejnych tomach publikacji NISTIR 8011.



Rysunek 8: Łańcuch przyczynowo-skutkowy od elementów zabezpieczeń do rezultatów w zakresie bezpieczeństwa

Defekt może być zauważony na poziomie elementu zabezpieczenia, całego zabezpieczenia, kontroli defektu i/lub na poziomie ostatecznego rezultatu. Analiza przyczyn źródłowych obejmuje:

- spojrzenie wstecz na elementy zabezpieczeń, aby sprawdzić, czy nieskuteczność którychś z nich mogła spowodować wadę; oraz
- spojrzenie w przód, aby sprawdzić wpływ (pozytywny lub negatywny) na pożądany rezultat w zakresie bezpieczeństwa.

Drugi krok nie powinien być ignorowany, ponieważ spojrzenie w przód może poskutkować stwierdzeniem, że dana nieskuteczność nie zagraża pożądanemu rezultatowi w zakresie bezpieczeństwa, lub że nie ma ona na niego znaczącego negatywnego wpływu. Informacje uzyskane w wyniku analizy przyczyn źródłowych są wykorzystywane do nadania priorytetu wysiłkom mającym na celu naprawę nieprawidłowo działających środków bezpieczeństwa lub do określenia, czy można zaakceptować ryzyko związane z nieprawidłowym działaniem danego zabezpieczenia.

7.2.1 *Sposób przeprowadzenia analizy przyczyn źródłowych: środki bezpieczeństwa*

W przypadku stwierdzenia, że dane zabezpieczenie lub jego element nie działa prawidłowo, należy zastanowić się, dlaczego tak się dzieje. W niektórych przypadkach przyczyna może być oczywista, a właściwym rozwiązaniem może być zwyczajne usunięcie pojedynczego defektu. W innych przypadkach pierwotna przyczyna może być bardziej skomplikowana.

Rzecz jasna, jeśli potrzebna poprawka nie została zastosowana lub ustawienie konfiguracyjne jest nieprawidłowe, zwykle można natychmiast zmniejszyć ryzyko poprzez zastosowanie poprawki lub dostosowanie ustawienia. Jeśli jednak takie problemy stale się powtarzają, warto poszukać przyczyny głębiej. Jednym z kluczowych czynników, których należy poszukiwać w tego rodzaju analizie przyczyn źródłowych, jest istnienie problemu systemowego powodującego powtarzające się defekty.

W tym przypadku warto pomyśleć o oczekiwanym cyklu życia wdrożenia środka bezpieczeństwa i sprawdzić, czy przyczyną problemu jest defekt z wczesnego etapu cyklu życia (tj. defekt techniczny). Oto przykładowe pytania, które mogą ułatwić przeprowadzenie tej analizy.

- Czy zdolność lub funkcja środka bezpieczeństwa wspierająca zdolność została dodana pod koniec cyklu życia systemu, w związku z czym poczyniono zbyt mało przygotowań i planów, czy też funkcja bezpieczeństwa nie jest jeszcze optymalna?
- Czy wprowadzono odpowiednią politykę w celu kierowania wdrażaniem i zarządzania środkami bezpieczeństwa?
- Czy wymagania były właściwie zdefiniowane?
- Czy jednoznacznie jest określona odpowiedzialność za unikanie i naprawianie defektów?
- Czy defekt występuje w przestrzeni między systemami, gdzie może być przeoczony przez oba systemy?

- Czy użytkownicy zachowują się w sposób, który powstrzymuje wzrost lub obniża poziom bezpieczeństwa (np. nie przestrzegają zasad i/lub procedur) i co można zrobić, aby zmienić ich zachowanie?
- Czy administratorzy mogą łatwo uzyskać informacje potrzebne do uniknięcia problemów? Na przykład w Active Directory trudno jest się dowiedzieć, jakie uprawnienia użytkownik dziedziczy z grup nadrzędnych.
- Czy wdrożenie środka bezpieczeństwa było zautomatyzowane (np. zautomatyzowane scentralizowane zarządzanie poprawkami)? Czy automatyczny mechanizm działa prawidłowo?
- Czy w przypadku środków wdrażanych i zarządzanych ręcznie personel posiada niezbędne zasoby, przeszkolenie i narzędzia?
- Czy do wdrożenia środka bezpieczeństwa zastosowano odpowiednie narzędzia i metody?
- Czy w planie wdrożenia przewidziano odpowiednie fundusze, personel i inne zasoby na potrzeby wdrożenia?
- Czy zgodnie z polityką personel operacyjny jest zobowiązany do wykonywania tak wielu zadań związanych z bezpieczeństwem, że są nimi nadmiernie obciążeni?
- Czy wdrożony środek bezpieczeństwa został odpowiednio przetestowany?
- Inne?

Znalezienie takich problemów w organizacji, zwłaszcza jeśli dotyczą one wielu systemów, może być ważnym zadaniem zarówno dla samej organizacji, jak i dla audytorów. Takie ustalenia są znacznie ważniejsze niż lista konkretnych defektów wykryta podczas warsztatów typu Red Team czy ocena pojedynczego systemu. Wprawdzie analiza ta jest trudniejsza niż zgłaszanie pojedynczych defektów środków bezpieczeństwa, jednak znalezienie i rozwiązanie problemów systemowych może mieć znacznie większy wpływ na poprawę programów bezpieczeństwa niż naprawianie różnych zabezpieczeń.

7.2.2 *Sposób przeprowadzenia analizy przyczyn źródłowych: typy defektów*

W przypadku niepomyślnych wyników kontroli defektów konieczne są trzy poziomy analizy przyczyn źródłowych:

1. Ustalenie przyczyn specyficznych dla danego przypadku.
2. Ustalenie, który środek bezpieczeństwa nie działa prawidłowo.
3. Ustalenie przyczyn systemowych.

Poziom 1: Ustalenie przyczyn specyficznych dla danego przypadku. Zazwyczaj polega na ustaleniu, czy pożądana specyfikacja lub stan rzeczywisty są błędne.

a. Czy specyfikacja stanu pożądanego była błędna?

b. Czy stan rzeczywisty był błędny?

We współpracy z SO i SSO wyznaczony personel operacyjny analizuje każdy konkretny przypadek, aby zdecydować, czy opcja (a) lub (b) odnosi się do danego defektu. Równie ważne jest ustalenie, co spowodowało, że defekt jest zgodny z opcją (a) lub (b).

Przykład 1: Administrator systemu podłączył do sieci produkcyjnej wiele urządzeń bez uprzedniego dodania ich do autoryzowanej ewidencji, ich prawidłowego skonfigurowania i zainstalowania poprawek. Ustalenie, że jest to źródłowa przyczyna, wskazuje, że opcja (b), błąd stanu rzeczywistego, jest problemem, ponieważ to stan rzeczywisty (brak poprawek, źle skonfigurowane urządzenia w sieci, a nie błąd w ewidencji) jest defektem. W tym przypadku rozwiązaniem nie jest wyłącznie uzyskanie autoryzacji, przeprowadzenie konfiguracji i instalacja poprawek w urządzeniach, ale również upewnienie się, że administrator systemu rozumie znaczenie przestrzegania procedur operacyjnych.

W odniesieniu do przykładu 1 należy również zauważyć, że nieprawidłowe działanie dotyczy przynajmniej jednego zabezpieczenia lub elementu zabezpieczenia związanego z zarządzaniem stanem rzeczywistym.

