Ministerstwo Cyfryzacji

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 1800-26
NSC 1800-26A
NSC 1800-26B
NIST SP 1800-26C

30 października 2023

Integralność danych - wykrywanie i reagowanie na oprogramowanie ransomware i inne zdarzenia destrukcyjne

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

Niniejsza publikacja **NSC 1800-26, *Integralność danych - wykrywanie i reagowanie na oprogramowanie ransomware i inne zdarzenia destrukcyjne***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events.*

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 poradniku źródłowym, na podstawie którego powstały niniejsze zalecenia. W przypadku, gdy tożsame pojęcie zostało zdefiniowane również w powszechnie obowiązujących aktach prawnych lub

normatywnych, a ich definicja różni się od tej zamieszczonej w niniejszej publikacji, wówczas należy stosować sformułowania zawarte w tych aktach/w obiegu prawnym.

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 NSC 7298, ***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.

[1] Kluczowi uczestnicy zarządzania ryzykiem - patrz NSC 800-18; NSC 800-37, NSC 7298.

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował szereg standardów i wytycznych w celu zapewnienia jednolitego podejścia do problematyki bezpieczeństwa informacji i systemów informacyjnych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji i systemów informacyjnych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością działalności i majątku organizacji, osób fizycznych i państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych. Dzięki jednolitemu podejściu do zarządzania ryzykiem ułatwia także wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[2]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania innych standardów.

Publikacje NIST, co do zasady nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

[2] International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.

+48222455922

sekretariat.dc@cyfra.gov.pl

Spis treści

Spis ilustracji

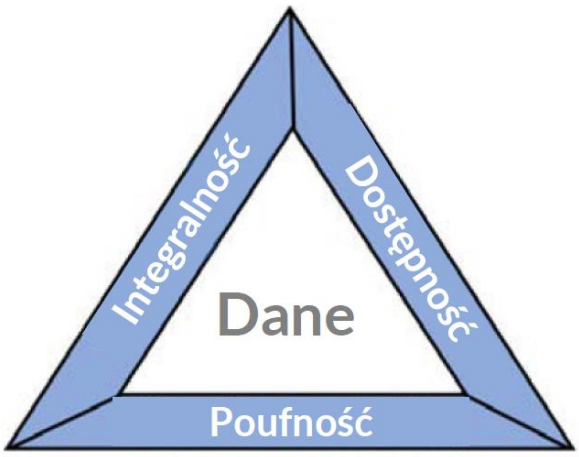
Spis tabel

NSC 1800-26A

Streszczenie

Na triadę CIA (*ang. confidentiality*, *integrity*, *availability*) składają się trzy niżej opisane filary bezpieczeństwa informacji: poufność, integralność i dostępność.

- Poufność – zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych.
- Integralność – zabezpieczenie przed nieprawidłową modyfikacją lub zniszczeniem informacji oraz zapewnienie niezaprzeczalności i autentyczności informacji.
- Dostępność – zapewnienie terminowego i niezawodnego dostępu do informacji i wykorzystania tej informacji.

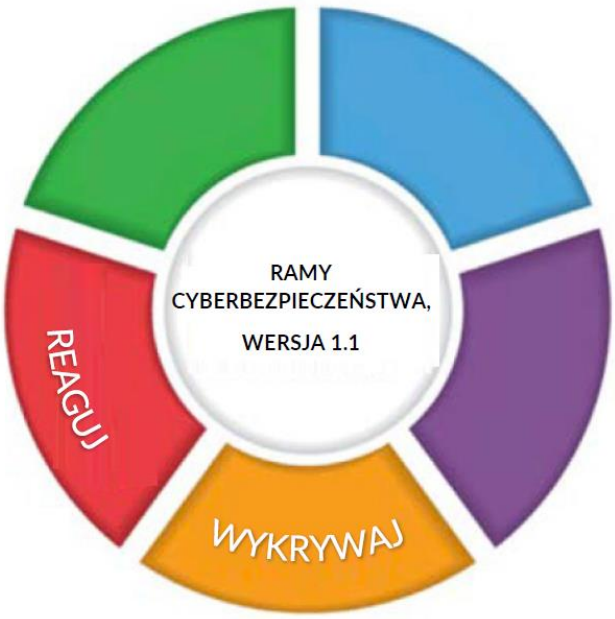


Niniejsza seria przewodników metodycznych skupia się na integralności danych: właściwości polegającej na tym, że dane nie zostały zmienione w nieautoryzowany sposób. Integralność danych obejmuje dane podczas ich przechowywania, przetwarzania i przesyłania.[3]

- Destrukcyjne oprogramowanie złośliwe (*ang. malware*), oprogramowanie wymuszające okup (*ang. ransomware*), działanie złośliwych insiderów (*ang. malicious insider activity*), a nawet pomyłki przy działaniu w dobrej wierze powodują, że organizacje muszą wykrywać i reagować na zdarzenie wpływające

[3] Uwaga: niniejsze definicje zostały zaczerpnięte z publikacji NSC 800-12.

na integralność danych. Organizacje muszą mieć pewność szybkiego wykrycia tych zdarzeń oraz odpowiedniej reakcji na nie.



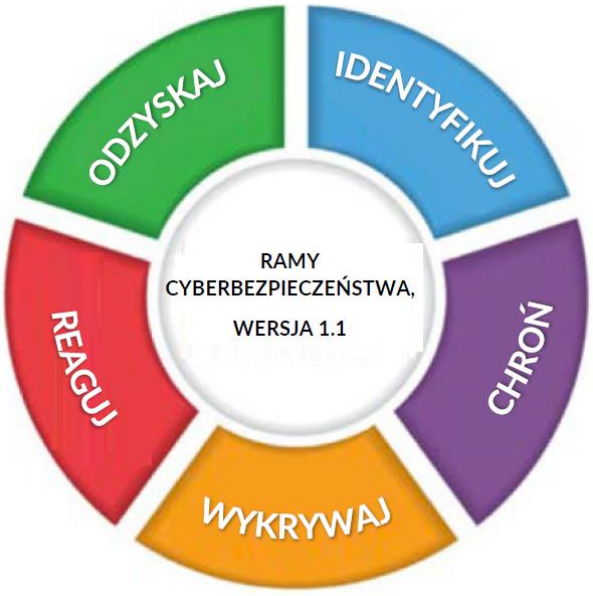
- Ataki przeciwko danym należącym do organizacji mogą narażać pocztę elektroniczną, dokumentację pracowniczą i informacje o klientach — wpływając na działalność organizacji, jej przychody i reputację.
- Przykłady ataków na integralność danych obejmują nieautoryzowane wprowadzanie, usuwanie lub modyfikowanie danych w informacjach firmowych takich jak poczta elektroniczna, dokumentacja pracownicza, dokumentacja finansowa i dane o klientach.
- Narodowe Centrum Doskonalenia Cyberbezpieczeństwa (*ang. National Cybersecurity Center of Excellence - NCCoE*) NIST zbudowało środowisko laboratoryjne służące opracowaniu metod skutecznego wykrywania i reagowania na zdarzenie dotyczące integralności danych w różnych biznesowych środowiskach informatycznych, aby niezwłocznie reagować na zdarzenie celem zapobieżenia całkowitemu naruszeniu zasad ochrony.
- Niniejszy przewodnik metodyczny cyberbezpieczeństwa (*ang. Cybersecurity Practice Guide*) pokazuje sposób, w jaki organizacje mogą opracować i wdrażać odpowiednie działania w przypadku wykrycia zdarzenia dotyczącego integralności danych.

WYZWANIE

Niektóre organizacje podlegają atakom systemowym zmuszającym je do przerywania działalności. Jeden z wariantów ataku na integralność danych – oprogramowanie wymuszające okup (*ang. ransomware*) – szyfruje dane, pozostawiając je w stanie niezdolnym do użytku. Inne ataki na integralność danych mogą mieć bardziej dynamiczny charakter, atakując urządzenia, rozprzestrzeniając się „na boki" poprzez sieci i stale wyrządzając szkody w całej organizacji. W obu przypadkach występują charakterystyczne zachowania— jak np. w niewyjaśniony sposób zaszyfrowane pliki lub niestandardowa aktywność sieciowa — dające możliwość natychmiastowego wykrycia zdarzenia i szybkiej reakcji w celu opanowania niekorzystnych skutków.

ROZWIĄZANIE

W kwietniu 2018 r. NIST opublikował wersję 1.1 Ram Cyberbezpieczeństwa, aby pomóc organizacjom w lepszym opanowaniu i ograniczaniu ryzyka w zakresie cyberbezpieczeństwa infrastruktury krytycznej i innych sektorów. Zasadnicza część Ram Cyberbezpieczeństwa zawiera pięć niżej wymienionych funkcji.



- **Identyfikuj –** opracowanie podejścia organizacji do zarządzania ryzykiem w zakresie cyberbezpieczeństwa wobec systemów, ludzi, zasobów, danych i zdolności.
- **Chroń –** opracowanie i wdrożenie odpowiednich środków bezpieczeństwa w celu zapewnienia świadczenia usług krytycznych.
- **Wykrywaj –** opracowanie i wdrożenie odpowiednich działań mających na celu stwierdzenie wystąpienia zdarzenia związanego z cyberbezpieczeństwem.

- **Reaguj –** opracowanie i wdrożenie odpowiednich środków pozwalających na podjęcie działań w związku z wykrytym zdarzeniem związanym z cyberbezpieczeństwem.
- **Odzyskaj –** opracowanie i wdrożenie odpowiednich działań w celu utrzymania planów odporności i przywrócenia wszelkich zdolności lub usług, które zostały osłabione w wyniku zdarzenia związanego z cyberbezpieczeństwem.

Więcej informacji znajduje się w Framework for Improving Critical Infrastructure Cybersecurity v1.1.

Stosując Ramy Cyberbezpieczeństwa w zakresie integralności danych, niniejszy przewodnik metodyczny informuje organizacje o sposobie szybkiego **wykrywania** i **reagowania** na ataki na integralność danych przez realizację odpowiednich działań, które natychmiast powiadamiają o zdarzeniach dotyczących integralności danych.

NCCoE opracowało i wdrożyło rozwiązanie obejmujące wiele wspólnie działających systemów w celu **wykrycia** nadchodzącego zdarzenia związanego z zapewnieniem cyberbezpieczeństwa integralności danych. Rozwiązanie to podaje ponadto wskazówki jak **reagować** na wykryte zdarzenie. Łączne realizowanie tych funkcji zapewnia organizacjom posiadanie niezbędnych narzędzi postępowania w czasie ataku na integralność danych.

NCCoE przeanalizowało istniejące technologie zapewniające następujące zdolności:

- **wykrywanie zdarzeń**
- **monitorowanie integralności**
- **rejestrowanie**
- **raportowanie**
- **ograniczanie i powstrzymywanie**
- **informatykę śledczą/analitykę**

Chociaż do celów tego zadania NCCoE użyło zestawu produktów komercyjnych, niniejszy przewodnik nie zatwierdza tych konkretnych produktów ani nie gwarantuje ich zgodności z jakimikolwiek inicjatywami regulacyjnymi. Eksperci bezpieczeństwa informacyjnego waszej organizacji powinni wskazać produkty najlepiej dopasowane do waszych dotychczasowych narzędzi i infrastruktury systemu informacyjnego. Wasza organizacja może przyjąć to rozwiązanie albo inne, które odpowiada w całości niniejszym wskazówkom, lub też można korzystać z niniejszego podręcznika jako punkt wyjścia dla indywidualnego doboru i wdrożenia części rozwiązania.

KORZYŚCI

Przewodnik metodyczny cyberbezpieczeństwa NSC 1800-26 *Integralność danych - wykrywanie i reagowanie na oprogramowanie wymuszające okup i inne zdarzenia destrukcyjne* może pomóc waszej organizacji w:

- opracowaniu strategii wykrywania i reagowania na zdarzenie dotyczące cyberbezpieczeństwa w zakresie integralności danych;
- ułatwieniu skutecznego wykrywania i reagowania na niekorzystne zdarzenia, utrzymaniu operacji oraz zapewnieniu integralności i dostępności danych o krytycznym znaczeniu dla wspierania działalności organizacji;
- zarządzaniu ryzykiem organizacji.

PARTNERZY/WSPÓŁPRACOWNICY TECHNOLOGICZNI

Organizacje uczestniczące w tym projekcie przedstawiły swoje możliwości w odpowiedzi na otwarte zaproszenie dla wszystkich źródeł ze środowiska akademickiego i przemysłu (sprzedawców i integratorów) posiadających odpowiednie kompetencje w zakresie bezpieczeństwa. Następujący respondenci posiadający odpowiednie zdolności lub składniki produktów (określani w niniejszym dokumencie jako „partnerzy technologiczni/współpracownicy") podpisali umowę o współpracy badawczo-rozwojowej (*ang. Cooperative Research and Development Agreement - CRADA*), aby współpracować z NIST w ramach konsorcjum w celu zbudowania tego przykładowego rozwiązania:

- Cisco Systems;
- Glasswall Government Solutions;
- Micro Focus;
- Semperis;
- Symantec Corporation;
- Tripwire.

Niektóre podmioty komercyjne, sprzęt, produkty lub materiały mogą być identyfikowane poprzez nazwę lub logo firmy lub inne oznaczenia w celu potwierdzenia ich udziału w tej współpracy lub w celu odpowiedniego opisania procedury eksperymentalnej lub koncepcji. Taka identyfikacja nie ma na celu sugerowania specjalnego statusu lub relacji z NIST lub rekomendacji lub zatwierdzenia przez NIST lub NCCoE; nie ma również na celu sugerowania, że podmioty, sprzęt, produkty lub materiały są koniecznie najlepszymi dostępnymi dla danego celu.

NSC 1800-26B

Podejście, architektura i charakterystyka bezpieczeństwa

ZASTRZEŻENIE

Niektóre podmioty gospodarcze, sprzęt, produkty lub materiały mogą być wymienione z nazwy lub przez wskazanie logo firmy albo innego oznaczenia w celu potwierdzenia ich udziału w niniejszej współpracy lub w celu prawidłowego opisu procedury eksperymentalnej lub koncepcji. Taka identyfikacja nie ma na celu podkreślenia szczególnego statusu lub związku z NIST ani rekomendacji czy zatwierdzenia przez NIST lub NCCoE; nie ma na celu również wskazania, że te podmioty, sprzęt, produkty lub materiały są bezwzględnie najlepsze dla tego celu.

NARODOWE CENTRUM DOSKONALENIA CYBERBEZPIECZEŃSTWA

Narodowe Centrum Doskonalenia Cyberbezpieczeństwa (*National Cybersecurity Center of Excellence - NCCoE*), stanowiące część Narodowego Instytutu Standaryzacji i Technologii (*National Institute of Standards and Technology - NIST*), jest ośrodkiem współpracy jednoczącym wysiłki organizacji branżowych, organów publicznych i instytucji akademickich w zakresie rozwiązywania najbardziej newralgicznych problemów dotyczących cyberbezpieczeństwa. Takie partnerstwo publiczno-prywatne umożliwia tworzenie praktycznych rozwiązań w zakresie cyberbezpieczeństwa dla konkretnych branż oraz w odpowiedzi na szersze międzysektorowe wyzwania technologiczne. Poprzez konsorcja oparte na kooperacyjnych umowach badawczo-rozwojowych (*ang. Cooperative Research and Development Agreement - CRADA*) obejmujących partnerów technologicznych — od czołowych firm z listy Fortune 50 po mniejsze spółki specjalizujące się w bezpieczeństwie informacji — NCCoE stosuje standardy i najlepsze praktyki dla opracowania modułowych, adaptowalnych,

przykładowych rozwiązań cyberbezpieczeństwa przy wykorzystaniu technologii dostępnych na rynku. NCCoE dokumentuje te przykładowe rozwiązania w serii Publikacji Specjalnych NIST 1800, która mapuje zdolności do Ram Cyberbezpieczeństwa NIST i wyszczególnia czynności potrzebne innym podmiotom do naśladowania przykładowego rozwiązania. Ośrodek NCCoE został założony w 2012 r. przez NIST w partnerstwie ze stanem Maryland oraz hrabstwem Montgomery w stanie Maryland.

Więcej informacji na temat NCCoE znajduje się pod adresem https://www.nccoe.nist.gov/.

Więcej informacji na temat NIST znajduje się pod adresem https://www.nist.gov.

PRZEWODNIKI METODYCZNE NIST W ZAKRESIE CYBERBEZPIECZEŃSTWA

Przewodniki metodyczne NIST w zakresie cyberbezpieczeństwa (Publikacje Specjalne serii 1800) dotyczą konkretnych wyzwań z zakresu cyberbezpieczeństwa w sektorze publicznym i prywatnym. Są one praktycznymi i przystępnymi podręcznikami ułatwiającymi przyjmowanie opartego na standardach podejścia do cyberbezpieczeństwa. Pokazują osobom zajmującym się bezpieczeństwem informacji jak wdrażać przykładowe rozwiązania pomagające im dostosować się do odpowiednich standardów i dobrych praktyk oraz zapewnia użytkownikom listy materiałów, pliki konfiguracyjne i inne informacje niezbędne do wdrożenia podobnego podejścia.

Dokumenty w ramach tej serii opisują przykładowe wdrożenia praktyk cyberbezpieczeństwa jakie mogą być dobrowolnie wprowadzone przez organizacje. Dokumenty te nie opisują przepisów prawnych czy praktyk obowiązkowych ani też same nie mają charakteru prawa.

ABSTRAKT

Oprogramowanie wymuszające okup (*ang. ransomware*), zagrożenia wewnętrzne (*ang. insider threats*) a nawet pomyłki popełnione w dobrej wierze stanowią stałe zagrożenie dla organizacji zarządzających danymi w różnej formie. Zasoby i struktury baz danych, pliki systemowe, konfiguracje, pliki użytkownika, kod aplikacji i dane klientów stanowią potencjalny cel uszkodzenia i zniszczenia danych.