Przykład 2: Administrator systemu podłączył wiele urządzeń do sieci produkcyjnej po uzyskaniu ich autoryzacji oraz prawidłowym skonfigurowaniu i zainstalowaniu poprawek. Administrator zapomniał jednak umieścić je wcześniej w ewidencji autoryzowanych składników systemu. Ustalenie, że jest to źródłowa przyczyna, wskazuje, że opcja (a), błąd specyfikacji stanu pożądanego, jest problemem, ponieważ

specyfikacja stanu pożądanego (nieuwzględnienie prawidłowo autoryzowanego urządzenia w ewidencji) jest defektem. W tym przypadku rozwiązaniem jest po prostu wprowadzenie urządzeń do ewidencji i upewnienie się, że administrator systemu rozumie potrzebę dodawania autoryzowanych urządzeń do ewidencji składników systemu przed umieszczeniem ich w sieci.

W odniesieniu do przykładu 2 należy również zauważyć, że nieprawidłowe działanie dotyczy przynajmniej jednego zabezpieczenia lub elementu zabezpieczenia związanego z zarządzaniem specyfikacją stanu pożądanego.

Podsumowując, określenie, czy przyczyną jest opcja (a) czy (b), pomaga również ustalić, które elementy zabezpieczeń nie działają prawidłowo – związane ze specyfikacją stanu pożądanego czy ze stanem rzeczywistym. W celu określenia, które konkretnie elementy zabezpieczeń nie działają prawidłowo, może być konieczna dodatkowa analiza.

Poziom 2: Określenie, które środki bezpieczeństwa nie działają prawidłowo. Należy użyć tabel powiązań zabezpieczeń z kontrolami defektów, przyporządkowujące określone kontrole defektów do określonych elementów zabezpieczeń, które mogą powodować niepomyślny wynik kontroli defektu. Tabele mogą zwiększyć dokładność analizy, ponieważ różne elementy zabezpieczeń, które mogą powodować niepowodzenie kontroli defektu, są bardziej szczegółowe, a tym samym bardziej przydatne do analizy. Tabela powiązań znajduje się w każdym tomie dotyczącym konkretnej zdolności. Tabele powiązań wyglądają w przybliżeniu jak w tabeli 20.

Tabela 20: Hipotetyczny sposób wyszukiwania zabezpieczeń testowanych w ramach kontroli defektu.

Wspierające elementy zabezpieczeń: Składnik zdolności oceniany w ramach tej kontroli defektu jest wspierany przez każdy z poniższych elementów zabezpieczenia. W związku z tym, jeżeli którykolwiek wspierający środek bezpieczeństwa nie będzie działać prawidłowo, kontrola defektu, w ramach której oceniany jest składnik zdolności, zakończy się niepowodzeniem. Tym samym w ramach kontroli defektu testuje się również, pośrednio, elementy zabezpieczenia.

Identyfikator kontroli defektu	**Zabezpieczenie bazowe – poziom wpływu**	**Sortowalny kod elementu zabezpieczenia**	**Kod elementu zabezpieczenia z publikacji NSC 800-53**
HWAM-F01	Niski	AC-19-b	AC-19(b)
HWAM-F01	Niski	CM-08-a	CM-8(a)
HWAM-F01	Niski	CM-08-b	CM-8(b)
HWAM-F01	Umiarkowany	AC-20-z-02-z	AC-20(2)
HWAM-F01	Umiarkowany	CM-03-b	CM-3(b)
HWAM-F01	Umiarkowany	CM-03-c	CM-3(c)
HWAM-F01	Wysoki	CM-03-z-01-a	CM-3(1)(a)
HWAM-F01	Wysoki	CM-03-z-01-b	CM-3(1)(b)
HWAM-F01	Wysoki	CM-03-z-01-d	CM-3(1)(d)

Przykład ten nie obejmuje wszystkich zabezpieczeń, które mogły spowodować niepomyślny wynik tej kontroli defektu. Pełna lista znajduje się w tomie dotyczącym odpowiedniej zdolności do ochrony.

Tabele wspierających elementów zabezpieczeń, przedstawione w całości, znajdują się w każdym tomie dotyczącym konkretnej zdolności, w podrozdziale 3.2, i noszą nazwę *Tabele i szablony składników zdolności oraz kontroli defektów*. Dla każdej kontroli defektu znajduje się tam tabela zatytułowana: *Wspierające elementy zabezpieczeń*.

W tym przypadku osoba analizująca przyczyny źródłowe określa, czy wszystkie wdrożone środki bezpieczeństwa związane z kontrolą defektu działają zgodnie z przeznaczeniem. Jeżeli niektóre lub wszystkie środki bezpieczeństwa nie działają prawidłowo, konieczne może być dokonanie napraw / zmian przez osoby wdrażające zabezpieczenia lub podjęcie decyzji o akceptacji ryzyka przez osobę autoryzującą (z odpowiednim uzasadnieniem).

Należy pamiętać, że po zidentyfikowaniu błędnie działających zabezpieczeń przeprowadzana jest dodatkowa analiza (przyczyn źródłowych), jak opisano w podrozdziale 7.2, Analiza przyczyn źródłowych, w celu ustalenia, dlaczego nie działają one prawidłowo.

Poziom 3: Analiza systemowa: W ramach analizy systemowej poszukuje się przyczyn powtarzających się awarii lub defektów inżynieryjnych i dąży do znalezienia systemowych rozwiązań. W powyższym przykładzie 1 dla poziomu 1, przedmiotowe defekty mogły wystąpić wielokrotnie, ponieważ administrator systemu:

- nie ma możliwości poprawnego skonfigurowania i zainstalowania poprawek na urządzeniach, dopóki nie znajdą się one w sieci produkcyjnej;
- nie przeszedł szkoleń koniecznych, aby wiedzieć, jak przygotować urządzenia przed umieszczeniem ich w sieci produkcyjnej;
- ma zbyt wiele obowiązków i wybiera drogę na skróty, aby nadążyć z wykonywaniem powierzonej mu pracy;
- nie zna procedur operacyjnych; i/lub
- inne możliwe przyczyny.

Jak zauważono powyżej, przeprowadzenie analizy przyczyn źródłowych w celu ustalenia, czy istnieją leżące u podstaw defekty systemowe, i odnalezienia takich przyczyn źródłowych może być bardziej istotne niż skupienie się na pojedynczych defektach.

Po zidentyfikowaniu przyczyn należy przeanalizować również skutki. W tym kontekście można sobie postawić pytanie: Jak ważny jest konkretny problem w kontekście całej organizacji i jej tolerancji na ryzyko? Dla przykładu można rozważyć trzy przypadki przedstawione w tabeli 21: *Scenariusze skutków / analizy skutków, dotyczące nieprzypisania menedżera do urządzenia w sieci*.

Tabela 21: Scenariusze skutków / analizy skutków

Przypadek	Przykładowy scenariusz:	Przykładowa analiza skutków
A	Nie wyznaczono konkretnego menedżera urządzeń i choć ktoś sumiennie zarządza urządzeniami, osoba ta zapomniała zarejestrować urządzenia w ewidencji składników systemu.	Stosunkowo niskie ryzyko krótkoterminowe, ponieważ urządzenie jest w rzeczywistości zarządzane, ale należy zająć się brakiem wyznaczonego menedżera urządzeń, aby osoba odpowiedzialna otrzymywała i reagowała na odpowiednie listy defektów w przyszłości.
B	Urządzenie zostało umieszczone w sieci produkcyjnej w celach testowych, więc nie zostało dodane do ewidencji składników systemu. Urządzenie z czasem stało się podatne na atak z powodu braku poprawek i zarządzania konfiguracją, a zależne od niego obiekty oceny mogą być atakowane za jego pośrednictwem.	Stosunkowo wysokie ryzyko, które prawdopodobnie wzrośnie. Oprócz usunięcia urządzenia z sieci, należy zadbać o szkolenia dla menedżerów urządzeń, aby zapobiec takim zachowaniom w przyszłości.