Szybkie, precyzyjne i dogłębne wykrywanie i reagowanie na utratę integralności danych może oszczędzić organizacji dużo czasu, pieniędzy i kłopotu. O ile ludzka wiedza i umiejętności stanowią istotny element tych zadań, to odpowiednie narzędzia i przygotowanie są ważne dla minimalizacji przestojów i strat wynikłych ze zdarzeń dotyczących integralności danych. NCCoE, we współpracy z członkami społeczności przedsiębiorców i sprzedawcami rozwiązań w dziedzinie cyberbezpieczeństwa, stworzyło przykładowe rozwiązanie odpowiadające na takie wyzwania w zakresie integralności danych. Niniejszy projekt przedstawia metody i zestaw potencjalnych narzędzi wykrywających, ograniczających i powstrzymujących zdarzenia z zakresu integralności danych w komponentach sieci organizacyjnej. Wskazuje także narzędzia i strategie stanowiące pomoc dla zespołu ds. bezpieczeństwa w reagowaniu na takie zdarzenie.

SŁOWA KLUCZOWE

wektor ataku *(ang. attack vector);* integralność danych (*ang. data integrity*); aktor zagrożenia (*ang. malicious actor*); oprogramowanie złośliwe (*ang. malware*); wykrywanie oprogramowania złośliwego (ang. *malware detection)*; reakcja na oprogramowanie złośliwe (ang. *malware response)*; oprogramowanie wymuszające okup (ang. *ransomware)*.

1. PODSUMOWANIE

Organizacje stoją wobec niemal stałego zagrożenia destrukcyjnym złośliwym oprogramowaniem, oprogramowaniem wymuszającym okup, złośliwym działaniem insidera, czy nawet pomyłkami popełnianymi w dobrej wierze, które mogą zmienić lub zniszczyć dane krytyczne. Te rodzaje niekorzystnych zdarzeń ostatecznie wpływają na integralność danych (*ang. Data Integrity - DI*). Organizacje muszą być zdolne do wykrywania i reagowania na ataki na integralność danych.

Narodowe Centrum Doskonalenia Cyberbezpieczeństwa (NCCoE) Narodowego Instytutu Standaryzacji i Technologii (NIST) zbudowało środowisko laboratoryjne służące opracowaniu metod skutecznego wykrywania i reagowania na zdarzenie dotyczące zniekształcenia danych w różnych środowiskach informatycznych (IT) organizacji. Przykładowe rozwiązanie przedstawione w tym przewodniku przedstawia propozycję skonstruowaną w laboratorium NCCoE. Umożliwia ono wykrywanie i łagodzenie zdarzeń DI, jednocześnie ułatwiając analizę tych zdarzeń.

Celem niniejszego przewodnika metodycznego w zakresie cyberbezpieczeństwa jest pomoc organizacjom w:

- wykrywaniu złośliwej i podejrzanej aktywności generowanej w sieci przez użytkowników lub z aplikacji, które mogłyby wskazywać na zdarzenie dotyczące integralności danych;
- ograniczaniu i powstrzymywaniu skutków zdarzeń mogących spowodować utratę integralności danych;
- monitorowaniu integralności organizacji w zakresie wykrywania zdarzeń i analizy post factum;
- wykorzystaniu funkcji rejestrowania i raportowania celem przyspieszenia czasu reakcji na zdarzenia dot. integralności danych;
- analizowaniu zdarzeń dot. integralności danych w zakresie ich oddziaływania na sieć, urządzenia i dane organizacji;

- analizowaniu zdarzeń dot. integralności danych w celu poszerzania i udoskonalania środków obrony organizacji przed atakami w przyszłości.

Niniejsza publikacja ma następującą strukturę:

- Rozdział 1: „Podsumowanie" prezentuje zadanie podjęte w projekcie NCCoE wraz z pogłębionym spojrzeniem na podejście, architekturę oraz użyte przez nas charakterystyki bezpieczeństwa, rozwiązanie wskazane w odpowiedzi na wyzwanie, korzyści z rozwiązania oraz partnerów technologicznych uczestniczących w budowie, demonstrowaniu i dokumentowaniu rozwiązania. Rozdział 2: „Jak korzystać z niniejszego przewodnika" wyjaśnia jak czytelnicy — osoby podejmujące decyzje w biznesie, kierownicy programów i informatycy (np. administratorzy systemów) — mogą korzystać z każdej części przewodnika.
- Rozdział 3: „Podejście" stanowi szczegółowe opracowanie zakresu projektu i opisuje założenia, na których oparto tworzenie platformy bezpieczeństwa, szacowanie ryzyka informujące twórców platformy, oraz technologie i komponenty otrzymane od współpracowników branżowych umożliwiających stworzenie platformy testowej.
- Rozdział 4: „Architektura" opisuje scenariusze wykorzystania wspierane przez platformy bezpieczeństwa projektu, w tym funkcje Ram Cyberbezpieczeństwa [1] wspomagane przez każdy komponent dostarczony przez współpracowników.
- Rozdział 5: „Analiza charakterystyki bezpieczeństwa" podaje szczegóły dotyczące narzędzi i technik, z których korzystano przy prowadzeniu szacowania ryzyka.
- Rozdział 6: „Rozważania dotyczące przyszłych rozwiązań" jest krótkim opracowaniem innych wdrożeń z zakresu bezpieczeństwa danych uznanych przez NIST za zgodne z zasadniczymi funkcjami Ram Cyberbezpieczeństwa: identyfikuj, chroń, wykrywaj, reaguj i odzyskuj.

1.1. WYZWANIE

Skrupulatne gromadzenie danych ilościowych i jakościowych jest istotne dla organizacji wszelkiego typu i wielkości. Może wpływać na wszystkie aspekty działalności, w tym podejmowanie decyzji, transakcje, badania, wyniki i rentowność. Kiedy takie zbiory danych podlegają atakowi na integralność danych poprzez

nieautoryzowane wprowadzanie, usuwanie lub modyfikowanie danych, taki atak może wpływać na wiadomości e-mail, dokumentację pracowniczą, dokumentację finansową i dane o klientach, czyniąc je nieprzydatnymi bądź niewiarygodnymi. Niektóre organizacje podlegają atakom systemowym powodującym czasowe zaprzestanie funkcjonowania. Jeden z wariantów ataku na integralność danych — oprogramowanie wymuszające okup (*ang. ransomware*) — szyfruje dane i zatrzymuje je, a napastnik żąda płatności w zamian za klucz służący do odszyfrowania.

W przypadku wystąpienia zdarzenia dot. integralności danych, organizacje powinny mieć zdolność wykrywania i reagowania w czasie rzeczywistym. Wczesne wykrywanie i ograniczanie mogą zredukować potencjalny wpływ takich zdarzeń, w tym uszkodzenie plików organizacji, infekcję systemów i naruszenie zasad ochrony kont. Ponadto organizacje powinny móc wyciągać wnioski ze zdarzeń DI celem poprawy swoich środków obrony. Analiza zachowań złośliwych na poziomie sieci, poziomie użytkownika, poziomie plików może ujawnić wady w systemie bezpieczeństwa organizacji. Usunięcie tych wad, chociaż nie należy do tematyki niniejszego podręcznika, jest często możliwe jedynie dopiero po ich wykryciu i tylko za pomocą posiadania odpowiedniego rozwiązania.

1.2. ROZWIĄZANIE

NCCoE wdrożyło rozwiązanie zawierające odpowiednie działania podczas i bezpośrednio po zdarzeniu dot. integralności danych. Rozwiązanie to składa się z wielu systemów współdziałających w celu wykrycia i reakcji na zdarzenia uszkodzenia danych w standardowych komponentach organizacji. Komponenty te obejmują serwery pocztowe, bazy danych, urządzenia użytkowników końcowych, infrastrukturę wirtualną i serwery udostępniania plików. Ponadto, ważną funkcją z kategorii „Reaguj” Ram Cyberbezpieczeństwa jest poprawa środków obrony — niniejszy przewodnik zawiera komponenty pomagające przy analizie zdarzeń DI i służących udoskonalaniu środków obrony przeciw nim. NCCoE przeanalizowało istniejące technologie zapewniające zdolności takie jak:

- **wykrywanie zdarzeń**
- **monitorowanie integralności**

- **rejestrowanie**
- **raportowanie**
- **ograniczanie i powstrzymywanie**
- **informatyka śledcza/analityka**

Opracowując to rozwiązanie, korzystano z poniższych standardów i wskazówek, które również dla Państwa organizacji mogą być źródłem odpowiednich standardów i dobrych praktyk:

- NIST Framework for Improving Critical Infrastructure Cybersecurity (określane też jako Ramy cyberbezpieczeństwa NIST [1]
- NIST Interagency or Internal Report (NISTIR) 8050: *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy* [2]
- NIST Special Publication (SP) 800-30 Rev. 1: *Guide for Conducting Risk Assessments*[4] [3]
- NIST SP 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach[5] [4]
- NIST SP 800-39: *Managing Information Security Risk*[6] [5]
- NIST SP 800-40 Rev. 3: *Guide to Enterprise Patch Management Technologies* [6]
- NIST SP 800-53 Rev. 4: *Security and Privacy Controls for Federal Information Systems and Organizations*[7] [7]
- Federal Information Processing Standard 140-2: Security Requirements for Cryptographic Modules [8]
- NIST SP 800-86: *Guide to Integrating Forensic Techniques into Incident Response* [9]

[4] Patrz polskojęzyczna publikacja NSC 800-30.

[5] Patrz polskojęzyczna publikacja NSC 800-37.

[6] Patrz polskojęzyczna publikacja NSC 800-39.

[7] Patrz polskojęzyczna publikacja NSC 800-53.

- NIST SP 800-92: *Guide to Computer Security Log Management* [10]
- NIST SP 800-100: *Information Security Handbook: A Guide for Managers*[8] [11]
- NIST SP 800-34 Rev. 1: *Contingency Planning Guide for Federal Information Systems* [12]
- Office of Management and Budget, Circular Number A-130: Managing Information as a Strategic Resource [13]
- NIST SP 800-61 Rev. 2: *Computer Security Incident Handling Guide* [14]
- NIST SP 800-83 Rev. 1: *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [15]
- NIST SP 800-150: *Guide to Cyber Threat Information Sharing* [16]
- NIST SP 800-184: *Guide for Cybersecurity Event Recovery* [17]

1.3. KORZYŚCI

Przewodnik metodyczny cyberbezpieczeństwa może pomóc Państwa organizacji w:

- opracowaniu planu wdrożenia dotyczącego wykrywania i reagowania na zdarzenia dotyczące cyberbezpieczeństwa
- ułatwieniu wykrywania, reagowania i analizy zdarzeń dot. integralności danych w celu poprawy środków obrony i ograniczania skutków
- zachowaniu integralności i dostępności danych o krytycznym znaczeniu dla wspierania działalności gospodarczej
- zarządzaniu ryzykiem organizacji (zgodnie z zasadami zawartymi w Ramach Cyberbezpieczeństwa)

[8] Patrz polskojęzyczna publikacja NSC 800-100.

2. JAK KORZYSTAĆ Z NINIEJSZEGO PRZEWODNIKA

Niniejszy przewodnik metodyczny cyberbezpieczeństwa przedstawia wzór referencyjny oparty na standardach i przekazuje użytkownikom informacje potrzebne do odtworzenia rozwiązania dotyczącego wykrywania i reakcji na zdarzenia w zakresie integralności danych. Ten wzór referencyjny jest modułowy i może być użyty w całości bądź w części.

Niniejszy przewodnik zawiera trzy części:

- NSC 1800-26A: Streszczenie.
- NSC 1800-26B: Podejście, architektura i charakterystyka bezpieczeństwa – co tworzymy i dlaczego **(tutaj jesteś).**
- NIST SP 1800-26C[9], *Przewodniki: „How-to”* – instrukcje tworzenia przykładowego rozwiązania.

  Ze względu na zawartość merytoryczną przewodników (nazwy produktów i plików, zrzuty ekranów, komendy wiersza poleceń, oprogramowanie, itp.) odsyłamy do oryginalnej wersji angielskiej.

Zależnie od twojej funkcji w organizacji, możesz wykorzystywać niniejszy przewodnik w rozmaity sposób:

Osoby podejmujące decyzje w biznesie, w tym kierownictwo ds. bezpieczeństwa i technologii, będą zainteresowane *Streszczeniem*, NSC 1800-26A, które opisuje poniższe zagadnienia:

- wyzwania stojące przed organizacjami w zakresie wykrywania i reagowania na zdarzenia dot. integralności danych;
- przykładowe rozwiązanie opracowane w NCCoE;
- korzyści z zastosowania przykładowego rozwiązania.

Zarządzający sprawami technicznymi lub programem bezpieczeństwa zajmujący się

[9] Patrz publikacja anglojęzyczna: SP 1800-26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events | CSRC (nist.gov)

sposobami identyfikacji, wyjaśniania, oceny i ograniczania ryzyka będą zainteresowani niniejszą częścią przewodnika, NSC 1800-26B, opisującą co wykonano i dlaczego. Szczególnie interesujące mogą być poniższe działy:

- Dział 3.4.1, „Ryzyko", który przedstawia opis przeprowadzonej analizy ryzyka.
- Dział 3.4.2, „Mapa środków bezpieczeństwa", który mapuje charakterystykę bezpieczeństwa tego przykładowego rozwiązania do standardów cyberbezpieczeństwa i dobrych praktyk.

Możesz przekazać treść *Streszczenia*, NSC 1800-26A członkom waszego kierownictwa, aby lepiej zrozumieli wagę przyjęcia rozwiązania opartego na standardach, służącego wykrywaniu i reagowaniu na zdarzenia dot. integralności danych.

Informatycy chcący wdrożyć podobne podejście mogą uznać całą taką praktykę za przydatną. Mogą skorzystać z części „How-to" publikacji NIST SP 1800-26C, aby odtworzyć całość lub część rozwiązania stworzonego w laboratorium NCCoE. Sekcja „how-to" przewodnika pokazuje instrukcję instalacji, konfiguracji i integracji konkretnego produktu dla wdrożenia przykładowego rozwiązania. Nie powielamy dokumentacji produktu sporządzonej przez producenta, która jest powszechnie dostępna. Pokazujemy raczej sposób, w jaki włączyliśmy te produkty w nasze środowisko dla stworzenia przykładowego rozwiązania.

Przewodniki metodyczne cyberbezpieczeństwa zawarte w publikacji NIST SP 1800-26C zakładają, że informatycy mają doświadczenie we wdrażaniu produktów z zakresu bezpieczeństwa w organizacji. Chociaż do celów tego wyzwania użyliśmy zestawu produktów komercyjnych, niniejszy przewodnik nie zatwierdza tych konkretnych produktów. Wasza organizacja może przyjąć to rozwiązanie albo inne, które odpowiada w całości niniejszym wskazówkom, albo też możecie korzystać z niniejszego przewodnika jako punkt wyjścia dla indywidualnego doboru i wdrożenia części rozwiązania wykrywania i reagowania w zakresie integralności danych. Eksperci ds. bezpieczeństwa w organizacji powinni wskazać produkty najlepiej dopasowane do waszych dotychczasowych narzędzi i infrastruktury systemu informacyjnego. Mamy nadzieję, że będziecie starali się stosować produkty zgodne z obowiązującymi

standardami i dobrymi praktykami. Dział 3.5, „Technologie" wymienia zastosowane przez nas produkty i mapuje je na środki cyberbezpieczeństwa zapewniane przez to rozwiązanie referencyjne.

Przewodniki metodyczne cyberbezpieczeństwa nie opisują „tego jedynego" rozwiązania, a jedno z możliwych rozwiązań. Jest to proponowana wskazówka.

2.1. KONWENCJE TYPOGRAFICZNE

Poniższa tabela przedstawia konwencje typograficzne użyte w tej części.

Krój pisma/Symbol	Znaczenie	Przykład
Kursywy	Nazwy plików i nazwy ścieżek; odesłania do dokumentów nie będące hiperłączami; nowe pojęcia; oraz symbole zastępcze	Aby uzyskać więcej wskazówek nt. zastosowania i stylu, zob. *NCCoE Style Guide*.
Pogrubienie (Bold)	Nazwy menu, opcji, przyciski polecenia i pola	Wybierz **File** > **Edit.**
Czcionka o stałej szerokości znaków (monospace)	Polecenia wprowadzane do wiersza poleceń; dane wyjściowe na ekranie; przykłady próbek kodu i kody stanu	mkdir
Pogrubiona czcionka o stałej szerokości znaków (monospace bold)	Polecenia użytkownika wprowadzane do wiersza poleceń skontrastowane z danymi wyjściowymi	**service sshd start**

Tekst niebieski	Łącze do innych części dokumentu, adresu sieciowego URL lub adresu poczty elektronicznej	Wszystkie publikacje NSC są dostępne pod adresem: Narodowe Standardy Cyberbezpieczeństwa

3. PODEJŚCIE

W oparciu o główne punkty wyrażone w publikacji NISTIR 8050: *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy* (2015), NCCoE realizuje szereg projektów w zakresie integralności danych w celu mapowania zasadniczych funkcji Ram Cyberbezpieczeństwa NIST. Projekt ten skupia się wokół zasadniczych funkcji „Wykryj" i „Reaguj", polegających na wykrywaniu i reagowaniu na ataki na integralność danych. Naruszenie ochrony może pochodzić ze złośliwych stron internetowych, wiadomości e-mail dostosowanych do adresata, zagrożeń wewnętrznych i pomyłek popełnionych w dobrej wierze. Aby wykryć te zdarzenia należy wprowadzić rozwiązania monitorujące. Z chwilą wykrycia, istotna jest szybka reakcja na zagrożenie, aby ograniczyć potrzebę działań naprawczych po wystąpieniu zdarzenia. Inżynierowie NCCoE, współpracując ze społecznością zainteresowanych (*ang. Community of Interest, COI*) zdefiniowali wymagania dla tego projektu z zakresu integralności danych.

Członkowie COI, do których należą uczestniczący dostawcy wymienieni w tym dokumencie, mają wkład w opracowanie architektury i wzoru referencyjnego, dostarczając technologie spełniające wymagania projektu oraz pomagając w instalacji i konfiguracji tych technologii. Przewodnik metodyczny cyberbezpieczeństwa podkreśla podejście zastosowane do opracowania rozwiązania referencyjnego NCCoE. Komponenty obejmują szacowanie i analizę ryzyka, projekt logiczny, opracowanie kompilacji, testowanie i ocenę oraz mapowanie środków bezpieczeństwa. Niniejszy przewodnik ma na celu dostarczenie praktycznych wskazówek dla każdej organizacji zainteresowanej wdrożeniem rozwiązania w zakresie wykrywania i reagowania na zdarzenia związane z cyberbezpieczeństwem.