Przypadek	Przykładowy scenariusz:	Przykładowa analiza skutków
C	Zaistniała potrzeba szybkiego rozszerzenia sieci na potrzeby reakcji na klęskę żywiołową, a kierownictwo zaakceptowało ryzyko wynikające z umieszczenia nieautoryzowanych urządzeń o podwyższonym ryzyku w segmencie sieci bez wcześniejszej autoryzacji na np. 10 tygodni w celu zaspokojenia tej potrzeby. Autoryzacja i inne działania normalizujące sytuację mają nastąpić przed upływem 10 tygodni.	Ryzyko umiarkowane do wysokiego. Fakt, że ryzyko zostało zaakceptowane przez właściwą osobę zarządzającą wskazuje, że nie wystąpił problem systemowy. Możliwe jednak, że organizacja mogłaby znaleźć sposób na lepsze przygotowanie się do takich incydentów, aby uniknąć konieczności akceptacji takiego ryzyka w przyszłości.

Ponieważ zautomatyzowany system oceny środków bezpieczeństwa zwykle identyfikuje defekty na poziomie kontroli defektów, zdolność do zidentyfikowania zarówno przyczyn źródłowych, jak i skutków niepomyślnych wyników kontroli defektów, jak opisano powyżej, ma zasadnicze znaczenie. W przypadku ustalenia istotnych przyczyn systemowych, może istnieć konieczność stworzenia nowych specyfikacji stanu pożądanego w obszarach wspomagających (np. poprzez przeszkolenie administratorów systemu w zakresie określonej umiejętności). Następnie należy wprowadzić zmiany w polityce i odpowiednie kontrole defektów dla nowych specyfikacji stanu pożądanego.

8. ROLE I OBOWIĄZKI

Celem niniejszego dokumentu jest przedstawienie podejścia operacyjnego do wdrażania zautomatyzowanych ocen środków bezpieczeństwa. W rozdziale tym, oprócz obowiązków kierowniczych, zdefiniowane są role i obowiązki operacyjne.

8.1 *Zdefiniowane obowiązki w zakresie zarządzania*

Role i obowiązki w zakresie zarządzania bezpieczeństwem informacji określone w dokumencie NSC 800-37 wskazują, kto ponosi ostateczną odpowiedzialność oraz ma uprawnienia do nadzorowania bezpieczeństwa systemu i zapewnienia spełnienia wymogów bezpieczeństwa udokumentowanych w planie bezpieczeństwa systemu. Odpowiedzialność za zadanie operacyjne, polegające na faktycznym znajdowaniu defektów systemu i reagowaniu na nie, nie jest określona, ale zazwyczaj personel pełniący role operacyjne podlega osobom z przypisanymi rolami na poziomie zarządzania określonymi w dokumencie NSC 800-37.

NSC 800-37 przypisuje odpowiedzialność zarządczą za wykrywanie defektów bezpieczeństwa i reagowanie na defekty na poziomie systemu przez SO i SSO w następujący sposób:

Tabela 22: Obowiązki SO i SSO

Rola	Obowiązki
Właściciel systemu (*ang. System Owner - SO*)	*Właściciel systemu* to osoba w organizacji odpowiedzialna za zakup, rozwój, integrację, modyfikację, eksploatację, utrzymanie i utylizację systemu. SO jest odpowiedzialny za uwzględnienie interesów operacyjnych społeczności użytkowników (tj. użytkowników, którzy potrzebują dostępu do systemu, aby spełnić wymagania związane z misją, działalnością lub operacjami) oraz za zapewnienie zgodności z wymogami bezpieczeństwa informacji.
System Security Officer (SSO)	*System Security Officer* jest osobą odpowiedzialną za zapewnienie utrzymania odpowiedniego stanu bezpieczeństwa operacyjnego systemu i ściśle współpracuje z właścicielem systemu (SO). SSO pełni również rolę głównego doradcy we wszystkich sprawach, technicznych i innych, dotyczących bezpieczeństwa systemu.

Jest mało prawdopodobne, aby SO lub SSO faktycznie podłączał urządzenia do sieci, instalował oprogramowanie, ustawiał wartości konfiguracyjne i instalował poprawki oprogramowania. A przecież są to codzienne zadania operacyjne, służące do zarządzania większością defektów w zakresie bezpieczeństwa punktów końcowych. Dlatego, mimo że osoby te ponoszą ogólną odpowiedzialność za zarządzanie systemem i jego stanem bezpieczeństwa, role SO i SSO mogą być uzupełnione bardziej szczegółowymi rolami operacyjnymi, niezbędnymi do wykonywania codziennych zadań związanych z bezpieczeństwem informacji.

8.2 *Obowiązki operacyjne w zakresie ISCM*

Role i obowiązki operacyjne w zakresie ISCM służą do realizacji zadań, które osoby z przypisaną rolą kierowniczą zazwyczaj delegowałyby innym osobom (patrz tabela 23: *Hipotetyczny przykład ról operacyjnych ISCM dla zdolności HWAM*). W zależności od wielkości i złożoności systemu, role operacyjne mogą być stanowiskami pełnoetatowymi lub zadania mogą być wykonywane wraz z innymi obowiązkami. Organizacje mogą również zdecydować się na przypisanie ról operacyjnych ISCM do SO lub SSO. Każda organizacja może zdefiniować role operacyjne ISCM w różny sposób, jednak celem jest zapewnienie, aby obowiązki operacyjne były przypisane do ról, a następnie do osób lub zespołów o wystarczających możliwościach wykonywania roli. Dlatego zdefiniowane tu role są przykładami, które mają pomóc we wdrożeniu zautomatyzowanej oceny i reakcji oraz w utrzymaniu pożądanego stanu bezpieczeństwa systemu. Organizacje mają dużą swobodę w sposobie wyznaczania ról ISCM. Na przykład mogą chcieć podzielić role, zmienić ich nazwy i/lub połączyć je w celu odzwierciedlenia lokalnej praktyki. Odpowiednie przydzielenie prawdopodobnie będzie się znacznie różnić w przypadku dużych i małych organizacji.

Tabela 23: Hipotetyczny przykład ról operacyjnych ISCM dla zdolności HWAM

Kod roli	Tytuł roli	Opis roli	Typ roli
DM	Menedżer urządzeń (*ang. Device Manager – DM*)	Menedżer urządzeń (DM) przypisany do konkretnego urządzenia lub grupy urządzeń w przypadku HWAM, jest faktycznym zarządcą stanu urządzenia i jest odpowiedzialny za dodawanie/usuwanie urządzeń z sieci oraz za konfigurację sprzętu dla każdego urządzenia (dodawanie i usuwanie urządzeń sprzętowych i komponentów urządzeń). DM jest określony w specyfikacji inwentaryzacji stanu pożądanego. DM może być osobą lub grupą osób. Jeśli jest to grupa, to wyznaczany jest kierownik grupy.	Menedżer operacyjny
DSM	Menedżer stanu pożądanego i osoba autoryzująca (*ang. Desired State Manager and Authorizer – DSM*)	DSM jest potrzebny zarówno dla sieci docelowej ISCM, jak i dla każdego obiektu oceny. DSM zapewnia, że dane określające stan pożądany odpowiedniej zdolności ochrony są wprowadzane do danych o stanie pożądanym systemu ISCM i są dostępne do kierowania podsystemem gromadzenia danych o stanie rzeczywistym oraz do identyfikacji defektów. DSM dla sieci docelowej ISCM rozwiązuje również wszelkie niejasności dotyczące tego, która granica autoryzacji systemu ma defekty. Osoby autoryzujące dzielą część odpowiedzialności DSM, autoryzując określone elementy (np. urządzenia, oprogramowanie lub ustawienia), a tym samym definiując stan pożądany. DSM nadzoruje i organizuje te działania.	Menedżer operacyjny

Należy zauważyć, że na potrzeby tego przykładu nie wszystkie role są wyszczególnione. Pełna lista ról znajduje się w odpowiednim tomie dotyczącym danej zdolności.

Podstawowe dane ISCM to lista defektów, na które należy zareagować. Listy defektów są kierowane do wcześniej określonych ról operacyjnych i/lub zespołów, a zatem przedstawiają tylko te defekty, za które dana rola i/lub zespół jest odpowiedzialny. Jeśli listy defektów nie są ukierunkowane na konkretne role i/lub zespoły, działania związane z reagowaniem na defekty mogą nie być odpowiednio przydzielane lub podejmowane na co dzień. Aby temu zaradzić, można odpowiednio skonfigurować hierarchię pulpitu ISCM i efektywnie przydzielać działania związane z reakcją do odpowiednich ról/zespołów, biorąc pod uwagę prawidłowe informacje o rolach operacyjnych.

Role operacyjne opisują, która osoba lub zespół jest przydzielony do reagowania na określone typy defektów. W związku z tym w tabelach defektów wymieniono rolę odpowiedzialną za koordynację reakcji na każdy defekt. W tabelach defektów są sugerowane potencjalne działania naprawcze, ale mogą one wymagać wprowadzenia lub zatwierdzenia przez SO i/lub SSO. Dodatkowo, jeśli ryzyko ma być zaakceptowane, wymagana jest zgoda osoby autoryzującej.

Wreszcie, pewne role operacyjne dotyczą defektów, których nie można przypisać do konkretnego systemu. Na przykład przypisanie systemowe nieautoryzowanych urządzeń wykrytych w sieci docelowej ISCM może być nieznane. Na poziomie sieci definiuje się specjalną rolę do zarządzania nieprzypisanymi defektami.

Role operacyjne są uzupełnieniem ról zarządczych określonych w dokumencie NSC 800-37. Jednak przy każdej zdolności podano dodatkowe szczegóły, aby wyjaśnić, w jaki sposób należy przeprowadzać zautomatyzowane oceny środków bezpieczeństwa. Każda organizacja może również swobodnie decydować, której z ról kierowniczych podlegają pracownicy pełniący role operacyjne.

9. ZWIĄZEK ZAUTOMATYZOWANEJ OCENY ŚRODKÓW BEZPIECZEŃSTWA Z RAMAMI ZARZĄDZANIA RYZYKIEM

Teraz, gdy proces automatycznej oceny środków bezpieczeństwa został zdefiniowany, ważne jest, aby pokazać, w jaki sposób proces ten odwzorowuje zadania 4 etapu RMF - *Ocena* - z NSC 800-37, oraz udokumentować, jak procesy specyficzne dla ISCM mogą być wykorzystane do utworzenia wymaganej dokumentacji RMF.

Należy zwrócić uwagę, że pomimo użycia terminu *dokumentacja*, nie ma wymogu, aby drukowane były różne dokumenty lub aby były to dokumenty opisowe.
W rzeczywistości może być możliwe czytanie wielu wymaganych dokumentów bezpośrednio na pulpitach nawigacyjnych ISCM.

Warto przechowywać dane o trendach na odpowiednich poziomach agregacji. Organizacje mają jednak możliwość swobodnego określenia, czy chcą przechowywać szczegółowe (na poziomie obiektu oceny) wyniki oceny z każdego dnia. Ogólnie, wystarczające jest posiadanie bieżących szczegółowych wyników oceny i zbiorczych danych dotyczących trendów.

9.1 *Powiązanie ISCM z konkretnymi zadaniami oceny RMF*

Poniższe rozdziały odnoszą się do zadań 4-1 do 4-4 RMF, określonych w NSC 800-37, i wyjaśniają, jak zautomatyzowane dane ISCM mogą być wykorzystane do terminowego tworzenia dokumentacji.

ZADANIE 4-1: Opracowanie, przegląd i zatwierdzenie planu oceny środków bezpieczeństwa.

Tomy dotyczące poszczególnych zdolności zawarte w niniejszym dokumencie NISTIR 8011 stanowią szablon do opracowania i przeglądu wymaganego planu oceny bezpieczeństwa. Należy pamiętać, że niezależnie od sposobu opracowania planu oceny bezpieczeństwa, zatwierdzenie planu jest obowiązkiem organizacji.

Szablon planu oceny bezpieczeństwa jest najpierw wyrażony w opisie środka bezpieczeństwa dla każdego zabezpieczenia, jak pokazano w przykładzie na *rysunku 7: Przykład opisu planu oceny bezpieczeństwa uzupełnionego o tabele kontroli defektów*, oraz w *tabeli 15: Przykładowe wiersze z opisem hipotetycznego składnika zdolności do ochrony i kontroli defektu.*

Tomy dotyczące każdej zdolności zawierają opis planu oceny bezpieczeństwa dla każdego stosowanego zabezpieczenia. Organizacje mogą wykorzystać ten opis w takiej formie, dostosować go do swoich potrzeb i/lub opracować własny. Przykłady obszarów, w których organizacje mogą dostosować opisy, obejmują między innymi następujące kwestie:

- stosowanie w opisach nazw specyficznych dla organizacji odnoszących się do ról i obowiązków;
- wyjaśnienie zakresu sieci docelowych ISCM; lub
- wykonanie dodatkowych rodzajów ocen.

Tabele kontroli defektów i opisy planu oceny bezpieczeństwa stanowią razem dokumentację planu oceny bezpieczeństwa dla zabezpieczeń i elementów zabezpieczeń w zakresie możliwości zautomatyzowanej oceny środków bezpieczeństwa ISCM i są zgodne z wytycznymi zadania 4-1 NSC 800-37. Opisy dotyczące zabezpieczeń są podsumowane w tabelach alokacji środków bezpieczeństwa dla każdego poziomu zabezpieczeń, opisanych w podrozdziale 6.7, Tabele alokacji środków bezpieczeństwa. Należy pamiętać, że zabezpieczenia i elementy zabezpieczeń są oceniane przy użyciu ręcznych metod proceduralnych, natomiast plan oceny bezpieczeństwa jest również dokumentowany zgodnie z wytycznymi zadania 4-1 publikacji NSC 800-37.

ZADANIE 4-2: Dokonanie oceny środków bezpieczeństwa zgodnie z procedurami oceny określonymi w planie oceny bezpieczeństwa.

Tabele alokacji środków bezpieczeństwa zawierają kolumnę odpowiedzialności diagnostycznej (patrz tabela 19: Tabela alokacji hipotetycznych środków bezpieczeństwa — przykład). W przypadku gdy jest to przypisane do kontroli ISCM, program ISCM automatyzuje określone kontrole defektów. Tam, gdzie odpowiedzialność za diagnostykę nie jest przypisana do kontroli ISCM, jest ona przypisana do pracowników organizacji w celu wykonania ręcznej oceny proceduralnej. Szczegółowe informacje znajdują się w tabelach alokacji środków bezpieczeństwa w każdym tomie dokumentu NISTIR 8011, dotyczącym konkretnej zdolności.