3.1. ODBIORCY

Niniejszy przewodnik jest przeznaczony dla osób odpowiedzialnych za wdrażanie rozwiązań bezpieczeństwa w działalności wsparcia informatycznego organizacji. Obecne systemy informacyjne, szczególnie w sektorze prywatnym, często nie posiadają możliwości kompleksowego wykrywania, ograniczania zdarzeń z zakresu cyberbezpieczeństwa i wyciągania z nich wniosków. Platformy przedstawione

w ramach tego projektu oraz informacje dotyczące wdrożenia zawarte w niniejszym przewodniku metodycznym pozwalają na integrację produktów w celu wdrożenia systemu wykrywania i reagowania na zdarzenia dot. integralności danych. Komponenty techniczne mogą zainteresować administratorów systemów, menedżerów IT, menedżerów ds. bezpieczeństwa informacji oraz inne osoby bezpośrednio odpowiedzialne za bezpieczne i pewne funkcjonowanie sieci IT w organizacjach.

3.2. ZAKRES

Przewodnik podaje praktyczne, realistyczne wskazówki co do opracowania i wdrożenia rozwiązania z zakresu integralności danych zgodnego z zasadami zawartymi w NIST Framework for Improving Critical Infrastructure Cybersecurity (Ramy cyberbezpieczeństwa NIST) Volume 1, a w szczególności w funkcjach zasadniczych „Wykrywaj" i „Reaguj". Wykrywanie kładzie nacisk na opracowanie i wdrożenie odpowiednich działań dla wykrycia zdarzeń w czasie rzeczywistym, porównania bieżącego stanu systemu z normą oraz tworzenia zapisów audytu do wykorzystania w trakcie i po zdarzeniu. Reagowanie kładzie nacisk na ograniczanie zdarzeń w czasie rzeczywistym, analizę śledczą w trakcie i po zdarzeniu oraz raportowanie. Przykłady rezultatów w ramach tych funkcji to monitorowanie integralności, wykrywanie zdarzeń, rejestrowanie, raportowanie, informatyka śledcza i ograniczanie.

3.3. ZAŁOŻENIA

Projekt opiera się na następujących założeniach:

- Rozwiązanie zostało opracowane w środowisku laboratoryjnym. Środowisko to jest oparte na podstawowym obiekcie informatycznym organizacji. Nie odzwierciedla złożoności środowiska produkcyjnego: na przykład budowania w wielu lokalizacjach fizycznych, dostosowywania do skrajnych warunków pracy lub konfigurowania systemów celem spełnienia konkretnych potrzeb sieci/użytkownika. Wszystkie te wymagania mogą zwiększyć poziom złożoności niezbędny do wdrożenia rozwiązania w zakresie integralności danych.
- Organizacja ma dostęp do zestawu umiejętności i zasobów wymaganych do wdrożenia systemu wykrywania i reagowania na zdarzenia.

- W przypadku wystąpienia zdarzenia dot. integralności danych, organizacja stara się wykryć i ograniczyć szkody, które to zdarzenie powoduje.

3.4. SZACOWANIE RYZYKA

NSC 800-30 wskazuje, że ryzyko jest „miarą stopnia, w jakim podmiot jest zagrożony potencjalną okolicznością lub zdarzeniem, oraz jest zazwyczaj funkcją: (I) niekorzystnych skutków, które wystąpiłyby w przypadku zaistnienia okoliczności lub zdarzenia; i (II) prawdopodobieństwa wystąpienia zdarzenia". Definiuje szacowanie ryzyka jako „proces identyfikacji, estymacji i ustalania priorytetów ryzyka dla działalności organizacji (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacji, osób fizycznych, innych organizacji i państwa, wynikających z działania systemu informacyjnego. Część zarządzania ryzykiem obejmuje analizy zagrożeń i podatności oraz bierze pod uwagę środki ograniczania ryzyka wynikające z planowanych lub wprowadzonych zabezpieczeń".

NCCoE zaleca, aby wszelkie dyskusje na temat zarządzania ryzykiem, w szczególności na poziomie organizacji, rozpoczynały się od kompleksowego zapoznania się z dokumentem NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*[10] – stanowiącym materiał publicznie dostępny. Wytyczne Risk Management Framework (RMF) w całości okazały się nieocenione, dając podstawę do oceny ryzyka, na podstawie której opracowano projekt, charakterystykę bezpieczeństwa kompilacji i niniejszy przewodnik.

Przeprowadzono dwa rodzaje szacowania ryzyka:

- Wstępną analizę czynników ryzyka omawianych z instytucjami finansowymi, handlu detalicznego i hotelarskimi. Analiza ta doprowadziła do stworzenia projektu dot. integralności danych i pożądanego stanu ochrony bezpieczeństwa. Dodatkowe informacje o uczestnikach można znaleźć w dokumencie NISTIR 8050, *Executive Technical Workshop*.

[10] Patrz polskojęzyczna publikacja NSC 800-37.

- Analizę sposobu zabezpieczenia komponentów wchodzących w skład projektu i zminimalizowania wszelkich podatności jakie mogą być przez wprowadzane przez te komponenty. Zob. Dział 5, Analiza charakterystyki bezpieczeństwa.

3.4.1. RYZYKO

Korzystając z wytycznych zawartych w serii publikacji NIST dotyczących ryzyka, NCCoE współpracowało z instytucjami finansowymi oraz Centrum Wymiany i Analizy Informacji Sektora Finansowego (*ang. Financial Sector Information Sharing and Analysis Center*) celem zidentyfikowania najbardziej istotnych czynników ryzyka, z jakimi spotyka się ta grupa podmiotów gospodarczych. Uczestniczyło w konferencjach i spotkaniach z przedstawicielami sektora finansowego, aby określić główne zagrożenia dla bezpieczeństwa działalności gospodarczej. W toku tych dyskusji wyłonił się obszar, jakim należy się zająć — integralność danych. Po opracowaniu dokumentu NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*, który skupiał się głównie na odzyskiwaniu jako aspekcie integralności danych, NCCoE stwierdził, że istnieje potrzeba opracowania wytycznych w dziedzinach wykrywania zdarzeń cyberbezpieczeństwa i reagowania na nie w czasie rzeczywistym.

Rozpatrując ryzyko z perspektywy wykrywania zdarzeń w cyberprzestrzeni i reagowania na nie podczas ich realizacji, musimy wziąć pod uwagę nie tylko wpływ zdarzenia na aktywa organizacji, ale także zagrożenia dla tych aktywów i potencjalne podatności, które te zagrożenia mogą wykorzystać.

Omawiając zagrożenia dla zasobów organizacji z punktu widzenia integralności danych, bierzemy pod uwagę następujące czynniki:

- złośliwe oprogramowanie,
- zagrożenia wewnętrzne,
- zdarzenia spowodowane błędem ludzkim,
- naruszenia zasad ochrony zaufanych systemów.

Rodzaje podatności, które bierzemy pod uwagę w związku z tymi zagrożeniami, obejmują:

- podatności typu zero-day,
- podatności spowodowane przestarzałymi lub niezałatanymi systemami,
- podatności/błędy w oprogramowaniu niestandardowym,
- inżynierię społeczną i zdarzenia wywołane przez użytkowników,
- niedostateczną kontrolę dostępu.

Potencjalny wpływ na organizację z powodu zdarzenia dot. integralności danych obejmuje:

- niewydolność systemów,
- modyfikację/usunięcie aktywów organizacji,
- negatywny wpływ na reputację organizacji.

Analiza zagrożeń i podatności oraz potencjalny wpływ na organizację daje wyobrażenie o ryzyku dla organizacji w odniesieniu do DI. Publikacja NSC SP 800-39 skupia się na biznesowym aspekcie ryzyka na poziomie organizacji. Taka wiedza jest niezbędna do dalszej analizy ryzyka, reagowania na nie/ograniczania jego skutków oraz monitorowania ryzyka.

Poniżej podano podsumowanie ustalonych strategicznych obszarów ryzyka oraz środki ich ograniczania:

- Wpływ na funkcjonowanie systemu – zapewnienie dostępności dokładnych danych lub utrzymanie akceptowalnego poziomu integralności danych zmniejsza ryzyko naruszenia dostępności systemów.
- Koszt wdrożenia — jednorazowe wdrożenie wykrywania i reagowania na zdarzenia dotyczy integralności danych oraz używanie go we wszystkich systemach może obniżyć nakłady ponoszone na utrzymanie ciągłości działania systemu.
- Zgodność z istniejącymi standardami branżowymi — przyczynia się do spełniania wymagań branżowych dotyczących utrzymania ciągłości planu operacji.

- Utrzymanie reputacji i wizerunku publicznego – pomaga zmniejszyć szkody wyrządzane przez aktywne zdarzenia i ułatwia zdobycie informacji potrzebnych do wyciągania wniosków ze zdarzeń.
- Większy nacisk na integralność danych – obejmuje nie tylko utratę poufności, ale także szkody wynikające z nieautoryzowanej zmiany danych (zgodnie z NISTIR 8050).

Następnie dokonano przełożenia zidentyfikowanych czynników ryzyka na funkcje bezpieczeństwa i podkategorie według Ram Cyberbezpieczeństwa NIST.

W Tabeli 3-1 zmapowane zostały kategorie i podkategorie Ram Cyberbezpieczeństwa ze środkami bezpieczeństwa standardu NSC 800-53 oraz standardów i dobrych praktyk ISO/IEC 27001:2013 oraz NIST SP 800-181.

3.4.2. MAPA ŚRODKÓW BEZPIECZEŃSTWA

Jak wyjaśniono w Dziale 3.4.1, NCCoE zidentyfikowało Funkcje i Podkategorie bezpieczeństwa według Ram Cyberbezpieczeństwa, które projekt referencyjny miał wspierać poprzez proces analizy ryzyka. Był to pierwszy krytyczny krok w przygotowaniu wzoru referencyjnego i przykładowej implementacji w celu ograniczenia czynników ryzyka. Tabela 3-1 wymienia listę Funkcji i Podkategorii Ram Cyberbezpieczeństwa, o których mowa, oraz mapuje je na odpowiednie standardy NIST, standardy branżowe i dobre praktyki. Odnośniki podają punkty walidacyjne rozwiązania w miejscu, gdzie wymieniają konkretne zdolności bezpieczeństwa, jakimi powinno charakteryzować się rozwiązanie odnoszące się do podkategorii Ram Cyberbezpieczeństwa. Organizacje mogą skorzystać z Tabeli 3-1 ,aby zidentyfikować podkategorie Ram cyberbezpieczeństwa i środki z NSC 800-53, którymi są zainteresowane.

Podczas porównywania Funkcji Ram Cyberbezpieczeństwa z możliwościami produktu zastosowanego w niniejszym przewodniku metodycznym należy wziąć pod uwagę, że:

- Niniejszy przewodnik metodyczny, choć koncentruje się głównie na zdolnościach wykrywania/reagowania, wykorzystuje również podkategorię PR.DS-6 - Chroń. Dzieje się tak przede wszystkim dlatego, że tworzenie integralności zabezpieczeń bazowych jest wykorzystywane do porównywania podczas wykrywania ataków, ale jest tworzone przed rozpoczęciem ataku.
- Nie wszystkie wytyczne dotyczące podkategorii Ram Cyberbezpieczeństwa można wdrożyć przy użyciu technologii. Każda organizacja wdrażająca rozwiązanie z zakresu integralności danych musiałaby przyjąć procesy i polityki organizacyjne wspierające wzór referencyjny. Na przykład niektóre podkategorie w ramach funkcji Ram Cyberbezpieczeństwa o nazwie Reaguj to procesy i polityki, które należy opracować przed wdrożeniem zaleceń.

Tabela 0-1 Mapa podstawowych komponentów DI projektu referencyjnego Ram Cyberbezpieczeństwa

Cybersecurity Framework v1.1				**Standardy i dobre praktyki**	
Funkcja	**Kategoria**	**Podkategoria**	**NSC 800-53**	**ISO/IEC 27001: 2013**	**NIST SP 800-181**
CHROŃ (PR)	Bezpieczeństwo danych (PR.DS)	PR.DS-6: Mechanizmy sprawdzania integralności stosowane są do weryfikacji oprogramowania, oprogramowania układowego i integralności informacji.	SC-16, SI-7	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4,	OM-DTA-001
WYKRYWAJ (DE)	Anomalie i zdarzenia (DE.AE)	DE.AE-1: Zabezpieczenie bazowe operacji sieciowych i przewidywanych przepływów danych dla użytkowników i systemów zostało ustanowione i jest kontrolowane.	AC-4, CA-3, CM-2, SI-4	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2,	SP-ARC-001

Cybersecurity Framework v1.1				Standardy i dobre praktyki	
Funkcja	**Kategoria**	**Podkategoria**	**NSC 800-53**	**ISO/IEC 27001: 2013**	**NIST SP 800-181**
		DE.AE-2: Wykryte zdarzenia są analizowane w celu zrozumienia celów i metod ataku.	AU-6 CA-7, IR-4, SI-4	A.12.4.1, A.16.1.1, A.16.1.4,	PR-CDA-001
		DE.AE-3: Dane o zdarzeniu są zbierane i korelowane z danymi z wielu źródeł i sensorów.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	A.12.4.1, A.16.1.7,	CO-OPS-001, PR-CIR-001
		DE.AE-4: Określony zostaje wpływ zdarzeń.	CP-2, IR-4, RA-3, SI-4	A.16.1.4,	PR-INF-001
	Ciągłe monitorowanie bezpieczeństwa (DE.CM)	DE.AE-5: Ustalone są progi alarmowe incydentów.	IR-4, IR-5, IR-8	A.16.1.4,	PR-CIR-001
		DE.CM-1: Sieć jest monitorowana pod kątem wykrycia potencjalnych zdarzeń w zakresie cyberbezpieczeństwa.	AC-2, AU- 12, CA-7, CM-3, SC-5, SC-7, SI-4		OM-NET-001
		DE.CM-3: Aktywność pracowników jest monitorowana pod kątem wykrycia potencjalnych zdarzeń w zakresie cyberbezpieczeństwa.	AC-2, AU- 12, AU-13, CA-7, CM- 10,	A.12.4.1, A.12.4.3,	AN-TWA-001

Cybersecurity Framework v1.1				Standardy i dobre praktyki	
Funkcja	**Kategoria**	**Podkategoria**	**NSC 800-53**	**ISO/IEC 27001: 2013**	**NIST SP 800-181**
			CM-11		
		DE.CM-4: Wykrywane są złośliwe kody.	SI-3, SI-8	A.12.2.1	SP-DEV-001
		DE.CM-5: Wykrywane są nieautoryzowane kody mobilne.	SC-18, SI-4, SC-44	A.12.5.1, A.12.6.2,	SP-DEV-001
		DE.CM-7: Prowadzone jest monitorowanie pod kątem nieautoryzowanego personelu, połączeń, urządzeń i oprogramowania.	AU-12, CA- 7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	A.12.4.1, A.14.2.7, A.15.2.1	AN-TWA-001
	Procesy wykrywania (DE.DP)	DE.DP-2: Czynności wykrywania spełniają wszystkie obowiązujące wymagania.	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	A.18.1.4, A.18.2.2, A.18.2.3	PR-CDA-001
REAGUJ (RS)	Planowanie reagowania (RS.RP)	RS.RP-1: Plan reagowania jest wykonany podczas lub po incydencie.	CP-2, CP-10, IR-4, IR-8	A.16.1.5	PR-CIR-001
	Komunikacja (RS.CO)	RS.CO-2: Incydenty są zgłaszane zgodnie z ustalonymi kryteriami.	AU-6, IR-6, IR-8	A.6.1.3, A.16.1.2	IN-FOR-002
	Analiza (RS.AN)	RS.AN-1: Badane są powiadomienia z systemów wykrywania	AU-6, CA-7,	A.12.4.1, A.12.4.3,	PR-CDA-001

Cybersecurity Framework v1.1				Standardy i dobre praktyki	
Funkcja	**Kategoria**	**Podkategoria**	**NSC 800-53**	**ISO/IEC 27001: 2013**	**NIST SP 800-181**
			IR-4, IR-5, PE-6, SI-4	A.16.1.5	
		RS.AN-2: Wpływ incydentu jest rozumiany.	CP-2, IR-4	A.16.1.4, A.16.1.6	PR-CIR-001
		RS.AN-3: Przeprowadzono badania śledczo-informatyczne.	AU-7, IR-4	A.16.1.7,	IN-FOR-002
		RS.AN-4: Incydenty zostały przydzielone do kategorii zgodnie z planami reagowania	CP-2, IR-4, IR-5, IR-8	A.16.1.4	PR-CIR-001
	Ograniczanie (RS.MI)	RS.MI-1: Incydenty są powstrzymane.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001
		RS.MI-2: Incydenty są ograniczone.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001

3.5. TECHNOLOGIE

Tabela 3-2 zawiera listę wszystkich technologii użytych w tym projekcie i przedstawia mapowanie pomiędzy aplikacjami ogólnymi, konkretnym użytym produktem i zabezpieczeń, które zapewnia dany produkt. Wyjaśnienia kodów podkategorii Ram Cyberbezpieczeństwa znajdują się w Tabeli 3-1.