ZADANIE 4-3: Przygotowanie raportu z oceny bezpieczeństwa, dokumentującego zagadnienia, ustalenia i zalecenia na podstawie oceny środków bezpieczeństwa.

Pulpit nawigacyjny organizacji zapewnia wymaganą dokumentację wyników oceny, jeśli jest odpowiednio skonfigurowany przez organizację. Konfiguracja ta obejmuje grupowanie ocenianych obiektów według granicy uprawnień, a także według dziedziczonych wspólnych środków bezpieczeństwa.

Informacje z raportu oceny bezpieczeństwa obejmują:

- szczegółowe listy defektów według systemu, podmiotu odpowiedzialnego, urządzenia itd.;
- szczegółowe listy defektów, które przyczyniają się do największego ogólnego ryzyka;
- określone przez organizację priorytety wskazujące, które defekty należy usunąć w pierwszej kolejności;
- sumaryczne poziomy ryzyka według zdolności, menedżera mitygacji skutków, systemu itp.
- oszacowanie konsekwencji danego poziomu ryzyka w celu ułatwienia podejmowania decyzji w zakresie zarządzania ryzykiem, decyzji inwestycyjnych itp.

Informacje z raportu oceny bezpieczeństwa wygenerowane przez pulpit nawigacyjny organizacji są akceptowalne niezależnie od tego, czy zostaną wydrukowane na papierze, czy przedstawione w formie elektronicznej. Podobnie jak w przypadku planu oceny bezpieczeństwa z zadania 4-1, raportowanie oceny bezpieczeństwa zabezpieczeń i elementów zabezpieczeń ocenianych metodami ręcznymi / proceduralnymi jest również dokumentowane zgodnie z wytycznymi zadania 4-3.

ZADANIE 4-4: Przeprowadzenie wstępnych działań naprawczych w zakresie środków bezpieczeństwa w oparciu o ustalenia i zalecenia zawarte w sprawozdaniu z oceny bezpieczeństwa oraz ponowna ocena naprawionych środków bezpieczeństwa w stosownych przypadkach.

Pulpit nawigacyjny organizacji przedstawia ustalenia dotyczące defektów w formie listy priorytetowych zadań do wykonania przez każdą osobę/zespół odpowiedzialny za łagodzenie skutków (remediację). Za działania naprawcze odpowiada każda osoba autoryzująca (w przypadku akceptacji ryzyka), SO, SSO oraz osoby (role operacyjne) wyznaczone w pulpicie nawigacyjnym organizacji do mitygacji ryzyka (np. menedżerowie urządzeń).

Zautomatyzowane narzędzia oceny są często w stanie zapewnić standard okresowej oceny skuteczności środków bezpieczeństwa znacznie częściej niż było to możliwe wcześniej lub jest to możliwe w przypadku ocen ręcznych/proceduralnych. Jednocześnie organizacje zachowują swobodę w określaniu częstotliwości kontroli defektów i związanych z tym raportów opartych na pulpicie nawigacyjnym, jeśli defekty są kontrolowane np. co cztery (4) dni (lub częściej), co wspiera dwa cele:

- pozwala to stronie odpowiedzialnej dowiedzieć się, czy działanie mitygujące zakończyło się sukcesem; oraz
- pojawia się alert, jeśli defekt znów wystąpi.

Rzeczywiste działania naprawcze nie są prowadzone, jednak listy działań o ustalonym priorytecie oraz częstotliwość kontroli defektów w ramach ISCM silnie wspierają wykonywanie zadania 4-4 dla środków bezpieczeństwa w ramach oceny ISCM.

ZAŁĄCZNIK A – REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[32]	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-30	Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne – na podstawie NIST SP 800-30
NSC 800-34	Poradnik planowania awaryjnego – na podstawie NIST SP 800-34
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-39	Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53A	Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B

[32] Narodowe Standardy Cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl (www.gov.pl)

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[32]	
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60
NSC 800-61	Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego – na podstawie NIST SP 800-61
NSC 7298	Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa

PUBLIKACJE ANGLOJĘZYCZNE[33]

POLITYKI, DYREKTYWY, INSTRUKCJE, ROZPORZĄDZENIA I MEMORANDA

1. Office of Management and Budget Circular A-130, July, 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

NORMY

1. NIST National Institute of Standards and Technology Federal Information Processing Standards Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. https://doi.org/10.6028/NIST.FIPS.199

WYTYCZNE I SPRAWOZDANIA MIĘDZYRESORTOWE

1. National Institute of Standards and Technology Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1

2. National Institute of Standards and Technology Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 (updated June 5, 2014). https://doi.org/10.6028/NIST.SP.800-37r1

3. National Institute of Standards and Technology Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011. https://doi.org/10.6028/NIST.SP.800-39

4. National Institute of Standards and Technology Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015). https://doi.org/10.6028/NIST.SP.800-53r4

[33] Publikacje angielski zostały podane w celach uzupełniających dla osób zainteresowanych.

5. National Institute of Standards and Technology Special Publication (SP) 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, December 2014 (updated December 18, 2014). https://doi.org/10.6028/NIST.SP.800-53Ar4

6. National Institute of Standards and Technology Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008. https://doi.org/10.6028/NIST.SP.800-115

7. National Institute of Standards and Technology Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011. https://doi.org/10.6028/NIST.SP.800-137

8. National Institute of Standards and Technology Special Publication (SP) 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, September 2016. https://doi.org/10.6028/NIST.SP.800-160

9. National Institute of Standards and Technology Interagency Report (NISTIR) 7298 Revision 2, *Glossary of Key Information Security Terms*, May 2013. https://doi.org/10.6028/NIST.IR.7298r2

10. National Institute of Standards and Technology Interagency Report (NISTIR) 7756 (DRAFT), *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture*, January 2012. http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7756

ZAŁĄCZNIK B – SŁOWNIK

Załącznik B zawiera definicje pojęć z zakresu cyberbezpieczeństwa, stosowane w publikacji NISTIR 8011.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

Terminologia angielska	Terminologia polska	Definicja
Actual State	Stan rzeczywisty	Obserwowalny faktyczny stan lub zachowanie obiektu oceny (urządzenia, oprogramowania, osoby, danych uwierzytelniających, konta itp.) w momencie, w którym strona zbierająca dane generuje informacje związane z bezpieczeństwem. W szczególności stan rzeczywisty obejmuje stany lub zachowania, które mogą wskazywać na obecność defektów zabezpieczeń.
Anomalous Event Response and Recovery Management	Zarządzanie reagowaniem na zdarzenia nietypowe oraz odzyskiwaniem danych	Patrz *Zarządzanie reagowaniem na zdarzenia nietypowe i usuwaniem ich skutków* .
Agency Dashboard	Pulpit nawigacyjny organizacji	Pulpit nawigacyjny na poziomie organizacyjnym, który: a) gromadzi dane z systemu zbierania danych; oraz b) przedstawia szczegółowe dane i defekty na poziomie obiektu oceny upoważnionym pracownikom organizacji.