Tabela 0-2 Produkty i technologie

Komponent	Produkt	Funkcja	Podkategorie Ram cyberbezpieczeństwa
Monitorowanie integralności	Tripwire Enterprise v8.7	• Zapewnia hashe plików i sprawdzanie integralności plików i oprogramowania niezależnie od typu pliku. • Zapewnia monitorowanie integralności danych. • Zapewnia monitorowanie integralności dla Active Directory	PR.DS-6, DE.AE-1, DE.CM-3, DE.CM-7
	Semperis Directory Services Protector (DSP) v2.7		
Wykrywanie zdarzeń	Cisco Advanced Malware Protection (AMP) v5.4	• Zapewnia możliwość odbioru informacji o nowych zagrożeniach. • Zapewnia możliwość statycznego wykrywania złośliwego oprogramowania.	DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-7
	Glasswall FileTrust ATP for Email v6.90.2.5		
	Cisco Stealthwatch v7.0.0		

Komponent	Produkt	Funkcja	Podkategorie Ram cyberbezpieczeństwa
	Semperis DSP v2.7	• Zapewnia możliwość dynamicznego wykrywania złośliwego oprogramowania. • Zapewnia możliwość wykrywania złośliwych załączników wiadomości e-mail. • Zapewnia możliwość skanowania sieci w poszukiwaniu anomalii. • Zapewnia możliwość monitorowania zachowania użytkownika pod kątem anomalii. • Zapewnia możliwość skanowania załączników wiadomości e-mail pod kątem odchyleń od specyfikacji typu pliku lub polityki organizacji.	
Rejestrowanie	Micro Focus ArcSight Enterprise Security Manager (ESM) v7.0 Patch 2 Tripwire Log Center v7.3.1	• Zapewnia zdolności audytowania i rejestracji w dziennikach, konfigurowalne według polityki organizacji. • Koreluje dzienniki zdarzeń cyberbezpieczeństwa z informacjami o użytkowniku. • Zapewnia automatyzację rejestrowania.	DE.AE-1, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-3, DE.CM-7, RS.AN-2

Komponent	**Produkt**	**Funkcja**	**Podkategorie Ram cyberbezpieczeństwa**
Informatyka śledcza/analityka	Cisco AMP v5.4 Symantec Security Analytics v8.0.1 Micro Focus ArcSight ESM v7.0 Patch 2 Symantec Information Centric Analytics (ICA) v6.5.2	• Zapewnia środki informatyki śledczej do retrospektywnego śledzenia skutków złośliwego oprogramowania. • Zapewnia analizę ruchu sieciowego. • Zapewnia możliwość analizowania plików przesyłanych w sieci. • Zapewnia zdolności analizy w celu znalezienia anomalii w działalności organizacji.	DE.AE-2, DE.AE-4, DE.CM-1, RS.RP-1, RS.AN-1, RS.AN-2, RS.AN-3
Ograniczanie i powstrzymywanie	Cisco AMP v5.4 Cisco Identity Services Engine (ISE) v2.4 Glasswall FileTrust ATP for Email v6.90.2.5 Semperis DSP v2.7	• Zapewnia możliwość lokalnego izolowania plików w środowisku testowym. • Zapewnia możliwość egzekwowania polityki w całej organizacji. • Zapewnia możliwość poddawania kwarantannie urządzeń w całej organizacji. • Zapewnia możliwość oczyszczania plików poprzez rekonstrukcję plików. • Zapewnia możliwość cofania zmian w usługach domenowych.	DE.CM-5, RS.RP-1, RS.MI-1, RS.MI-2

Komponent	Produkt	Funkcja	Podkategorie Ram cyberbezpieczeństwa
Raportowanie	Micro Focus ArcSight ESM v7.0 Patch 2	• Zapewnia możliwość wysyłania alertów bezpieczeństwa w oparciu o politykę organizacji. • Zapewnia możliwość dostarczania raportów o kondycji organizacji. • Zapewnia możliwość dostarczania raportów dotyczących wykrywania złośliwego oprogramowania w całej organizacji.	DE.AE-5, RS.RP-1, RS.CO-2

4. ARCHITEKTURA

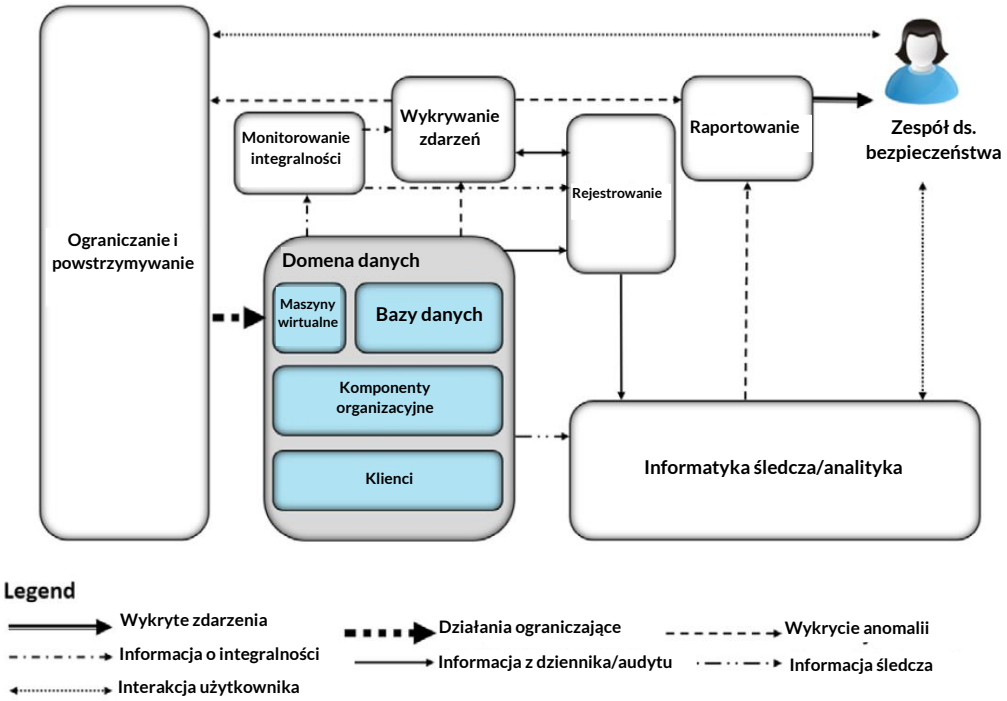
Niniejszy rozdział przedstawia architekturę wysokiego poziomu stosowaną do wdrożenia rozwiązania dot. integralności danych służącego wykrywaniu i reagowaniu na oprogramowanie wymuszające okup i inne zdarzenia destrukcyjne.

4.1. OPIS ARCHITEKTURY

4.1.1. ARCHITEKTURA WYSOKIEGO POZIOMU

Rozwiązanie dot. integralności danych jest przeznaczone do realizacji funkcji i podkategorii bezpieczeństwa opisanych w Tabeli 3-1 i składa się ze zdolności przedstawionych na rysunku 4-1.

Rysunek 0-1 Architektura wysokiego poziomu dla zdolności Wykrywaj i Reaguj dot. integralności danych



- **Monitorowanie integralności** zapewnia zdolność porównywania bieżących stanów systemu z ustalonymi zabezpieczeniami bazowymi.

- **Wykrywanie zdarzeń** zapewnia zdolność wykrywania bieżących zdarzeń i może składać się z wykrywania włamań, wykrywania złośliwego oprogramowania, wykrywania anomalii u użytkowników i innych zdarzeń, w zależności od ustalonego modelu zagrożeń w organizacji.
- **Rejestrowanie** (*ang. logging*) zapisuje i przechowuje wszystkie pliki dziennika wytwarzane przez komponenty w organizacji.
- **Informatyka śledcza/analityka** zapewnia zdolność badania/analizy dzienników (logów) i maszyn w organizacji w celu wyciągania wniosków ze zdarzeń DI.
- **Ograniczanie i powstrzymywanie** pozwalają na reagowanie na zdarzenia DI poprzez powstrzymywanie i ograniczanie zdolności zagrożenia do oddziaływania na system.
- **Raportowanie** zapewnia możliwość zgłaszania wszystkich działań w organizacji i w ramach architektury referencyjnej do analizy przez zespół ds. bezpieczeństwa.

Te zdolności wzajemnie współpracują, aby zapewnić funkcje wykrywania i reagowania pod kątem integralności danych. Zdolność monitorowania integralności gromadzi informacje o integralności przed nastąpieniem ataku, tak aby w momencie ataku zachowane zostały zapisy wszystkich zmian w plikach/systemie. W połączeniu z wykrywaniem zdarzeń, zapisy te nie tylko funkcjonują jako narzędzie podające informacje służące odzyskiwaniu, ale także jako wczesne wskaźniki naruszenia. Wykrywanie zdarzeń wykorzystuje te zapisy oraz swoje własne mechanizmy do aktywnego wykrywania zdarzeń w miarę ich występowania i podejmowania odpowiednich działań poprzez inne komponenty architektury referencyjnej. Rejestrowanie gromadzi informacje z wykrywania zdarzeń i monitorowania integralności w celu wykorzystania ich w funkcjach reagowania. Ograniczanie i powstrzymywanie zapewniają zdolności zatrzymania trwających ataków i ograniczenia ich wpływu na system. Informatyka śledcza/analityka umożliwia analizę dzienników i sposobu zachowania zagrożeń, aby pomóc organizacji w wyciągnięciu wniosków z ataku. Raportowanie zapewnia zdolności przekazywania odpowiednim podmiotom informacji z analizy i rejestrowania ich u tych podmiotów zarówno podczas,

jak i po ataku. Informacje uzyskane z tych ataków mogą być wykorzystane w produktach należących do funkcji Identyfikuj według Ram Cyberbezpieczeństwa, aby wskazać te podatności występujące w organizacji, które należy naprawić.

4.1.2. KOMPONENTY ARCHITEKTURY

4.1.2.1 Monitorowanie integralności

Komponent monitorowania integralności zapewnia możliwość testowania, zrozumienia i pomiaru skali ataków na pliki i komponenty w organizacji. Rozpatrując integralność danych z perspektywy wykrywania i reagowania na aktywny atak, możliwość śledzenia zmian w plikach ma krytyczne znaczenie. Zmiany integralności zasobów mogą zapewnić mechanizm wczesnego wykrywania poprzez śledzenie zmian wprowadzonych w nietypowych momentach lub przez śledzenie użytkowników, którzy zazwyczaj nie wprowadzają takich zmian. Ponadto zmiany śledzone podczas zdarzenia dot. integralności danych mogą być wykorzystane do podania informacji służącej w procesie odzyskiwania; dostarczają informacji o tym, jakie zmiany zaszły, kiedy zmiany zaczęły się pojawiać, a także o tym, jakie programy były zaangażowane w zmiany.

Monitorowanie integralności zazwyczaj wymaga, aby operacyjne zabezpieczenie bazowe było podjęte przed rozpoczęciem zdarzenia dot. integralności danych — to zabezpieczenie bazowe jest używane do porównania ze stanem systemu podczas ataku.

Do monitorowania integralności używamy kombinacji dwóch narzędzi: Tripwire Enterprise i Semperis DSP. Gdy zabezpieczenie bazowe zostanie wprowadzone przed atakiem, Tripwire Enterprise przechowuje informacje o integralności wybranych danych we wszystkich systemach. Po uruchomieniu „check”, Tripwire gromadzi wszystkie zmiany, które wystąpiły w monitorowanych plikach w tych systemach. Zmiany te są przekazywane do komponentu rejestrowania, który może następnie raportować i alarmować o nich, stając się wskaźnikiem zdarzenia dot. integralności danych. Ponadto zebrane zmiany mogą zostać wykorzystane do wyeliminowania skutków działania złośliwego oprogramowania w systemie.

Semperis DSP zapewnia podobną funkcję, ale z naciskiem na Active Directory. Zmiany wprowadzone w użytkownikach, grupach i innych usługach Active Directory są gromadzone i mogą być używane do powiadamiania administratorów o potencjalnie złośliwej aktywności. Biorąc pod uwagę wrażliwość Active Directory, Semperis DSP nie opiera się na jednym źródle informacji, ale zamiast tego monitoruje wiele aspektów Active Directory. Pomaga to zapewnić przechwytywanie wszelkich zmian uprawnień lub poświadczeń uprzywilejowanych, w tym zmian, które atakujący próbują ukryć (na przykład omijając audyt zabezpieczeń).

4.1.2.2 Wykrywanie zdarzeń

Komponent wykrywania zdarzeń zapewnia możliwość wykrywania zdarzeń w miarę ich występowania. Można to osiągnąć poprzez łączenie mechanizmów w zależności od potrzeb organizacji. Analiza dzienników monitorowania integralności może wskazywać na złośliwe działanie. Wykrywanie złośliwego oprogramowania, wykrywanie anomalii na podstawie zachowania i wykrywanie intruzów są potencjalnymi przykładami wykrywania zdarzeń. Celem tego komponentu jest wykrywanie zdarzeń w miarę ich występowania, wyzwalanie odpowiednich reakcji i dostarczanie informacji o ataku zespołowi ds. bezpieczeństwa.

Do wykrywania zdarzeń używamy kombinacji narzędzi. Cisco AMP służy do wykrywania złośliwych plików. Glasswall FileTrust ATP for Email służy do identyfikowania złośliwych załączników wiadomości e-mail, które nie są zgodne ze standardami plików i polityką organizacji. Cisco Stealthwatch jest wykorzystywany do wykrywania złośliwej aktywności w sieci. Z kolei Semperis DSP jest używany do wykrywania zmian w usłudze Active Directory. Informacje pochodzące z tych czterech źródeł mogą być skorelowane w celu zidentyfikowania złośliwych wzorców zachowań użytkowników.

4.1.2.3 Rejestrowanie

Rejestrowanie z każdego komponentu służy kilku funkcjom w architekturze, mającym na celu wykrywanie aktywnych zdarzeń dot. integralności danych i reagowanie na nie. Dzienniki są tworzone poprzez monitorowanie integralności i wykrywanie zdarzeń, co pomaga innym komponentom w reagowaniu na aktywne zdarzenia. Zarówno ograniczanie i powstrzymywanie, a także informatyka śledcza/analityka wykorzystują

dzienniki do informowania o swoich działaniach — dzienniki informują o tym, jakich systemów dotyczy zdarzenie i jakie programy powodują to zdarzenie. Ponadto dzienniki te pomagają w podjęciu decyzji, jakie kroki należy podjąć w celu zaradzenia atakowi i ochrony przed nim w przyszłości.

Dla zapewnienia zdolności rejestrowania, używamy kombinacji dwóch narzędzi: Micro Focus ArcSight i Tripwire Log Center. O ile celem Tripwire Log Center w tej kompilacji jest przede wszystkim zbieranie, przekształcanie i przekazywanie dzienników z Tripwire Enterprise do ArcSight, to ArcSight ma szerszą funkcję. ArcSight zbiera logi z różnych źródeł w organizacji, takich jak wykrywanie zdarzeń i monitorowanie integralności, a także dzienniki zdarzeń systemu Windows i syslogi Ubuntu. Celem takiego szeroko zakrojonego gromadzenia dzienników jest stworzenie podstawy dla komponentu informatyki śledczej/analityki.

4.1.2.4 Ograniczanie i powstrzymywanie

Komponent ograniczania i powstrzymywania zapewnia możliwość ograniczenia wpływu destrukcyjnego zdarzenia na organizację. Dla zwiększenia skuteczności, komponent ten może współdziałać z zespołem bezpieczeństwa i może mieć możliwość automatycznego reagowania na określone zdarzenia dot. integralności danych. Reakcja ta może obejmować wstrzymanie wykonywania powiązanych programów, wyłączenie kont użytkowników, odłączenie systemu od sieci i wiele innych, zależnie od zagrożenia. Inne działania mogą obejmować usunięcie oprogramowania z systemu, ponowne uruchomienie usług lub skopiowanie zagrożenia do bezpiecznego środowiska w celu analizy.

Do zapewnienia zdolności ograniczania i powstrzymywania używamy kombinacji narzędzi. Cisco AMP zapewnia możliwość natychmiastowego usuwania złośliwych plików — w połączeniu ze zdolnością wykrywania zdarzeń można to wykorzystać do natychmiastowego reagowania na złośliwe oprogramowanie w systemach użytkowników. Cisco ISE zapewnia funkcje kwarantanny, które mogą być wykorzystane do reagowania na wykryte złośliwe oprogramowanie i niewystarczającą ochronę maszyn, a także na zdarzenia sieciowe w Stealthwatch. Semperis DSP zapewnia możliwość natychmiastowego i automatycznego przywracania wykrytych zmian

w Active Directory, ograniczając użycie backdoorów i innych złośliwych zmian w domenie. Semperis DSP może również wyłączać konta użytkowników, aby zapobiec dalszym zmianom dokonywanym przez naruszone lub złośliwie utworzone konta. Glasswall zapewnia możliwość sanityzacji złośliwych lub niezgodnych z przepisami załączników wiadomości e-mail, zanim jeszcze trafią do skrzynki odbiorczej użytkownika, eliminując w ten sposób złośliwe treści w załącznikach wiadomości e-mail.

4.1.2.5 Informatyka śledcza/analityka

Komponent informatyki śledczej/analityki wykorzystuje dzienniki generowane przez wykrywanie zdarzeń i umożliwia organizacji odkrywanie źródła i skutków zdarzenia DI oraz poznania sposobów ewentualnego zapobiegania podobnym zdarzeniom w przyszłości. Komponent ten zwykle pozwoli organizacji na analizę złośliwego oprogramowania lub dzienników związanych z wykonaniem złośliwego oprogramowania i poda informacje np. o serwerach, z którymi komunikuje się złośliwe oprogramowanie czy o sygnaturze pliku wykonywalnego, w celu poprawy wykrywalności złośliwego oprogramowania w przyszłości. Ponadto, pożądana może być możliwość zbadania maszyn dotkniętych przez złośliwe oprogramowanie pod kątem trwałych skutków. Informacje uzyskane z analizy informatyczno-śledczej mogą być również wykorzystane do wzmocnienia ochrony organizacji przed złośliwym oprogramowaniem i potencjalnego zreformowania polityki w organizacji.

Do informatyki śledczej/analityki używamy kombinacji narzędzi. Cisco AMP umożliwia przeglądanie historii złośliwych plików dla określenia ich źródła i przepływu w organizacji. Symantec Security Analytics zapewnia możliwość analizy ruchu sieciowego w podobny sposób. ArcSight ESM zapewnia zdolności korelacji zdarzeń dla dzienników zebranych z niemal wszystkich pozostałych zdolności, umożliwiając przetwarzanie zdarzeń przed zgłoszeniem ich do zespołu ds. bezpieczeństwa. Symantec ICA zapewnia dodatkowe zdolności analizy dla dzienników, a także agregacji i wizualizacji niektórych potencjalnie złośliwych ruchów w organizacji. Produkty te pomagają w przyszłości zapobiegać takim atakom, jak również ustalają zakres wpływu zdarzenia na system.

4.1.2.6 Raportowanie

Komponent raportowania jest przede wszystkim interfejsem pomiędzy różnymi elementami architektury a zespołem ds. bezpieczeństwa. Umożliwia on alarmowanie na podstawie zdarzeń za pośrednictwem poczty elektronicznej oraz pulpitów nawigacyjnych, w zależności od potrzeb organizacji. Zdolności raportowania są najlepiej wykorzystywane przez cały czas trwania zdarzenia — mogą być używane do ostrzegania zespołu ds. bezpieczeństwa, gdy zdarzenie się rozpoczyna, jak również do regularnych aktualizacji stanu, gdy zdarzenia nie mają miejsca lub właśnie się zakończyły.

Do raportowania używamy systemu Micro Focus ArcSight. ArcSight może wysyłać alerty e-mail i generować raporty na podstawie prowadzonej przez siebie korelacji i analizy dzienników. Zapewniając integrację jak największej liczby istotnych dzienników z możliwościami rejestrowania ArcSight, możemy używać różnych wskaźników do wyzwalania alertów, gdy określone dzienniki lub zestawy dzienników są odbierane przez ArcSight.

5. ANALIZA CHARAKTERYSTYKI BEZPIECZEŃSTWA

Celem analizy charakterystyki bezpieczeństwa jest zrozumienie, w jakim stopniu projekt spełnia swój cel, czyli zademonstrowanie rozwiązania wykrywania i reagowania w zakresie integralności danych. Ponadto ma na celu poznanie zalet i wad przykładowego rozwiązania w zakresie bezpieczeństwa.

5.1. ZAŁOŻENIA I OGRANICZENIA

Analiza charakterystyki bezpieczeństwa ma następujące ograniczenia:

- Nie jest to ani kompleksowy test wszystkich komponentów bezpieczeństwa, ani ćwiczenie w „roli agresora" (*ang. red-team exercise*).
- Nie jest w stanie zidentyfikować wszystkich podatności.
- Nie obejmuje infrastruktury laboratoryjnej. Przyjmuje się, że urządzenia są „utwardzone" (*ang. hardened*). Testowanie tych urządzeń ujawniłoby jedynie słabości w implementacji, które nie byłyby istotne dla osób adoptujących tę architekturę referencyjną.

5.2. TESTOWANIE KOMPILACJI

Celem analizy charakterystyki bezpieczeństwa jest zrozumienie, w jakim stopniu moduł konstrukcyjny spełnia swój cel wykrywania zdarzeń dot. integralności danych i reagowania na nie. Ponadto projekt ma na celu ułatwienie analizy tych zdarzeń w trakcie i po ataku. Dodatkowo ma na celu poznanie zalet i wad wzoru referencyjnego w zakresie bezpieczeństwa.

5.3. SCENARIUSZE I USTALENIA

Jeden z aspektów przeprowadzanej oceny bezpieczeństwa obejmował sprawdzenie, w jakim stopniu wzór referencyjny odnosi się do charakterystyki bezpieczeństwa, jaką miał wspierać. Podkategorie Ram Cyberbezpieczeństwa zostały użyte do zapewnienia struktury oceny bezpieczeństwa poprzez zapoznanie się z określonymi działami każdego standardu cytowanego w odniesieniu do podkategorii. Cytowane działy zawierają punkty walidacyjne, których oczekuje się od przykładowego rozwiązania. Wykorzystanie podkategorii Ram Cyberbezpieczeństwa jako podstawy zorganizowania przeprowadzonej analizy pozwoliło na systematyczne rozważenie,

w jakim stopniu wzór referencyjny wspiera zamierzoną charakterystykę bezpieczeństwa.

Poniżej znajdują się scenariusze opracowane celem przetestowania różnych aspektów tej architektury. Bardziej szczegółowe rozwiązania i mapowanie wymagań tych scenariuszy do Ram Cyberbezpieczeństwa można znaleźć w Załączniku D.

5.3.1. WEKTOR ATAKU RANSOMWARE POPRZEZ WEB I SAMOPROPAGACJĘ

5.3.1.1 Scenariusz

Poniższy scenariusz został zasymulowany w celu przetestowania ochrony architektury przed oprogramowaniem wymuszającym okup (ang. *ransomware*).

Użytkownik przez pomyłkę pobiera ransomware z zewnętrznego serwera internetowego. Gdy użytkownik uruchamia złośliwe oprogramowanie, generuje ono klucz kryptograficzny, który jest odsyłany z powrotem do zewnętrznego serwera internetowego. Złośliwe oprogramowanie wykorzystuje następnie exploit eskalacji uprawnień do rozprzestrzeniania się w sieci. Złośliwe oprogramowanie szyfruje pliki na maszynach, na których się rozprzestrzeniło i żąda zapłaty w zamian za odszyfrowanie tych plików.

5.3.1.2 Rozwiązanie

Moduł konstrukcyjny zapewnia istotną głęboką obronę przed tym przypadkiem użycia.

Funkcja **wykrywania zdarzeń** zapewnia możliwość wykrywania złośliwego oprogramowania w systemie oraz generowania dzienników i alertów na podstawie tej aktywności. Pozwala również na wykrywanie podejrzanych zachowań sieciowych, takich jak propagacja.

Zdolność **ograniczania i powstrzymywania rozprzestrzeniania** zapewnia możliwość zatrzymania wykonywania oprogramowania ransomware i usunięcia go z systemu. Ponadto umożliwia kwarantannę zaatakowanych maszyn z sieci po wykryciu złośliwej aktywności.

Funkcja **monitorowania integralności** zapewnia możliwość gromadzenia zmian w plikach, w tym zmian dokonanych przez oprogramowanie wymuszające okup, a także pierwszego utworzenia lub pobrania oprogramowania ransomware do systemu.

Po przesłaniu do **rejestrowania**, dzienniki te w połączeniu z innymi zapisami logów mogą posłużyć do zidentyfikowania zakresu ataku.

Zdolność **raportowania** używa dzienników z powyższych zdolności do zgłaszania złośliwej aktywności i poprawienia czasu reakcji.

Zdolność **informatyki śledczej/analityki** analizuje dzienniki związane ze zdarzeniem w celu dostarczenia informacji, które mogą być wykorzystane do wzmocnienia obrony przed atakiem w przyszłości. Obejmuje to strony Web, z którymi oprogramowanie to się łączyło lub z którego zostało pobrane, sygnaturę pliku wykonywalnego i zakres ataku.

5.3.1.3 Pozostałe kwestie

Ze względu na to, że złośliwe oprogramowanie występuje w wielu postaciach, konieczne jest posiadanie wielu warstw obrony przed nim, a jednocześnie aktywne działanie na rzecz poprawy tej obrony. Wczesna obrona przed złośliwym oprogramowaniem oznacza umieszczenie znanych złośliwych witryn na liście witryn zakazanych. Ponieważ jednak musi to być zrobione całkowicie przed nastąpieniem ataku, jest to poza zakresem tej kompilacji.

Nasza kompilacja sugeruje by to szczególnie zdolność informatyki śledczej/analityki była narzędziem informowania i wzmacniania ochrony organizacji przed przyszłymi atakami. Jest to funkcja kategorii „Reaguj” — uczenie się na wyciąganiu wniosków z ataków może stanowić podstawę obrony przed takimi atakami w przyszłości, zarówno w fazach ataku „Chroń”, jak i „Wykrywaj”. Jednym z takich środków obrony wskazanym przez kategorię Reaguj może być umieszczenie na liście zakazanych, a innym wykrywanie zdarzeń.

5.3.2. DESTRUKCYJNE OPROGRAMOWANIE ZŁOŚLIWE POPRZEZ WEKTOR USB

5.3.2.1 Scenariusz

Poniższy scenariusz został zasymulowany w celu przetestowania ochrony architektury przed oprogramowaniem destrukcyjnym.

Użytkownik znajduje nieoznakowane urządzenie USB (*ang. Universal Serial Bus*) i wkłada je do swojego systemu. Urządzenie USB zawiera złośliwe oprogramowanie,

które może działać automatycznie lub przy interakcji użytkownika. Złośliwe oprogramowanie modyfikuje i usuwa pliki użytkownika, usuwa tekst z plików tekstowych i całkowicie usuwa wszelkie znalezione pliki multimedialne. Oprogramowanie nie oferuje mechanizmu odzyskiwania, jak to może być w przypadku oprogramowania wymuszającego okup, dążąc jedynie do uszkodzenia plików.

5.3.2.2 Rozwiązanie

Kompilacja udostępnia kilka mechanizmów do wykrywania i ograniczania tego przypadku użycia.

Zdolność **monitorowania integralności** zapewnia możliwość wykrycia zmian w systemie plików, umożliwiając wykrywanie i rejestrowanie zmian i usunięć. Ponadto w dziennikach znajdują się informacje o tym, jaki to program (a co za tym idzie, gdzie program się znajdował – czyli na dysku USB).

Zdolność **rejestrowania** służy do zbierania logów z monitorowania integralności i wykorzystania w przyszłości, a także z dzienników zdarzeń systemu Windows w celu monitorowania użycia dysków zewnętrznych w porównaniu z normalnym użyciem.

Zdolność **wykrywania zdarzeń** zapewnia możliwość wykrywania złośliwego oprogramowania na urządzeniu USB włożonym do systemu. Może również wykryć wykonanie tych plików.

Zdolność **ograniczania i powstrzymywania rozprzestrzeniania** zapewnia możliwość zatrzymania wykonywania złośliwych plików, a także usunięcia tych plików z dysku USB.

5.3.2.3 Pozostałe kwestie

Ataki z wykorzystaniem USB nie zawsze mają postać ukrytego złośliwego oprogramowania opartego na plikach. Ponieważ ataki USB umożliwiają bezpośrednie połączenie ze sprzętem systemu, mogą mieć na celu zniszczenie systemu za pomocą ataków elektrycznych lub polegać na podszywaniu się pod klawiaturę lub inne urządzenia by uniknąć wykrycia i uzyskać uprawnienia. Ataki te można lepiej ograniczyć dzięki skrupulatnej polityce bezpieczeństwa fizycznego i ograniczeniom dotyczącym typów dozwolonych podłączanych urządzeń. Zaawansowane ataki polegające na manipulacji sprzętem mogą być coraz trudniejsze do wykrycia po

podłączeniu do systemu. Rozwiązanie zapobiegawcze obejmujące kopie zapasowe, bezpieczeństwo fizyczne i edukację pracowników jest często bardziej skuteczne.

5.3.3. PRZYPADKOWE USUNIĘCIE MASZYNY WIRTUALNEJ ZA POMOCĄ SKRYPTU OBSŁUGI

5.3.3.1 Scenariusz

Poniższy scenariusz został zasymulowany w celu przetestowania ochrony architektury przed zdarzeniami związanymi z integralnością danych występującymi na maszynach wirtualnych.

Skrypt rutynowej obsługi w systemie powoduje błąd. Podczas operacji przenoszenia w systemie Hyper-V, skrypt usuwa ważną maszynę wirtualną (VM). Skrypt obsługi z błędem tego typu może być skutkiem ubocznym normalnego działania systemu lub błędem popełnionym przez pracownika organizacji. Przewiduje się, że kompilacja ograniczy szkody wyrządzone maszynom wirtualnym w takim incydencie.

5.3.3.2 Rozwiązanie

Kompilacja zapewnia kilka metod wykrywania i analizowania tego przypadku użycia. Błędy w kodzie niestandardowym są często trudne do wykrycia w czasie wykonywania, ponieważ są zwykle uruchamiane przez programy uprzywilejowane. Klasyfikowanie ich jako złośliwego oprogramowania lub nawet jako „niezamierzonych” zmian jest często niepożądane.

Zdolność **monitorowania integralności** zapewnia możliwość wykrywania zmian w konfiguracjach maszyn wirtualnych, umożliwiając wykrycie i zarejestrowanie usunięcia maszyny wirtualnej. Ponadto informacje o tym, jaki program (tj. skrypt rutynowej obsługi) są zawarte w dziennikach.

Zdolność **rejestrowania** zapewnia możliwość gromadzenia informacji o tych zdarzeniach na przyszłość

Zdolność **informatyki śledczej/analityki** zapewnia możliwość analizy zdarzeń po fakcie, aby umożliwić zespołowi ds. bezpieczeństwa zrozumienie wpływu, usunięcie błędu w skrypcie i zapewnienie informacji dla procesu przywracania.

5.3.3.3 Pozostałe kwestie

Takie rozwiązanie pomoże zidentyfikować skrypt wywołujący zmianę lub usunięcie konfiguracji, ale ostatecznie niektórych rzeczy nie można za jego pomocą zautomatyzować. Zrozumienie wpływu zdarzenia wymaga pracy zespołu ds. bezpieczeństwa, a kompilacja ma na celu zapewnienie narzędzi dla zespołu ds. bezpieczeństwa.

Rozwiązanie błędu w skrypcie obsługi będzie również zwykle wymagało zaangażowania ze strony administratorów systemu. Ocena, czy skrypt powinien zostać usunięty, wyłączony lub pozostawiony uruchomiony podczas procesu naprawy, jest konieczna i może zależeć od rozmiaru skryptu, zasobów, których dotyczy problem, oraz dostępności zasobów, które można przeznaczyć na rozwiązanie błędu. Z tych względów, to organizacja musi zdecydować, czy nieprawidłowo działający skrypt powinien być traktowany jak złośliwe oprogramowanie (zobacz inne scenariusze dotyczące złośliwego oprogramowania), czy też jako skrypt organizacji, ponieważ proces naprawy może być długotrwały i wykracza poza zakres kategorii Wykryj/Reaguj ujęty w Ramach cyberbezpieczeństwa NIST.

5.3.4. TWORZENIE BACKDOORA POPRZEZ WEKTOR E-MAIL

5.3.4.1 Scenariusz

Poniższy scenariusz został zasymulowany w celu przetestowania ochrony architektury przed złośliwymi załącznikami do wiadomości e-mail.

Użytkownik nieświadomie otwiera złośliwy załącznik otrzymany w wiadomości e-mail. Po otwarciu, załącznik niepostrzeżenie pobiera pliki z zewnętrznego serwera Web. Następnie tworzy kilka niezatwierdzonych kont backdoorowych na serwerze uwierzytelniającym. Oczekuje się, że kompilacja ograniczy skutki takiego incydentu.

5.3.4.2 Rozwiązanie

Kompilacja zapewnia kilka warstw obrony wobec tego przypadku użycia. Funkcja **monitorowania integralności** przesyła dzienniki zmian plików i zmian w Active Directory do zdolności rejestrowania, umożliwiając rejestrowanie i wykrywanie zarówno pobierania złośliwego załącznika, jak i zmian w strukturze kont systemu.

Zdolności **rejestrowania i raportowania** umożliwiają generowanie na podstawie zdarzeń alertów umożliwiając zespołowi ds. bezpieczeństwa szybkie podjęcie działań w celu ich rozwiązania.

Zdolność **wykrywania zdarzeń** umożliwia wykrywanie w dwóch punktach czasowych — zarówno przed dotarciem załącznika do skrzynki odbiorczej użytkownika oraz, w razie niepowodzenia, po pobraniu załącznika do systemu.

Zdolność **ograniczania i powstrzymywania rozprzestrzeniania** zapewnia ograniczanie przed dotarciem załącznika do skrzynki odbiorczej użytkownika, jak również wtedy, gdy znajduje się on w systemie użytkownika.

Zdolność **informatyki śledczej/analityki** umożliwia wyświetlanie ruchu sieciowego generowanego przez załącznik podczas pobierania złośliwych plików z serwera WWW. Może to informować obronę organizacji w kategorii „Chroń” Ram cyberbezpieczeństwa, zanim podobne zdarzenia wydarzą się w przyszłości.

5.3.4.3 Pozostałe kwestie

Innym środkiem obrony, który może częściowo zapobiegać temu przypadkowi użycia jest wykrycie e-maila jako spamu. Ponieważ jednak często jest to funkcja dostawcy poczty e-mail, a nie odrębne rozwiązanie zabezpieczające, nie jest ono dostępne dla tej kompilacji.

Kompilacja sugeruje szczególnie użycie zdolności informatyki śledczej/analityki do informowania i wzmacniania obrony organizacji przed przyszłymi atakami. Jest to funkcja kategorii „Reaguj” — uczenie się czerpiąc wnioski z ataków może stanowić podstawę obrony przed takimi atakami w przyszłości, zarówno w fazach ataku „Chroń”, jak i „Wykrywaj”.

5.3.5. MODYFIKACJA BAZY DANYCH POPRZEZ ZŁOŚLIWEGO INSIDERA

5.3.5.1 Scenariusz

Poniższy scenariusz został zasymulowany w celu przetestowania ochrony architektury przed niepożądaną modyfikacją bazy danych.

Złośliwy insider ma dostęp do bazy danych organizacji za pośrednictwem Web. Insider wykorzystuje podatność na stronie Web w celu usunięcia dużej części bazy danych.

Choć scenariusz ten dotyczy podatności Web, do niepożądanego modyfikowania bazy danych mogą zostać wykorzystane też inne podatności. Oczekuje się, że kompilacja ograniczy wpływ, jaki użytkownik może mieć na bazę danych

5.3.5.2 Rozwiązanie

Kompilacja zapewnia kilka warstw obrony wobec tego przypadku użycia. Zdolność **monitorowania integralności** służy do wykrywania zmian w bazie danych.

Zmiany te są przekazywane do zdolności **rejestrowania**, która zbiera również informacje o żądaniach Web.

Zdolność **raportowania** umożliwia generowanie alertów i szybkie informowanie zespołu ds. bezpieczeństwa o anomaliach w oparciu o logi.

Zdolność **informatyki śledczej/analityki** jest użyta do badania złośliwego dostępu oraz identyfikowania strony z podatnością na zagrożenia. Ponieważ podatność ta jest podatnością w kodzie niestandardowym, ważne jest, aby wprowadzono mechanizmy gromadzenia informacji dla zapewnienia wystarczających informacji do usunięcia tej podatności.

5.3.5.3 Pozostałe kwestie

Ten przypadek użycia podkreśla potrzebę kompilacji zorientowanej na reagowanie, aby współpracować z kompilacją zorientowaną na identyfikację. Identyfikacja i usuwanie podatności w niestandardowym kodzie są czasami możliwe tylko poprzez zbieranie informacji dopiero po wykorzystaniu podatności. Kompilacja dostarcza mechanizmów do zbierania takich informacji, ale ostatecznie to do zespołu ds. bezpieczeństwa należy usunięcie podatności i wyciągnięcie wniosków z ataku.