Terminologia angielska	Terminologia polska	Definicja
Assessment Boundary	Granica oceny	Zakres (obiektów oceny objętych zakresem) wdrożenia systemu zbierania danych (ISCM) organizacji, do którego stosowana jest ocena obiektów. Zazwyczaj granica oceny obejmuje całą sieć do jej zewnętrznego obwodu.
Assessment Completeness	Kompletność oceny	Poziom, w jakim generowane w ramach ciągłego monitorowania, informacje związane z bezpieczeństwem są gromadzone dla wszystkich obiektów oceny i wszystkich mających zastosowanie kontroli defektów w określonym czasie.
Assessment Criterion/Criteria	Kryteria oceny	Reguły logiczne pozwalające automatycznie lub ręcznie wykrywać defekty. Zazwyczaj kryterium oceny w systemie ISCM określa, co w specyfikacji stanu pożądanego jest porównywane ze stanem rzeczywistym oraz warunki, które wskazują na występowanie defektu.
Assessment Object	Obiekt oceny	Patrz *Obiekt*, *Ocena*.
Assessment Timeliness	Terminowość oceny	Zakres, w jakim generowane przez ciągłe monitorowanie informacje związane z bezpieczeństwem są zbierane w określonym czasie (lub z jaką częstością).
Asset	Zasób	Zasoby o pewnej wartości, które organizacja posiada lub wykorzystuje.

Terminologia angielska	Terminologia polska	Definicja
Behavior Management	Zarządzanie zachowaniami	Patrz *Zdolność do ochrony*, *Zarządzanie zachowaniami*.
Capability	Zdolność do ochrony	Patrz *Zdolność do ochrony*, *Bezpieczeństwo*.
Capability, Anomalous Event Detection Management	Zdolność do ochrony, Zarządzanie wykrywaniem zdarzeń nietypowych	Zdolność systemu ISCM, służąca do identyfikowania rutynowych i nieoczekiwanych zdarzeń mogących zagrozić bezpieczeństwu w pewnych ramach czasowych, co zapobiega lub zmniejsza wpływ (tj. konsekwencje) zdarzeń w możliwym zakresie.
Capability, Anomalous Event Response Recovery Management	Zdolność do ochrony, Zarządzanie wykrywaniem zdarzeń nietypowych	Zdolność systemu ISCM, zapewniająca, że występuje reakcja zarówno na zdarzenia rutynowe, jak i nieoczekiwane oraz wymagające reakcji w celu utrzymania funkcjonalności i bezpieczeństwa (po ich zidentyfikowaniu) w ramach czasowych, co zapobiega lub zmniejsza wpływ (tj. konsekwencje) zdarzeń w możliwym zakresie.
Capability, Behavior Management	Zdolność do ochrony, Zarządzanie Zachowaniami	Zdolność systemu ISCM zapewniająca, że ludzie są świadomi oczekiwanego zachowania związanego z bezpieczeństwem i są w stanie wykonywać swoje obowiązki, aby zapobiegać celowym i niezamierzonym zachowaniom, które zagrażają bezpieczeństwu informacji.

Terminologia angielska	Terminologia polska	Definicja
Capability, Boundary Management	Zdolność do ochrony, Zarządzanie granicami	Zdolność systemu ISCM, która dotyczy następujących obszarów sieci i granic fizycznych: **Granice fizyczne** — zapewnienie, że ruch (osób, nośników, sprzętu itp.) do/z obiektu fizycznego nie zagraża bezpieczeństwu. **Filtry** — zapewnienie, że ruch do/z sieci informatycznej (a więc poza zasięgiem ochrony fizycznej obiektu) nie narusza bezpieczeństwa. To samo dotyczy enklaw wydzielonych w ramach sieci informatycznej. **Inne** — należy zapewnić ochronę informacji (z odpowiednią siłą), gdy jest to konieczne do ochrony poufności i integralności, niezależnie od tego, czy informacje są w trakcie tranzytu czy przechowywania.
Capability, Configuration Settings Management	Zdolność do ochrony, Zarządzanie ustawieniami konfiguracyjnymi	Zdolność systemu ISCM, służąca do identyfikowania ustawień konfiguracyjnych (*ang. Common Configuration Enumerations [CCE]*) na urządzeniach, które mogą być wykorzystane przez atakujących do skompromitowania urządzenia i użycia go jako platformy, z której można naruszyć bezpieczeństwo sieci.

Terminologia angielska	Terminologia polska	Definicja
Capability, Credentials and Authentication Management	Zdolność do ochrony, Zarządzanie poświadczeniami i uwierzytelnianiem	Zdolność systemu ISCM do zapewnienia, że autoryzowani użytkownicy mają poświadczenia i metody uwierzytelniania wymagane (tylko i wyłącznie) do wykonywania swoich obowiązków, przy jednoczesnym ograniczeniu dostępu do tych zasobów, które są im niezbędne.
Capability, Event Preparation Management	Zdolność do ochrony, Zarządzanie przygotowaniem zdarzeń	Zdolność systemu ISCM do zapewnienia procedur i zasobów umożliwiających reagowanie zarówno na rutynowe, jak i nieoczekiwane zdarzenia, które mogą zagrozić bezpieczeństwu. Nieoczekiwane zdarzenia to na przykład rzeczywiste ataki i sytuacje awaryjne (klęski żywiołowe), takie jak pożary, powodzie i trzęsienia ziemi itp.
Capability, Hardware Asset Management	Zdolność do ochrony, Zarządzanie zasobami sprzętu	Zdolność systemu ISCM, służąca do identyfikowania niekontrolowanych urządzeń, które mogą być wykorzystane przez atakujących do naruszenia urządzenia i użycia go jako platformy, z której można naruszyć bezpieczeństwo sieci.
Capability, ISCM	Zdolność do ochrony, ISCM	Patrz *Zdolność sytemu ISCM do ochrony*.

Terminologia angielska	Terminologia polska	Definicja
Capability, Manage and Assess Risk	Zdolność do ochrony, Zarządzanie ryzykiem i jego ocena	Zdolność systemu ISCM do zmniejszenia liczby przypadków znaczącego wykorzystania podatności innych zdolności *non-meta*[34], które mogą wystąpić, ponieważ w procesie zarządzania ryzykiem nie udało się prawidłowo zidentyfikować i ustalić priorytetów działań i inwestycji niezbędnych do obniżenia profilu ryzyka.
Capability, Perform Resilient Systems Engineering	Zdolność do ochrony, Realizacja inżynierii odpornych systemów (SE)	Zdolność systemu ISCM, która: • skupia się na ograniczeniu udanych przypadków wykorzystania innych zdolności *non-meta*, występujących z powodu nieodpowiedniego projektu, inżynierii, wdrożenia, testowania lub innych kwestii technicznych przy wdrażaniu lub monitorowaniu zabezpieczeń związanych z innymi zdolnościami *non-meta*. • Ograniczenie udanych przypadków wykorzystania innych zdolności *non-meta*, występujących z powodu nieodpowiednich definicji wymagań, polityki, planowania i/lub innych kwestii dotyczących zarządzania przy wdrażaniu i/lub monitorowaniu zabezpieczeń związanych z innymi zdolnościami *non-meta*.

[34] *Non-meta* – termin oznacza korzystanie z niekonwencjonalnych dla danej dziedziny praktyk.