5.3.6. MODYFIKACJA PLIKÓW POPRZEZ ZŁOŚLIWEGO INSIDERA

5.3.6.1 Scenariusz

W celu przetestowania obrony architektury przed złośliwą modyfikacją plików i kopii zapasowych zasymulowano następujący scenariusz.

Zakłada się, że złośliwy insider wykradł w sposób nietechniczny dane uwierzytelniające na poziomie administratora. Stosując te poświadczenia, wykorzystuje zdalne sesje Windows PowerShell do jednolitej modyfikacji na korzyść

pracowników informacji o akcjach pracowniczych znajdujących się na kilku maszynach. Celem tego ataku jest również system kopii zapasowych organizacji, aby zmodyfikować wszystkie zapisy poprzednich informacji o akcjach. Oczekuje się, że opisane powyżej aspekty kompilacji ograniczą możliwości użytkownika w zakresie namierzania i modyfikowania danych organizacji oraz kopii zapasowych. Metoda zabezpieczania poświadczeń administratora została uznana za wykraczającą poza zakres tego rozwiązania.

5.3.6.2 Rozwiązanie

Kompilacja zapewnia kilka warstw obrony wobec tego przypadku użycia. Zdolność **monitorowania integralności** wykrywa zmiany w plikach i kopiach zapasowych spowodowane przez złośliwego insidera.

Po przekazaniu do zdolności **rejestrowania i raportowania**, kompilacja może informować o tych zmianach. Nieprawidłowości lub różnice w stosunku do normalnego harmonogramu tworzenia kopii zapasowych są ważnymi wskaźnikami naruszenia zasad ochrony (kompromitacji danych).

Gdy zespół ds. bezpieczeństwa zostanie powiadomiony o złośliwym insiderze, może użyć zdolności **ograniczania i powstrzymywania rozprzestrzeniania**, aby uniemożliwić mu dostęp.

5.3.6.3 Pozostałe kwestie

Złośliwi insiderzy są groźnymi przeciwnikami, ponieważ mają już pewien poziom dostępu do systemu. Istnienie złośliwych insiderów poszerza obszar zagrożeń organizacji i wymaga obrony zarówno przed wewnętrznymi jak i zewnętrznymi maszynami. Z tego powodu kompilacja zawiera środki ograniczenia przed zagrożeniami już obecnymi wewnątrz organizacji, a nie tylko zagrożeniami pochodzącymi z zewnątrz. Obejmuje to możliwość wyłączania kont użytkowników, poddawania maszyn kwarantannie i monitorowania ruchu sieciowego pochodzącego z organizacji.

5.3.7. TWORZENIE BACKDOORA PRZEZ ZAATAKOWANY SERWER AKTUALIZACJI

5.3.7.1 Scenariusz

Poniższy scenariusz został zasymulowany w celu przetestowania ochrony architektury przed skompromitowanymi serwerami aktualizacji.

Serwer aktualizacji, który obsługuje maszynę organizacji został zaatakowany i dostarcza maszynie organizacji aktualizację zawierającą backdoora. Aktualizacja zawiera podatną wersję *vsftpd*, co pozwala atakującemu na uzyskanie dostępu na poziomie root do maszyny aktualizowanej przez zaatakowany serwer. Oczekuje się, że kompilacja ograniczy wpływ zaatakowanego serwera aktualizacji.

5.3.7.2 Rozwiązanie

Kompilacja posiada kilka warstw obrony wobec tego rodzaju przypadku użycia **Monitorowanie integralności** wykrywa zmiany w programach, dostarczając informacji o tym jak i kiedy program został zmieniony. Wykrywa również zmiany w plikach dokonane przez intruza.

Zdolność **wykrywania zdarzeń** jest wykorzystywana do wykrywania złośliwych aktualizacji poprzez wykrywanie sygnatur. Ponadto, wykrywa ona połączenie z otwartym portem dokonane przez atakującego.

Zdolność **ograniczania i powstrzymywania rozprzestrzeniania** jest używana do usunięcia/objęcia kwarantanną złośliwej aktualizacji, zatrzymując dostępność portu. Może być również użyta do poddania kwarantannie maszyny z sieci, aby zapobiec rozprzestrzenianiu się włamania i usunąć dostęp atakującego.

5.3.7.3 Pozostałe kwestie

Wykorzystanie zdolności wykrywania zdarzeń do wykrywania zakłada w dużej mierze, że aktualizacja została zgłoszona jako podatna na atak albo poprzez dobrze znaną historię podatności, albo poprzez kanały wymiany informacji. W niektórych przypadkach nowych ataków niestandardowych, zdolność wykrywania zdarzeń nie byłaby w stanie tego wykryć od razu. Jednak kompilacja zapewnia inne narzędzia, jak np. monitorowanie aktywności sieciowej, które mogą ostrzegać pracowników ds. bezpieczeństwa przed takimi atakami.

Użycie kompilacji identyfikującej i chroniącej integralność danych wraz z umieszczaniem na liście zakazanych i ochroną sieciową jako elementu obrony jest korzystne, ponieważ przypadek użycia, który wymaga połączenia z nieużywanym portem, zostałby całkowicie odrzucony przez listę zatwierdzonych portów.

6. ROZWAŻANIA DOTYCZĄCE PRZYSZŁYCH ROZWIĄZAŃ

NCCoE opracowuje ogólny przewodnik łączący architektury różnych projektów dot. integralności danych: Identyfikuj, Chroń, Wykrywaj, Reaguj i Odzyskuj. Architektury te mają pewne wspólne cechy, takie jak monitorowanie integralności, a także pewne potencjalne integracje i cykle, które nie mogły być wyrażone w tylko jednym z przewodników metodycznych. Różne funkcje Ram Cyberbezpieczeństwa mają na celu przygotowanie i informowanie się nawzajem, a przewodnik ogólny zajmuje się tymi kwestiami.

NCCoE rozważa również dodatkowe projekty bezpieczeństwa danych, które mapują do zasadniczych funkcji Ram Cyberbezpieczeństwa: Identyfikuj, Chroń, Wykrywaj, Reaguj i Odzyskuj. Projekty te będą koncentrować się na poufności danych — ochronie systemów organizacji przed atakami, które mogłyby naruszyć poufność danych.

ZAŁĄCZNIK A LISTA AKRONIMÓW

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

Akronim	Terminologia angielska	Terminologia polska
AMP	Advanced Malware Protection	Zaawansowana ochrona przed oprogramowaniem złośliwym
ATP	Advanced Threat Protection	Zaawansowana ochrona przed zagrożeniami
COI	Community of Interest	Wspólnota interesów
DE	Detect	Wykrywaj
DI	Data Integrity	Integralność danych
DSP	Directory Services Protector	Ochrona usług katalogowych
ESM	Enterprise Security Manager	Manager bezpieczeństwa organizacji
ICA	Information Centric Analytics	Analityka ukierunkowana na informacje
ISE	Identity Services Engine	Silnik usług tożsamościowych
IT	Information Technology	Technologia informacyjna
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission	Międzynarodowa Organizacja Normalizacyjna/Międzynarodowa Komisja Elektrotechniczna
NCCoE	National Cybersecurity Center of Excellence	Narodowe Centrum Doskonałości Cyberbezpieczeństwa
NIST	National Institute of Standards and Technology	Narodowy Instytut Standardów i Technologii
NISTIR	NIST Interagency or Internal Report	Międzyagencyjny lub wewnętrzny raport NIST
PR	Protect	Chroń
RMF	Risk Management Framework	Ramy zarządzania ryzykiem
RS	Respond	Reaguj

Akronim	Terminologia angielska	Terminologia polska
SP	Special Publication	Publikacja specjalna
USB	Universal Serial Bus	Uniwersalna magistrala szeregowa
VM	Virtual Machine	Maszyna wirtualna
vsftpd	Very Secure File Transfer Protocol Daemon	Serwer FTP dla systemów uniksowych, w tym Linuxa

ZAŁĄCZNIK B SŁOWNIK

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

Akronim	Terminologia angielska	Terminologia polska
Architektura	**Architecture**	Wysoce ustrukturyzowana specyfikacja akceptowalnego podejścia w ramach rozwiązania określonego problemu. Architektura zawiera opisy wszystkich komponentów wybranego, akceptowalnego rozwiązania, pozwalając jednocześnie na zmienność pewnych szczegółów poszczególnych komponentów w celu spełnienia powiązanych ograniczeń (np. koszty, środowisko lokalne, akceptowalność dla użytkownika). Źródło: FIPS 201-2
Audyt	**Audit**	Niezależny przegląd i badanie zapisów i działań w celu oceny adekwatności środków bezpieczeństwa i zapewnienia zgodności z ustalonymi politykami i procedurami operacyjnymi Źródło: CNSSI 4009-2015
Backdoor /tylna furtka	**Backdoor**	Nieudokumentowany sposób uzyskania dostępu do systemu komputerowego. Backdoor stanowi potencjalne zagrożenie bezpieczeństwa. Źródło: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 2
Bezpieczeństwo informacji	**Information Security**	Ochrona informacji i systemów informacyjnych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, uszkodzeniem, modyfikacją i zniszczeniem, w celu zapewnienia poufności, integralności i dostępności. Źródło: FIPS 199 (44 U.S.C., Sec. 3542)

Akronim	Terminologia angielska	Terminologia polska
Ciągłe monitorowanie	**Continuous Monitoring**	Utrzymywanie stałej świadomości w celu wspierania decyzji organizacji dotyczących ryzyka. Źródło: NIST SP 800-137
Cyberbezpieczeństwo	**Cybersecurity**	Zapobieganie naruszeniom, ochrona i odtwarzanie systemów komputerowych, systemów łączności elektronicznej, usług łączności elektronicznej, łączności przewodowej i łączności elektronicznej, w tym informacji w nich zawartych, w celu zapewnienia ich dostępności, integralności, uwierzytelniania, poufności i niezaprzeczalności. Źródło: CNSSI 4009-2015 (NSPD-54/HSPD-23)
Dane	**Data**	Podzbiór informacji w formacie elektronicznym, który umożliwia ich pobieranie lub przesyłanie. Źródło: CNSSI-4009
Dziennik	**Log**	Zapis zdarzeń zachodzących w systemach i sieciach organizacji. Źródło: NIST SP 800-92
Insider	**Insider**	Podmiot znajdujący się w obwodzie zabezpieczeń, który jest upoważniony do dostępu do zasobów systemowych, ale używa ich w sposób niezatwierdzony przez osoby, które udzieliły autoryzacji. Źródło: NIST SP 800-82 Rev. 2 (RFC 4949)
Integralność danych	**Data Integrity**	Właściwość polegająca na tym, że dane nie zostały zmienione, zniszczone lub utracone w sposób nieautoryzowany lub przypadkowy. Źródło: CNSSI-4009

Akronim	Terminologia angielska	Terminologia polska
Kerberos	**Kerberos**	System uwierzytelniania opracowany w Massachusetts Institute of Technology (MIT). Kerberos został zaprojektowany dla umożliwienia dwóm stronom wymiany informacji prywatnych w sieci publicznej. Źródło: NIST SP 800-47
Kontrola dostępu	**Access Control**	Proces uznawania lub odrzucania konkretnych wniosków o: 1) uzyskanie i korzystanie z informacji i związanych z nimi usług przetwarzania informacji; 2) wejście do konkretnych obiektów fizycznych (np. budynków specjalnych, obiektów wojskowych, przejść granicznych) Źródło: Federal Information Processing Standard (FIPS) 201; CNSSI-4009
Kopia zapasowa	**Backup**	Kopia plików i programów sporządzona w celu ułatwienia odzyskiwania w razie potrzeby. Źródło: NIST SP 800-34 Rev. 1
Maszyna wirtualna	**Virtual Machine**	Oprogramowanie, które pozwala pojedynczemu hostowi uruchomić jeden lub więcej systemów operacyjnych gości. Źródło: NIST SP 800-115
Naruszenie zasad ochrony **(Kompromitacja)**	**Compromise**	Ujawnienie informacji osobom nieuprawnionym lub naruszenie polityki bezpieczeństwa systemu, w którym mogło dojść do nieuprawnionego, celowego lub niezamierzonego ujawnienia, modyfikacji, zniszczenia lub utraty obiektu. Źródło: NIST SP 800-32

Akronim	Terminologia angielska	Terminologia polska
Oprogramowanie złośliwe	**Malware**	Program wprowadzony do systemu, zazwyczaj potajemnie, z zamiarem naruszenia poufności, integralności lub dostępności danych, aplikacji lub systemu operacyjnego ofiary. Źródło: NIST SP 800-111
Podatność	**Vulnerability**	Słabość systemu informacyjnego, procedur bezpieczeństwa systemu, wewnętrznych zabezpieczeń lub implementacji, która może zostać wykorzystana lub wywołana przez źródło zagrożenia. Źródło: FIPS 200 (zaadaptowane z CNSSI 4009)
Prywatność	**Privacy**	Zapewnienie, że poufność i dostęp do niektórych informacji o podmiocie są chronione. Źródło: NIST SP 800-130
Ramy zarządzania ryzykiem	**Risk Management**	Zapewniają zdyscyplinowany i ustrukturyzowany proces, który integruje bezpieczeństwo informacji i działania dot. zarządzania ryzykiem z cyklem życia systemu. Źródło: NIST SP 800-82 Rev. 2 (NIST SP 800-37)
Ryzyko	**Risk**	Poziom wpływu na działania organizacji (w tym misję, funkcje, wizerunek lub reputację), aktywa organizacji lub osoby fizyczne, wynikający z działania systemu informacyjnego, biorąc pod uwagę potencjalny wpływ zagrożenia i prawdopodobieństwo wystąpienia tego zagrożenia. Źródło: FIPS 200

Akronim	Terminologia angielska	Terminologia polska
Ryzyko bezpieczeństwa informacji	**Information Security Risk**	Ryzyko dla operacji organizacyjnych (w tym misji, funkcji, wizerunku, reputacji), aktywów organizacyjnych, osób, innych organizacji i państwa ze względu na możliwość nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji i/lub systemów. Źródło: CNSSI 4009-2015 (NIST SP 800-30 Rev. 1)
System informacyjny	**Information System**	Dyskretny zbiór zasobów informacyjnych zorganizowanych w celu gromadzenia, przetwarzania, utrzymywania, używania, udostępniania, rozpowszechniania lub dysponowania informacjami. Źródło: FIPS 200 (44 U.S.C., Sec. 3502)
Szacowanie ryzyka	**Risk Assessment**	Proces identyfikacji zagrożeń dla bezpieczeństwa systemu i określania prawdopodobieństwa ich wystąpienia, wynikającego z nich wpływu oraz dodatkowych zabezpieczeń, które mogłyby ograniczyć ten wpływ. Stanowi element zarządzania ryzykiem i jest synonimem analizy ryzyka. Źródło: NIST SP 800-63-2
Środek bezpieczeństwa (Zabezpieczenie)	**Security Control**	Środek ochrony systemu. Źródło: NIST SP 800-123

ZAŁĄCZNIK C REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[11]	
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 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18
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

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

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[11]	
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
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 800-82	Przewodnik w zakresie bezpieczeństwa systemów sterowania przemysłowego– na podstawie NIST SP 800-82

PUBLIKACJE ANGLOJĘZYCZNE[12]

[1]	A. Sedgewick, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, National Institute of Standards and Technology, Gaithersburg, Maryland, Apr. 2018, 55 pp. Dostępne na: https://www.nist.gov/cyberframework/framework.
[2]	L. Kauffman, N. Lesser and B. Abe, *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy*, NISTIR 8050, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2015, 155 pp. Dostępne na: https://nccoe.nist.gov/sites/default/files/library/nistir-8050-draft.pdf
[3]	G. Stoneburner, *et al*., *Guide for Conducting Risk Assessments*, NIST Special Publication (SP), 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95 pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-30r1.
[4]	R. Ross, *et al*., *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST Special Publication (SP) 800-37, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010, 101pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-37r1.
[5]	R. Ross *et al*., *Managing Information Security Risk*, NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, 87pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-39.
[6]	M. Souppaya *et al*., *Guide to Enterprise Patch Management Technologies*, NIST Special Publication (SP) 800-40 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 25pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800- 40r3.
[7]	R. Ross *et al*., *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013, 461pp. Dostępne na: https://doi.org/10.6028/NIST.SP.800- 534.

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

[8] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-3, Mar. 2019, 65pp. Dostępne na: https://csrc.nist.gov/publications/detail/fips/140/3/final.

[9] K. Kent *et al.*, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication (SP) 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2006, 121pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-86.

[10] K. Kent and M. Souppaya, *Guide to Computer Security Log Management*, NIST Special Publication (SP) 800-92, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2006, 72pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-92.

[11] P. Bowen *et al.*, *Information Security Handbook: A Guide for Managers*, NIST Special Publication (SP) 800-100, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2006, 178pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-100.

[12] M. Swanson *et al.*, *Contingency Planning Guide for Federal Information Systems*, NIST Special Publication (SP) 800-34 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2010, 148pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800- 34r1.

[13] Office of Management and Budget (OMB), *Management of Federal Information Resources*, OMB Circular No. A-130, November 2000. Dostępne na: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[14] M. Souppaya *et al.*, *Guide to Enterprise Patch Management Technologies*, NIST Special Publication (SP) 800-61 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2012, 25pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[15] M. Souppaya and K. Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, NIST Special Publication (SP) 800-83 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013, 46pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-83r1.

[16] C. Johnson *et al.*, *Guide to Cyber Threat Information Sharing*, NIST Special Publication (SP) 800-150, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2016, 42pp. Dostępne na: http://dx.doi.org/10.6028/NIST.SP.800-150.

[17] M. Bartock *et al.*, *Guide for Cybersecurity Event Recovery*, NIST Special Publication (SP) 800-184, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2016, 52pp. http://dx.doi.org/10.6028/NIST.SP.800-184.

ZAŁĄCZNIK D OCENA FUNKCJONALNA

Przeprowadzono funkcjonalną ocenę przykładowej implementacji integralności danych (DI), skonstruowanej w laboratorium, w celu sprawdzenia, czy spełnia ona swój cel wykrywania zdarzeń DI i reagowania na nie. Ponadto projekt ten ma na celu analizę wydarzeń mających pomóc w odzyskaniu i ochronie organizacji przed przyszłymi atakami. W ocenie potwierdzono, że przykładowa implementacja może spełniać następujące funkcje:

- Wykrywanie złośliwego działania w sieci, złośliwego kodu mobilnego, wykonania kodu złośliwego i nieautoryzowanego zachowania użytkownika.
- Powstrzymywanie i analizowanie tego typu zdarzeń.
- Ograniczanie skutków tych zdarzeń w miarę ich występowania.
- Zgłaszanie odpowiednich szczegółów do wykorzystania przy ograniczaniu i ochronie przed przyszłymi zdarzeniami.

Dział D.1 opisuje format i składniki przypadków testów funkcjonalnych. Każdy przypadek testu funkcjonalnego ma na celu ocenę zdolności przykładowej implementacji do wykonywania funkcji wymienionych powyżej i wyszczególnionych w Dziale D.1.

D.1 PLAN TESTÓW FUNKCJONALNYCH INTEGRALNOŚCI DANYCH

Jeden z aspektów oceny bezpieczeństwa obejmował sprawdzenie, w jakim stopniu wzór referencyjny odnosi się do charakterystyki bezpieczeństwa, jaką miał wspierać. Podkategorie Ram Cyberbezpieczeństwa zostały użyte do zapewnienia struktury oceniania bezpieczeństwa poprzez zapoznanie się z określonymi działami każdego standardu cytowanego w odniesieniu do tej podkategorii. Cytowane działy zawierają punkty walidacyjne, których oczekuje się od przykładowego rozwiązania. Wykorzystanie podkategorii Ram Cyberbezpieczeństwa jako podstawy zorganizowania analizy pozwoliło na systematyczne rozważenie, w jakim stopniu wzór referencyjny wspiera zamierzoną charakterystykę bezpieczeństwa.

Plan ten obejmuje przypadki testowe niezbędne do przeprowadzenia oceny funkcjonalnej implementacji przykładowej DI, która jest obecnie wdrażana w laboratorium w National Cybersecurity Center of Excellence.

Testowane wdrożenie opisano w Rozdziale 4.

Każdy przypadek testowy składa się z wielu obszarów, które łącznie określają cel testu, specyfikę wymaganą do wykonania testu oraz sposób oceny jego wyników. Tabela 6-1 opisuje każdy obszar przypadku testowego.

Tabela 0-3 Obszary przypadku testowego

Obszar przypadku testowego	Opis
Wymaganie nadrzędne	Określa wymaganie najwyższego rzędu lub szereg wymagań najwyższego rzędu prowadzących do wymogu podlegającego badaniu.
Wymóg podlegający badaniu	Określa definicję pozostałej części obszarów przypadków testowych. Wskazuje zdolność podlegającą ocenie.
Opis	Opisuje cel przypadku testowego.
Powiązane podkategorie Ram cyberbezpieczeństwa	Wymienia środki bezpieczeństwa wg NSC 800-53. którymi zajmuje się przypadek testowy.
Warunki wstępne	Stan początkowy przypadku testowego. Warunki wstępne wskazują różne elementy stanu początkowego, takie jak wymagana konkretna konfiguracja zdolności czy konkretny protokół i treść.
Procedura	Szereg następujących po sobie czynności wymaganych do wdrożenia przypadku testowego. Procedura może składać się z pojedynczej sekwencji czynności lub wielu sekwencji czynności (z rozgraniczeniem) wskazujących na wariantowość procedury testowej.
Oczekiwane wyniki	Oczekiwane wyniki dla każdego wariantu procedury testowej.
Rzeczywiste wyniki	Wyniki zaobserwowane.

Obszar przypadku testowego	Opis
Wynik ogólny	Ogólny wynik testu jako zaliczony/niezaliczony. W niektórych przypadkach testowych określenie ogólnego wyniku może być bardziej złożone, na przykład określenie zaliczony/ niezaliczony na podstawie odsetka zidentyfikowanych błędów.

D.2 WYMAGANIA PRZYPADKU ZASTOSOWANIA INTEGRALNOŚCI DANYCH

Tabela 6-2 określa wymagania funkcjonalne DI, o których mówi plan testu i związane z nim przypadki testowe.

Tabela 0-4 Wymagania dotyczące zdolności

ID[13] CR[14]	Wymaganie nadrzędne	Wymaganie podrzędne 1	Przypadek testowy
CR 1	Przykładowa implementacja DI ma wykrywać i reagować na złośliwe oprogramowanie, które szyfruje pliki i wyświetla komunikat z żądaniem zapłaty.		Data Integrity DR[15]-1
CR 1.a		Zmiany integralności plików są gromadzone i rejestrowane.	Data Integrity DR-1
CR 1.b		Dostęp jest wstrzymany.	Data Integrity DR-1
CR 1.c		Plik wykonywalny jest identyfikowany jako szkodliwy przy użyciu listy	Data Integrity DR-1

[13] Numer CR.

[14] Wymagania dotyczącego zdolności *(ang. CR - Capability Requirements).*

[15] Wykrywaj i reaguj – (*ang. Detecting and Responding - DR*).

ID[13] CR[14]	Wymaganie nadrzędne	Wymaganie podrzędne 1	Przypadek testowy
		niedozwolonych elementów (*ang. denylist*).	
CR 1.d		Plik wykonywalny jest identyfikowany jako szkodliwy na podstawie analizy, a lista niedozwolonych elementów zostaje zaktualizowana.	Data Integrity DR-1
CR 1.e		Wykonanie zostało wstrzymane.	Data Integrity DR-1
CR 1.f		Pobrane pliki są identyfikowane jako szkodliwe za pomocą listy niedozwolonych elementów.	Data Integrity DR-1
CR 1.g		Pobrane pliki są identyfikowane jako szkodliwe na podstawie analizy, a lista niedozwolonych elementów jest aktualizowana.	Data Integrity DR-1
CR 1.h		Pobieranie niedozwolonych elementów jest zablokowane.	Data Integrity DR-1
CR 1.i		Wykrywane są próby propagacji.	Data Integrity DR-1
CR 1.j		Zablokowano możliwość propagacji w maszynach próbujących rozsyłać dane.	Data Integrity DR-1
CR 1.k		Wykryto podejrzany ruch sieciowy i zaktualizowano listę niedozwolonych elementów.	Data Integrity DR-1

ID[13] CR[14]	Wymaganie nadrzędne	Wymaganie podrzędne 1	Przypadek testowy
CR 2	Przykładowa implementacja DI ma wykrywać i reagować na złośliwe oprogramowanie wprowadzane poprzez Universal Serial Bus (USB), które modyfikuje i usuwa dane użytkownika.		Data Integrity DR-2
CR 2.a		Zmiany integralności plików są gromadzone i rejestrowane.	Data Integrity DR-2
CR 2.b		Dołączenie urządzenia USB zostaje wykryte i zarejestrowane.	Data Integrity DR-2
CR 2.c		Plik wykonywalny jest zidentyfikowany za pomocą listy niedozwolonych elementów jako złośliwy.	Data Integrity DR-2
CR 2.d		Plik wykonywalny jest zidentyfikowany jako złośliwy w wyniku analizy, a lista niedozwolonych elementów jest zaktualizowana.	Data Integrity DR-2
CR 2.e		Złośliwy plik wykonywalny zostaje zatrzymany lub usunięty.	Data Integrity DR-2
CR 3	Przykładowa implementacja DI ma wykrywać i reagować na usunięcie maszyny wirtualnej.		Data Integrity DR-3
CR 3.a		Zmiany w integralności maszyny wirtualnej są gromadzone i rejestrowane.	Data Integrity DR-3

ID[13] CR[14]	Wymaganie nadrzędne	Wymaganie podrzędne 1	Przypadek testowy
CR 3.b		Zdarzenie powodujące usunięcie maszyny wirtualnej jest analizowane.	Data Integrity DR-3
CR 4	Przykładowa implementacja DI ma wykrywać i reagować na złośliwe oprogramowanie otrzymane za pośrednictwem phishingowej wiadomości e-mail.		Data Integrity DR-4
CR 4.a		Zmiany integralności konfiguracji są gromadzone i rejestrowane.	Data Integrity DR-4
CR 4.b		Wiadomość e-mail jest zidentyfikowana jako złośliwa przy użyciu listy niedozwolonych elementów.	Data Integrity DR-4
CR 4.c		Wiadomość e-mail jest zidentyfikowana w wyniku analizy jako złośliwa, a lista niedozwolonych elementów jest zaktualizowana.	Data Integrity DR-4
CR 4.d		Wiadomości e-mail są usuwane lub wrzucane do spamu.	Data Integrity DR-4
CR 4.e		Załącznik jest zidentyfikowany jako złośliwy za pomocą listy niedozwolonych elementów.	Data Integrity DR-4
CR 4.f		Załącznik jest identyfikowany jako złośliwy na podstawie analizy, a lista niedozwolonych elementów jest aktualizowana.	Data Integrity DR-4

ID[13] CR[14]	Wymaganie nadrzędne	Wymaganie podrzędne 1	Przypadek testowy
CR 4.g		Wykonywanie arkusza kalkulacyjnego zostaje zatrzymane, a lista niedozwolonych elementów jest aktualizowana w razie potrzeby.	Data Integrity DR-4
CR 4.h		Pliki do pobrania są identyfikowane jako złośliwe przy użyciu listy niedozwolonych elementów.	Data Integrity DR-4
CR 4.i		Pobrane pliki są identyfikowane na podstawie analizy jako złośliwe, a lista niedozwolonych elementów jest aktualizowana.	Data Integrity DR-4
CR 4.j		Złośliwy plik wykonywalny zostaje zatrzymany lub usunięty.	Data Integrity DR-4
CR 4.k		Wykryto podejrzany ruch sieciowy i zaktualizowano listę niedozwolonych elementów.	Data Integrity DR-4
CR 5	Przykładowa implementacja DI ma wykrywać i reagować na zmiany w bazie danych wprowadzone przez podatność serwera WWW w niestandardowym kodzie.		Data Integrity DR-5
CR 5.a		Zmiany integralności bazy danych są gromadzone i rejestrowane.	Data Integrity DR-5
CR 5.b		Informacje o interakcji klienta z usługa internetową są gromadzone i rejestrowane.	Data Integrity DR-5

ID[13] CR[14]	Wymaganie nadrzędne	Wymaganie podrzędne 1	Przypadek testowy
CR 5.c		Informacje pochodzące z ataku są zgłaszane celem wykorzystania w procesie ochrony przed przyszłymi zdarzeniami.	Data Integrity DR-5
CR 6	Przykładowa implementacja DI ma wykrywać i reagować na ukierunkowane modyfikacje dokonywane przez złośliwych insiderów z podwyższonymi uprawnieniami.		Data Integrity DR-6
CR 6.a		Zmiany w integralności plików są gromadzone i rejestrowane.	Data Integrity DR-6
CR 6.b		Zmiany w integralności kopii zapasowej są gromadzone i rejestrowane.	Data Integrity DR-6
CR 6.c		Wykryte zmiany są raportowane.	Data Integrity DR-6
CR 6.d		Skojarzone konta użytkowników są zamykane.	Data Integrity DR-6
CR 7	Przykładowa implementacja DI wykrywa włamanie dokonane za pośrednictwem zaatakowanego serwera aktualizacji i reaguje na nie.		Data Integrity DR-7
CR 7.a		Zmiany integralności programu są gromadzone i rejestrowane.	Data Integrity DR-7

ID[13] CR[14]	Wymaganie nadrzędne	Wymaganie podrzędne 1	Przypadek testowy
CR 7.b		Pobrana usługa jest zidentyfikowana jako złośliwa przy użyciu listy niedozwolonych elementów.	Data Integrity DR-7
CR 7.c		Pobrana usługa jest identyfikowana w drodze analizy jako szkodliwa, a lista niedozwolonych elementów jest aktualizowana.	Data Integrity DR-7
CR 7.d		Usługa zostaje zatrzymana i przywrócona lub usunięta.	Data Integrity DR-7
CR 7.e		Witryna pobierania jest tymczasowo dodana do listy niedozwolonych elementów.	Data Integrity DR-7
CR 7.f		Wykryty został port otwarty przez usługę.	Data Integrity DR-7
CR 7.g		Otwarty port zostaje zamknięty.	Data Integrity DR-7
CR 7.h		Wykryto włamanie do zainfekowanej maszyny.	Data Integrity DR-7
CR 7.i		Włamanie do zainfekowanej maszyny jest powstrzymane.	Data Integrity DR-7

D.3 PRZYPADEK TESTOWY: INTEGRALNOŚĆ DANYCH DR-1

Tabela 0-5 Identyfikator przypadku testowego Integralność danych DR-1

Wymaganie nadrzędne	(CR 1) Przykładowa implementacja DI ma wykrywać i reagować na złośliwe oprogramowanie, które szyfruje pliki i wyświetla komunikat z żądaniem zapłaty.
Wymaganie testowalne	(CR 1.a) Monitorowanie integralności, Rejestrowanie, Raportowanie; (CR 1.c, CR 1.d, CR 1.f, CR 1.g, CR 1.i) Wykrywanie zdarzeń; (CR 1.b, CR 1.e, CR 1.j) Ograniczanie i powstrzymywanie; (CR 1.h, CR 1.k) Informatyka śledcza i analityka
Opis	Wykazanie, że rozwiązanie DI ma możliwości wykrywania zachowań typowych dla oprogramowania wymuszającego okup i odpowiedniego ograniczania tych zachowań.
Powiązane podkategorie Ram cyberbezpieczeństwa	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2,DE.CM-4, DE.CM-7, DE.DP-2, DE.AE-1, DE.CM-1
Warunki wstępne	Użytkownik przechodzi do złośliwej witryny i klika na reklamę aplikacji do usuwania wirusów. Ta rzekoma aplikacja do usuwania wirusów stanowi oprogramowanie ransomware, które propaguje się w domenie i szyfruje pliki użytkownika.
Procedura	Zdolność **monitorowania integralności** jest użyta do monitorowania i rejestrowania zmian integralności plików. Zdolność **rejestrowania** i zdolność **raportowania** są użyte do powiadamiania zespołu ds. bezpieczeństwa o zmianach dotyczących integralności plików i o potencjalnie szkodliwych zdarzeniach. Zdolność **wykrywania zdarzeń** jest wykorzystywana do wykrywania oprogramowania wymuszającego okup w czasie rzeczywistym przed lub w trakcie wykonywania. Jest również

	używany do wykrywania propagacji oprogramowania wymuszającego okup. Zdolność **ograniczania i powstrzymywania** jest używana do zatrzymania wykonywania oprogramowania wymuszającego okup i usunięcia go z systemu. Jest również wykorzystywana do kwarantanny zainfekowanych maszyn po wykryciu naruszenia. Zdolność **informatyki śledczej/analityki** jest użyta do wykrywania złośliwych hostów i stron internetowych otwieranych przez oprogramowanie wymuszające okup.
Oczekiwane wyniki (do zaliczenia)	Kompilacja może monitorować i raportować zmiany integralności plików (CR 1.a). Maszyna jest poddawana kwarantannie w przypadku wykrycia złośliwego oprogramowania (CR 1.b). Złośliwe pliki wykonywalne są identyfikowane poprzez wykrywanie lub analizę sygnatur (CR 1.c, CR 1.d). Uniemożliwia się wykonywanie złośliwych plików wykonywalnych (CR 1.e). Złośliwe pobrania są zidentyfikowane poprzez wykrywanie lub analizę sygnatur (CR 1.f, CR 1.g). Zapobiega się złośliwemu pobieraniu (CR 1.h). Wykryto rozprzestrzenianie się złośliwych plików wykonywalnych (CR 1.i). Uniemożliwiono rozprzestrzenianie się złośliwych plików wykonywalnych (CR 1.j). Ruch sieciowy jest przechwytywany i analizowany pod kątem podejrzanej aktywności (CR 1.k).
Rzeczywiste wyniki	**Tripwire Enterprise (monitorowanie integralności)** służy do skutecznego wykrywania zmian w plikach w zaatakowanych systemach.

	ArcSight ESM (rejestrowanie) służy do rejestrowania zdarzeń związanych z wykrywaniem zdarzeń i monitorowaniem integralności do wykorzystania w raportowaniu i informatyce śledczej/analityce. **ArcSight ESM (raportowanie)** służy do skutecznego zgłaszania złośliwej aktywności wykrytej w dziennikach. **Cisco AMP (wykrywanie zdarzeń)** jest użyte do skutecznego wykrycia złośliwego pliku wykonywalnego. **Cisco AMP (ograniczanie i powstrzymywanie)** jest użyte do skutecznego usuwania złośliwych plików wykonywalnych z zaatakowanych systemów. **Cisco Stealthwatch (wykrywanie zdarzeń)** jest użyte do skutecznego przechwytywania złośliwego lub podejrzanego ruchu sieciowego z pliku wykonywalnego. **Cisco ISE (ograniczanie i powstrzymywanie)** jest z użyty do skutecznej kwarantanny zaatakowanych maszyn. **Symantec Security Analytics (informatyka śledcza/analityka)** jest z użyty do przeglądania ruchu sieciowego generowanego przez oprogramowanie wymuszające okup pod kątem potencjalnie złośliwych hostów i witryn internetowych. **Symantec ICA (informatyka śledcza/analityka)** wyświetla odpowiednie zdarzenia z ArcSight do analizy, aby pomóc w identyfikacji złośliwych plików do wykorzystania w wykrywaniu przyszłych zdarzeń, a także do usunięcie przez zespół ds. bezpieczeństwa.
Wynik ogólny	Zaliczono. Wszystkie wymagania dla tego przypadku użycia są spełnione.