Terminologia angielska	Terminologia polska	Definicja
Capability, Privilege and Account Management	Zdolność do ochrony, Zarządzanie przywilejami i kontami	Zdolność systemu ISCM do zapewnienia, że autoryzowani użytkownicy mają tylko i wyłącznie przywileje konieczne do wykonywania swoich obowiązków, aby ograniczyć dostęp do tych zasobów, które są im niezbędne.
Capability, Security	Zdolność do ochrony, Bezpieczeństwo	Zestaw wzajemnie wzmacniających się środków bezpieczeństwa wdrażanych metodami technicznymi, fizycznymi i proceduralnymi. Takie środki bezpieczeństwa są zwykle wyznaczane, aby osiągnąć wspólny cel związany z bezpieczeństwem informacji.
Capability, Software Asset Management	Zdolność do ochrony, Zarządzanie zasobami oprogramowania	Zdolność systemu ISCM, służąca do identyfikowania nieautoryzowanego oprogramowania na urządzeniach, które może być wykorzystane przez atakujących do naruszenia urządzenia i użycia go jako platformy, z której można naruszyć bezpieczeństwo sieci.
Capability, Trust Management	Zdolność do ochrony, Zarządzanie zaufaniem	Zdolność systemu ISCM, która zapewnia, że osoby niezaufane nie mają dostępu do sieci (aby zapobiec atakom wewnętrznym).
Capability, Vulnerability Management	Zdolność do ochrony, Zarządzanie podatnościami na zagrożenia	Zdolność systemu ISCM, służąca do identyfikowania podatności (*ang. Common Vulnerabilities and Exposures - CVE]*) na urządzeniach, które mogą być wykorzystane przez atakujących do

Terminologia angielska	Terminologia polska	Definicja
		skompromitowania urządzenia i użycia go jako platformy, z której można naruszyć bezpieczeństwo sieci.
CDM	CDM	Patrz Program ciągłej diagnostyki i mitygacji skutków *Continuous Diagnostics and Mitigation*.
CMaaS	CMaaS	Patrz *Ciągłe monitorowanie jako usługa*
Collection System	System zbierania danych	System, który zbiera dane o stanie rzeczywistym i porównuje je ze specyfikacją stanu pożądanego w celu znalezienia defektów zabezpieczeń.
Collector	Moduł zbierający dane	Zazwyczaj jest to zautomatyzowany czujnik, który zbiera dane o stanie rzeczywistym. Stanowi element systemu zbierania danych.
Configuration Settings Management	Zarządzanie ustawieniami konfiguracyjnymi	Patrz *Zdolność do ochrony, Zarządzanie ustawieniami konfiguracyjnymi*.
Continuous Diagnostics and Mitigation (CDM)	Program ciągłej diagnostyki i mitygacji skutków	Program ustanowiony w celu zapewnienia odpowiednich, opartych na ryzyku i opłacalnych ocen cyberbezpieczeństwa oraz bardziej efektywnego przydzielania zasobów cyberbezpieczeństwa dla organizacji.
Control Item	Element zabezpieczenia	Patrz *Element środka bezpieczeństwa*.
Dashboard	Pulpit nawigacyjny	Patrz *Pulpit nawigacyjny organizacji*

Terminologia angielska	Terminologia polska	Definicja
Defect	Defekt	To zdarzenie wynikające z przeprowadzonego procesu poszukiwania defektów, podważające wynik oceny bezpieczeństwa przedmiotu oceny. Defekt wskazuje na osłabiony stan bezpieczeństwa, który zwiększa ryzyko wystąpienia incydentu.
Defect Check	Kontrola defektu	**Kontrola defektu** jest sposobem oceny oświadczeń o zgodności. Kontrola defektów: • jest określana jako test (w stosownych przypadkach); • może być zautomatyzowana; • wyraźnie definiuje konkretną specyfikację stanu pożądanego, która jest następnie porównywana z odpowiednim stanem rzeczywistym w celu określenia wyniku testu; • dostarcza informacji, które mogą pomóc w określeniu stopnia skuteczności kontroli/poziomu ryzyka, który jest akceptowalny; • sugeruje opcje reakcji na ryzyko; oraz • ocenia stan pożądany.

Terminologia angielska	Terminologia polska	Definicja
Defect Type	Typ defektu	Rodzaj defektu, który może wystąpić w wielu przedmiotach oceny. Ogólnie, obecność lub brak typu defektu badana jest poprzez kontrolę defektu.
Desired State	Stan pożądany	Patrz *Specyfikacja stanu pożądanego*.
Desired State Specification	Specyfikacja stanu pożądanego	Zdefiniowana wartość, lista lub reguła (specyfikacja), która a) stwierdza lub b) umożliwia ustalenie stanu pożądanego przez organizację w celu zmniejszenia zagrożenia bezpieczeństwa informacji. Specyfikacja stanu pożądanego jest na ogół deklaracją polityki.
Device	Urządzenie	W ocenie automatycznej rodzaj obiektu oceny, który jest albo adresowalnym przez IP (lub równoważnym) składnikiem sieci, albo składnikiem wymiennym, który ma znaczenie dla bezpieczeństwa.
Device Role	Rola grupy urządzeń	Rola grupy urządzeń to urządzenia o takich samych zasadach działania. Na przykład biała lista oprogramowania dla serwera jest prawdopodobnie inna niż dla stacji roboczej. Dlatego serwery i urządzenia mają zwykle oddzielne role grup urządzeń. Przykłady ról wysokiego poziomu obejmują punkt końcowy użytkownika, serwer, urządzenie sieciowe, urządzenie komórkowe i inne urządzenia. Każda z nich może być dalej

Terminologia angielska	Terminologia polska	Definicja
		podzielona. Na przykład serwery mogą być podzielone na wiele podkategorii (np. serwer bazy danych, serwer poczty elektronicznej, serwer plików, serwer DNS, serwer DHCP, serwer uwierzytelniania). Rola urządzenia jest wymagana, gdy organizacja chce, aby grupy urządzeń miały różne zasady dotyczące np. autoryzowanego oprogramowania, ustawień i/lub poprawek.
Federal Dashboard	Rządowy pulpit nawigacyjny	Instancja pulpitu, która: • gromadzi dane zbiorcze z pulpitów nawigacyjnych na poziomie podstawowym w wielu organizacjach; oraz • nie zbiera defektów na poziomie obiektu oceny danych lub wad. Podsumowuje defekty na poziomie rządowym oraz kategorie obiektów oceny. Nie podsumowuje defektów na poziomie lokalnym (bazowym) ani kategorii lokalnych (bazowych).
Foundational Defect Checks	Fundamentalne kontrole defektów	Kontrole defektów, które ujawniają nieskuteczność zabezpieczeń, mające podstawowe znaczenie dla celów danej zdolności (np. HWAM, SWAM lub zarządzanie ustawieniami konfiguracyjnymi), której dotyczy kontrola defektu.

Terminologia angielska	Terminologia polska	Definicja
Hardware Asset Management	Zarządzanie zasobami sprzętowymi	Patrz *Zdolność do ochrony, Zarządzanie zasobami sprzętowymi*.
Identifier	Identyfikator	Coś (dane), co identyfikuje obiekt oceny lub inną jednostkę będącą przedmiotem zainteresowania (jak kontrola defektów). W kategoriach bazy danych jest to klucz główny lub potencjalny, który może być użyty do jednoznacznej identyfikacji obiektu oceny, aby nie był mylony z innymi obiektami.
ISCM Capability	Zdolność ISCM	Zdolność ochrony z następującymi dodatkowymi cechami: • Celem (pożądanym rezultatem) każdej zdolności jest zajęcie się określonym rodzajem (rodzajami) scenariuszy ataków lub wykorzystania luk w zabezpieczeniach. • Każda ze zdolności skupia się na atakach na określone obiekty oceny. • Istnieje realny sposób na zautomatyzowanie ISCM w zakresie zdolności do ochrony. Zdolność ta zapewnia ochronę przed obecnymi scenariuszami ataku.

Terminologia angielska	Terminologia polska	Definicja
ISCM Dashboard	Panel nawigacyjny ISCM	Hierarchia pulpitów nawigacyjnych ułatwiająca raportowanie odpowiednich informacji związanych z bezpieczeństwem na wielu poziomach organizacyjnych.
Limit, Specification	Ograniczenie, Specyfikacja	Stan wskazujący, że ryzyko przekroczyło akceptowalny poziom i że konieczne jest natychmiastowe działanie w celu zmniejszenia ryzyka, lub system/obiekt oceny może wymagać wycofania z produkcji (unieważnienia uprawnień do działania).
Local Defect Checks	Lokalne kontrole defektów	Kontrole defektów, które organizacja dodaje do Fundamentalnych kontroli defektów, opierają się na ocenie jej własnych potrzeb i tolerancji ryzyka. Lokalna kontrola defektów wspiera lub wzmacnia Fundamentalne kontrole defektów. Organizacje mogą zdecydować o niestosowaniu danej lokalnej kontroli defektów w przypadkach, gdy nie wybrano/wdrożono zabezpieczeń wspierających.
Manage Boundaries	Zarządzanie granicami	Patrz *Zdolność do ochrony, Zarządzanie granicami*.
Manage Credentials and Authentication	Zarządzanie poświadczeniami i uwierzytelnianiem	Patrz *Zdolność do ochrony, Zarządzanie poświadczeniami i uwierzytelnianiem*.

Terminologia angielska	Terminologia polska	Definicja
Manage Privileges	Zarządzanie przywilejami	Patrz *Zdolność do ochrony, Zarządzanie przywilejami i kontami*.
Object	Obiekt	Patrz *Obiekt, Ocena*.
Object, Assessment	Obiekt, Ocena	Obiekty oceny identyfikują konkretne pozycje podlegające ocenie i jako takie mogą mieć jeden lub więcej defektów zabezpieczeń. Obiekty oceny obejmują *specyfikacje*, *mechanizmy*, *działania* i *osoby*, które z kolei mogą obejmować, między innymi urządzenia, produkty oprogramowania, pliki wykonawcze oprogramowania, dane uwierzytelniające, konta, przywileje kont, elementy, do których przyznawane są przywileje (w tym dane i obiekty fizyczne) itp. Patrz NSC 800-53A.
Ongoing Assessment	Ocena bieżąca	Ciągła ocena skuteczności wdrażania środków bezpieczeństwa; nie jest ona oddzielona od ISCM, ale stanowi podzbiór działań ISCM.
Prepare for Events	Przygotowanie do zdarzeń	Patrz *Zdolność do ochrony, Zarządzanie przygotowaniem zdarzeń*.
Regular Expression	Wyrażenie regularne	Sekwencja znaków (lub słów), która tworzy wzorzec wyszukiwania, używany głównie do dopasowywania wzorców do łańcuchów lub dopasowywania łańcuchów.

Terminologia angielska	Terminologia polska	Definicja
Risk	Ryzyko	Miara stopnia zagrożenia organizacji przez potencjalną okoliczność lub zdarzenie. Zazwyczaj jest funkcją: a. niekorzystnych skutków, które powstałyby w przypadku wystąpienia okoliczności lub zdarzenia; oraz b. prawdopodobieństwa ich wystąpienia. Na prawdopodobieństwo wpływa łatwość wykorzystania luki w zabezpieczeniach oraz częstotliwość, z jaką obiekt oceny jest obecnie atakowany.
Risk (ISCM Capability)	Ryzyko (zdolność systemu ISCM do ochrony)	Patrz *Zdolność do ochrony, Zarządzanie ryzykiem i jego ocena*.
Risk Management	Zarządzanie ryzykiem	Patrz *Zdolność do ochrony, Zarządzanie ryzykiem i jego ocena*.
Security Capability	Zdolność do ochrony	Patrz *Zdolność do ochrony, Bezpieczeństwo*.
Security Control Item	Elementy zabezpieczeń	Wszystkie lub wybrane wymagania środków bezpieczeństwa zawarte w NSC 800-53, wyrażone jako oświadczenie do wdrożenia i ocenie. Zarówno zabezpieczenia, jak i ich rozszerzenia są traktowane jako elementy zabezpieczeń. Zabezpieczenia i ich rozszerzenia są dalej dzielone, jeżeli wiele wymogów bezpieczeństwa w ramach zabezpieczeń lub ich rozszerzeń ujętych w NSC 800-53 ma format listy: a, b, c itd.

Terminologia angielska	Terminologia polska	Definicja
Specification Limit	Granice specyfikacji	Patrz *Granica, Specyfikacja*.
Software Asset Management	Zarządzanie zasobami oprogramowania	Patrz *Zdolność do ochrony, Zarządzanie zasobami oprogramowania*.
Sub-Capability	Składnik zdolności do ochrony	Składnik, który wspiera osiągnięcie większej zdolności. W niniejszej publikacji NISTIR 8011 każda zdolność jest podzielona na elementy niezbędne i wystarczające do wspomagania realizacji celu większej zdolności.
Trust	Zaufanie	Patrz *Zdolność do ochrony, Zarządzanie zaufaniem*.
Trust Management	Zarządzanie zaufaniem	Patrz *Zdolność do ochrony, Zarządzanie zaufaniem*.
Unmanaged Device	Niekontrolowane urządzenie	Urządzenie znajdujące się w zakresie oceny, które jest nieautoryzowane lub, jeśli jest autoryzowane, nie jest przypisane do administrowania.
Vulnerability Management	Zarządzanie podatnościami	Patrz *Zdolność do ochrony, Zarządzanie podatnościami*.

ZAŁĄCZNIK C – AKRONIMY I SKRÓTY

Wybrane akronimy i skróty użyte w niniejszej publikacji zostały rozwinięte poniżej.

Dodatkowo patrz: NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*

Akronim	Terminologia angielska	Terminologia polska
A&A	Assessment and Authorization	Ocena i autoryzacja
CAESARS	Continuous Asset Evaluation, Situational Awareness, and Risk Scoring	Ciągła ocena zasobów, świadomość sytuacyjna i ocena ryzyka
CCE	Common Configuration Enumeration	ujednolicone identyfikatory problemów z konfiguracją systemu
CDM	Continuous Diagnostics and Mitigation	Ciągła diagnostyka i łagodzenie skutków
ISCM-TN	Information Security Continuous Monitoring Target Network	Strategia ciągłego monitorowania bezpieczeństwa informacji – sieć docelowa
CSM	Configuration Settings Management	Zarządzanie ustawieniami konfiguracyjnymi
CVE	Common Vulnerabilities and Exposures	słownik identyfikatorów odpowiadających powszechnie znanym podatnościom oraz zagrożeniom, a także standard ich nazewnictwa
CWE	Common Weakness Enumeration	Wyliczenie powszechnych słabości

DHS	Department of Homeland Security	Departament Bezpieczeństwa Wewnętrznego USA
HWAM	Hardware Asset Management	Zarządzanie zasobami sprzętowymi
ISCM	Information Security Continuous Monitoring	Strategia ciągłego monitorowania bezpieczeństwa informacji
NVD	National Vulnerability Database	krajowa baza podatności
RMF	Risk Management Framework	ramy zarządzania ryzykiem
SO	System Owner	Właściciel systemu
SSO	System Security Officer	osoba kluczowa ds. Bezpieczeństwa systemu
SWAM	Software Asset Management	Zarządzanie zasobami oprogramowania