D.4 PRZYPADEK TESTOWY: INTEGRALNOŚĆ DANYCH DR-2

Tabela 0-6 Identyfikator przypadku testowego Integralność danych DR-2

Wymaganie nadrzędne	(CR 2) Przykładowa implementacja DI ma wykrywać i reagować na złośliwe oprogramowanie wprowadzane poprzez Universal Serial Bus (USB), które modyfikuje i usuwa dane użytkownika.
Wymaganie testowalne	(CR 2.a) Monitorowanie integralności; (CR 2.b, CR 2.c) Wykrywanie zdarzeń; (CR 2.d) Informatyka śledcza i analityka; (CR 2.e) Ograniczanie i powstrzymywanie.
Opis	Wykazanie, że rozwiązanie DI umożliwia wykrywanie zachowania typowego dla destrukcyjnego oprogramowania złośliwego i może odpowiednio je ograniczać.
Powiązane podkategorie Ram cyberbezpieczeństwa	DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Warunki wstępne	Użytkownik dołącza niezidentyfikowany dysk USB do swojego komputera. Kliknięcie pliku na dysku powoduje natychmiastowe zniszczenie wszystkich plików znajdujących się na komputerze.
Procedura	Zdolność **monitorowania integralności** jest użyta do monitorowania zmian integralności systemu. Zdolność **rejestrowania** jest użyta do zbierania dzienników od zdolności monitorowania integralności. Zdolność **wykrywania zdarzeń** jest używana do wykrywania złośliwych plików na USB dołączonym do systemu. Zdolność **ograniczania i powstrzymywania** jest używana do zapobiegania wykonywaniu złośliwych plików.

Oczekiwane wyniki (do zaliczenia)	Kompilacja może monitorować i raportować zmiany integralności plików (CR 2.a). Kompilacja może wykrywać dołączenie USB (CR 2.b). Złośliwe pliki wykonywalne są identyfikowane poprzez wykrywanie lub analizę sygnatur (CR 2.c, CR 2.d). Uniemożliwiono wykonywanie złośliwych plików wykonywalnych (CR 2.e).
Rzeczywiste wyniki	**Tripwire Enterprise (monitorowanie integralności)** z powodzeniem wykrywa zmiany dokonane przez plik wykonywalny uruchomiony z USB. **ArcSight ESM (rejestrowanie)** z powodzeniem zbiera dzienniki od zdolności monitorowania integralności. Ponadto, przypadki dołączenia urządzenia USB mogą być zbierane z wykorzystaniem polityki grupy Windows. **Cisco AMP (wykrywanie zdarzeń)** z powodzeniem wykrywa złośliwe pliki na dysku USB. **Cisco AMP (ograniczanie i powstrzymywanie)** natychmiast usuwa złośliwe pliki w systemie, jeśli zostaną skopiowane. Zapobiega również wykonaniu, jeśli plik zostanie uruchomiony z dysku USB.
Wynik ogólny	Zaliczono (częściowo). Cisco AMP nie usuwa natychmiast pliku z dysku USB po jego podłączeniu, jeśli użytkownik nie przeprowadzi żadnej czynności (kopiowania lub wykonania). Ponieważ jednak obie te czynności wywołują usunięcie, nie jest to istotne niedociągnięcie, ponieważ plik jest poza tym nieszkodliwy.

D.5 PRZYPADEK TESTOWY: INTEGRALNOŚĆ DANYCH DR-3

Tabela 0-7 Identyfikator przypadku testowego: Integralność danych DR-3

Wymaganie nadrzędne	(CR 3) Przykładowa implementacja DI ma wykrywać i reagować na usunięcie maszyny wirtualnej.
Wymaganie testowalne	(CR 3.a) Monitorowanie integralności; (CR 3.b) Informatyka śledcza i analityka.
Opis	Wykazanie, że rozwiązanie DI może wykrywać i analizować zdarzenia w zakresie integralności danych dotyczące maszyn wirtualnych.
Powiązane podkategorie Ram cyberbezpieczeństwa	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Warunki wstępne	Skrypt rutynowej obsługi zawiera błąd, który przypadkowo usuwa maszynę wirtualną.
Procedura	Zdolność **monitorowania integralności** jest użyta do monitorowania zmian integralności systemu. Zdolność **rejestrowania** jest użyta do zbierania dzienników od zdolności monitorowania integralności. Zdolność informatyki **śledczej/analityki** stosowana jest do analizowania dzienników i określania przyczyn zdarzeń dot. integralności.
Oczekiwane wyniki (do zaliczenia)	Kompilacja może monitorować i raportować zmiany w integralności plików (CR 3.a). Kompilacja może analizować wpływ zdarzeń dot. integralności danych (CR 3.b).

Rzeczywiste wyniki	**Tripwire Enterprise (monitorowanie integralności)** **z** powodzeniem monitoruje i rejestruje zmiany w konfiguracji maszyn wirtualnych. **ArcSight ESM (rejestrowanie)** z powodzeniem zbiera dzienniki i raportuje zdarzenia generowane przez zdolność monitorowania integralności, umożliwiając szybszy czas reakcji. **Symantec ICA (informatyka śledcza/analityka)** **z** powodzeniem wyświetla odpowiednie zdarzenia z ArcSight do analizy, aby pomóc w identyfikacji pliku, który powoduje usunięcie.
Wynik ogólny	Zaliczono Wszystkie wymagania dla tego przypadku użycia są spełnione.

D.6 PRZYPADEK TESTOWY: INTEGRALNOŚĆ DANYCH DR-4

Tabela 0-8 Identyfikator przypadku testowego Integralność danych DR-4

Wymaganie nadrzędne	(CR 4) Przykładowa implementacja DI ma wykrywać i reagować na złośliwe oprogramowanie otrzymane w drodze phishingowej wiadomości e-mail.
Wymaganie testowalne	(CR 4.a) Monitorowanie integralności i Rejestrowanie; (CR 4.b, CR4.e, CR 4.h, CR 4.k) Wykrywanie zdarzeń; (CR 4.c, CR 4.f, CR 4.i) Informatyka śledcza i analityka; (CR 4.d, CR 4.g, CR 4.j) Ograniczanie i powstrzymywanie.
Opis	Wykazanie, że rozwiązanie DI może wykrywać i analizować złośliwe załączniki i reagować na złośliwe zmiany w konfiguracji.
Powiązane podkategorie Ram cyberbezpieczeństwa	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Warunki wstępne	Użytkownik otrzymuje phishingową wiadomość e-mail z załączonym złośliwym arkuszem kalkulacyjnym. Arkusz kalkulacyjny zostaje pobrany i otwarty, powodując zmiany kont w Active Directory.
Procedura	Zdolność **monitorowania integralności** zostaje użyta do wykrywania i rejestrowania tworzenie konta. Informacje te są przekazywane do zdolności **rejestrowania**, wraz z innymi dostępnymi informacjami usługi Active Directory. Załącznik wiadomości e-mail został wykryty jako złośliwy przez zdolność **wykrywania zdarzeń** i ograniczony przez zdolność **ograniczania i powstrzymywania**, zarówno gdy plik znajduje się w skrzynce odbiorczej, jak i gdy jest w systemie użytkownika. Rozwiązanie może dokonywać, z wykorzystaniem **informatyki śledczej/analityki**, przeglądu ruchu sieciowego generowanego

	przez plik, gdy ten wysyła do złośliwego serwera WWW żądanie pobrania plików.
Oczekiwane wyniki (do zaliczenia)	Kompilacja może monitorować i raportować zmiany integralności plików (CR 4.a). Złośliwe wiadomości e-mail są identyfikowane poprzez wykrywanie lub analizę sygnatur (CR 4. b, CR 4. c). Wiadomości e-mail zidentyfikowane jako złośliwe są umieszczane w spamie lub usuwane (CR 4.d). Złośliwe załączniki są identyfikowane poprzez wykrywanie lub analizę sygnatur (CR 4.e, CR 4.f). Uniemożliwia się wykonywanie złośliwych plików wykonywalnych (CR 4.g). Złośliwe pobrania są zidentyfikowane poprzez wykrywanie lub analizę sygnatur (CR 1.f, CR 1.g). Uniemożliwia się wykonywanie złośliwych plików wykonywalnych (CR 4.j). Ruch sieciowy jest przechwytywany i analizowany pod kątem podejrzanej aktywności (CR 4.k).

Rzeczywiste wyniki	**Semperis DSP (monitorowanie integralności) z** powodzeniem monitoruje i rejestruje zmiany w Active Directory. **ArcSight ESM (rejestrowanie)** z powodzeniem zbiera dzienniki i raportuje zdarzenia generowane przez zdolność monitorowania integralności, umożliwiając szybszy czas reakcji. **Glasswall FileTrust (wykrywanie zdarzeń) z** powodzeniem identyfikuje złośliwy załącznik przed dotarciem do skrzynki odbiorczej użytkownika. **Glasswall FileTrust (ograniczanie i powstrzymywanie)** z powodzeniem ogranicza złośliwy załącznik przed jego dotarciem do skrzynki odbiorczej użytkownika. Złośliwy plik zostaje pomyślnie załadowany do **Cisco AMP (wykrywanie zdarzeń)** w celu wykrywania sygnatur. **Cisco AMP (wykrywanie zdarzeń)** z powodzeniem ogranicza plik, gdy ten zostaje stwierdzony na stacjach roboczych użytkownika. **Symantec Security Analytics (Informatyka śledcza/analityka)** jest zastosowany do skutecznego wykrycia ruchu sieciowego związanego z pobieraniem plików ze złośliwego serwera.
Wynik ogólny	Zaliczono (częściowo). Wiadomości e-mail nie są umieszczane do spamie (CR 4.b-d); zamiast tego załącznik jest ograniczany przed dotarciem do skrzynki odbiorczej użytkownika. Umieszczanie wiadomości e-mail w spamie jest często funkcją infrastruktury e-mail.

D.7 PRZYPADEK TESTOWY INTEGRALNOŚĆ DANYCH DR-5

Tabela 0-9 Identyfikator przypadku testowego: Integralność danych DR-5

Wymaganie nadrzędne	Przykładowa implementacja DI ma wykrywać i reagować na zmiany w bazie danych wprowadzone przez podatność serwera Web w niestandardowym kodzie.
Wymaganie testowalne	(CR 5.a) Monitorowanie integralności; (CR 5.b) Rejestrowanie; (CR 5.c) Raportowanie.
Opis	Wykazanie, że rozwiązanie DI może wykrywać i reagować na wykorzystanie podatności w kodzie niestandardowym prowadzące do ataku na bazę danych.
Powiązane podkategorie Ram cyberbezpieczeństwa	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Warunki wstępne	Podatność w kodzie źródłowym strony Web zostaje odkryta przez złośliwego insidera. Insider wykorzystuje tę podatność do usunięcia znacznych części bazy danych.
Procedura	Zdolność **monitorowania integralności** zostaje użyta do wykrywania zmian w bazie danych. Zdolność **rejestrowania** zostaje użyta do monitorowania zmian w bazie danych i do rejestrowania żądań sieciowych. Zdolność **raportowania** jest użyta do powiadamiania zespołu ds. bezpieczeństwa o istotnych zmianach w bazie danych. Zdolność **informatyki śledczej/analityki** jest użyta do badania złośliwego dostępu oraz identyfikowania strony z podatnością na zagrożenia.
Oczekiwane wyniki (do zaliczenia)	Kompilacja może monitorować i raportować zmiany w integralności plików (CR 5.a).

	Wykryto złośliwą interakcję z serwerem WWW (CR 5.b). Informacje o ataku podawane są do wykorzystania w utrzymaniu systemów organizacji (CR 5. c).
Rzeczywiste wyniki	**Tripwire Enterprise (monitorowanie integralności) z** powodzeniem monitoruje zmiany w konfiguracji bazy danych. **ArcSight ESM (rejestrowanie)** z powodzeniem rejestruje zmiany w bazie danych i żądania sieciowe. **ArcSight ESM (raportowanie)** z powodzeniem alarmuje zespół ds. bezpieczeństwa o zmianach w bazie danych. **Symantec Security Analytics (informatyka śledcza/analityka** pozwala na identyfikację żądań sieciowych, które mogły spowodować to usunięcie, pomagając w identyfikacji podatności serwera Web w niestandardowym kodzie.
Wynik ogólny	Zaliczono Wszystkie wymagania dotyczące tego przypadku użycia są spełnione.

D.8 PRZYPADEK TESTOWY: INTEGRALNOŚĆ DANYCH DR-6

Tabela 0-10 Identyfikator przypadku testowego: Integralność danych DR-6

Wymaganie nadrzędne	(CR 6) Przykładowa implementacja DI ma wykrywać i reagować na ukierunkowane modyfikacje dokonywane przez złośliwych insiderów z podwyższonymi uprawnieniami.
Wymaganie testowalne	(CR 6.a, 6.b) Monitorowanie integralności; (CR 6.c) Raportowanie; (CR 6.d), Ograniczanie i powstrzymywanie.
Opis	Wykazanie, że rozwiązanie DI może wykrywać i reagować na ukierunkowane modyfikacje aktywów i kopii zapasowych dokonywane przez złośliwych insiderów.
Powiązane podkategorie Ram cyberbezpieczeństwa	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Warunki wstępne	Złośliwy insider próbuje zmodyfikować wybrane informacje zarówno w systemach organizacji jak i systemach kopii zapasowych korzystając z poświadczeń uzyskanych z zewnątrz.
Procedura	Zdolność **monitorowania integralności** jest użyta do wykrywania zmian w systemie plików. Zdolność **raportowania** służy do powiadamiania zespołu ds. bezpieczeństwa o zmianach w krytycznych zasobach danych. Zdolność **ograniczania i powstrzymywania** jest wykorzystywana do zapobiegania przed wprowadzaniem dalszych modyfikacji przez złośliwego użytkownika.
Oczekiwane wyniki (do zaliczenia)	Kompilacja może monitorować i zgłaszać zmiany w integralności plików (CR 6.a, CR 6.b). Informacja o ataku jest zgłaszana w celu wykorzystania przy reagowaniu na zagrożenie (CR 6.c).

	Działania kont użytkowników skojarzonych z atakiem są powstrzymane (CR 6.d).
Rzeczywiste wyniki	**Tripwire Enterprise (monitorowanie integralności) z** powodzeniem wykrywa zmiany w plikach i kopiach zapasowych spowodowane przez złośliwego insidera. **ArcSight ESM (raportowanie)** z powodzeniem raportuje i alarmuje administratorów poprzez e-mail o zmianach wprowadzonych w plikach przez złośliwego insidera. **Semperis DSP (ograniczanie i powstrzymywanie)** pomyślnie wyłącza konta użytkowników skojarzone z działaniami złośliwego insidera.
Wynik ogólny	Zaliczono wszystkie wymagania dotyczące tego przypadku użycia są spełnione.

D.9 PRZYPADEK TESTOWY: INTEGRALNOŚĆ DANYCH DR-7

Tabela 0-11 Identyfikator przypadku testowego: Integralność danych DR-7

Wymaganie nadrzędne	(CR 7) Przykładowa implementacja DI wykrywa włamanie dokonane za pośrednictwem zaatakowanego serwera aktualizacji i reaguje na nie.
Wymaganie testowalne	(CR 7.a) Monitorowanie integralności; (CR 7.b) Wykrywanie zdarzeń; (CR 7.c) Informatyka śledcza i analityka; (CR 7.d, CR 7.e) Ograniczanie i powstrzymywanie.
Opis	Wykazanie, że rozwiązanie DI może wykryć złośliwą aktualizację z zaatakowanego serwera aktualizacji, a także wykryć i zareagować na wynikające z tego włamanie.
Powiązane podkategorie Ram cyberbezpieczeństwa	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2, DE.CM-4, DE.CM-7, DE.AE-1, DE.CM-1,
Warunki wstępne	Zewnętrzny serwer aktualizacji został zaatakowany, a stacja robocza użytkownika próbuje dokonać aktualizacji z tego serwera.
Procedura	Zdolność **monitorowania integralności** zostaje użyta do wykrywania zmian w integralności programów i plików. Zdolność **wykrywania zdarzeń** jest wykorzystana do wykrywania złośliwej aktualizacji. Użyta jest również do wykrywania połączenia z maszyną. Zdolność **ograniczania i powstrzymywania** jest użyta do zatrzymania wykonywania aktualizacji i jej usunięcia. Jest ona również użyta do powstrzymania włamania.
Oczekiwane wyniki (do zaliczenia)	Kompilacja może monitorować i raportować zmiany integralności plików (CR 7.a).

	Złośliwa aktualizacja jest identyfikowana poprzez wykrywanie lub analizę sygnatur (CR 7.b, CR 7.c). Złośliwa usługa zostaje zatrzymana i przywrócona lub usunięta (CR 7.d) Inni użytkownicy tymczasowo zostają pozbawieni dostępu do tego serwera aktualizacji (CR 7.e). Wykryto port otwarty przez usługę (CR 7.f). Port otwarty przez usługę zostaje zamknięty (CR 7.g). Wykryto włamanie (CR 7.h). Włamanie jest powstrzymane (CR 7.i).
Rzeczywiste wyniki	**Tripwire Enterprise (monitorowanie integralności)** jest wykorzystane do identyfikowania zmian w programach w systemie, a także wszelkich zmian dokonanych przez atakującego. **Cisco AMP (wykrywanie zdarzeń)** jest użyte do wykrywania złośliwej aktualizacji. **Cisco Stealthwatch (wykrywanie zdarzeń)** jest użyte do wykrywania połączenia z maszyną przez nietypowy port. **Cisco AMP (ograniczanie i powstrzymywanie)** jest wykorzystane do zatrzymania wykonywania pliku i usunięcia go, zamykając w ten sposób narażony port. **Cisco ISE (ograniczanie i powstrzymywanie)** jest użyte do odłączania zagrożonych maszyn od sieci, aby zapobiec rozprzestrzenianiu się włamania.
Wynik ogólny	Zaliczono (częściowo). Wydaje się, że w momencie opracowywania niniejszego przewodnika Cisco AMP nie obsługuje blokowania sieci na komputerach z systemem Unix — obsługuje tylko wykrywanie (obsługuje jednak blokowanie sieci w przypadkach użycia systemu Windows, więc podobny

	przypadek użycia na komputerach z systemem Windows mógłby potencjalnie zadziałać). Zamiast tego polegamy na ochronie sieci, zdolności DI Chroń, aby zapobiec dalszemu dostępowi do serwera aktualizacji; oraz na zdolności ograniczania Cisco AMP, aby zaradzić wszelkim znanym złośliwym plikom pobranym z serwera

NIST SP 1800-26C

Przewodniki „How-to”

Dokument w języku angielskim – patrz publikacja:

SP 1800-26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events | CSRC (nist.gov)

Przewodniki „How-to” (SP 1800-26C) są integralną częścią publikacji NIST SP 1800-26.